ESSENTIALS OF DATA SECURITY

for Public Entities

SECOND EDITION

Click Wisely

A PUBLICATION OF MINNESOTA COUNTIES INTERGOVERNMENTAL TRUST

TABLE OF CONTENTS

Everyone Plays a Part in Data- and Cybersecurity

Data- and cybersecurity is more than a collection of technical software and service solutions. It involves a commitment from everyone in the organization to maintain security, to recognize and report threats, and to respond accordingly.

This guide is not intended to be, nor is it, a technical resource. Rather **this guide should be used to stimulate conversations among an organization's leaders and provide them with information and strategies to help the organization secure data (electronic or paper) and the data systems**.

This resource should be shared at multiple levels within an organization, including information technology (IT) managers, elected board members, executive directors and administrators, department heads, managers, and others as appropriate (e.g., safety committee).

KNOW THREATS, ESTABLISH RISK MANAGEMENT STRATEGIES

Maintaining vigilance and being aware of new threats as they emerge is necessary for everyone within the organization. To this end, the guide includes:

- Information about the threats, best practices to manage threats and policy recommendations
- Checkups that provide an opportunity to determine which security areas need improvement for the organization
- Key terms in the Glossary

As the threats to data-and cybersecurity rapidly evolve and systems used by member organizations are varied, this guide often leaves specifics up to the information technology professionals within the organization.

Evaluate Organization's Current Security Status

Knowing **where the organization currently is with its security systems, policies and employee awareness and practices** can help it determine where to spend its dollars and time to further strengthen security efforts.

Some pointers to assists with this:

- List and review the technical solutions in place: Are they adequate to meet current threats to the public entity?
- List and review nontechnical practices:
  - Does the organization have adequate policies to govern data security (e.g., computer acceptable use, password, mobile device, remote work, etc.)?
  - Does the organization conduct regular reviews and updates of these policies?
  - Does the organization provide regular training for employees about policies and enforce the policies?
  - Does the organization provide regular threat training to employees, including how to identify threats and steps to report a known or suspected threat?
  - Does the organization followup with employees who fail knowledge tests?

EXPERIENCING AN INCIDENT?

If an organization is currently dealing with an incident, **follow coverage requirements** either provided through MCIT or a commercial carrier if the organization has purchased coverage outside of MCIT.

MCIT CYBER COVERAGE

MCIT provides its members with data compromise and cyberattack coverage. This guide does not offer details about that coverage. Members should consult the current year's MCIT Coverage Document for full terms, conditions and exclusions of coverage.

See Resources for other places to learn about cyber coverage. Members may also call their MCIT risk management consultant at **866.547.6516** to discuss questions about coverage.

Cyber coverage, provided to members through MCIT assists organizations in financially responding to data security incidents.*

MCIT coverage is for specific exposures and requires certain responsibilities of members, particularly in reporting incidents, assisting with incident investigation and mitigating losses.

It is incumbent upon members to understand coverage, including:

- Which incidents are and are not covered
- Limits of coverage
- Members' obligations before and after an incident
- Crucial timelines

This is all detailed in the current year's MCIT Coverage Document and is subject to modification.

Members should be aware that a data- or cyber-incident could exceed the limits of coverage, even though limits have historically been adequate to fully cover most claims.

MCIT has assembled a panel of attorneys and forensic IT professionals that is available to assist in the event of a covered claim.

Due Diligence

To help prevent and minimize data compromise and cyberliability events, members are expected to provide and maintain all of the following:

- Appropriate physical security for their premises, computer systems and hard copy files

- Appropriate computer and internet security
- Backups of computer data at appropriate intervals
- Transaction protection, such as for processing credit cards, debit cards and check payments
- Appropriate protocols for disposing of files containing personally identifying information that is private or sensitive

Reporting Claims

Members with exclusive cyber coverage with MCIT should report known or suspected incidents to MCIT as soon as practicable using the member portal (link at *MCIT.org*). In the case of a **ransomware attack, call MCIT immediately**, rather than reporting online to expedite response protocols.

Members with a separate policy should also notify MCIT about the incident as soon as practicable.

The sooner an incident is reported to MCIT, the faster steps can be taken to minimize its impact.

MCIT promptly initiates the claims handling investigation and response in coordination with the member.

Members should provide all such information relating to the event or threat as MCIT may reasonably request. This is necessary to determine if any outside services are required to mitigate the situation and to help with the investigation. This may include forensic IT partners and/or breach counsel.

TRAIN EMPLOYEES

Educating employees to recognize threats to data security is an important part of an organization's data- and cybersecurity plan. Several chapters of this guide have corresponding Quick Takes on Data Security—ready-to-use mini training scripts—and employee handouts that provide succinct information about a specific data security threat and steps individuals can take to keep information secure.

All Quick Takes are intended to be customized with details about the organization's specific policies and procedures.

Download Quick Takes on Data Security and handouts at *MCIT.org*.

Outside Cyber Policies

If members have purchased cyberinsurance from an outside carrier, that coverage is primary, and MCIT's coverage is secondary.

For members with private policies, they should review their policies and understand the specific terms, conditions and exclusions therein. That includes specific due diligence and reporting requirements.

Guide Assumes Exclusive MCIT Coverage

References made to coverage terms, conditions, exclusions and response services made in this guide are exclusively related to MCIT coverage. As such, members that have cyber policies outside of MCIT may have different terms, conditions, exclusions and response services.

* Members should read the entire Privacy or Security (Cyber) Event Coverage section of the MCIT Coverage Document for a full explanation of coverage, including coverage conditions, exclusions and definitions, and the Coverage Declarations, all of which affect the coverage and coverage limits provided. Coverage is subject to change each year.

RESOURCES

CURRENT YEAR'S MCIT COVERAGE DOCUMENT: Mailed to the member's primary contact each December.

CURRENT YEAR'S COVERAGE SUMMARY BOOKLET (*MCIT.ORG*): Document that summarizes and generally explains coverage available to members through MCIT, including cyber coverage.

CYBER COVERAGE VIDEOS (*MCIT.ORG*): Series of short videos that summarize MCIT's coverage terms, limits, conditions and exclusions.

"CYBERSECURITY SELF-ASSESSMENT" PRODUCED BY MCIT (*MCIT.ORG*): A broad checklist that an organization uses internally to assist in identifying data security areas it needs to strengthen.

Data- and Cybersecurity Overview

Data- and cybersecurity is a significant responsibility of and necessity for local governments. Without it, the organization faces the potential for damage to its systems, business interruption, loss of critical data and the exposure of private/nonpublic and sensitive information of others.

Maintaining data security in the face of real, daily threats from a variety of threat actors and employee errors is the responsibility of everyone in the organization.

Damages to a public entity from data compromises and cyberattacks are often costly, both financially and nonmonetarily. Money is required to correct security issues, restore lost or damaged data, handle legal action and pay regulatory fines. The nonfinancial costs to a public entity can be damaging to an organization's reputation, lowered employee morale and loss of the public's trust.

It is best if an organization has a robust data security program and response plan established *before* an incident occurs. Ideally, the time to assess the strengths of the entity's programs and plans is before an attack or data compromise happens.

Even if the organization has experienced a data security incident in the past, leadership should still **establish baseline security measures and continue to work to further strengthen and improve risk management** relative to data security.

Using enterprise risk management methods, this guide is designed to assist in an organization's efforts.

THE THREATS

Those who seek unauthorized access to sensitive data and systems, referred to as threat actors (a.k.a. hackers), continually discover and plan new ways to achieve their goals. They **want a variety of information from local governments, as well as to disable governments' computer systems and networks** for their own purposes.

Not all data compromises arise from threat actors infiltrating a computer system. An equally **significant threat to data security is when paper documents, flash drives, laptops, etc. are lost, stolen or accidentally released**.

On top of that is old-fashioned **con artists who dupe victims out of their money** through misdirected payment fraud.

Monetary Gains

Besides stealing credit card and financial information, thieves frequently target other types of sensitive information that local government entities have in their electronic and paper records. Some examples include Social Security numbers, health information, social services data, law enforcement records and employment data.

In fact, **nonfinancial private information can sell for significant amounts**, particularly health information that is used to commit fraud against insurance providers.

Another tactic used by threat actors is to deploy **ransomware, which infiltrates a system and holds the data or system hostage** and may threaten to release private data on the dark web until the owner of the data/system pays a ransom.

RECOMMENDED POLICIES

Formal policies provide clarity on expectations for employee conduct and consistent enforcement of those standards.

Regarding data security, public entities are encouraged to have the following policies.

- **Acceptable use policy** (for computers, internet, email/text and the like) targeted at user/employee behavior
- **Account validation policies** provide expectations and procedures for validating the authenticity of third-party requests, especially if it involves a major security change or transfer or money (another user behavior-focused policy)
- **Access control policies** primarily address technical tools to prevent unauthorized access to data and systems, such as the use of multifactor authentication
- **Endpoint security policies**, especially for mobile devices, address technical tools that block malware from connecting to other assets
- **Email security policies** include tools that range from scanning emails and blocking phishing emails to endpoint protection software to stop malware
- **Data backup and recovery policies** help reduce the impact of a successful attack (if an organization has adequate and accessible backups, it can be less costly to recover from a ransomware or other malware attack)
- **Records retention policy** that sets the length various official records must be kept with an expectation that records will be destroyed after that period passes
- **Business email compromise policy** that brings together all of the controls and employee behaviors needed to prevent and lessen the impact of these breaches
- **Security awareness training and education policy** that outlines the minimum requirements of employee security training program, including content and compliance provisions.
- **Phishing prevention policy** that provides guidelines and processes for the identification, prevention and reporting of phishing scams
- **Mobile Device:** Explains acceptable uses for mobile devices used for work purposes. Employer may need separate policies governing employer-owned devices and employee-owned devices
- **Remote Work (if allowed):** Have an information security section in line with other information security policies

Each policy should include its enforcement and consequences rules.

Nonfinancial Motivations

Consider, too, that some threat actors are not out for financial gain. Instead certain individuals **infiltrate organizations' systems to release sensitive documents or information, freeze access to websites, deface websites** in an effort to effect change or to damage the reputation of an organization, **or to interfere with political processes and elections**.

Often known as hacktivism, these attacks can be personally or politically motivated.

Hacktivism is not limited to national or international issues; local concerns can be just as contentious. For example, after Freddie Gray's death due to injuries sustained while in police custody in 2015, hacktivists froze the City of Baltimore's main website for several hours.

Another motive for threat actors is espionage and interference in a political system by foreign governments. The release of emails from the Democratic National Committee prior to the 2016 presidential election is an example of this.

Because counties are responsible for **elections**, they **are a potential target** for threat actors seeking to influence or discredit the electoral process.

Threat actors may also **want to cripple an organization's ability to carry out normal operations** by deleting information or encrypting it and preventing staff from accessing the information.

When combined with hacktivism or personal grudges, which are sometimes perpetrated by disgruntled current or former employees, the goal of a ransomware attack may simply be to damage an organization rather than to receive money.

THE DEFENSE

Given all of the threats to a public entity's data and system security, the **best defense for protecting the organization includes continuous vigilance and an organization-wide approach**.

Everyone in the organization, including elected officials, department heads, employees and contractors/partners, **needs to support security programs and plans**.

Although information technology specialists work to secure computer systems and continually monitor them for compromises, **often the weakest link is an individual user** who succumbs to a phishing attack,*shares his or her password with others or carelessly dumps sensitive documents in an open trash bin.

Successful data and systems security requires practicing enterprise risk management that involves:

- Creating and enforcing policies
- Implementing data security software and hardware

- Developing a response plan and a business continuity plan
- Training employees
- Following best practices

It also **requires that everyone be vigilant** against possible attacks that seek to obtain data or access to secure systems or locations.

SECURITY PRIORITIES

An organization should **employ basic technical measures** as its first line of defense to secure its data and data systems.

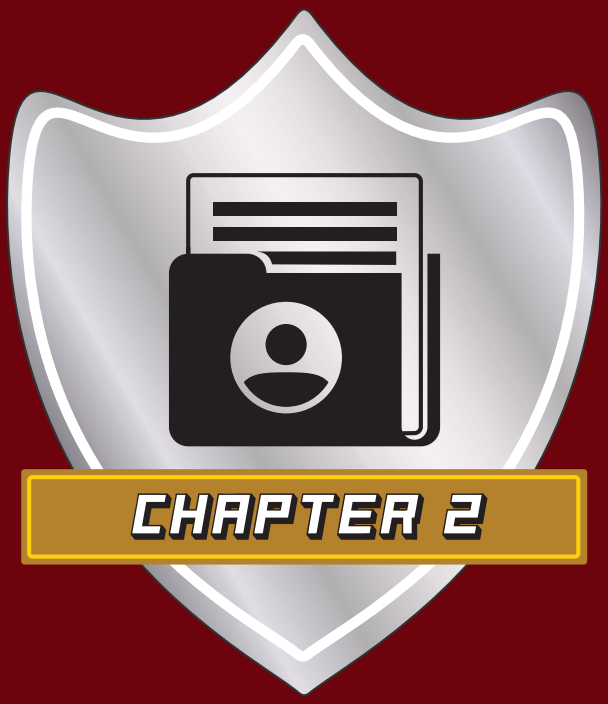
Technical priorities should include:

- **Access security measures,** such as firewalls, passwords, multifactor authentication and active directory (a centralized database and control system for managing users, computers and network resources on a Windows-based network)
- **Email filtering** that identifies and prevents known or potential scams from delivering to account inboxes
- **Vulnerability scanning**, an automated process that uses software tools to find security weaknesses in computer systems, networks and applications before attackers can exploit them
- **Installation management** of software and hardware that includes processes and policies for installing, updating and removing software and hardware on an IT system and networks to ensure they remain secure, stable and compliant
- **Security information and event management (SEIM)**, a solution that collects, analyzes and correlates security data from across an organization's IT systems. It centralizes event information so IT can identify suspicious patterns, investigate incidents, streamline response efforts and meet compliance requirements.

Nontechnical security priorities should be:

- **Requiring good email hygiene of employees**—using email only as a temporary or transitory location for information (not long-term storage) and using encryption for sending and receiving sensitive data *(see Chapter 13)*
- **Managing data** so as to remove unnecessary files from the organization's systems and to secure those records that must be kept *(see Chapter 3)*
- **Employee training about security threats**—how they can recognize them and steps to take to keep their data safe *(see Chapter 15)*

*Phishing is when individuals are tricked into disclosing sensitive, valuable or private information through deceptive computer-based means, commonly through email.



Data Privacy Laws

The increasing use of technology adds a layer of complexity to the creation, collection, maintenance, storage and dissemination of government data. It is important for public entities to understand the most common data privacy laws applicable to government agencies, general requirements relative to private data and risk management recommendations.

Some government entities have found themselves at the center of unwanted media attention and litigation over the release of not public data or the unauthorized access of that data. This litigation can be expensive and time consuming, but it also can be embarrassing and erode public trust in the government entity.

This chapter provides a general description of the obligations for data protection under a few privacy laws. Organizations should refer to each statute for its specific requirements and applications when making decisions.

MINNESOTA GOVERNMENT DATA PRACTICES ACT (MGDPA)

The vast majority of data maintained or collected by a government entity is considered "government data." Requirements relative to the collection, storage, use and dissemination of government data is governed by Minnesota Statutes, Chapter 13, the Minnesota Government Data Practices Act.

One broad classification of data is "not public" (both on individuals and not on individuals).

Among other data, not public data includes:

- Most health data
- Most personnel data for employees and volunteers
- Most public health data on individuals
- Most welfare data on individuals
- Workers' compensation data
- Certain civil investigative data
- Names of reporters alleging maltreatment of minors or vulnerable adults
- Security information
- Trade secrets
- Attorney-client privilege

The MGDPA classifies how this information must be stored and who may have access to it. **Typically not public data can only be accessed by the data subject and those who work for the public entity whose job reasonably requires access.** It also requires certain notices be provided prior to collecting not public/private data on individuals.

Collection of Data

Any time a government entity collects private or confidential data from an individual, the government entity must give a Tennessen Warning.

With limited exceptions, private or confidential data on an individual may not be collected, stored, used or disseminated by government entities for any purposes other than those stated within the Tennessen Warning. However, if the individual provides written informed consent of the use or release of data, it is permissible (Minn. Stat. § 13.04, subd 2).

Security of Data

The MGDPA also places **requirements on public entities to protect the accuracy and security of not public data**. An entity's responsible authority (person whose duties are day-to-day administration of MGDPA) must implement appropriate security safeguards for all records containing data on individuals.

The responsible authority must also develop a policy incorporating these procedures, which may include governing access to the data if sharing of the data with other government entities is authorized by law.

When not public data is being disposed, it must be done so that its contents cannot be determined (Minn. Stat. 13.05, Subd. 5). Public entities should review their storage policies for hard copies of data, as well as electronic forms of data.

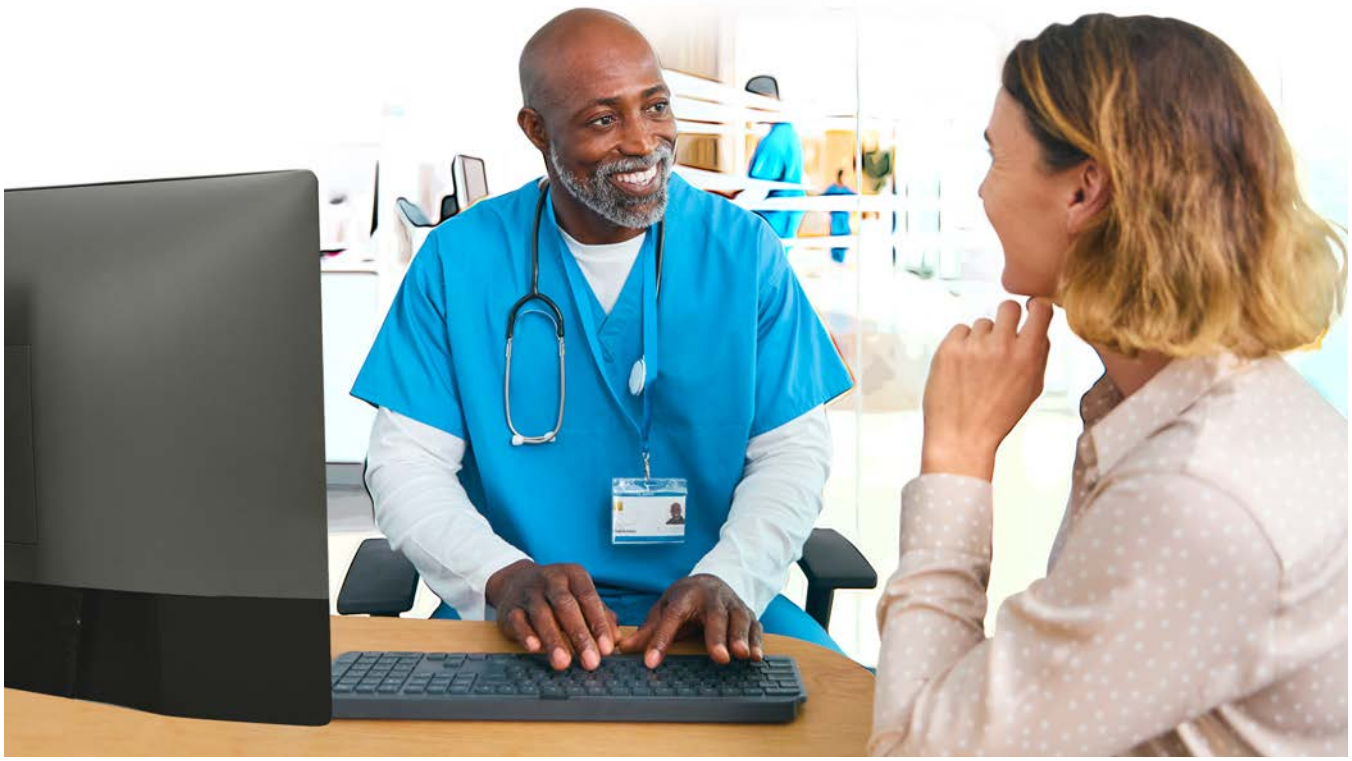
MGDPA BEST PRACTICES

Procedures public entities may want to consider implementing to protect the security of data:

- Ensure that all devices/equipment containing not public data are password protected and employees log off when leaving them.
- Review and understand how data is collected, stored, transmitted and destroyed on technology platforms.
- Educate employees about the need to protect not public data, including conversations and social media posts containing such data.
- Restrict not public data from being taken from offices except when required for business purposes or allowed by policy.
- Ensure appropriate safeguards are implemented for not public data stored on mobile devices, such as encryption tools or firewalls.
- Ensure appropriate training and safeguards are in place if not public data may be accessed remotely.
- If data is stored off site (storage building or "the cloud"), ensure contracts incorporate security safeguards. *See Chapter 4: Vendor Contracts and Chapter 8: Cloud Data Storage*
- Entities should train employees, especially ones with access to not public data, about the policies/rules and responsibilities, and possible ramifications for failing to comply with them.

MEDICAL DATA

Public entities receive medical data in several ways. The reasons that they have medical data determine the rules and responsibilities surrounding its



security. Below is a synopsis of key rules and their requirements.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA regulates "protected health information," which includes information relating to the individual's:

- Past, present or future physical or mental health or condition
- Receipt of health care services
- Past, present or future payment for the receipt of health care

Protected health information **also includes details that identify the individual** or for which there is a reasonable basis to believe the information can be used to identify the individual.

Protected health information may only be disclosed as allowed or required by the privacy rule or by consent of the individual who is the subject of the information. **HIPAA also has security requirements with which covered entities must comply**.

Members that have covered entity functions should work closely with legal counsel to ensure compliance with HIPAA.

MEDICAL DATA BEST PRACTICES

- Determine what rules and regulations apply to the different medical data maintained by the entity.
- If the entity is a covered entity or business associate under HIPAA, ensure that proper security measures are implemented.
- Pay special attention to medical data that may be stored, accessed or transmitted on mobile devices. Ensure that the network connection is secure and that sufficient firewall and encryption programs are utilized.
- Train employees dealing with medical data regarding the rules and responsibilities relative to it.

Minnesota Health Records Act

Minnesota has a state law that governs medical records: the Medical Health Records Act found in Minnesota Statutes, Sections 144.291 to 144.298.

Although this provision is more limited in scope than HIPAA, it may have requirements that affect public entities. For example, Minnesota Statutes, Section 144.293, Subdivision 2 **prohibits disclosure of a health record received directly from a provider** unless the entity or person has consent, specific statutory authority or a court order.

Medical Data and Minnesota Government Data Practices Act

Even if a public entity is not subject to HIPAA requirements, much of the health data will be classified as not public under the MGDPA. **Accordingly the organization should ensure that:**

- Steps are taken to protect the security of data
- Data is not being accessed or released without legal authority or authorization
- The entity follows risk management suggestions

MHRA, ADA, FMLA

Public entities may also collect health or medical data as part of the employment context, such as a pre-employment physical where allowed; documentation received in accordance with an employee's request for a reasonable accommodation under the Minnesota Human Rights Act (MHRA) or Americans with Disabilities Act (ADA), or medical leave under the Family and Medical Leave Act (FMLA).

When an employer collects medical information for any of these purposes, it should review the limitations for each of the above rules. For all the rules, **the employer should keep all the medical data in a separate file** and not in the employee's general personnel file.

Individuals who are authorized to access medical data are more limited than those who may access personnel data. Medical data should be kept in a secure location.

DEPARTMENT OF MOTOR VEHICLE SERVICES DATA

Data maintained by the Motor Vehicle Services Division of the Minnesota Department of Public Safety is a state database, and local government entities have limited ability to create database safeguards. However, it is important that public entities train staff about the restrictions associated with the use of the system. Protections for this data exist both under federal and state laws.

Driver's Privacy Protection Act (DPPA)

The Driver's Privacy Protection Act (18 U.S.C. §§ 2721; 2725) is a federal statute that prohibits individuals from knowingly obtaining, disclosing or using personal information from a motor vehicle database for unauthorized purposes. **Protected information includes the individual's:**

- Photograph
- Social Security number
- Driver identification number
- Name
- Address (not ZIP code)
- Telephone number
- Medical or disability information

Protected information does not include information about accidents, driver's license violations and status. (Some of this information may be protected by the Minnesota Government Data Practices Act or other state law.)

MOTOR VEHICLE DATA BEST PRACTICES

Local public entities do not maintain or store motor vehicle data. Rather access to it is via the state database and system.

Public entities do not have the ability to conduct their own audits or create certain database safeguards (such as only allowing a certain number of accesses before needing to log back in, or triggering a flag in the system.) However, pubic entities have some ability to control the risk.

- Assess who has access to the database and ensure only individuals with a need for access have it.
- Ensure former employees' access to the database is shut off.
- Require all staff to attend training regarding appropriate use of data.
- Enforce and train about policies regarding accessing and disseminating private data.
- Discipline, where appropriate, for violations of policies and procedures.
- Create an environment where employees know such conduct will not be tolerated.

RESOURCES

MINNESOTA GOVERNMENT DATA PRACTICES ACT: AN INTRODUCTION" PRODUCED BY MINNESOTA COUNTIES INTERGOVERNMENTAL TRUST (*MCIT.ORG*): Overview of the statute, including information about data classification and requirements of government entities relative to the data it collects, maintains, creates, receives and disseminates.

"HIPAA AND MINNESOTA GOVERNMENT ENTITIES" PRODUCED BY MINNESOTA DEPARTMENT OF ADMINISTRATION, DATA PRACTICES OFFICE: Frequently asked questions related to this data privacy law and government entities.

The statute identifies **14 situations where obtaining, disclosing or using personal information is permissible**. The exception applicable to public entities is that access to and using data is permissible for law enforcement to perform police work or any government agency to carry out its functions.

Violation of the statute may result in a civil lawsuit with damages and an award of reasonable plaintiff's attorney fees. There is an argument that the statute does not require proof of actual injury to receive damages. Plaintiffs often claim that a person is entitled to $2,500 for each violation of the DPPA, plus reasonable attorney fees. Claimants routinely demand $10,000 per violation.

Minnesota State Law

Public entities need to be concerned about state law as well. Minnesota law provides further restrictions on use.

Minnesota Statutes, Section 171.07, Subdivision 1a restricts use of driver's license photos to:

- The issuance and control of driver's licenses
- Criminal justice agencies for:
  - Investigation and prosecution of crimes
  - Service of process
  - Enforcement of no contact orders
  - Location of missing persons
  - Investigation and preparation of cases for criminal, juvenile and traffic court, and supervision of offenders
- Public defenders for the investigation and preparation of cases for criminal, juvenile and traffic courts
- Child support enforcement purposes under Minnesota Statutes, Section 256.978

COVERAGE

MCIT cyber coverage can apply to claims alleging violations of the MGDPA and the DPPA. MCIT carved out an exception for those claims that also allege a violation of civil rights by extending MCIT's public employees liability coverage in addition to the cyber coverage, subject to the coverage limit.

Currently, MCIT excludes claims for hospitals and nursing homes. A HIPAA claim arising from such facilities would likely be excluded from coverage.

See MCIT Coverage Document for all coverage details.

DATA PRIVACY LAWS CHECKUP

Are computers that contain private data password protected, and do employees log off when leaving them unattended? ☐ YES ☐ NO	**ACTION ITEMS**
Are employees trained about the need to protect private data, including conversations and social media posts, as well as their roles and responsibilities relative to not public data? ☐ YES ☐ NO	
Is private data restricted from being taken from government offices except when required for business purposes or allowed by policy? ☐ YES ☐ NO	
For data stored off site (e.g., in "the cloud"), do contracts with vendors incorporate security safeguards? ☐ YES ☐ NO	
Have rules and regulations been identified that apply to various medical data maintained by the organization? ☐ YES ☐ NO	
If the organization is a covered entity or business associate under HIPAA, are proper security measures implemented? ☐ YES ☐ NO	
For mobile devices, is the network connection that stores, accesses or transmits private or not public data secured and encrypted? ☐ YES ☐ NO	
Are only employees who need access to motor vehicle databases given access to them? ☐ YES ☐ NO	
Is access to databases shut off for individuals who leave employment or whose responsibilities no longer require access to databases? ☐ YES ☐ NO	
Have employees been trained about appropriate use of motor vehicle data? ☐ YES ☐ NO	
Are employees disciplined for violations of data privacy policies? ☐ YES ☐ NO	

Data Management

Undeniably local governmental entities create, disseminate and maintain a great deal of information and records that are necessary for them to deliver their public services. This large amount of data increases the threat landscape for data compromises. However, public entities are not obligated to retain all of that data forever.

Adopting a culture of maintaining only the information that is necessary for business purposes and required under the Minnesota Official Records Act (Minn. Stat. §15.17) and Records Management Statute (Minn. Stat. §138.17) can help limit the volume of data that is vulnerable to threat actors.

An example of what can go terribly wrong when data is kept for longer than necessary is the 2021 breach of a University of Minnesota database containing three decades worth (1989-2021) of full names, addresses, phone numbers, Social Security numbers, driver's license or passport information, university ID numbers, birth dates and demographic information of prospective students, students, employees and program participants.

The U of M's data retention schedule says that everything except transcripts should be destroyed no later than 10 years after graduation and seven years after employment.

The university had to send notifications to approximately 2 million individuals and faced several lawsuits because of the breach.

DATA MANAGEMENT LAWS

The **Minnesota Official Records Act** mandates that officers and agencies at all levels of government make and preserve all records necessary to a full and accurate knowledge of their activities.

The **Records Management Statute** provides that it is the duty of the governing body of each county, municipality and other subdivision of government to establish and maintain an active continuing program for the economical and efficient management of the organization's records.

Part of records management involves the **timely destruction of records in a responsible manner**. These records may be in electronic or paper format.

It is the content of the record that makes it an official record, not the medium. The public entity's obligation to keep data secured does not end when the retention period indicates time for disposal.

WHAT TO KEEP AND FOR HOW LONG

Public entities must have and follow a records retention schedule (Minn. § 138.17, subd. 7). This schedule dictates how long the entity must retain official records.

This also means that **once the retention period has expired, the public entity no longer must maintain the data and can destroy it**.

Information, documents and data that are not official records should be kept only as long as there is a business need for them. Destroying extraneous documents and data as soon as possible is key from a data security standpoint.

To manage the amount of data a public entity maintains, it should:

- Ensure that all employees understand what information they have that is an official record, what is not and how the records retention schedule applies to that.
- Provide time for and require that employees securely destroy files regularly to comply with the retention schedule or business purpose needs. An example would be that the entire organization dedicates one day a year to purge files, documents and data.
- Notify employees to maintain data that is responsive to a claim, lawsuit or litigation hold even if it is beyond the term of the records retention schedule.

Email and Data Storage

Employees may use email as a convenient place to store messages, information, records, documents and data as part of their day-to-day workflow. In practice, this makes the organization more vulnerable to data compromise, as email systems are typically less secure than the organization's file servers, for example.

Members should work with staff to **move information necessary for their work to more secure storage options outside of email**. *See Chapter 13: Secure Email Practices*

LEASED EQUIPMENT

Public entities may lease or rent electronic data processing equipment, such as copiers, printers and other items that accept, process and store data. In these cases, the **lease agreement should have terms that outline how data will be wiped or destroyed from the equipment when it is returned to the vendor**.

Sometimes the public entity wants to have control of this process, while others prefer to have the vendor take care of data destruction. If the equipment vendor destroys the entity's data, the entity should request proof of destruction.

See Chapter 4: Vendor Contracts for more information.

OBLIGATION TO SECURE DATA THROUGH DESTRUCTION

Neither the Official Records Act nor the Records Management Statute specifies a mechanism for destruction of records. There is, however, a requirement that records containing not public data be destroyed in a way that prevents their contents from being determined.

Not public data is defined in Section 13.02, Subdivision 8a of the Minnesota Government Data Practices Act. "Not public data" are any government data classified by statute, federal law or temporary classification as confidential, private, nonpublic or protected nonpublic.

Simply throwing the data into the garbage is not a secure method of destruction. As data exists in multiple forms, secure destruction of data applies to both electronic and nonelectronic formats.

Secure Destruction

The format of the data determines many of the best practices for destroying it securely.

With electronic formats, it is important to remember that **private or nonpublic data may be retained on more than one device**, including computers, laptops, tablets, smart phones, flash drives, copiers, scanners, printers and fax machines. Removal and destruction of all data copies are necessary.

When removing items from service, these devices should have their data storage (hard drive, disk or backup media) wiped or otherwise destroyed. Staff should be trained about secure data destruction to reduce the risk of unsecured destruction.

The organization should consider having one person or department handle all secure destruction. This may help in consistently following best practices, contractual agreements and records retention policies.

Best Practices for Securely Destroying Electronic Data

- **Use programs to delete particular items securely**. Searches for sanitation tools or disk drive sanitation can reveal these programs. Always consult with local IT prior to installing or operating new software.
- When physically destroying equipment, **impair any disk drives and remove hard drives** from machines. The hard drive can then be destroyed by pulverizing, disintegrating or incinerating it, or the drive could be wiped.
- For mobile devices, **manually delete all sensitive data and reset the device** to factory specifications according to the manufacturer's instructions. If the device itself is to be removed from service, destroy by pulverizing, disintegrating or incinerating it. Multiple vendors offer these services.

Best Practices for Securely Destroying Nonelectronic Data

- **Use a cross cut shredder**. Depending on the style of shredder, this can also be used for CDs or DVDs, ID badges or other forms of data.
- **Paper may also be pulverized** or disintegrated using disintegrator devices, as well as incinerated. Multiple vendors offer these services.

In addition to destroying data, destroying or deactivating identification badges or other means of access to secure areas should be done for employees or vendors when employment status changes. *See Chapter 11: User Authentication*

RESOURCES

QUICK TAKES ON DATA SECURITY PRODUCED BY MINNESOTA COUNTIES INTERGOVERNMENTAL TRUST (*MCIT.ORG*): Ready-to-use mini training scripts and employee handouts provide succinct information about specific data security threats and steps employees can take to keep information secure.

WHAT IS AN OFFICIAL RECORD?

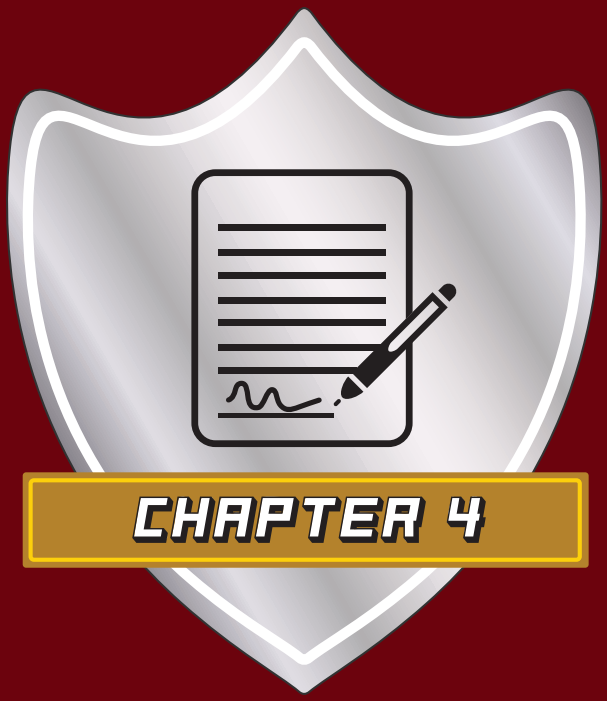
An official record documents a government entity's "official activities." **An official record describes an entity's official functions, business activities and transactions.**

Official records have value:

- Formal communications among staff or with the public
- Policies and procedures and documentation of changes to those
- Fiscal information about expenditures, authorizations for specific programs and actions
- Instructions, guidance others will need in the future

DATA MANAGEMENT CHECKUP

Is the staff trained about records retention, including: • What qualifies as an official record? ☐ **YES** ☐ **NO** • The organization's records retention schedule? ☐ **YES** ☐ **NO**	**ACTION ITEMS**
Are employees required to destroy unnecessary records in a timely manner, either because no longer needed for a business purpose or has reached maximum retention per the retention schedule? ☐ **YES** ☐ **NO**	
Is the staff trained about secure data destruction? ☐ **YES** ☐ **NO**	
Are methods in place to ensure secure destruction is consistently carried out according to the organization's requirements, for example, being assigned to an individual or department? ☐ **YES** ☐ **NO**	
Have rules and regulations been identified that apply to various medical data maintained by your organization? ☐ **YES** ☐ **NO**	
Are data from computers, mobile devices, printers, copiers, fax machines and other devices securely destroyed? ☐ **YES** ☐ **NO**	
Are physical resources (paper, CDs, DVDs, etc.) shredded or otherwise securely destroyed? ☐ **YES** ☐ **NO**	
Are processes in place to ensure that data on leased electronic processing equipment (e.g., printer, copier) is securely destroyed when the equipment is returned to its owner? ☐ **YES** ☐ **NO**	



Vendor Contracts

A local government may find that using skilled and trusted third-party information technology (IT) professionals and services for the organization can provide significant efficiencies and expertise without adding to headcount.

Contracting for technology services is not a way to eliminate harm that can be caused from a cybersecurity standpoint. Having technically trained professionals with eyes on the organization's technology stack can be excellent insulation from cyberthreats. However, an arrangement for such services brings its own complexities that must be managed along with in-house data security measures.

To help ensure that the public entity's data remains secure, it should establish written contracts with all individuals or companies that access, collect, maintain, manipulate or store organization data in any format.

It is critical that the contractual agreement is well-crafted from the start to manage risks and eliminate ambiguity in the event of a data compromise or cyber event.

The cybersecurity considerations when contracting for IT services addressed in this chapter focus on those areas that pertain to data and network risk management. A contract with a managed service provider (MSP) should also include provisions that address other areas of business management, such as the vendor's service hours, its pricing and the like.

WHAT IS A MANAGED SERVICE PROVIDER?

Managed service providers (MSPs) are **often instrumental in setting up new technology and keeping existing programs and devices online**. MSPs:

- Offer a variety of services, such as for networks, applications, infrastructure and security
- May provide (or not) ongoing regular support and active administration on a customer's premises, the MSP's data center (hosting) or in a third-party data center (cloud)
- Could offer their own proprietary services and/or other providers' services

Typically, the level of service provided depends on the service agreement.

MSPs are not employees of the entity even though they may feel like it, particularly if they are on site often or co-located with the public entity. Organizations need to remember that **MCIT coverage does not extend to MSPs or other third-party contractors**.

CONDUCT DUE DILIGENCE ON POTENTIAL VENDOR

The organization should evaluate the MSP's data- and cybersecurity measures before deciding to enter into a contractual service arrangement.

Private or nonpublic information is likely to be visible to technology vendors. The organization ensures that internal staff are acutely aware of and trained on data protection requirements and the appropriateness of use when it comes to sensitive information.

Likewise, the organization must take steps to verify that the MSP's systems are adequate to maintain and safeguard the security of this data. This would include understanding the service provider's:

CONTRACT REVIEW

Members can request that MCIT review contracts from a risk management perspective before entering into an agreement. This service is provided at no cost, and members can reach a risk management consultant toll-free at **866.547.6516**. MCIT cannot provide technical legal advice about MSP contracts.

- Password protocols
- Ways it secures pathways in and out of the organization's systems
- Use of multifactor authentication and encryption
- Security policies and procedures.

In short, the **MSP should provide details about how it physically, technically and administratively controls access to and use of the organization's private and nonpublic data, as well as the organization's network and systems**.

To do this, the entity may want to have the MSP complete a due diligence questionnaire. Standardized questionnaires are available from several sources that can be modified to meet the organization's needs. Also, the "Cybersecurity Self-assessment" available at *MCIT.org/resources* can be used as a starting point for a due diligence questionnaire.

If the MSP passes the due diligence test, then the entity can move on to negotiating provisions of the contract for service. The agreement should explicitly detail important points of how the professional relationship will work for both parties.

INCLUDE INSURANCE, INDEMNIFICATION PROVISIONS

The contract with a managed service provider should include **provisions that protect the organization in the event that the MSP is negligent** and causes harm to the entity. These provisions include hold harmless and indemnification language, as well as insurance requirements.

MSPs may try to cap their damages or limit their liability in the agreement to the amount of, or some multiple of, the fee paid under the contract. This may be significantly inadequate to cover a potential loss.

Just as a contract for an electrician should make the organization whole if the electrician's work sparks a fire that damages the facility beyond the cost of the contracted services, the agreement with an MSP should include hold harmless and indemnification provisions where the MSP is held responsible for its negligent acts, including covering the costs of attorney fees and breach notification costs, among other expenses incurred due to the negligence.

The **MSP should carry adequate bonding and insurance coverage** to ensure that the service provider can cover costs of potential negligent acts.

UNDERSTAND BUSINESS CONTINUITY AND EMERGENCY MANAGEMENT PLANS

The agreement with an MSP should **require that the service provider has business continuity and redundancy resilience** to safeguard against any potential gaps in service or support should the vendor have an abrupt or unexpected change in its business.

The MSP should provide the organization with a copy of its business continuity plan. If it does not provide a plan, this is a red flag, and the entity should be wary of the vendor's reliability and ability to bounce back from an incident.

The MSP should also **provide the organization with its disaster recovery test results regularly**. This allows the organization to confirm that the service provider's recovery capabilities are actually sufficient.

ESTABLISH SCOPE OF SERVICE

Setting the professional expectation is paramount when initiating a contract for service. **Ensure that the scope of service is clearly outlined and includes dispute resolution language in the agreement.**

- Provisions should detail exactly what services the MSP is providing in exchange for the fee.
- Keep in mind that if a service is not noted in the agreement, the MSP is likely not obligated to provide it.
- If the agreement does not include data security services for the organization, then the organization is left to address that aspect of its IT risks independent of the MSP.

For example, when purchasing set up of a network

SAMPLE DATA- AND CYBERSECURITY LIABILITY LANGUAGE FOR CONTRACTORS

Cyber coverage varies greatly from policy to policy; therefore, the following contract language is suggested for all contracts with service providers, including but not limited to information technology (IT) consultants, social services providers and partners, public health vendors and payroll service companies.

Sample Language

Contractor shall procure and maintain for the duration of the contract insurance against claims arising out of its services and including, but not limited to loss, damage, theft or other misuse of data, infringement of intellectual property, invasion of privacy, and breach of data.

Contractor shall have and keep in force, cyber liability insurance, with limits not less than $2,000,000 per occurrence or claim, $4,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Contractor in the Agreement and shall include, but not be limited to, claims involving infringement of intellectual property; including infringement of copyright, trademark, or trade dress; invasion of privacy violations; information theft; damage to or destruction of electronic information; release of private information; alteration of electronic information; extortion; and network security. The policy shall provide coverage for breach response costs, regulatory fines and penalties, and credit monitoring expenses.

The policy must include the client, its officers, agents, and employees as additional insured.

RESOURCES

"3 CONTRACT ISSUES TO WATCH: MANAGE RISKS," PRODUCED BY MINNESOTA COUNTIES INTERGOVERNMENTAL TRUST (*MCIT.ORG*): Article addresses assumption of liability, sufficient liability limits and proper coverage as three key contract issues to help manage risks in agreements.

"COVERAGES AND LIABILITY LIMITS FOR INDEPENDENT CONTRACTORS" PRODUCED BY MINNESOTA COUNTIES INTERGOVERNMENTAL TRUST (*MCIT.ORG*): Article reviews recommendations for minimum coverages and liability limits, including general requirements, certificate of insurance, specific insurance, and hold harmless and indemnification agreement.

"INDEPENDENT CONTRACTORS LIMITS OF LIABILITY" PRODUCED BY MINNESOTA COUNTIES INTERGOVERNMENTAL TRUST (*MCIT.ORG*): Article provides tips for how to work with independent contractors to ensure that they have adequate liability insurance limits in place to match the organization's policies and projects' risk exposures.

"RED FLAGS IN CONTRACTS" PRODUCED BY MINNESOTA COUNTIES INTERGOVERNMENTAL TRUST (*MCIT.ORG*): Article discusses areas to review in legal contracts before finalizing agreements, particularly places to look to ensure the organization is not assuming unwanted liability.

from an MSP, the agreement may not include ongoing troubleshooting for the system or cybersecurity services. If the organization needs these services, the agreement needs to account for them.

DETAIL SECURITY IMPLICATIONS AND OBLIGATIONS

The agreement with an MSP should describe how the product or service implicates information security. What, if any, connectivity is necessary to the entity's system?

The details in this area help determine that risks are addressed elsewhere in the contract, such as the necessary insurance requirements.

Data Practices Requirements

If an MSP has access to sensitive databases, computer programs and the like, the organization needs to **establish and call out the obligations the vendor has to maintain the privacy, confidentiality and security of that government data**, such as adherence to the Minnesota Government Data Practices Act (MGDPA), Health Insurance Portability and Accountability Act (HIPAA) and so on.

If the MSP is contracted to perform any of the government entity's functions, it is subject to the requirements of the MGDPA. The Act requires that the contract terms make it clear that all data created, collected, received, stored, used, maintained or disseminated by the private service provider in performing the government functions are subject to the MGDPA's requirements and that the private service provider must comply with those requirements as if it were a government entity.

Additionally, unless otherwise excluded by law, the MGDPA requires that in any contract where the government entity discloses government data on individuals to the MSP, the **MSP must administer and maintain that data on individuals in accordance with the Act**.

Organizations should not agree to confidentiality provisions that exceed the provisions of the Minnesota Government Data Practices Act.

CONTROL PHYSICAL ACCESS

Beyond contract management, organizations should develop policies and procedures for secure physical access and data storage rooms to manage the risks relative to vendors and third parties working on site.

See Chapter 9: Secure Physical Access and Data Storage Rooms.

Cyber and Physical Access Security Provisions

Contracts should include **provisions regarding both cyber and physical access security**, particularly if vendors bring electronic devices or equipment and log in to any of the organization's systems. The infamous 2013 hack of retailer Target and its customers came from a breach of Target's heating, ventilation and air conditioning vendor.

Data security requirements may also include:

- Requirement to provide a written information security program that reasonably and appropriately engages physical, technical and administrative safeguards to:
  - Ensure the confidentiality, integrity and availability of organization data stored within or transmitted to or from the MSP's systems.
  - Protect against reasonably anticipated threats or hazards to security or integrity of organization data or services; and unauthorized access to, uses of or disclosures of organization data.
    - Ensure compliance with all applicable laws by the MSP, its officers, employees, contractors, etc.
- Meeting minimum security measures as established by law or a reputable agency, such as the National Institute of Standards and Technology (NIST).
- Electronically transferring data classified as private or not public only when encrypted.

REVIEW PERFORMANCE REGULARLY

To ensure that the MSP is meeting its security obligations, the organization may want to include provisions that allow it to **monitor the vendor's obligations**. This may include access to:

- Compliance certifications
- Assessment of how faithfully the MSP has reported all known material breaches of security, fraud and other irregularities
- The MSP's corporate ethics and social responsibility policies

TERMINATION PROCEDURES

In the event that a organization may need to terminate a business relationship with an MSP, it is best to have the termination steps and obligations called out before the relationship even starts. The termination plan should be sufficiently detailed to prevent disputes.

The MSP likely will have access to the organization's critical data and services, so if the working relationship abruptly changes, clearly outlined obligations in the agreement will become critical to maintaining the organization's normal business functions during a transition or termination of services.

At a minimum, the MSP should be obligated to assist with the transmission of data or transition to another vendor.

Furthermore, ensuring that a past vendor no longer has access to data and information once its services are no longer needed is critically important to meeting the organization's data security obligations.

The organization may also need to include provisions for when and how the **vendor should securely destroy the organization's data** that the MSP has in its systems.

SET EXPECTATIONS IN EVENT OF CYBERINCIDENT

MCIT members that do not have an outside cyber insurance policy are obligated to notify MCIT immediately in the event of a suspected or confirmed data compromise or cyberincident to comply with coverage conditions. If the member contracts for IT services, the **member is still the responsible party for notifying MCIT of an incident, not the MSP.**

Similarly, members are required to report cybersecurity incidents to Minnesota IT Services.* This includes when a government contractor or vendor that provides services to the member has a cybersecurity incident if the incident affects the member.

The MSP contract should **outline how the service provider will notify the organization if it discovers an issue and the timelines** required for that notification. Best practice is to require the MSP to notify the organization immediately upon discovery.

The organization should consider requesting a written security plan from the MSP that details the steps the vendor takes in the event of a breach.

Require Cooperation

Beyond the need for immediate reporting, the member and MCIT need consistent cooperation from any outside technology vendors in the event of a data compromise or cyberincident. This may mean cooperation with an investigation, and plans for communicating with the public or procedures for notifying victims, for example.

In the case of a data breach or cyberincident, MCIT works toward a resolution with the member and MCIT's forensic and legal expert partners. The MSP may not be included in certain conversations to preserve attorney-client privilege.

Also, a conflict of interest may occur if the MSP were the party responsible for causing the event.

The MSP likely will not be part of decision-making on how to proceed toward a resolution of an incident. However, it may be engaged to help execute a plan.

That expectation of cooperation with MCIT in the event of a cyberincident should be included in the terms of the agreement.

OTHER CONSIDERATIONS FOR MSP AGREEMENTS

Define Terms

Most contracts include a section defining key terms related to the agreement. This is important so that the organization and the vendor agree on what terms mean going forward in the contract and then in the working relationship.

Terms that may need to be defined in an MSP contract, among others, are:

- Private data
- Nonpublic data
- Cyberincident
- Security incident
- Data breach

Software, Hardware Purchasing

If the organization intends to have an MSP involved in software or hardware procurement, the service contract should spell out how these agreements and renewals will be managed.

When the organization maintains the ownership and contract duration of various hardware and software programs directly rather than an MSP, the entity has greater control of the procurement process and eliminates potential entanglements in

the event that the entity may need to separate from the managed service provider.

MSP's Access to Data

Restrict the MSP's access only to data necessary to complete the scope of provided services. In doing so, the organization limits the points of vulnerability to its systems and data, and thus, the potential for a cyberincident or data compromise.

SEEK LEGAL, RISK MANAGEMENT ADVICE

Contracting for IT services can involve complex issues. Prior to signing a new, renewed or modified agreement with an MSP, organizations should **have the contract reviewed by appropriate legal counsel and risk management personnel**. Their change recommendations should be implemented so as to protect the organization.

Remember that each agreement for services will require an individual review and language specific to the facts and circumstances of that agreement. The **language used in one section of a contract may not apply to or be sufficient for the same section in an agreement for a different IT service**, for instance.

* See Minn. Stat. § 16E.36; 2024 Minn. Laws Ch. 123, art. 17, § 24.

HOSTING OTHERS' DATA

When an organization hosts another entity's data, the arrangement should be detailed in a formal legal agreement. This arrangement should consider the areas discussed in this chapter and those outlined in *Chapter 8: Cloud Data Storage.*

VENDOR CONTRACTS CHECKUP

Are security measures included in contracts? ☐ **YES** ☐ **NO**	**ACTION ITEMS**
Is encryption required for transmittal for data classified as not public? ☐ **YES** ☐ **NO**	
Does the contract require notification of potential breaches, and require defense and indemnification for breaches caused by the vendor's actions? ☐ **YES** ☐ **NO** • Does the agreement require cooperation of the vendor in event of a data security incident? ☐ **YES** ☐ **NO**	
Prior to signing, are contracts reviewed by appropriate legal and risk management personnel when contracts are new, renewed or modified? ☐ **YES** ☐ **NO**	
Does the vendor have cyberinsurance with sufficient coverage and limits of coverage to address the potential contract risks? ☐ **YES** ☐ **NO**	
Has the vendor passed the entity's due diligence test? ☐ **YES** ☐ **NO**	
Does the organization understand and accept the vendor's business continuity plan? ☐ **YES** ☐ **NO**	
Does the agreement hold the vendor to statutory requirements for data security, such as the MGDPA, HIPAA, etc.? ☐ **YES** ☐ **NO**	
Does the organization review the vendor's performance regularly? ☐ **YES** ☐ **NO**	
Are termination procedures adequately outlined, including procedures for transferring data back to the organization? ☐ **YES** ☐ **NO**	

Incident Preparation, Response and Recovery

Before a data compromise or cyberattack occurs, an organization should position itself to respond to and recover from the attack with minimal disruption. This requires a data and systems inventory, as well as a solid response plan, ongoing practice of it and periodic updating of the plan.

An incident response plan addresses responsibilities, incident identification, triage, notification, investigation (forensics), threat/vulnerability removal and recovery. A business continuity plan is also important to keep operations functioning while recovering from an incident. Some parts of the plan may involve the skills and expertise of outside parties, most of whom MCIT has a contract with to be able to immediately deploy their assistance (for members whose primary cyber coverage is with MCIT).

It is important to respond to incidents in a timely, organized manner. Mishandled incidents can exacerbate the situation and delay data restoration efforts, increase costs and damage the organization's reputation.

INFORMATION TECHNOLOGY INVENTORIES

Before creating an incident response plan, **the organization should develop thorough inventories of:**

- Vital operations
- IT hardware, software and connections to third-party services (e.g., databases, cloud-based services, etc.), noting those that are essential to operations
- Access permissions for employees to data, systems, connections
- Third parties, vendors or other organizations or agreements to carryout the business continuity plan

IT inventories can be used to:

- Identify vulnerabilities
- Create contingency plans should the vulnerabilities lead to a compromise
- Ensure that all systems and data that should be backed up are actually being backed up

These inventories should be recorded and then updated regularly as changes occur. Tip: *Keep an offline copy of the inventory to access if the system is compromised.*

Organizations should identify the following in its equipment and data inventory:

- Equipment and devices to which employees, vendors and the public have access. In the event of a compromise or change of employment/vendor status, the inventory can help with the prompt recovery of equipment.
- Private or nonpublic data and protected health information storage locations. This data may be stored in multiple formats and locations.
- List of those who have electronic or physical access to sensitive or protected data, software or systems.
- Databases maintained by the entity.
- Databases maintained by others that are regularly used by the entity.
- Programs and accounts to which employees have access other than databases.
- Backups of data, software and hardware, where they are located and who has access to them.

The organization should identify the most crucial data and systems on the inventory, and give priority to their backups to help recover the network and data quickly if an incident were to occur.

NETWORK/SYSTEM TESTING, MONITORING

Network/system **penetration testing** is another tool an organization can use to **identify data compromise and cybersecurity vulnerabilities**.

A penetration test attempts to replicate how a threat actor would try to gain access to the organization's system or network by identifying unknown vulnerabilities in the organization's system. This test is typically done after the system is believed to be secure, when its security systems are thought to be strong and in working order.

Test results can be used to further strengthen system security and inform the incident response plan development.

Networks and systems must also be monitored. This involves several layers of protection at the IT level. Network or system monitoring often includes:

- Intrusion prevention systems
- Intrusion detection systems
- Network vulnerability management systems or other programs

Regardless of the programs or devices used to monitor a network, they should be continually maintained and updated without lapses in monitoring.

INCIDENT RESPONSE PLANS

After creating IT inventories and conducting a system test, the organization can develop an incident response plan to address potential data compromises.

Any incident response plan must comply with the requirements of state and federal laws.

After a data compromise, one of the most important elements is time. **Prompt action can help limit the incident's effects**. Organization's need to **think of an incident response in terms of minutes and hours**, not days and weeks.

Although every incident response plan is unique to an organization, all plans should address the following, and the plan should be practiced and reviewed periodically and updated as necessary.

Ensure Plan Adheres to MCIT Coverage*

Ensure that requirements of MCIT coverage are part of the response plan:

- **Notify MCIT of the incident as soon as practicable.** Be sure to assign specific individuals to do this and ensure they have active credentials for the member portal. In a ransomware incident, immediately call MCIT in addition to submitting electronic notification. Tip: *Use a device that is not connected to the compromised system to make the report.*
- **Provide and maintain:**
  - Physical security of the premises
  - Computer systems and hard copy files
  - Computer and internet security
  - Backups of computer data
  - Transaction protection (e.g., for processing credit cards, debit cards, check payments)
  - Protocols for securely disposing of private or sensitive files
- **Participate in a phone consultation with the MCIT-assigned breach counsel** prior to notifying individuals affected by a data breach or compromise.
- **Do not admit liability, incur any expenses or assume any obligation** without the prior consent of

COMPLY WITH MCIT COVERAGE CONDITIONS*

Although it is important to react quickly to a suspected data compromise incident, members must still comply with MCIT cyber coverage conditions in order for coverage potentially to apply.

Members must:

- **Give notice to MCIT of any suspected incident or known privacy or security event,** including cyberextortion, as soon as practicable. This includes an event that may reasonably be expected to give rise to a claim.
- **Provide all such information relating to the event or threat** as MCIT may reasonably request.
- **Be available to participate in a phone consultation with MCIT/MCIT's breach counsel** prior to notifying individuals affected by a data breach or compromise.
- **Require consistent cooperation from any outside technology vendors.** This may mean cooperation with an investigation, and plans for communicating with the public or procedures for notifying victims, for example.
- **Not admit liability, incur any expense or assume any obligation** without the prior consent of MCIT/MCIT's breach counsel.
- **Only make public comments after consultation with and approval from MCIT's breach counsel and/or forensics expert.**

See MCIT Coverage Document.

DEALING WITH AN INCIDENT

If an organization is faced with a data security incident, it should take these steps:

- Follow the organization's incident response plan, including contacting MCIT immediately*
- If an incident response plan does not exist:
  - Secure data/system
  - Lock down and repair—perform necessary actions to prevent further damage to the organization
  - Contact MCIT promptly to report the incident*
    - MCIT will review coverage for repair of affected systems and see if legal review is needed to determine whether a legally defined data breach occurred, and identify forensic IT to identify the scope of the incident
- Perform changes to prevent it from happening again

MCIT/MCIT's breach counsel. Expenses incurred prior to MCIT's approval are the member's responsibility.

As the organization develops its response plan, remember that MCIT's breach counsel may engage IT forensic experts as necessary to assist with an incident.

Incident Response Team and Responsibilities

An incident response team should be established, including management, emergency response and technical employees. The plan should include responsibilities for each team organization and areas of the organization.

If the organization contracts for IT services, designate an internal contact.

A good incident response plan provides **full contact information and includes a backup person for each role** in case of unavailability.

Tip: *A copy of the contact information should be saved in an offline format in case it is inaccessible due to a system compromise.*

MCIT assigns breach counsel and computer forensic experts as needed as part of coverage. These individuals can be key partners to minimize an incident and speed recovery.

Breach counsel provides objective and appropriate expertise based on his or her training and experience with prior events, and provides needed guidance to the organization for its response.

This expertise likely does not exist among the organization's staff, especially where communication with the public is concerned. The breach counsel also maintains all internal communications as privileged.

A computer forensics expert examines a potentially compromised computer, server or network; confirms and analyzes the extent of an incursion; and fixes the problem promptly. Any delay in this step of the process can allow further incursion by the malicious attacker, theft or corruption of data; delay in return to normal operations; and result in an erosion of trust with the public.

Incident Identification

Plans should include a **means to identify that an attack or compromise occurred**.

- Methods should be established for employees or vendors to inform the organization of lost or stolen equipment, successful phishing attacks or other potential data compromises.
- IT staff should gather and document facts surrounding the incident. Network security event logs are often vital in helping verify the date, time and machine involved in an incident.

Any report of a possible data compromise should be reviewed by the incident response team and appropriate measures taken to limit its effects. Steps often include shutting down compromised systems to limit further damage.

Triage and Lock Down

This step **begins to determine the extent of the incident.** Data compromises could involve only one document (electronic or hard copy) or device (e.g., a laptop), or could involve an organization-wide compromise of data. The scope of the incident determines which steps to take.

Schedule regular briefings with appropriate department heads and staff to plan for work activities that will likely be restricted for days or weeks, depending on the severity of the incident.

Begin to identify which devices, systems and data have been affected and which may not be available.

IT should:

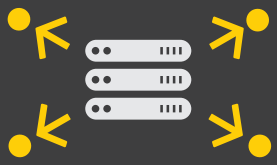
- Secure the data and/or system

AVOID THESE COMMON CYBERINCIDENT RESPONSE MISSTEPS

Entities may take steps that it thinks is helpful in a cyberincident response, but actually may end up making the situation worse. Below are actions a member *should not do* when responding to a cyberincident.

Do not delete any files and start to restore from backups. Doing this will likely obfuscate or destroy valuable evidence that is crucial to determining what happened and what, if any, data has been accessed or exfiltrated that may trigger notification requirements under state or federal law.

Do not issue media statements or give interviews. Rather if necessary, issue a statement indicating that the entity is experiencing a network event and has engaged experts to assist with it. See Public Relations section of this chapter for more.



Do not let outside parties have access to the organization's computers or network, regardless of how experienced or well-intentioned they are. The incident should be considered a crime scene and treated as any other crime scene. This includes limiting information and access only to those who are authorized to engage in the incident response effort.

Do not contact threat actors. Any communications with them should be handled by the MCIT assigned incident response experts, as they will have experience crafting specific communications designed to yield potentially valuable intelligence from the threat actors to help determine data that may have been affected.

Do not tell departments they will be back up in a day. Regardless of how solid and complete the organization's backups may be, containment, assessment, preservation and eradication can take days or weeks. The member should let departments know leadership will share accurate information as it becomes available, but the extent of the incident is still being determined.

Do not attempt to "hack back" or access IP addresses that the member thinks may be related to the attack or the exfiltration of data. Not only is this illegal, but it can also result in damaging important evidentiary information or in some cases, the ability to decrypt.

- Lock down and remove the threat
- If forensic IT is involved, follow its recommendations on when to remove the threat

Notification

Once a compromise is suspected or has been identified, members should immediately contact MCIT.* Contacting MCIT is required prior to taking other actions so that cyber coverage applies. MCIT is keenly aware of the time-sensitive nature of these occurrences and has a process in place to facilitate a quick, collaborative response.

Further notification may be required, including contacting members of the organization, vendors, legal counsel, Minnesota Department of Human Services or Office of Civil Rights, and/or the public. Notification can also include public or media relations.

MCIT's assigned breach counsel conducts a legal review to determine whether a legally defined data breach occurred and the reporting or notification that is required if any.

If the event is real, the organization should consider contacting law enforcement after approval from breach counsel. **Law enforcement assists the organization in properly documenting and storing evidence** to protect the necessary chain of custody for evidence to be used in court. This step is especially important if the incident involves extortion.

If management decides that it wants to pursue and prosecute the network attacker, law enforcement must be notified as soon as it is verified that the incident is real. In most cases, law enforcement agencies will not step in and take over the incident. However, they will work with the team to ensure that its actions stay within the law and do not violate rights.

Investigation

The investigation, often referred to as forensics, should determine how a compromise occurred. Based on the scope of the incident, an MCIT assigned computer forensics partner may be needed to consult with or conduct the investigation. MCIT coverage provides for this service.*

To facilitate the investigation, the organization should:

- Secure all logs, audits, notes, documentation and other evidence
- Secure the chain of custody of evidence

Threat/Vulnerability Removal

Containing, minimizing and correcting the problem that led to the compromise should be the priority.

Continuing to operate with compromised systems increases potential risks and can contribute to the severity of a data compromise. Computer forensics experts may assist with this process.

Public Relations

The organization should **designate a spokesperson as the only person authorized to speak on behalf of the entity**. Employees and elected officials should not speak with the media or discuss the event outside of a "need-to-know" group of key organization personnel, legal counsel and forensic investigators.

Threat actors often monitor news related to their targeted victims and may use this information to inflict

additional damage or leverage against the organization in any negotiations. This is particularly common with ransomware situations.

The organization may need to engage a skilled public relations specialist to help communicate publicly about the incident and deal with the press. Members should only take this step on the advice of the MCIT assigned breach counsel.

If absolutely necessary to address media inquiries, the only released information should be **limited to "the organization is experiencing a network event and has engaged outside experts to assist in determining the scope and extent of the situation."**

Once more details are available, accurate and appropriate communications can be developed for public release as deemed necessary.

Without guidance from the MCIT assigned breach counsel, members should not:

- Issue media statements or give interviews
- Share any information the organization may have received from the FBI or other agencies

Restore Systems and Return to Operations

The organization should determine if backup files are in fact available and viable. If not, this will affect the organization's response options and strategy.

In consultation with computer forensics experts as applies, the organization should begin to restore data from backup files.

Data compromises can make continued operations difficult or impossible for many organizations. **A sound backup and redundancy system ensures that down time and recovery of data is minimized**.

Key to this is having accurate equipment and data inventories and adequate backup systems. Sometimes organizations think information is being backed up, but it is not. This is how entities can get into trouble during the recovery phase.

Frequently backing up data can be helpful in the recovery process (see Recovery and Business Continuity section later in this chapter).

Employee Training

Everyone in an organization has a responsibility to prevent and limit the effects of data compromises and cyberattacks. Although IT may be the only group that needs to understand fully the incident response plan, every employee should know its importance.

Each employee should be trained about the plan and his or her responsibilities, including the methods to report a possible data compromise.

Also, **employees must understand that they are not authorized to make public statements** about a data compromise, including directly to the press, via social media, or in conversation with members of the public, family or friends.

Full employee cooperation is needed to reduce the length of disruptions. When employees also know about basic security concepts, it helps limit the chances of a significant breach.

Practice, Review, Update Plans

An incident response plan is only as good as how well it is understood by those who have to implement it and how well it applies to the organization's systems and needs in real life.

Organizations should test their plans. This provides as close to real-world results as possible and gives staff an opportunity to learn their roles.

Tabletop exercises are one effective way to test plans using various hypothetical situations. Sample exercises are available from a number of sources, but an organization could develop its own to reflect its circumstances more specifically.

Lessons learned from the practices should be memorialized and used to update and refine the response plan.

Incident response plans should also be updated whenever systems, procedures, operations, job positions and so on change, as well as to keep up with current best practices.

After updates are made, the organization should practice and test the new plan. This is a continuous cycle of updating, testing and updating.

See Chapter 15: Training Employees and Officials

Ransomware has specific response recommendations. *See Chapter 6: Malware and Ransomware*

RECOVERY AND BUSINESS CONTINUITY

Certain cyberattacks specifically target the ability of an organization to conduct vital public entity opera-

MODEL INCIDENT RESPONSE PLANS FROM eRISKHUB

MCIT provides its members access to eRiskHub, an access-restricted site that offers a variety of cybersecurity information and resources. Model incident response plans are available from this site that organizations can tailor to their specific circumstances.

Members need an access code to set up an account with eRiskHub. Contact MCIT to request this code: **866.547.6516** or *info@mcit.org*.

tions or business. One of the most common methods is the use of malicious software, known as malware, that includes viruses and ransomware.

Malware typically corrupts, deletes or encrypts an entity's data, software or hardware, making it unusable or inaccessible.

Business Continuity Plan

Before any incident, the organization should develop a plan for how to maintain vital operations in the event of a data compromise or cyberattack. **The business continuity plan should be included as part of the incident response plan and follow a similar format**.

Business continuity plans can be used for multiple events, not just data- or cybersecurity situations. If a plan is already in place for fires, floods, natural disasters or other incidents, the organization should consider reviewing it and updating it to include data compromise and cybersecurity plans.

One of the first steps in the plan is to **identify the critical services to maintain**. These could include items such as dispatch, jail operations, road clearing or plowing operations, payroll and other functions.

Once critical services are determined, consider them from a data security or IT perspective:

- Identify the required hardware, software and connections necessary to complete the required services.
- Ensure that hardware and software are readily available should they need to be replaced or have additional copies on hand to reinstall programs.

Once the services and necessary IT equipment are determined, the next step is to **find alternative organizations or vendors to provide the needed services if the organization is unable to do so**. A good example of this is to establish or use mutual aid agreements with nearby public entities to assist with dispatch, law enforcement or public works activities.

Making these agreements before an incident happens helps keep services functioning with minimal disruptions. Attempting to make these plans during a disruptive event can be haphazard and result in increased cost and decrease the level of services provided.

It is advised to have these agreements in writing to communicate clear responsibilities and expectations prior to any event. *See Chapter 4: Vendor Contracts*

Other methods to maintain service may already be available to the organization, including backup locations that may provide services temporarily until the main locations are functioning again (e.g., a backup dispatch room).

Backup generators or other equipment can help keep systems running in the event of power outages or other damage. These backup devices should be inspected regularly to ensure their functionality in the event of an emergency or damage.

Enlisting the help of others with notification and media relations may also be necessary, depending on the scope of the event.

Data Backups

As some malware delete or encrypt data, having up-to-date backups of information is essential to maintain organizational operations.

Some best practices involving data backups include:

- **Identifying where data is stored.** It may be on servers, computers, mobile devices, in hard copy

records or other locations (see Equipment and Data Inventory section for more information). These should be included on backup schedules as needed.

- **Backing up data frequently**. The more often data is backed up, the more recent the backup data is when needed for restoration after a malicious attack.
- **Employing separate networks or locations**. Data backups should be stored on separate servers or equipment with no contact with the main servers (one ideally is offline). This limits the potential of malware affecting both the main and backup systems. Also storing data in multiple locations is an effective way to minimize dangers of fires or other disasters from affecting business continuity.
- **Using multiple formats to back up data**. Consider digitizing printed materials as an example.
- **Securing data storage locations**. Wherever the data backups are located, whether on site or in alternate locations, the data should be secure. Physical access should be restricted and proper data security measures taken. *See Chapter 9: Secure Physical Access and Data Storage Rooms*

**May be different for members that purchase a third party cyberinsurance policy.*

RESOURCES

"PLANNING: RESPONSE & RECOVERY" PRODUCED BY CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY: Links to various resources to assist in preparing for and responding to cyberattacks.

INCIDENT PREPARATION, RESPONSE AND RECOVERY PLAN CHECKUP

Has the organization completed an inventory of equipment and data storage? ☐ **YES** ☐ **NO**

Has the organization's computer and data systems undergone a penetration test to identify vulnerabilities? ☐ **YES** ☐ **NO**

- Have those vulnerabilities been addressed? ☐ **YES** ☐ **NO**
- Is there a regular testing schedule? ☐ **YES** ☐ **NO**

Does the organization have an incident response plan? ☐ **YES** ☐ **NO**

Does the plan address responsibilities, identification, triage, notification, investigation, threat/vulnerability removal, recovery and business continuity? ☐ **YES** ☐ **NO**

Are staff and vendors/contractors aware of their responsibilities? ☐ **YES** ☐ **NO**

Is the incident response plan regularly reviewed, tested and updated as necessary? ☐ **YES** ☐ **NO**

Are key staff members aware that they must contact MCIT and follow instructions from MCIT and its partners prior to taking action related to a data or cyberincident, including notifying people whose data may have been compromised (if the organization has cyber coverage exclusively with MCIT)? ☐ **YES** ☐ **NO**

Is a business continuity plan in place that includes:

- Inventory of vital operations? ☐ **YES** ☐ **NO**
- Inventory of IT hardware and software essential to those operations? ☐ **YES** ☐ **NO**
- Identification of third parties, vendors or neighboring organizations or agreements made to carry out the business continuity plan? ☐ **YES** ☐ **NO**
- Well-documented agreements with clear responsibilities in place with the above parties? ☐ **YES** ☐ **NO**

Is data backed up frequently? ☐ **YES** ☐ **NO**

Is data backed up in multiple formats and locations? ☐ **YES** ☐ **NO**

Are data backups secure? ☐ **YES** ☐ **NO**

- Is the storage location for data backups secure? ☐ **YES** ☐ **NO**
- Are backups secured electronically? ☐ **YES** ☐ **NO**
- Is at least one backup *not* connected to the organizations systems/network? ☐ **YES** ☐ **NO**

ACTION ITEMS

Malware and Ransomware

Malware is malicious software that disrupts, damages or gains unauthorized access to a computer or computer system. Once a device is infected, the malware can spread to other connected devices.

Criminals use malware for various purposes, such as to steal personal information, to commit fraud, to collect a ransom, for hacktivisim, etc. Malware, although pernicious, can often be avoided with vigilant employees and anti-malware solutions.

Ransomware gets a great deal of attention these days, but plain old malware can cause significant problems as well. Malware can:

- Log keystrokes and mine data to be used for a later attack of a system
- Disable safety and security systems that could cause physical injuries to workers
- Disable critical infrastructure systems
- Overwrite files
- Achieve other nefarious objectives

VECTORS OF ATTACK

Many forms of malware, particularly viruses and ransomware, **are transmitted by email**. *See Chapter 13: Secure Email Practices*

Message recipients are directed to download a file or to open a link that then downloads the malicious code. Often these messages **take the form of a social engineering attack, particularly phishing**, where the message tricks people into downloading malware. *See Chapter 12: Social Engineering*

Other vectors of attack can be:

- Click bait (malicious websites or pages)
- Business email compromise
- Unpatched software or zero-day exploits (attacks that take advantage of newly discovered vulnerabilities for which no patch has yet been released)
- Compromised credentials used to gain initial access (e.g., business email compromise)
- Malicious insiders intentional introduction of malware
- Removable media (e.g., flash drives)
- Misconfigured software, networks or cloud services

RANSOMWARE NEEDS SPECIFIC PREPARATION AND RESPONSE

Although no two ransomware incidents are exactly alike, following basic dos and don'ts can help an organization limit damage, recover faster and reduce the consequences of a cyberextortion incident.

Ransom amounts vary greatly from hundreds to hundreds of thousands, even millions, of dollars, depending on the virus, target and likelihood of being paid.

Ransomware attacks can cripple an organization by preventing it from doing business, and may result in costly fixes, litigation after the fact and negative public relations.

Data compromise incidents, particularly cyberextortion situations, are shown to be:

- Time consuming for staff in both response and recovery efforts, especially if response and business continuity plans are not in place
- Costly, particularly in the event of a noncovered or underinsured loss
- Interruptive in the delivery of services, including potentially critical ones to citizens
- Damaging to the organization's reputation

Once a computer is infected with ransomware, typically the remediation options are to either pay the ransom or replace the hardware, software and data. However, paying the ransom does not guarantee that ransomware will be removed.

It may be possible to decrypt the ransomware, as some of the variant types have flaws. Decryption codes for some variants are available that IT professionals can deploy for a fix.

2-pronged Approach to Extort Money

Most threat actors executing ransomware attacks use a two-pronged approach to extort money from victims:

1. Once they gain access to a network, they **extract data** from the network **before encrypting it on the network**. To increase the likelihood of payment, they frequently attempt to destroy backups of critical systems.
2. **They then demand payment:** 1) to provide a decryption key to unlock the data, and 2) to agree to delete whatever they have taken and not release the data on the dark web.

TYPES OF MALWARE

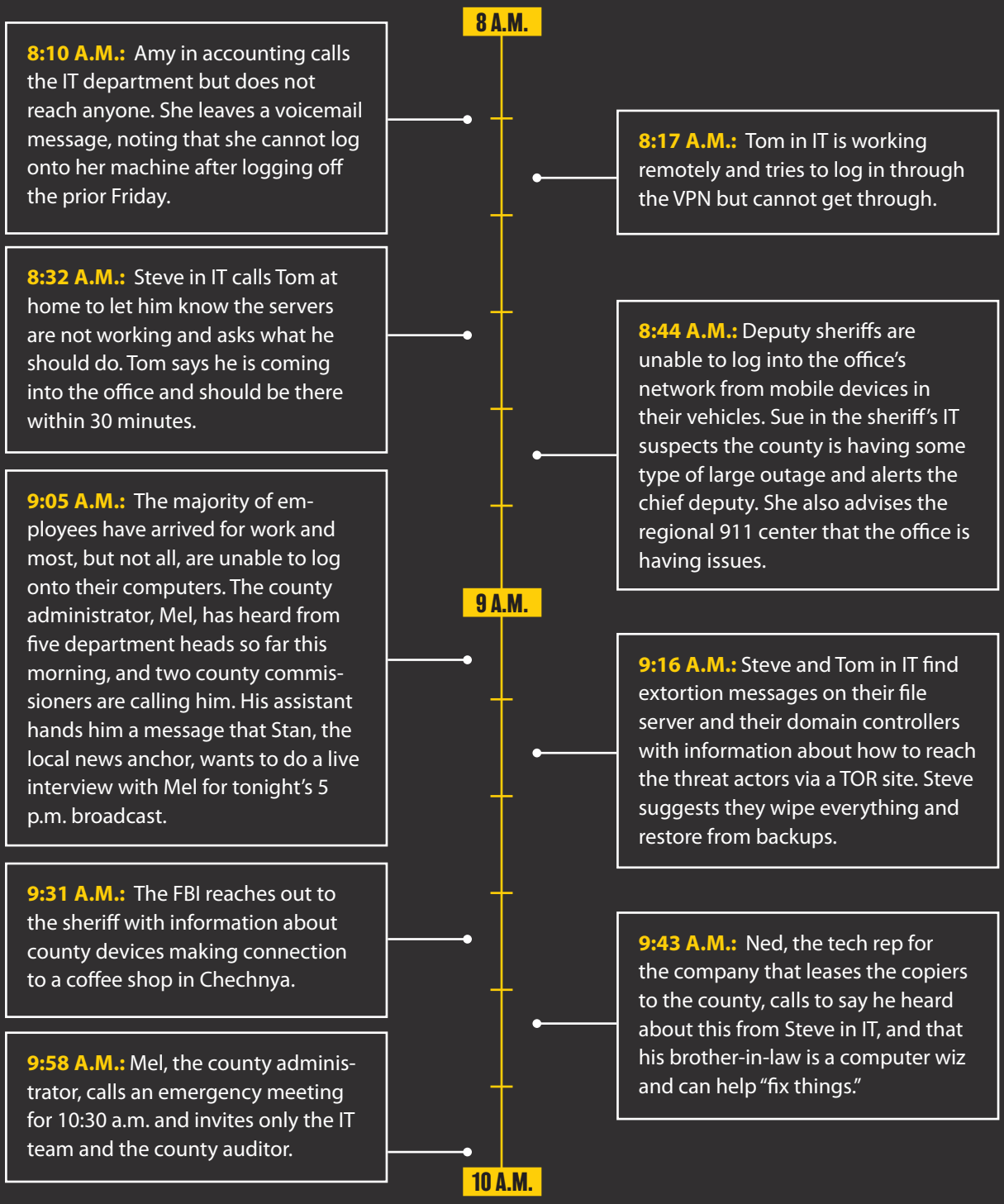
There are several types of malware:

- **Virus** spreads and damages the system's core functions, or deletes or corrupts files. Typically a virus needs some sort of user interaction to spread.
- **Trojan** disguised as legitimate software or included in legitimate software that has been tampered with, it creates back doors in the security to download malicious files and possibly steal sensitive information.
- **Spyware** hides in the background and watches what the user does online, such as noting passwords, credit card numbers, browsing habits and the like.
- **Adware** can undermine a system's security to serve ads to the user based on browser habits and give other malware/spyware a way in.
- **Ransomware** locks a computer/system/data and will not unlock it until a ransom is paid.
  - Perpetrators may also threaten to release information to the dark web unless the ransom is paid.

RANSOMWARE ATTACKS UNFOLD QUICKLY

Imagine you and your team came into the office on Monday morning and found most of your computers were not working and the data on your servers could not be accessed. What would your team do?

Consider this hypothetical ransomware attack timeline.



Although this may seem like a highly condensed and accelerated scenario, it is not. In many cases the situation evolves just this quickly, and in some cases, even faster.

In this scenario, even if an entity has viable backups that the threat actors were not able to destroy, the organization's data being released on the dark web can be highly damaging to the organization, both from a reputational and a litigious perspective.

When there is a ransomware attack, an organization needs to conduct an investigation to determine the extent of the incident, whether there has been unauthorized acquisition of government data and, if so, notify those residents whose data was affected according to legal obligations. MCIT's breach counsel and forensic experts assist with this.*

Incident Response

MCIT's cyberincident response team includes cyber forensic investigators who work in conjunction with and under the direction of MCIT's assigned breach counsel.* They have developed an incident response protocol. It helps limit the impact of an attack and determines, to the extent possible, when and how threat actors gained access to the network, as well as the specific data compromised.

Organizations should have a cyberincident response plan that identifies the incident response team and describes the procedures the organization will take in the event of an attack. *See Chapter 5: Incident Preparation, Response and Recovery*

It is important to note that a **ransomware incident is a crime scene and should be treated accordingly**. Valuable evidentiary data can be obfuscated or destroyed by IT teams rushing in to restore from backups (which may themselves contain malware).

Response efforts must balance the desire to return to normal operations with the need to accurately determine what occurred and what data was affected.

Immediate Steps to Take After Ransomware Attack

- **Pull the plug:** Disconnect devices from the network and isolate backups. Any devices that are shut down should be left off.
- **Call MCIT at 866.547.5616:*** Report the incident to MCIT as soon as possible. Do not wait hours, days or weeks. The sooner the organization alerts MCIT, the quicker the MCIT cyberincident response team can provide guidance.
- **Do not issue a statement:** Only with the guidance of the MCIT assigned breach counsel,* the organization can release a general statement that the entity is experiencing a network incident that is being investigated. Providing too many details can actually harm negotiations with the threat actors.
- **Preserve evidence:** Do not attempt to copy, restore or decrypt data until a plan to preserve

critical evidence has been created in conjunction with the MCIT cyberincident response team.

- **Do not contact threat actors:** Rather, let the MCIT cyberincident response team do this. They have extensive experience dealing with cyber-extortionists and are best equipped to communicate on the organization's behalf.
- **Start assessing damage:** Follow the entity's incident response plan, keeping in mind evidence preservation.
  - Start making a list of devices in the environment and note if they appear to be affected, what data resides on them and what functions they provide.
  - This is the first step in understanding the scope of the incident and understanding how much damage has occurred.
  - It also helps determine the organization's options for restoring data and services.

PREVENT MALWARE INFECTIONS

Organizations should take a multipronged approach to malware defense.

- **Back up data:**
  - Have a data backup and recovery plan for all critical information.
  - Perform and test regular backups to limit the impact of data or system loss and to expedite the recovery process.
  - Have multiple backup methods—at least one should be stored offline, as network-connected backups can become infected with malware, too.
- **Update systems and software regularly:** Vulnerable applications and operating systems are the target of most attacks. Ensuring that these are patched with the latest updates greatly reduces the number of potential entry points for an attacker. *See Chapter 7: Security Patches and Updates*
- **Deploy and maintain up-to-date anti-malware software:** Ensure that all software downloads from the internet are scanned prior to executing.
- **Review and update the organization's remote access policy if necessary to:**
  - Ensure a secure, encrypted virtual private network.
  - Address authentication and what devices may remotely connect to the network.

RESOURCES

"DATA BACKUP OPTIONS" PRODUCED BY UNITED STATES COMPUTER EMERGENCY READINESS TEAM, DEPARTMENT OF HOMELAND SECURITY: This resource details some pros and cons about common data backup options and best practices.

"MALWARE: HOW TO PROTECT AGAINST, DETECT AND REMOVE IT" PRODUCED BY FEDERAL TRADE COMMISSION CONSUMER ADVICE: Gives suggestions about how to best avoid, detect and remove malware from computers.

- **Train staff to be vigilant:**
  - Educate staff about steps they should take to keep the organization's system secure, such as safe web browsing, looking out for social engineering attacks, smart email use and user authentication methods. *See Chapter 11: User Authentication, Chapter 12: Social Engineering and Chapter 13: Secure Email Practices*
  - Review the organization's applicable policies and procedures with staff.
  - Explain what employees should do if they suspect that their computer is infected with malware and how employees can report an incident.
  - Routinely train employees to keep the issue front of mind for them. *See Chapter 15: Training Employees and Officials*

*May be different for members that purchase a third party cyberinsurance policy.

MALWARE AND RANSOMWARE CHECKUP

Do you have a plan for responding to a malware or ransomware attack? ☐ **YES** ☐ **NO**	**ACTION ITEMS**
Are all critical data backed up frequently and are backups tested? ☐ **YES** ☐ **NO**	
Is at least one back up stored offline? ☐ **YES** ☐ **NO**	
Are systems and software updated regularly? ☐ **YES** ☐ **NO**	
Has the remote access policy been reviewed and updated? ☐ **YES** ☐ **NO**	
Is adequate anti-malware software installed and kept current? ☐ **YES** ☐ **NO**	
Are employees trained to identify and respond appropriately to potential malware attacks? ☐ **YES** ☐ **NO**	

Security Patches and Updates

Threat actors continue to develop new and innovative methods to access computer systems, often by exploiting vulnerabilities in systems, networks and programs. To counter this, organizations should regularly install security patches and update their systems, networks and programs, especially as they reach end of life. Failing to update leaves the organization vulnerable to attacks.

One of the most well-known examples of a successful attack exploiting a software vulnerability was the 2017 WannaCry ransomware attack. It hit companies worldwide, infecting more than 200,000 computers in over 150 countries. The WannaCry attack exposed a specific Microsoft Windows vulnerability.

The United Kingdom's National Health Services (NHS) was greatly affected by this attack, bringing it to a standstill for several days. Most of the NHS devices infected with the ransomware were running a supported but unpatched operating system.

The health system had to cancel thousands of appointments and surgeries and relocate emergency patients from affected ERs. Staff reverted to using pen and paper and their own mobile devices as workarounds. The attack racked up a global cost of $8.1 billion.

BEST PRACTICES FOR APPLYING PATCHES OR UPDATES

A security patch/update management program is a useful method to ensure that updates are identified and installed on all devices.

This program should also **include regular audits to identify devices or programs missing important updates.** An organization should review its IT inventories to assist in the audit.

Organizations should look for hidden areas, those places that are connected to the network but are not necessarily accessed/used by employees daily. An example of a hidden connection might by a facility's HVAC system controls. A vulnerabilities scanning system could help identify hidden or forgotten software, hardware or systems that need to be updated or patched.

Other best practices for security patches:

- A patch management system can be used to determine which devices may still require updates.
- All programs, operating systems, networks and anti-malware software should be kept up to date.
- All computers, servers, networks and mobile devices used for work should be patched.
- Patches should be applied in a timely manner once vulnerabilities are discovered.

RESOURCES

"UNDERSTANDING PATCHES AND SOFTWARE UPDATES" PRODUCED BY CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY: Brief description of the importance of patching and how to find patches.

- Patches should not be optional to the end user for work-related equipment.
  - End users may have the option to delay updates but not prevent them.
- Patches should be applied by IT staff or upon IT direction—occasionally threat actors use the excuse of a patch or update to entice employees to download and install malicious software disguised as an update.
  - Train employees how to recognize bogus software update and patch alerts.
  - Employees should be instructed to confirm with IT that software updates are legitimate before launching them. *See Chapter 12: Social Engineering*

SECURITY PATCHES AND UPDATES CHECKUP

	ACTION ITEMS
Are patches managed by a system that identifies and applies updates in a timely manner? ☐ YES ☐ NO	
Is the patch management program regularly audited to identify problems and are any issues corrected? ☐ YES ☐ NO	
Are updates required and cannot be prevented by end users? ☐ YES ☐ NO	
Does the patch management system apply to all devices, programs, networks and systems? ☐ YES ☐ NO	
Are employees trained about how to identify bogus software update/patch alerts and to confirm updates before launching them? ☐ YES ☐ NO	

Cloud Data Storage

Electronic cloud storage can be a solution for organizations that need greater data storage capacity, data redundancy or easy access to data. Cloud storage is where data is stored on remote servers accessed through the internet. Cloud storage is available in two forms: private and public.

Along with its solutions, cloud storage presents potential risks. When evaluating storage providers, members should obtain details regarding the storage and its security.

CLOUD STORAGE

Cloud storage clients send files to a data server maintained, operated and managed by a cloud service provider.

Private cloud storage is where a vendor creates and maintains cloud storage solely for a customer. With private cloud storage, the owner of the data (not the vendor) owns all of the hardware, storage, firewalls, etc. that it uses in a data center and is responsible for its maintenance and updates.

A public cloud service provides storage to multiple clients and is more popular than a private arrangement. The hardware, storage, firewalls, etc. are owned by the host (vendor), and the vendor is responsible for maintenance and sometimes updates.

Amazon Web Services and Microsoft Azure Cloud Services are two examples of many cloud service providers. There are a variety of hybrid models that fall somewhere between the two as well.

Not all cloud services are the same. Some are only meant to be used for noncommercial purposes. Public entities should only use cloud services designed for

commercial businesses. **Organizations should ask about how data is stored** (e.g., all together, segregated) **and ensure the manner of storage meets any applicable laws** (e.g., Health Insurance Portability and Accountability Act, Minnesota Government Data Practices Act).

DOWNTIME

When an organization's cloud provider has technical problems and, therefore, is unavailable, it may affect the organization's ability to do business as usual.

Organizations should ask potential vendors for their scheduled downtimes, as well as their unscheduled downtimes, or reliability rate. Then the entity should decide the amount of downtime, both scheduled and unscheduled, that is permissible for its operations.

As part of any agreement, an organization should **consider negotiating a service level agreement that:**

- **States the expected reliability**, e.g., 99.9 percent, excluding scheduled downtimes
- Usually **outlines** timeframes for scheduled **downtimes**
- **Details negotiated penalties** for exceeding the allowable unscheduled downtime, including what amount will be considered a material breach of the contract

The benefit is that both parties have a written agreement regarding downtime.

SECURITY

Not all public cloud vendors are equal. Security of data—both in the security of the warehouse where the remote servers are physically stored and the electronic security of those servers—are important for organizations to understand before entering into a cloud storage contract.

Inquiries that may assist an organization to assess a vendor's security are:

- Is the data encrypted?
- How does the cloud vendor monitor for breaches? What is its breach experience?
- If a breach occurs, what process does the vendor follow for notifying organizations with which it has contracts? Who is responsible for sending any breach notices if needed?

WHEN HOSTING OTHERS' DATA, EVALUATE THESE CRITICAL AREAS

When done wisely, hosting data for another entity can be mutually beneficial, but it does come with risks. Recognizing pinch points on the front end is crucial for shared success.

An entity that stores the data of other entities should:

- Be able to satisfactorily answer the questions included in this chapter for a cloud data storage provider and respond to considerations outlined in *Chapter 4: Vendor Contracts*.
- Begin with the five critical areas detailed below when considering this type of arrangement.

The goal is to introduce process improvements and assign responsibilities among parties to allow for a shared environment to thrive. Members should work with legal counsel to protect themselves with a formal written agreement for services. The agreement should include much of what is highlighted below, along with other necessary provisions.

1. SECURITY

When an organization shares a storage space, physically or digitally, it inherently has shared vulnerability. It is important to limit and protect access so only trusted users are able to gain entry. Keep in mind the Minnesota Government Data Practices Act obligations and how the hosting arrangement will ensure compliance with the law. *See Chapter 2. Data Privacy Laws*

Beyond simply allowing or denying access, other security measures need to be instituted, such as continuous monitoring, access controls and content filtering.

The hosting agreement needs to establish which entity procures and renews any third-party security tools, programs or services; and who is responsible for continued use of such products and services.

2. PERFORMANCE

It is important for the organization to consider server allocation and amounts of storage needed and allowed. These two points can greatly impact functionality.

It is also wise to know any shared peak times of heavy traffic that can overtax the system and hinder performance. Known fluctuations in traffic can be managed ahead of time through load balancing and caching, as well as other actions and processes.

3. SCALABILITY

When an organization allows another entity to access its storage, the agreement should clearly detail what the other entity's needs are. Having file size requirements and limits identified on the front end should protect the hosting organization from internal battles among mutual parties for space.

When the host's digital footprint grows, so does its needs. The hosting party must understand what that means for upgrades and updates, and the impact to others or required maintenance. Establishing storage limits contains costs and helps avoid performance issues.

4. DATA PRIVACY

Arguably the most important concern on the list is privacy. It is paramount that compliance considerations are clear and segmentation is achieved to limit access and protect against unauthorized access or exfiltration of information.

Other steps may need to be taken if sensitive data is being housed. Beyond significant access controls, encryption (in transit and at rest) may be appropriate.

Establishing and adhering to an effective data life cycle management plan is also an effective step to reduce vulnerabilities and to reduce the amount of unnecessary data consumption.

Data life cycle basically refers to how long the data is necessary or required (i.e., records retention schedule or business need) to be maintained. Once it is no longer needed, it should be deleted. If it must be kept indefinitely, it can be removed from the server and retained in another storage method. *See Chapter 3: Data Management*

5. TECHNICAL SUPPORT

The hosting agreement needs to establish which entity is responsible and available to respond to technical issues.

Responsibility and availability go hand–in-hand, as critical functions or service may suffer if technical issues arise, which they unfortunately do.

Having clear directions to the workforce for reporting issues should be established and having technical folks available to match the needs of the services provided are crucial. If one entity is providing time-sensitive services in public safety, it is essential to have technical support at the ready to ensure no critical services go down and stay down for any significant period.

- What security compliance certifications do the data centers have?
- What is the vetting procedure for employees, subcontractors, etc. that have access to the servers or data?
- Is there an ability to inspect or audit data centers?

Organizations may want to consider encrypting data before backing it up in a cloud.* This may provide an extra layer of security if the cloud vendor suffers a breach.

REDUNDANCY

Members should find out if stored information is backed up by vendors. For example, many major cloud providers have multiple storage facilities located around the United States and some internationally. The purpose is that if the vendor suffers a catastrophic loss at one location, it can switch to another location's server(s) where the redundant data is stored. Local public entities that host others' data may not do this.

The cloud storage provider should tell the entity:

- Location of storage facilities
- Available security for each
- If a loss occurs, the time it takes to recover the data and make it available to organization

RECOVERY

Organizations should ensure that they **understand the scope of the data being backed up, the frequency of backups and the method via which the data will be recovered**.

For example, if the entity's local system is destroyed because of a natural disaster, is there an ability for the member's IT professional to begin restoring the system from any location? What other equipment would be necessary to accomplish such a task?

CONTRACTS

Negotiation

Organizations should inquire whether the terms of service/contract are negotiable. Some vendors may be more willing to negotiate terms than others.

Members of the State of Minnesota Cooperative Purchasing Venture (CPV) may want to review the cloud vendors and terms of those contracts, as they may be more favorable than an individual government entity may be able to negotiate.

Termination

Organizations **should know the method and cost of having its data returned** from the vendor if the contract is terminated. Members should also consider adding language that requires the vendor to assist in migrating data.

Organizations should consider implications, if any, of the Official Records Act and/or the Minnesota Government Data Practices Act. Discussions regarding the ability to retain and destroy data, including whether the data is actually destroyed, should be had when evaluating different providers.

Limitations of Liability

Most technology contracts have significant limitations of liability and waivers or warranties. **Organizations should review and understand exactly what damages they may or may not be able to recover.**

The key is to make a knowing decision and not be surprised if something goes wrong.

Insurance, Defense and Indemnification

As with any contract, organizations should **ensure that the liability of the risk is placed with the party that is able to manage the risk.**

If this is not possible, the entity should make an informed decision about accepting those risks and have discussions regarding what that may mean for the organization in the future.

OTHER CLOUD STORAGE SECURITY CONSIDERATIONS

Additional security considerations should be met if an organization stores data with a vendor:

- Data should be transmitted securely to the cloud provider
- Stored data should require strong encryption
- The cloud storage provider should meet minimum nationally recognized standards, such as from the National Institute of Standards and Technology (NIST), Statement on Standards for Attestation Engagements (SSAE) No. 16

- Physical access to servers or data storage locations should be restricted
- The cloud storage operator should include data redundancies to protect stored data in the event of physical damage, such as from fires or natural disasters

*Encryption is when data is altered to make it unusable to unauthorized users.

RESOURCES

"3 CONTRACT ISSUES TO WATCH," BY MINNESOTA COUNTIES GOVERNMENTAL TRUST (*MCIT.ORG*): Article addresses assumption of liability, sufficient liability limits and proper coverage as key contract issues to help manage risks.

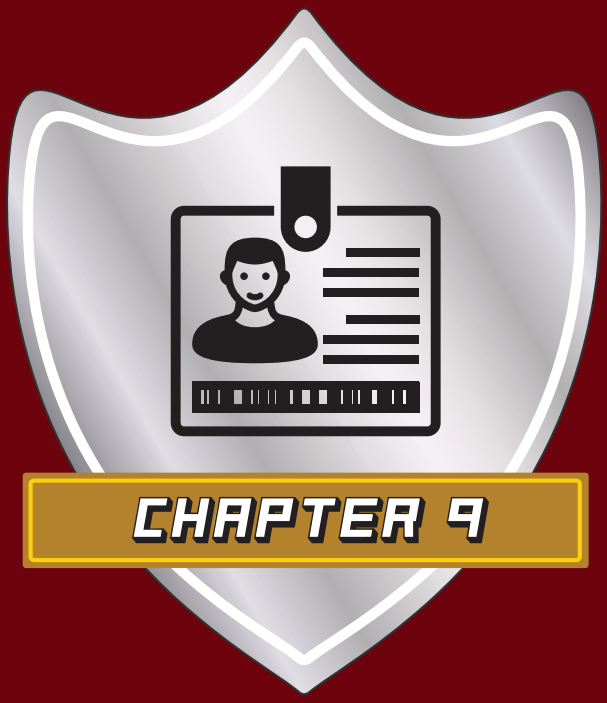
"COVERAGES AND LIABILITY LIMITS FOR INDEPENDENT CONTRACTORS" BY MINNESOTA COUNTIES GOVERNMENTAL TRUST (*MCIT.ORG*): Article reviews recommendations for minimum coverages and liability limits, including general requirements, certificate of insurance, specific insurance, and hold harmless and indemnification agreement.

"INDEPENDENT CONTRACTORS LIMITS OF LIABILITY" BY MINNESOTA COUNTIES GOVERNMENTAL TRUST (*MCIT.ORG*): Article provides tips for how to work with independent contractors to ensure that they have adequate liability insurance limits in place to match the member's policies and projects' risk exposures.

"RED FLAGS IN CONTRACTS" BY MINNESOTA COUNTIES GOVERNMENTAL TRUST (*MCIT.ORG*): Article discusses areas to review in legal contracts before finalizing agreements, particularly places to look to ensure that the member is not assuming unwanted liability.

CLOUD DATA STORAGE CHECKUP

Is stored data encrypted? ☐ **YES** ☐ **NO**	**ACTION ITEMS**
Do data storage locations offer redundancy? ☐ **YES** ☐ **NO**	
Does the cloud provider meet the organization's legal and security requirements? ☐ **YES** ☐ **NO**	
Is appropriate insurance, defense and indemnification language required of the service provider or is risk knowingly accepted? ☐ **YES** ☐ **NO**	
Does the organization understand the cloud provider's retention policy, destruction of data, and cost and method of returning the organization's data? ☐ **YES** ☐ **NO**	



Secure Physical Access and Data Storage Rooms

A variety of people, such as citizens, employees, board members, vendors and contractors, visit local government facilities daily. With so many people at any given location, preventing unauthorized persons from physically entering data storage rooms or accessing on-site systems should be a high priority.

SECURE DATA STORAGE

Organizations are encouraged to secure locations containing sensitive data and **adopt a secure physical access policy**.

In addition to preventing unauthorized entry, storage rooms should also be located and constructed so as to be protected from fires, floods, humidity, temperature extremes, pests, and power interruptions and surges.

Data should be backed up and stored in multiple locations and in various formats for increased redundancy and ease of restoration if needed.

PHYSICAL ACCESS POLICY

Preventing unauthorized people from stealing documents, accessing servers or uploading malware on premises is just as important as preventing unauthorized remote electronic access to data.

Setting up restricted areas where sensitive data and equipment are stored is a common way to secure data. Authorized individuals are often provided a badge, keypad lock code or key to access the area.

Organizations should develop a policy for what is stored in these areas and who has access to them.

Best Practices for a Physical Access Policy

- Staff should **not allow unauthorized persons into restricted areas** even if the individuals are known to the employee, including other employees.
  - Methods should be developed to address both familiar and unfamiliar people found in restricted areas without authorization.
- **Guidelines** should be established, followed and enforced **when removing or destroying private or nonpublic data from secure areas**.
- **All visitors, contractors or vendors** in a secure area should **have an ID, escort or both**.
- Staff should **securely store sensitive data** at workstations, particularly when away from the station, such as paper files, in locked cabinets or drawers.
- When away from workstations, staff should **lock computers and take their security fob/device** (for multifactor authentication) with them. *See Chapter 11: User Authentication*
- **Passwords and login information should be kept secret**, not written down. *See Chapter 11: User Authentication*
- **Staff should be trained** about the policy.
- The **policy** should be **reviewed regularly and updated** as necessary.

DATA STORAGE ROOMS

Data storage rooms are locations where files, servers, electronic backups or other records are often kept.

Data storage rooms should be designed or modified to the extent feasible to minimize the risk of loss from these hazards:

- Fire
- Excessive humidity
- Direct sunlight
- Water leaks
- Temperature extremes
- Power outages
- Lightning
- Pests

Best Practices for Data Storage Rooms

- **Lock doors** to limit access to authorized personnel only.
- **Follow all manufacturer guidelines** on electronic equipment with regard to temperature control and tolerable humidity levels.
- **Use temperature or humidity monitoring software** or services to inform maintenance and/or IT staff of elevated temperatures and conditions.
- **Be mindful of airflow** around servers or other electronic devices.
  - Poor airflow can impair the functionality of heating, ventilating and air conditioning systems.
  - Depending on the style of equipment, airflow may be required beneath equipment. Take care when selecting flooring options for server rooms or data storage rooms to provide for this air flow.
- **Consider using uninterruptible power supplies or battery backups** for critical systems or equipment.
  - These devices can help prevent damage to computer systems in the event of a power outage by allowing time for systems to shut down normally.
  - Battery backups add an extra layer of protection against power surges and allow users an opportunity to save information before it is lost.

KEEP MOBILE DEVICES SECURE

Just as important as keeping IT servers and data storage rooms secure is maintaining the physical security of mobile computing and data storage devices, as well as physical data files.

Employees should always be in control of items such as laptops, tablets, smart phones, flash drives and printed documents that contain or may provide access to sensitive data.

Public entities should consider policies and procedures for keeping these items secure. For example, members may not allow anyone other than authorized employees to use these devices or review documents; and may require employees to keep devices and data in secure locations when they are not using them, such as a locked desk drawer or in the locked trunk of a vehicle.

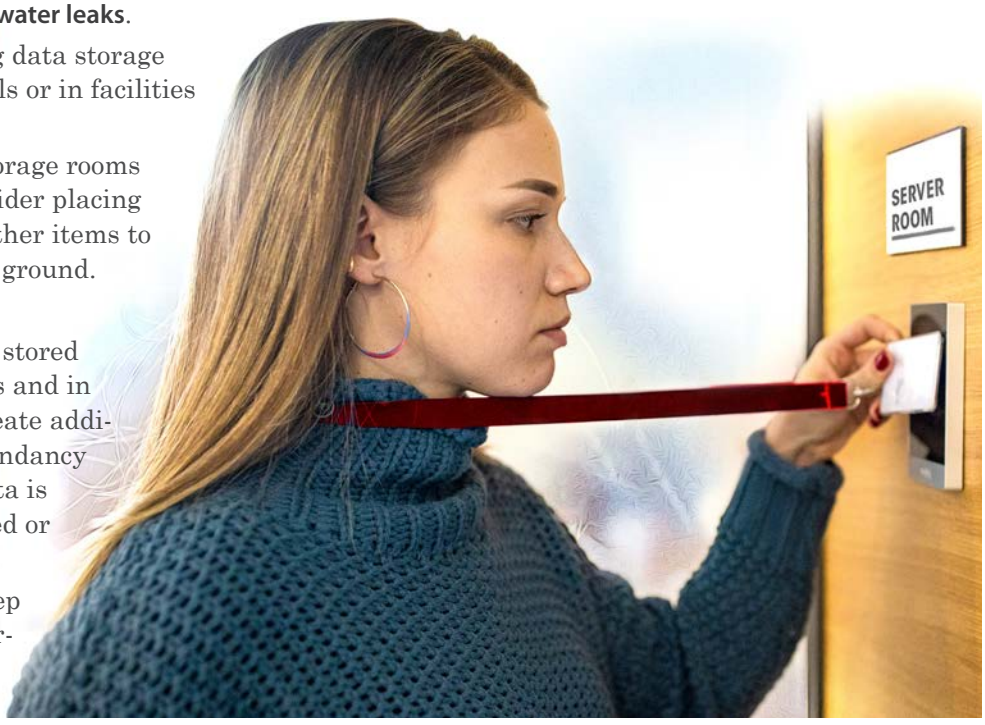
See Chapter 10: Mobile Devices and Remote Work

- **Understand the types of fire suppression systems, if any, in server/IT rooms,** as well as their associated hazards. There are a variety of fire suppression systems available, such as water and gas systems.
  - Gas systems can be less damaging to electronics or paper records. A gas system typically functions by displacing the oxygen a fire needs to burn. Care should be taken to prevent people from being in a room when a gas system activates.
  - A pre-action system requires the activation of both a smoke detector and sprinkler head to flow water. This type of system can help prevent accidental discharge through damage to pipes or sprinkler heads; however, it could create an electrocution hazard and heavy damage when discharged.
- **Install Type C fire extinguishers in server rooms**.
  - These are designed for extinguishing electrical fires and can prevent further damage to electrical components.
  - Dry-chemical or water-based extinguishers may damage electronic components.
- **Maintain at least 18 inches of clearance below sprinkler heads** to ensure functionality of fire suppression systems.
- **Avoid painting sprinkler heads or hanging items from them**.
- **Be aware of pests**. Data storage rooms may not be visited often, so occasionally pests (insects, mice) inhabit the space.
  - Boxes can make good nests for rodents, destroying the documents within.
  - To discourage pests, do not keep any food in data storage rooms and occasionally inspect the area for signs of their presence.
- **Plan ahead for flooding or water leaks**.
  - Consider positioning data storage rooms on upper levels or in facilities on higher ground.
  - For existing data storage rooms in lower levels, consider placing items on blocks or other items to keep them off of the ground.
- **Maintain data backups**.
  - Extra copies of data stored in different locations and in different formats create additional layers of redundancy in the event that data is lost, stolen, corrupted or destroyed.
  - These copies can keep an organization operational even after a serious situation.

RESOURCES

MINNESOTA OSHA CONSULTATION—WORKPLACE VIOLENCE PREVENTION, MINNESOTA DEPARTMENT OF LABOR AND INDUSTRY: Although focused more on personal safety, MN OSHA consultation can conduct security assessments on facilities at no charge. This information can be helpful in restricting access to important locations.

"DATA BACKUP OPTIONS" PRODUCED BY UNITED STATES COMPUTER EMERGENCY READINESS TEAM, DEPARTMENT OF HOMELAND SECURITY: This resource details some pros and cons of common data backup options and best practices.



SECURE PHYSICAL ACCESS AND DATA STORAGE ROOMS CHECKUP

Does the organization have a policy for restricting access to secure areas containing sensitive data? ☐ **YES** ☐ **NO**	**ACTION ITEMS**
Are employees trained about and follow the secure data access policy? Is the policy enforced consistently? ☐ **YES** ☐ **NO**	
Are plans in place to account for visitors or others (such as contractors) entering sensitive areas for other work? ☐ **YES** ☐ **NO**	
Are unauthorized personnel in restricted areas questioned for proper identification or escort? ☐ **YES** ☐ **NO**	
Are data storage rooms equipped with locking mechanisms that limit access to authorized staff? ☐ **YES** ☐ **NO**	
Are temperature and humidity regulated and monitored in data storage/server rooms? ☐ **YES** ☐ **NO**	
Are items stored so as not to restrict airflow around air-cooled equipment? ☐ **YES** ☐ **NO**	
Are fire sprinklers or suppression systems in place and appropriate for the types of data stored in the space? ☐ **YES** ☐ **NO**	
Are fire sprinklers or suppression system heads free of obstructions? ☐ **YES** ☐ **NO**	
Are regular checks conducted to identify and control pests in secured data areas? ☐ **YES** ☐ **NO**	
Is stored data protected from flooding or kept off of the floor? ☐ **YES** ☐ **NO**	
Is data backed up in multiple locations and formats? ☐ **YES** ☐ **NO**	
Is an uninterruptible power supply or battery backup in place for sensitive data storage equipment, and is it tested regularly? ☐ **YES** ☐ **NO**	

Mobile Devices and Remote Work

Mobile computing devices (e.g., laptop, tablet, smart phone) and remote work offer exciting possibilities for an organization to achieve its operational goals; however, they also increase the risk of data security incidents.

Members should consider a number of security issues when permitting remote work and the use of mobile devices for work purposes.

REGULATE SECURITY AND USE OF MOBILE DEVICES

An organization that allows mobile devices to be used for work purposes should consider adopting a policy regulating security and use. **The policy is important for security and to address data management, retention, privacy, and potential wage and hour issues:***

- The county attorney and/or other legal counsel should review the policy prior to its adoption because many laws may be implicated.
- The organization should train staff about the policy requirements and ensure its enforcement.
- The policy should address both electronic and physical security of devices that contain and/or connect to sensitive information or organization's network.

If the organization is going to utilize both employer-issued and personally owned devices, two separate policies should be considered. With personally owned devices, a government employer may be limited in its ability to verify updates, ensure security and/or obtain data from an individual employee's mobile device.

EMPLOYER-ISSUED MOBILE DEVICE USE POLICY

Items to consider for a policy addressing employer-issued mobile devices:

- **Guidelines for who may use the mobile device and for what purposes**. If employees may use the device for personal business, the entity should establish guidelines to ensure compliance with the Minnesota Government Data Practices Act (MGDPA) and other applicable data privacy laws. For example, only employees of the government entity who have a need to know have the ability to access private data stored or located on the phone. This may have the effect of prohibiting users other than the employee.
- **Guidelines for connecting the device to other equipment**, such as prohibiting employees from connecting the device to unsecured devices or networks. Connecting to unsecured devices or networks increases the likelihood that the content transmitted by or located on the device may be hacked.
- **Physical security guidelines** about how employees should maintain control of mobile devices (including flash drives) that contain or have access to sensitive data. For example, members may not allow anyone other than authorized employees to use these devices or review documents; and may require employees to keep devices in secure locations when they are not in use, such as a locked desk drawer or in the locked trunk of a vehicle.
- **Guidelines for installing applications** ("apps"), such as prohibiting users from installing apps without IT approval or to only use apps from trusted sources. Many apps require users to allow the app developer access to data stored on the device. Allowing this may violate the MGDPA and other privacy laws.
  - The apps for text messaging should be limited to those that are secure and encrypted, and approved by the organization's IT department.
- **Guidelines regarding which mobile data should be classified as official records** and the need to be archived on the employer's system.
  - Official records are determined by the content of the communication, not the medium by which it was transmitted or created. This may include text messages.
  - The entity should review which type of data will be solely stored on the mobile device and how or if that data needs to be transferred to the entity's archival system.
- **Procedure and timelines for staff to inform the employer of lost, stolen or potentially compromised devices.** Staff should be directed to report if a mobile device is no longer in their possession in a timely manner. The entity should consider installing software on the mobile device that allows it to be remotely wiped of all data.
- **A patch management program** for updating/patching mobile devices. When a potential security exposure is found on an operating system, the developer often issues a patch that addresses it. Failing to ensure that the latest patches

MOBILE DEVICE SECURITY BEST PRACTICES

The following best practices can help maintain the security of data on mobile devices. Some of the following may not be possible on employee-owned devices.

- Mobile devices should be **password protected and locked** when inactive.
- **Transmitting not public data should only be done over secure networks.** Any private or nonpublic data should be encrypted.
- The mobile device should have **software** installed to allow for users **to lock and wipe data remotely** should the phone be lost or stolen.
- Mobile devices and their associated apps should be **updated and patched regularly**. *See Chapter 7: Security Patches and Updates*
- Devices should be **securely wiped of all private data prior to removing them from service** or transferring them to new users.

are installed increases the risk that a threat actor may be able to access the mobile device and its content. *See Chapter 7: Security Patches and Updates*

- **Application of other policies to mobile devices**, such as MGDPA, password, etc. The government entity likely has policies that address the security and use of data in a nonmobile device setting. Consider stating that all policies apply to use of employer-owned mobile devices.
- **Staff should be trained not to send or reveal not public data** in an unsecured way. The entity should consider whether encryption software should be included on the mobile device. The entity should remember to consider security of text messaging.
- **Right of privacy.** Like with many acceptable use computer policies, the government employer may want to include a statement that there should be no expectation of privacy related to the information sent or stored on a government-issued mobile device.
- **Instruct nonexempt (hourly) employees** that work should only be performed during work hours. Managers must also be aware of this limitation.

EMPLOYEE-OWNED DEVICE USE POLICY

An organization may decide to allow employees to use a personal mobile computing device for work (sometimes referred to as "bring your own device"(BYOD)). This permission may be explicit or implicit. It is recommended that employers make an intentional decision regarding this use and have a policy addressing it for the organization to manage its risks.

When developing the policy, the organization must acknowledge that although it may have a legitimate interest in obtaining work-related data from an employee's personal device (e.g., MGDPA request, discovery for a lawsuit), the employee may have a reasonable expectation of privacy for the personal data stored there.

Because of this, the government entity should **keep the Fourth Amendment** (freedom from unreasonable search and seizure), **state laws** (such as Privacy of Communications Act) **and federal laws** (such as Stored Communications Act) **in mind when developing the policy.**

A WORD ABOUT TEXT MESSAGES

Text messaging is a growing medium for public entity employees to communicate with other employees and clients. Texting is convenient, but it is not always secure. If employees are allowed to text sensitive information, the app should be secured and have end-to-end encryption. This scrambles the message so that only the authorized recipient can decode the content.

However, if the device is compromised, encryption cannot guarantee that the sensitive information is not accessed by a threat actor.

See Chapter 11: User Authentication and Chapter 12: Social Engineering

Policy Considerations

The policy should:

- Notify the employee about and **outline how the employee may be required to provide the employer access to certain data on his or her device.**
- **Discuss the implications of a litigation hold** if it would include data stored solely on the employee's personal device
- **Include guidelines for which employees may use a personal device.** Because an employer may have less of an ability to manage security and access data on an employee's personal device, it may want to consider limitations of use (e.g., no communications that would be considered "official records" via text or other formats that do not route through the government entity's server).
  - The entity should have an understanding of the types and classifications of data that may be stored on an employee's personal device.
- **Outline conditions that must be satisfied** if an employee uses a personal mobile device for work purposes, **such as, prior approval from the organization and an agreement to abide by many of the security requirements** applicable to government-authorized devices:
  - Guidelines for connecting the device to other equipment, such as prohibiting employees from connecting the device to unsecured devices or networks
  - Physical security guidelines
  - Guidelines for updating the software system and installing security patches

CONCERNS ABOUT FLASH DRIVES

Flash drives are small external drives that can be plugged into any USB port. Flash drives make it easy for users to transport files. However, members may want to consider whether they allow employees to copy entity files onto flash drives to then be uploaded onto a device that is outside the security purview of the entity.

For example, an employee uses a flash drive to take files home so that he or she can work on them from a home computer. The danger is that the flash drive could become corrupted with a virus or other malware on the home computer. When the flash drive is plugged into the member's computer the next day, that malware could transfer to the member's system.

If members allow employees to plug flash drives into outside devices, they may want to look into security measures to ensure that flash drives do not transfer malware or other security threats to the member's system/network.

- Guidelines for installing apps, such as prohibiting users from installing apps without IT approval or to only use apps from trusted sources
- Installation of encryption software
- Application of other policies to mobile devices, such as MGDPA, password, etc.
- Procedure and timelines for staff to inform the employer of lost, stolen or potentially compromised devices
- Permission to install software and wipe device remotely if lost, stolen, etc. or before providing the phone to a third party

- **Include guidelines regarding which mobile data should be classified as an "official record,"** requiring archiving on an employer's system. Even if not considered official records, work-related communications should be transferred to the employer's server, including text messages.
- **Education related to the security of data** and who may access the data on the device. Many individuals allow family (including children) and friends to use and access their devices. If the device contains data protected by a privacy law, such as Health Insurance Portability and Accountability Act or the MGDPA, then such access may have to be limited.
- **Instruct nonexempt (hourly) employees that work should only be performed during work hours**. Managers must also be aware of this limitation.

REMOTE WORK AND SECURITY

Management must ensure that IT equipment and services are secured and satisfy the member's obligation to protect data and information even when employees work remotely.

Determine the Most Effective Technology

Employers need to ensure that the technology available to remote employees will enable them to be effectively and securely connected to the systems needed to complete their work.

The employer should determine what equipment it will provide for remote work and ensure that it is included on the member's electronic data processing equipment inventory.

If remote employees are asked to provide their own equipment, determine:

- How the employee will be compensated and technical support will be provided
- What system features and security are required—these considerations apply to any piece of equipment used for business purposes, including mobile devices

Ensure Data Security and Privacy

The organization should develop policies and procedures for ensuring data security and privacy in a remote work setting.

In addition to a secure electronic connection to the organization's systems and files, the employee should be required to ensure the physical security of devices and sensitive paper documents.

The organization should consider adopting these remote work security best practices:

- Require that the employee's **wifi is password protected**
- **Use a business virtual private network** (VPN), as it may be difficult to confirm the security of every employee's wifi connection
  - The VPN creates an encrypted connection over the internet between a device and a server (i.e., the employer's data system/network)
  - Apply multifactor authentication to the VPN log in to further secure the connection *See Chapter 11: User Authentication*
- **Require employees to destroy private data and nonpublic data in a secure manner,** e.g., shredding appropriately *See Chapter 3: Data Management*
- **Provide a secure virtual meeting platform** that allows for password-protected meetings to deter hacking, especially for meetings that discuss private, nonpublic or confidential information
- **Require employees to maintain physical security of materials and equipment** (protected from damage or misuse)
- **Maintain an inventory of all employer-owned and -issued equipment** in the remote office, including serial numbers when possible
- **Ensure that firewalls and virus protection are up to date** on computer/mobile devices
- **Make sure that encryption is used where appropriate and employees use the member-supplied email system** (not a personal email account)Tip: *Create a system for employees to use the organization's phone system while working remotely, rather than using their personal phone numbers and voicemail (e.g., employer-provided mobile phone or VOIP phone system)*
- **Remind employees that organization-owned or -issued devices and programs are for business purposes only**
- **Employees should store work files on organization devices,** not personal devices or drives

Be Ready to Manage Technology Problems

Although many organizations have a dedicated IT resource, certain employees may be too geographically dispersed for this arrangement. **Have a pre-arranged solution available so that when a technical problem emerges, employee connectivity is promptly restored**, and employees can continue their work effectively.

*Wage and hour issues are outside the scope of this resource.

RESOURCES

"PROTECTING PORTABLE DEVICES: PHYSICAL SECURITY" PRODUCED BY CYBER SECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY: Overview of threats and best practices to protect mobile devices.

"HOW TO COMMUNICATE SECURELY ON YOUR MOBILE DEVICE," PRODUCED BY CYBER SECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY: Overview of security threats when communicating via a mobile device and how to secure them.

QUICK TAKES ON DATA SECURITY PRODUCED BY MINNESOTA COUNTIES INTERGOVERNMENTAL TRUST (*MCIT.ORG*): Ready-to-use mini training scripts and employee handouts provide succinct information about specific data security threats and steps employees can take to keep information secure.

MOBILE DEVICE AND REMOTE WORK CHECKUP

	ACTION ITEMS
Does the organization have a mobile device policy? ☐ YES ☐ NO • Has staff been trained about the policy? ☐ YES ☐ NO • Does the policy outline whether personally owned devices are permissible and under what requirements? ☐ YES ☐ NO	
Does the organization have a mobile device policy? ☐ YES ☐ NO • Have employees been trained about the policy? ☐ YES ☐ NO	
Do mobile device policies include guidelines to: • Comply with the MGDPA? ☐ YES ☐ NO • Prevent connecting the device to unsecured networks or equipment? ☐ YES ☐ NO • Use only approved or trusted apps? ☐ YES ☐ NO • Contemplate storage of official records or items archived on the device? ☐ YES ☐ NO • Report lost or potentially compromised devices immediately? ☐ YES ☐ NO • Prevent the unsecured sending or sharing of private or not public data? ☐ YES ☐ NO • Include a statement explaining no expectation of privacy (employer-owned device policy)? ☐ YES ☐ NO • Provide guidelines requiring nonexempt (hourly) employees only to perform work during work hours? ☐ YES ☐ NO	
Are mobile devices used for work purposes locked or password protected? ☐ YES ☐ NO	
Are employees instructed to keep mobile devices physically secured? ☐ YES ☐ NO	
Are private and not public data encrypted on mobile devices used for work purposes? ☐ YES ☐ NO	
Can data be remotely wiped if the mobile device is lost, stolen or compromised? ☐ YES ☐ NO	
Are operating system and software patches and updates applied to the device regularly and in a timely manner? ☐ YES ☐ NO	
Is data wiped prior to retiring devices or transferring them to new users? ☐ YES ☐ NO	

User Authentication

User authentication is one of the keys to securing data. It allows only those who have permission to access data, a system or device to be able to do so. Most organizations use a variety of tools to make it nearly impossible for a threat actor to gain admission. Typical user authentication tools are passwords, multifactor authentication and encryption.

PASSWORDS, PASSPHRASES

A password or passphrase is a secret set of characters known only by the user to access devices, programs, data and sometimes locations. For this reason, passwords are common targets for threat actors.

Passwords are figuratively the keys to the kingdom. If they are not strong, unique and kept secret, it is akin to leaving the door wide open for threat actors to walk in and take what they want or corrupt systems.

Password Policy

To help secure electronic data, an organization should **develop a password policy that:**

- Explains the requirements and expectations for creating and updating passwords
- Includes rules prohibiting sharing passwords or storing them in unsecured locations
- Requires that staff be trained about password policies when beginning employment and retrained as neces-

sary (e.g., when the policy is changed)
- Includes a method of enforcement and outlines disciplinary measures should employees share passwords, leave passwords in unsecured areas, fail to update passwords or use insecure passwords

Various software programs require that users update passwords at certain intervals. Other software may require that passwords meet certain standards before being accepted.

With the ever-changing nature of technology and cybersecurity best practices, it is important to review and update the password policy periodically.

Secure Passwords

The following best practices can help create and maintain passwords difficult for threat actors to break. **Methods to create strong passwords should be included in the password policy**.

- As a general rule, **longer passwords are more secure** than shorter passwords. Current recommendations are to have at least 16 characters. Using passphrases can increase the length of a password while still being easy to remember (e.g., Basketballisgreat).
- Use passwords or passphrases that **mix capital and lowercase letters, numbers and special characters** to make them more complex.
- **Avoid words in the dictionary**. Deliberate misspellings or using numbers/symbols for letters can help (e.g., "basketballisgreat" could become "b@$k3Tb@11i$8reAt!").
- Use **unique passwords for each program, device, service or location**.
- Change passwords as needed, using the same rules for complexity as listed above. Certain programs force users to update passwords and can even rate password strength.
- **Keep passwords secret:**
  - Do not share passwords with anyone.
  - Avoid storing or writing down passwords in an easy-to-find location.

Changing Passwords

Current security recommendations indicate that as long as passwords are complex (a minimum of 16 characters, using symbols, numbers and lower- and uppercase letters), passwords can be changed less frequently than previous suggestions.

Cybersecurity experts have found that when employees are forced to change their passwords frequently, they tend to make easy-to-remember modifications that end up weakening the password. For example, the employee may use an old password and just add "1" to the end and keep this pattern going each time a change is required.

What is more important is that **new passwords are created as soon as a threat or actual compromise is**

WORK STATUS CHANGES

When individuals leave employment or change roles or departments within an organization, potential exists for data breaches. A policy to collect private and nonpublic data from employees and restricting their access to sensitive data when work status changes occur can help reduce risks. These risks also apply to vendors or contractors who have access to sensitive data.

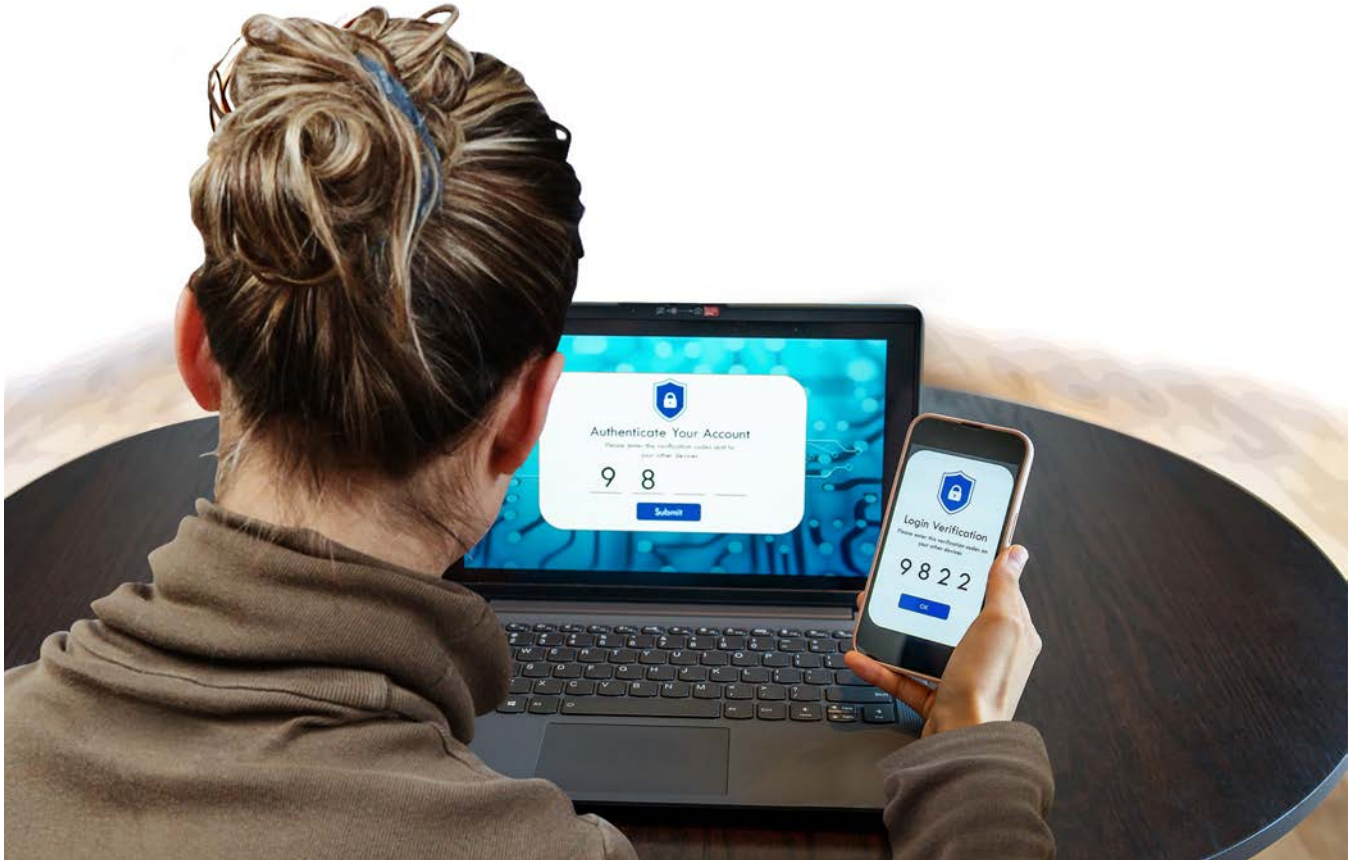
End/Change of Work

Similar to when employees begin work, a process should be developed for when an employee or contractor/vendor leaves work. With regard to data security, the policy should include the following best practices:

- **Gather any private, nonpublic data** the employee/contractor has in his or her possession. This could include data on electronic devices, either owned by the organization or owned by the individual.
- **Terminate electronic access to the organization's systems.** This could include disabling passwords or usernames. Remember to restrict access to email, as well as secure data.
- **Change log in usernames and passwords to outside systems** to which the employee had access.
- **Prevent physical access to secure areas** with private or nonpublic data. This could include collecting access badges or changing passcodes.
- Inform other employees that the individual/contractor no longer works for the organization.

When employees transfer to different job duties or departments, the employer should **follow a similar process** to gather materials and restrict access from the previous role as necessary.

See Chapter 4: Vendor Contracts and Chapter 9: Secure Physical Access and Data Storage Rooms



discovered. Again, the new passwords should be truly unique and follow the complexity rules noted above.

Password Managers

Password managers are a software tool that helps users securely store, generate and manage passwords for online accounts. The organization's **IT department should review and approve any use of a password manager** by employees to ensure that they are, in fact, secure services.

Because the password manager is a repository for each account's password, it is even more important for employees to **establish a long and complex password for the manager and to absolutely keep it secret and unique**.

MULTIFACTOR AUTHENTICATION

Using multifactor authentication is one of the top three ways security experts protect their information and systems.

Multifactor authentication (MFA) is a security enhancement that requires a user to present two or more pieces of evidence or credentials when logging in to an account, secure area or device.

The credentials fall into any of three categories:

- Something the user knows (e.g., password)
- Something the user has (e.g., smartcard, fob)
- Something the user is (e.g., fingerprint)

RESOURCES

"FORMULATE STRONG PASSWORDS AND PIN CODES" PRODUCED BY CYBER SECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY: Provides overview of problems when poor passwords are used and how to strengthen passwords.

QUICK TAKES ON DATA SECURITY PRODUCED BY MINNESOTA COUNTIES INTERGOVERNMENTAL TRUST (*MCIT.ORG*): Ready-to-use mini training scripts and employee handouts provide succinct information about specific data security threats and steps employees can take to keep information secure.

The credentials must come from two categories to enhance security, so entering two passwords would not be considered multifactor authentication. Rather the user may need to enter his or her username and password, then enter a temporary security code that is sent to his or her mobile phone or a fob.

This tightens security as it is unlikely that a threat actor would have both a password and the user's mobile phone or fob.

Before implementing multifactor authentication, the organization should **identify the data, systems and programs it needs to protect**.

Technical Solutions

The technical solution an organization chooses depends on its computing environment and how data is stored. For example, deploying MFA on remote access is an option but only one hurdle in a threat actor's quest for an organization's data.

Adding MFA to databases or internal software that accesses data the member needs to protect provides an additional protection.

If there is MFA available within the application, service or software, a simple internet search or use of the help menu should provide all the information one needs to implement MFA.

Human Solutions

Multifactor authentication can also be humans simply verifying requests. This is often the key to sidestepping a misdirected payment scam.

Misdirected payment fraud is typically when victims are actively deceived into transferring money to fraudulent destinations (address or account). For example, the organization may receive an email from a threat actor that mimics a legitimate vendor and asks that payments be made to a new account number.

A best practice is to establish a policy and procedures for processing payment changes:

- **Require staff to verify payment changes** before authorizing a change. Best practice would be to call the vendor or payee using a known, previously verified phone number. Another option is personally to visit the payee (e.g., an employee).
- **Verification using email is not advised**, but if used, start a new message to the vendor or payee and, again, use a known, previously verified email address for the vendor or payee. This should prevent the message from delivering to the perpetrators of the theft attempt. If the payment change request is via phone, verify the request by calling the phone number or emailing the address on record for the vendor, not the one the caller provides.
- The organization should **consider limiting the number of people authorized to make changes** to vendor's or payee's direct deposit or ACH information and train them on the policies and procedures.
- **Employees should be empowered to request verification for unusual requests**, even if they seemingly come from within the organization or from leadership.

To assist in avoiding payment scams, members can ask their bank to call a specific contact at the organization to verify a transfer of funds outside of the United States before processing the release of funds.

See Chapter 12: Social Engineering

ENCRYPTION

Employing **encryption** technology **offers another way for organizations to authenticate users**. Encryption is a process of turning readable content (plaintext) into encoded content (ciphertext). It can be used in a variety of places to secure sensitive data and verify authorized recipients.

One of its most valuable applications is **helping to secure emails and text messages.** Thus, allowing an organization to take advantage of these convenient and efficient communication methods for sending and receiving sensitive data, just like they do for public/not sensitive information.

Email and text messages are incredibly vulnerable to threat actors, as they can intercept messages in transit and easily gain access to inboxes. Even if an organization's messaging systems are secure, it cannot control the security on the recipient's end. **Encryption can protect messages in transit and in both the sender's and receiver's accounts**.

In the case of email and text messages, it encrypts the message so that only the intended recipient(s) can read it. When threat actors intercept an encrypted message, they see scrambled, unreadable text.

A WORD ABOUT 'SIGNAL-GATE'

A significant leak of intelligence about plans of a U.S. strike on Yemen occurred in 2025 when a journalist was inadvertently added to a group chat of top U.S. national security officials within the Signal app. Signal is operated by a nonprofit and provides end-to-end encryption for users' messages.

At the time of the leak, it was considered one of the safest messaging systems for the public but was not recommended (or approved in some circumstances) for government officials' communication of sensitive information.

Despite the app being "secure," what is important to take away from this situation is that human error created the leak (including an unauthorized person in the chat). No amount of encryption could have prevented this data breach.

The authorized recipient of an encrypted message, however, has a unique private key that unlocks the message and decodes the ciphertext and converts it to plaintext.

Messaging encryption can block a significant avenue of attack for threat actors and protect the privacy of those who have entrusted the organization with their sensitive information.

In addition, **encryption can help prevent threat actors from learning information related to the organization and its employees**, including log in credentials, that can be exploited to gain access to the entity's network, systems and files.

A text message caveat: Although some text messaging apps have end-to-end encryption, including Google Messages, iMessage, Signal and WhatsApp, others do not, such as mobile carrier text plans. And among those with encryption, they are not all the same. Some encrypt the message so even the messaging app provider cannot access message content while others do not have this security feature.

An organization should carefully consider encryption options for its systems and applications, including email and text messaging, to ensure encryption provides the level of security the organization wants. Keep in mind, that **the easier encryption is to use, the more likely that employees will use it**.

Employers should also **develop policies for sending and receiving sensitive and private data via email and text message,** and train employees on the policy, as well as on how to use encrypted messaging.

See Chapter 13: Secure Email Practices

USER AUTHENTICATION CHECKUP

PASSWORDS	ACTION ITEMS
Is a password policy in place that includes: • Requirements for password creation and complexity? ☐ YES ☐ NO • Frequency of password updates? ☐ YES ☐ NO • Measures to ensure that passwords remain private and difficult to access? ☐ YES ☐ NO • Means of enforcement? ☐ YES ☐ NO	
Is the staff trained about the password policy and retrained periodically or as updates occur? ☐ YES ☐ NO	
WORK STATUS CHANGES	
Is a policy in place for when employees and contractors/vendors leave work that: • Gathers all private and nonpublic data the individual or contractor/vendor has, including on electronic devices? ☐ YES ☐ NO • Prevents access to the organization's systems? ☐ YES ☐ NO • Prevents physical access to protected information? ☐ YES ☐ NO • Informs current employees about the status change? ☐ YES ☐ NO	
Does the policy also apply when an employee's or contractor's/ vendor's job role or department changes? ☐ YES ☐ NO	
MULTIFACTOR AUTHENTICATION (MFA)	
Does the organization apply MFA to all systems, programs and locations that contain or are connected to data requiring security? ☐ YES ☐ NO	
Are staff instructed on security requirements for their phone/fob for MFA system? ☐ YES ☐ NO	
Are human solutions employed to verify changes to payments? ☐ YES ☐ NO	
Does the organization use encrypted email and text messaging, especially for sending and receiving sensitive/private data? ☐ YES ☐ NO	
Are employees trained on when and how to use encryption? ☐ YES ☐ NO	
Are text messaging apps updated and checked to ensure end-to-end encryption? ☐ YES ☐ NO	
Does the organization have a policy about using encryption for email and text messaging? ☐ YES ☐ NO Are employees trained on this policy? ☐ YES ☐ NO	

Social Engineering: Phishing, Misdirected Payment Fraud, Business Email Compromise

Social engineering is the use of social skills and psychology to trick individuals into sharing sensitive, valuable or private information. The main objectives of social engineering attacks are to:

- Infiltrate systems and plant viruses or other malicious programs on the systems *(See Chapter 6: Malware and Ransomware)*
- Access, modify, delete, distribute or hold data or systems hostage
- Perpetrate fraudulent payment

As social engineering attacks are common, developing a means to combat them should be a priority for organizations. **Social engineering targets people** rather than systems or equipment, so **prevention efforts focus on a combination of multifactor authentication tools and educating staff** to recognize and address suspicious activities.

TYPES OF SOCIAL ENGINEERING

Social engineering attacks take many forms and can be deployed via email, websites, pop-up web pages, phone calls or in person.

Phishing

Phishing is the most common type of social engineering attack. Phishing attacks are deceptive emails sent to entice people to share sensitive information, or open attachments or click on links that install malware.

A phishing example is an email claiming to be from IT with a file attached. The email contains instructions to download and install the attachment as the newest security patch/update or risk losing computer access. If downloaded, the attachment installs malware on the system.

Business Email Compromise and Misdirected Payment Fraud

Business email compromise and misdirected payment fraud are variations of tricking organizations into sending payment or providing data or credentials to a threat actor posing as a trusted leader or business partner.

Usually the requests are "urgent" so as to fluster the receiver into complying without thinking through or verifying the requests.

Business Email Compromise

In business email compromise cons, cybercriminals impersonate trusted leaders to entice employees to provide data or account credentials or to send money.

Typical business email compromise scams:

- An email appears to come from the organization's leader requesting an immediate wire transfer to pay an invoice, which is fraudulent.
- A fraudulent request is sent from the organization's leader's compromised email account to staff responsible for W-2s or maintaining personnel information. The scammer requests employee W-2 information, which is then used to commit income tax refund fraud.
- An employee receives a request from a threat actor posing as management to purchase several gift cards for a work-related purpose. The message indicates that the manager is tight on time and needs the employee to provide the gift card codes to him or her.
- Urgent request to reset username and/or password that looks like it comes from the organization's IT department, partner (e.g., bank) or executive leadership. The link to reset the password actually takes the individual to a fraudulent location where the threat actor acquires the credentials to use later to infiltrate the account or system.

Misdirected Payment Fraud

The emails typically mimic known vendors, making it simple to fool victims. Local governments are easy targets for misdirected payment fraud, as publicly available board meeting agendas, summaries and minutes contain listings of vendors, items being purchased or bid and payment amounts.

Although MCIT provides misdirected payment fraud coverage, its limit can easily be exceeded.*

Common misdirected payment fraud scams:

- A threat actor posing as a known vendor/contractor sends an email requesting a change in where payment to the vendor is made, usually a new (fraudulent) routing and/or account number.
- A scammer poses as an employee and asks that the direct deposit of the employee's payroll be sent to a new (fraudulent) account.

Clickbait

Clickbait is a form of web-based social engineering, which may or may not be malicious. Clickbait is content whose purpose is to get users to click on links. This is often done with exaggerated or sensational headlines or photos and is commonly used by advertisers.

Unfortunately, threat actors also use clickbait to install malware once the link is clicked. Clickbait is often included with emails or other social engineering attack methods.

Fraudulent Calls

Phone calls can be social engineering attacks, too (called vishing). People claim to be in a position of authority, such as management, law enforcement, government organizations or IT. These calls would then demand sensitive information under threat of penalty.

An example is a call from someone claiming to be with the FBI asking for a Social Security number to avoid paying a fine.

In-person Cons

In-person social engineering attacks could be people posing as inspectors, co-workers, technicians, vendors or law enforcement. They may have valid-looking identification. In-person attacks also include people simply claiming to be in distress.

An example is a person arriving at the front desk with coffee stains over a pile of documents explaining that the documents for a big presentation are ruined. The individual would ask the receptionist to take a flash drive and print the documents saved on it. When plugged into a computer, the flash drive installs malware.

TECHNICAL TOOLS FILTER SCAMS

Several technical options are available to assist with preventing employees from even encountering social engineering attacks in the scope of their work. These include web browser and email filters, firewalls, sandboxes, anti-malware software, among others.

These security solutions are programmed to identify content this is high risk or likely to be a threat (i.e., phishing emails). However, technical solutions are not 100 percent effective.

SPOTTING AND AVOIDING MISDIRECTED PAYMENT FRAUD

These best practices can help members spot fraudulent requests before releasing funds:

- **Train all staff** in techniques to identify phishing scams and how to report them.
- Require that staff **verify payment changes before authorizing a change**. Best practice would be to call the vendor or payee using a known, previously verified phone number. Another option is personally to visit the payee.
- **Verification using email is not advised**, but if used, start a new message to the vendor or payee and, again, use a known, previously verified email address for the vendor or payee. This should prevent the message from delivering to the perpetrators of the theft attempt.
- Request that the **member's bank** call a specific contact at the member entity to **verify a transfer of funds outside of the United States** before processing the release of funds. Most local governments do not send money internationally, but misdirected payment fraud is often perpetrated by those outside of the U.S.
- **Red flag Green Dot Bank in email systems**. This online bank is frequently used in misdirected payment fraud scams.
- **Require the vendor or payee to complete and sign a new direct deposit or ACH form** to provide documentation if an issue arises. Provide the new form only to the individual's on-record, verified contact email or mailing address, or in person.
- **Have a policy and procedures for verifying payment change requests**. Train employees on the policy and enforce it.
- **Limit** the number of **individuals who can make changes** to a vendor's or payee's direct deposit or other payment information.
- **Investigate unusual requests**, ask questions and verify the authenticity of the request.

RECOGNIZING SOCIAL ENGINEERING ATTACKS

Most social engineering attacks involve common characteristics. Training staff to recognize these characteristics and to respond accordingly can help prevent attacks from succeeding.

SOCIAL ENGINEERING AND AI

With the development of generative artificial intelligence (AI) and its general availability, social engineering attacks are harder to detect. They are significantly more personalized, have fewer errors and may employ convincing deep fake images, audio clips and videos. *See Chapter 14: Safe Internet Browsing*

Some of the tried and true red flags for identifying social engineering may no longer appear because of AI (e.g., grammatical or spelling errors), but the basics remain the same.

Train employees to develop their skepticism muscle, to face the new world of AI:

- Typically legitimate workplace communications are not emotionally charged. If a message or request leans heavily on a strong emotion, especially when coupled with urgency, this is a potential scam.
- Look for signs a video, image or audio clip is a deep fake, such as inconsistent shadows, unnatural speech patterns, overly smooth skin on face, etc.
- Ask if this is a typical communication/request from the sender. If not, be wary of responding or taking the requested action.
- If a message falls into one of these general stories, it is a potential scam:
  - I'm your boss, and I need your help. Do not ask me any questions.
  - I'm from IT/cybersecurity/a technology vendor, and your system is compromised. We must move now.
  - I'm a vendor, and I'm terminating service immediately if you don't do something for me.
  - I'm with the postal service/shipper, and there was a problem with your package delivery. Click this link to resolve the issue.
  - I'm with a service or brand you trust, and your account has been hacked. Act now to fix it.
  - I'm with a service or brand you trust, and we have an amazing offer for you. Act now to claim it.

Best practices:

- Employers should craft employee training to align with the most common threats the staff is likely to face.
- Increase the frequency of training to keep the issue top of mind for employees.

AI is not just a threat, it can be used to help combat social engineering attacks. For example, behavioral analysis and anomaly detection are popular AI techniques that enable cybersecurity platforms to spot patterns that would indicate AI-enhanced malicious activities.

Social engineering attacks often involve:

- **Rushed requests that require a fast response or crucial time window**. Social engineering attacks rely on a person not asking for confirmation or checking with others prior to acting. Therefore, immediate responses are demanded.
- **Requests for sensitive, valuable or private information**. Most social engineering attacks ask for passwords, log in information, Social Security numbers, bank account numbers, credit card information or other data that is typically kept private or confidential. Requests for this information from any source should be treated with suspicion.
- **Threats**. This piece goes along with rushed requests in that negative consequences are frequently threatened if the request is not granted in a timely manner. Threats of fines, denied access, missed opportunities for easy money or employment termination are common.
- **Unsolicited contact**. Social engineering attacks are not typically in response to a request or other previous communication. Receiving an unsolicited communication should raise suspicions even if it seems to come from a known internal or external contact.
- **Emails**:
  - Social engineering attacks are often delivered through email, particularly phishing attacks, business email compromise and misdirected payment fraud.
  - The sender's address is frequently a different format from the rest of the organization. For example, all emails within the organization follow the format of "firstname.lastname@countyname.gov," but the message claiming to be from a manager, co-worker or IT is different (e.g., firstname.lastname@county.org).
- **Vague greeting and sender**. Often bulk phishing attempts do not send messages directed to individual people. Messages may start with "attention," "invoice attached," or another generic phrase. Similarly, messages that end with a title or vague location should be viewed with suspicion (e.g., Web Administrator, Help Desk).

- **Frequent misspellings and poor grammar**. Commonly, attacks originate in non-English speaking parts of the world, so spelling and grammar errors should arouse suspicion. Note: *Artificial intelligence is making it easier for threat actors to perfect their English usage.*
- **Clickbait** asks users to click on links or open attachments. This action is what deploys the malware.
- **Items in a spam/junk email folder**, which is typically unsolicited bulk commercial messages. Many IT departments and email providers have filters that automatically screen spam messages and direct them to the spam/junk folder. If a message is in the spam folder, it can be a clue that it may not be legitimate.

AVOID SOCIAL ENGINEERING ATTACKS

Members should consider these best practices to help avoid becoming victims of social engineering attacks:

- **Implement technical tools** that filter email for known and suspicious messages before they deliver to employees' inboxes.
- **Train staff regularly** about the common ways to recognize social engineering attacks and what to do if they receive suspicious messages or requests.
- Develop a **process to report suspicious requests** to determine their legitimacy.
- **Refer data requests to the responsible authority.**
- **Verify credentials** of any inspectors, vendors or others claiming to have business in staff-only areas prior to allowing entry per any applicable secure access policies. *See Chapter 9: Secure Physical Access and Data Storage Rooms*
- **Avoid clicking on any advertisements, messages or pop-ups** when browsing the internet. Certain advertisements, messages or other elements may attempt to trick individuals into clicking on them to install malware. Also use secure websites. *See Chapter 13: Secure Email Practices and Chapter 14: Safe Internet Browsing*

If individuals encounter a suspicious email, they should:

- Not click on any links or open any attachments.
- Hover over links to reveal the link's true address and see if it matches the intended site.
- Contact IT.
- Any suspicious email, phone call or visit should be reported to the designated individual (e.g., IT, supervisor or administrator).

RESOURCES

EMAIL SECURITY AWARENESS DIGITAL IMAGES, PRODUCED BY MINNESOTA COUNTIES INTERGOVERNMENTAL TRUST (*MCIT.ORG*): Series of digital images that highlight four keys to building awareness among employees about common email security concerns, including phishing and business email compromise. Images can be used in a variety of places and provide easy tips for employees to use to help keep the organization's systems and data secure.

QUICK TAKES ON DATA SECURITY PRODUCED BY MINNESOTA COUNTIES INTERGOVERNMENTAL TRUST (*MCIT.ORG*): Ready-to-use mini training scripts and employee handouts provide succinct information about specific data security threats and steps employees can take to keep information secure.

Other Practices Help Sidestep Social Engineering Attempts, Minimize Effects

In addition to the above best practices:

- **Employees should follow the organization's policy** and IT staff instructions when applying updates or patches to software. *See Chapter 7: Security Patches and Updates*
- **Multifactor authentication can be a way to sidestep the effects of social engineering.** Even if a threat actor were to acquire a user's password, he or she would likely not be able to get the second credential (e.g., temporary security code, smart card/fob or fingerprint) through social engineering in order to access a secured system. *See Chapter 11: User Authentication*
- The member should **develop a plan to respond to any potential data compromises,** including a means for employees to report any possible compromises related to a social engineering or other attack. *See Chapter 5: Incident Preparation, Response and Recovery*

*May be different for members that have a third party cyberinsurance policy.

SOCIAL ENGINEERING CHECKUP

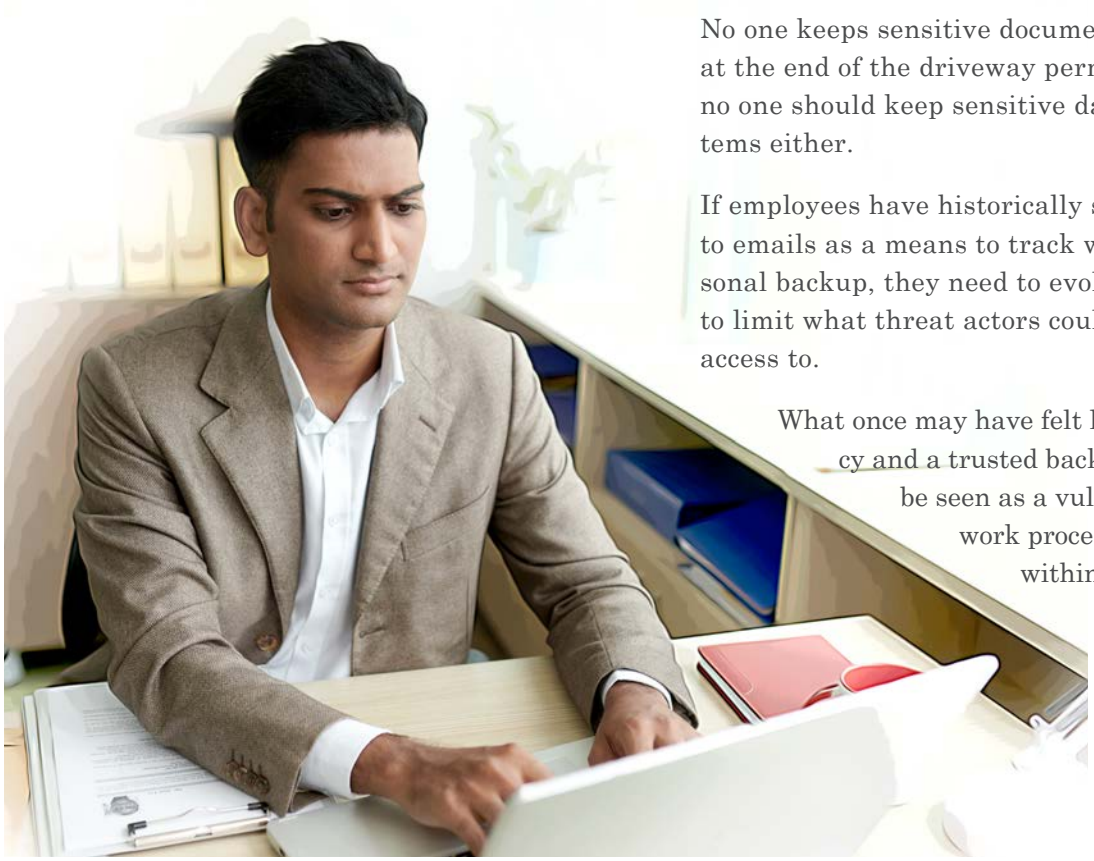
PASSWORDS	ACTION ITEMS
Are employees trained about recognizing common characteristics of social engineering attacks? ☐ **YES** ☐ **NO**	
Are employees trained about techniques to avoid data compromises from social engineering attacks? ☐ **YES** ☐ **NO**	
Are plans in place and are employees trained about how to report social engineering attacks and possible data compromises? ☐ **YES** ☐ **NO**	
Is multifactor authentication used to help prevent threat actors from gaining access to systems/data even if they acquire passwords? ☐ **YES** ☐ **NO**	
Are technical tools installed to filter and block likely phishing attempts from delivering to employee's email inboxes? ☐ **YES** ☐ **NO**	

Secure Email Practices

The most common vector for MCIT member cyber-related claims is email, and employee behavior frequently plays a role as well. In addition, using email to send or store private, nonpublic or other sensitive information exposes that data to email's inherent security weaknesses. The good news is that simple strategies can help reduce these vulnerabilities.

Take this situation as an example:

- An employee had more than a decade of emails saved in his email account. His account was hacked, giving bad actors access to years' worth of email contacts, personal information and documents saved in messages and attachments.
- The threat actors then proceeded to phish all of the email contacts and had access to hundreds of people's personal information.
- The hacked organization had to pay for sending hundreds of breach notifications, credit monitoring services for those whose information was leaked and public relations coaching on top of the expenses to eradicate the malware released on the employer's system.



No one keeps sensitive documents in a mailbox at the end of the driveway permanently. As such, no one should keep sensitive data in email systems either.

If employees have historically saved or held on to emails as a means to track work or as a personal backup, they need to evolve their practices to limit what threat actors could potentially gain access to.

What once may have felt like a great efficiency and a trusted back up, now needs to be seen as a vulnerability in the work process and a liability within the organization.

MANAGE DATA IN EMAIL SYSTEM

Email is excellent for sending and receiving communications, but it is risky to use it for long-term information and document storage.

Threat actors are constantly hunting for valuable information that can be stolen and used to extort money from the rightful owner or an organization.

Having sensitive information easily accessible in an email account can create an unnecessary and avoidable vulnerability.

Employees should ask themselves what information and how much would be readily available to threat actors if their email login credentials were stolen or the account were hacked in some other manner?

Email Should Be Pass Through, Not Storage System

Email is not intended to function as a data storage service. Rather it should be **treated like a physical mailbox, where individuals retrieve communications that are opened and either trashed or filed securely elsewhere.**

For employers that utilize a document management service or customer relationship management service program, once an email is uploaded to the system, employees should be instructed to remove the original message from the email system.

If an organization does not have such programs or services, employees should be trained on how and where to store essential information in secure places, such as private network drives.

After emails have been saved outside of an email account, employees should then delete messages from their accounts. If messages are left in the email inbox, the security threat has not been resolved.

ENCRYPTED EMAIL SYSTEMS

Sending sensitive data via regular email systems greatly increases the risk of a data compromise or breach. To avoid this, **encrypting email messages and attachments can help increase security**. This may involve using an outside service. *See Chapter 11: User Authentication*

Encryption alters data to make it unusable to unauthorized persons.

Using Encrypted Email

Encrypted email should be used whenever an organization sends or receives sensitive data.

Some examples of when to use encrypted email include:

- **Data classified as private or nonpublic** under the Minnesota Government Data Practices Act
- **Confidential health records** covered by the Health Insurance Portability and Accountability Act
- Any **payment card** industry **or other banking information** that could be used to make fraudulent purchases or for identity theft
- **Personally identifiable information** such as names, Social Security numbers, and date and place of birth
- **Other information deemed sensitive** by the organization, such as log in credentials

The process to use encrypted email varies depending on the service provider. Some common examples are:

- Adding an "encrypt and send" button
- Requiring users to add a keyword to a subject line (such as "encrypt") to encrypt an email
- Automatically screening emails for certain combinations of words, numbers or pictures that indicate sensitive information and encrypt the data automatically

The above are just samples of options. Regardless of the options chosen, retrieving encrypted messages almost always requires the recipient to log on to a website to access the message.

Staff should be trained about when and how to send and receive encrypted emails.

PRACTICE GOOD EMAIL HYGIENE

The security of an email account is critically important, as it is often a primary mode of business communication and data sharing. Beyond maintaining sound retention practices, employees must be diligent about protecting their email accounts on the front end.

How to Maintain Good Email Hygiene

- **Utilize strong passwords** and change the password as required or necessary. *See Chapter 11: User Authentication*

ENCRYPT TEXT MESSAGES

Just as emails that contain sensitive or private information should be encrypted to keep that data from being readable to threat actors, text messages with sensitive information should also be encrypted. *See Chapter 11: User Authentication*

- **Keep the password secret and unique**. Do not keep it in a visible note on the desktop, share with others or use a duplicate password associated with another log in.
- **Change tendencies or tactics that create unnecessary duplication** (e.g., CC'ing oneself on a sent email).
- **Establish a routine to purge unnecessary messages regularly**. Remember to delete messages from the sent, draft and trash boxes of the email account, as well as from the inbox.
- **Save necessary messages and attachments** outside of the email account **in a separate secure system**.
- **Utilize encrypted email** to send and receive private or sensitive data.

USE OF PERSONAL EMAIL FOR GOVERNMENT BUSINESS PURPOSES

The Minnesota Government Data Practices Act (MGDPA), as well as the government entity's records retention schedule, generally apply to emails and texts involving government business regardless of whether the messages are in a government-entity or a personal email account.

The use of personal email accounts, rather than the organization's provided email, for work purposes bypasses the organization's efforts to maintain electronic data security, as well as makes it more difficult to remain in compliance with the MGDPA.

Organizations should consider policies that require staff and elected officials to use the organization's email for work-related purposes. *See Chapter 2: Data Privacy Laws and Chapter 3: Data Management*

The decision of whether board members/elected officials must use government email or can use personal or outside employer email accounts for official government business is ultimately a policy decision

DATA MANAGEMENT COMPLIANCE

The Minnesota Official Records Act mandates that officers and agencies at all levels of government make and preserve all records necessary to a full and accurate knowledge of their activities. It is the content of the record that makes it an official record, not the medium.

Public entities must have and follow a records retention schedule (Minn. § 138.17, subd. 7). This schedule dictates how long the entity must retain official records.

This also means that once the retention period has expired, the public entity no longer must maintain the data and can destroy it.

Information, documents and data that are not official records should be kept only as long as there is a business need for them. Destroying extraneous documents and data as soon as possible is key from a data security standpoint.

See Chapter 3: Data Management

for the governing body. MCIT recommends discussing the topic thoroughly with legal counsel.

Data Retention and Retrieval

When a valid request for government data is made, the government entity has an obligation to provide access to that data, regardless of whether it is stored on the entity's computer system or its employee's/official's personal email account. Failure to provide access to government data when legally required could be a violation of the Data Practices Act.

Likewise, any litigation holds or litigation discovery requests would apply to emails involving a certain matter regardless if it is stored on a personal or government computer/email/system.

Under the Official Records Act and the Records Management Statute, a government entity can only destroy official records pursuant to the timelines found in the entity's approved records retention schedule.

Under these Acts, **an employee or official using a private email account has an obligation to retain and transfer any messages and attachments that are official records to the government entity for storage and retention**.

Data retention and retrieval can be more challenging when government and personal data are commingled in one email account. This can make it more difficult for the government entity to:

- Respond to a Data Practices Act or litigation related discovery request
- Secure data for records retention or a litigation hold

It can also be more inconvenient and cumbersome for the owner(s) of the account.

Data Privacy and Security

Officials/employees using personal email accounts should be aware and take affirmative action to ensure the privacy and security of the government data, particularly if receiving private data (such as personnel data) or attorney-client privileged communications. This may include confirming that the email service provider has appropriate safeguards in place to avert security breaches.

Individuals should also ensure no one else has access to their email accounts. Sharing an email account with a spouse or another individual may raise questions about whether that individual can access data that he or she has no legal right to view or whether attorney-client privilege has been waived.

As a best practice, **all accounts should have strong passwords and follow the government entity's policies and practices for data security.**

Outside Employer's Email

A board member using an outside employer's email account for government business may be similarly problematic. Many employers have policies or work under the presumption that all data housed in their accounts or servers can be viewed or accessed by management. **There could be a violation of the MGDPA if the outside employer views private government data**, even if it is on the employer's email server.

Board members who use their outside employer's email address for government business should be prepared to **instruct their employer to suspend routine business operations, such as automatic email deletion**, or to provide access to the employer's email account

if there is a government entity litigation hold or records request.

If an outside employer would be unwilling to do this, the board member should strongly consider using a government entity email account for government business.

If a personal or outside employer's email account is hacked or otherwise viewed by someone who should not have access to the government data, **the board member or official should immediately notify the government entity's administrative staff, legal counsel and IT department**. The government entity may need to investigate and take appropriate measures if a violation of the Data Practices Act or a data breach has occurred.

TECHNICAL TOOLS HELP SECURE EMAIL

A number of technical solutions can be used in combination to help improve the security of email. These generally filter messages coming in for those that contain known or potential threats or are spam, among others. The filters prevent the message from delivering to the recipient's inbox.

A sandbox could also be used to test email attachments or links for malicious code before delivering the message to an inbox.

If risky emails never reach an employee's inbox, then the individual cannot succumb to the social engineering attack.

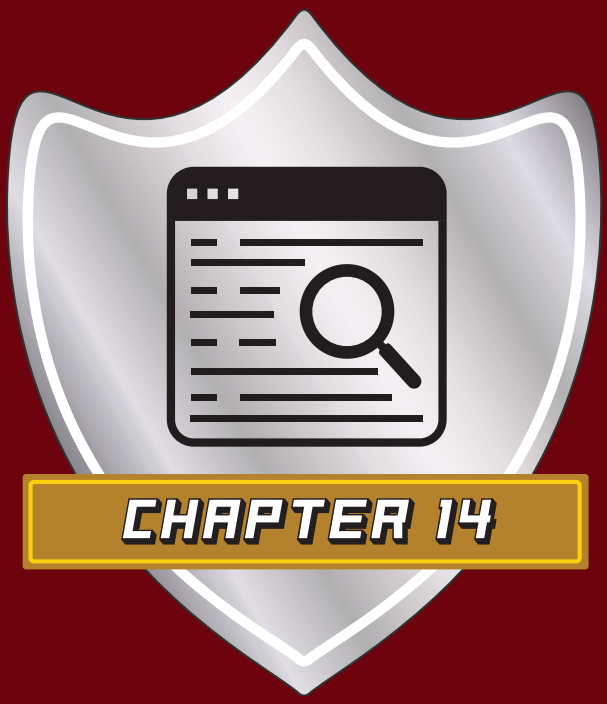
RESOURCES

EMAIL SECURITY AWARENESS DIGITAL IMAGES, PRODUCED BY MINNESOTA COUNTIES INTERGOVERNMENTAL TRUST (*MCIT.ORG*): Series of digital images that highlight four keys to building awareness among employees about common email security concerns, including phishing and business email compromise. Images can be used in a variety of places and provide easy tips for employees to use to help keep the organization's systems and data secure.

QUICK TAKES ON DATA SECURITY PRODUCED BY MINNESOTA COUNTIES INTERGOVERNMENTAL TRUST (*MCIT.ORG*): Ready-to-use mini training scripts and employee handouts provide succinct information about specific data security threats and steps employees can take to keep information secure.

SECURE EMAIL PRACTICES CHECKUP

Does the organization have a policy requiring the use of the organization's email system for work purposes? ☐ **YES** ☐ **NO**	**ACTION ITEMS**
When emailing sensitive information, are individuals required to use encrypted email? ☐ **YES** ☐ **NO**	
Are relevant employees trained about when to send encrypted emails? ☐ **YES** ☐ **NO**	
Are relevant employees trained about the methods and importance of sending and receiving encrypted email and retrained as necessary? ☐ **YES** ☐ **NO**	
Are employees instructed and trained to move sensitive data from email to a secure storage location? ☐ **YES** ☐ **NO**	
Are employees instructed and trained to purge their email account of unnecessary messages and duplicates in a timely manner? ☐ **YES** ☐ **NO**	



Safe Internet Browsing

The internet provides access to content from around the world, but it also offers avenues for malware *(see Chapter 6: Malware and Ransomware)* to enter and compromise systems.

The two primary ways that malware enters a system is through social engineering *(see Chapter 12: Social Engineering)* and unsafe browsing. Browsing is how people use and interact with the internet.

Although filters and controls may block the majority of browsing threats, staff should be educated to identify and avoid suspicious links and websites, and to use secure websites when entering sensitive data. The organization should also have ways to inform the IT department and other staff about any suspicious links or websites.

RECOGNIZING AND AVOIDING SUSPICIOUS LINKS, WEBSITES

Avoiding malicious online content requires that users recognize suspicious links and websites. Part of that involves understanding the sources and formats links and websites can take.

Most suspicious links arrive via email; others commonly arrive disguised as advertisements in pop-up web pages or clickbait. Pop-ups open a new browser window and interrupt browsing.

Pop-ups are regularly used for advertising but could contain links that download malware or direct the user to malware-infested websites.

Clickbait is outrageous or sensational headlines or photos that entice users to click on them.

Generative artificial intelligence (AI) can create deep fake content that looks real with a passing glance, making it even more en-

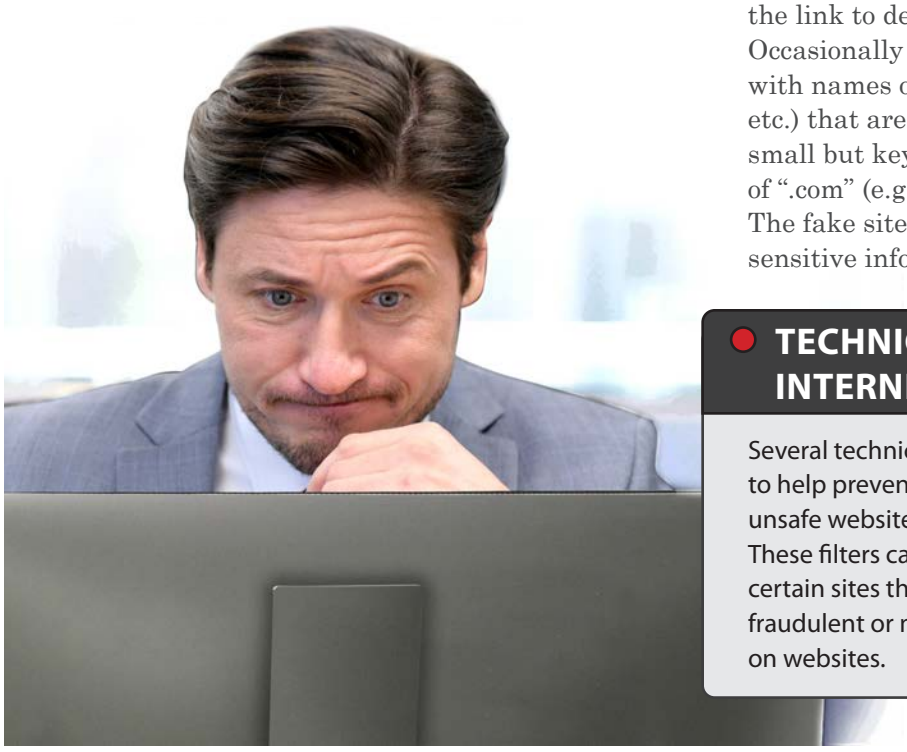
ticing but harder to determine if a link is potentially harmful (see below section for more).

Links can come in multiple formats. Not all links are blue underlined web addresses (e.g.," www.MCIT.org"). They can be:

- Text or web address without the blue underline (e.g., "Click here").
- Hidden in images, such as a picture of a close button, which can be especially difficult to spot when an advertisement or other item flashes across the screen (e.g., ).

Tips to Recognize, Avoid Suspicious Links, Websites, Content

- **Maintain a healthy skepticism.** Outrageous claims or anything that sounds too good or too bad to be true are common signs of clickbait. Do not click on these links or attachments.
- **Give images and video a second glance to look for signs they are AI created**:
  - Look at faces carefully: Is the skin on cheeks and forehead abnormally smooth or wrinkly, or does it not match the age of the hair and eyes?
  - Do the shadows appear where expected, especially around the eyes and eyebrows?
  - Does the speaker blink too much or too little?
  - Is there a mismatch in the size or color of the lips or teeth with the rest of the face?
  - If the person wears glasses, is there too much or not enough of a glare or the glare does not change when the person moves?
  - Are the speech patterns unusual or unnatural?
  - Does the language seem off somehow: generic, repetitive or scripted?
  - Is there a lack of emotion in the voice or is the emotion inappropriate for the conversation?
- **Avoid clickbait, pop-ups and advertisements.** As this is a common delivery route to either install malware or to direct the user to unsafe websites, the best plan is to avoid clicking on these entirely. Employees can block popups in their browser settings.
- **Look for poor spelling or grammar.** Commonly malware comes from other countries with creators who may have poor English skills. Encountering websites claiming to be from American government organizations or businesses with poor spelling and grammar should be treated with suspicion. Note: *Artificial intelligence is making it easier for non-English speakers to perfect their English usage.*
- **Review links**: Hovering a mouse over a link can reveal the link address either next to the cursor or along the bottom of the screen. Review the link to determine if it seems legitimate. Occasionally links may direct users to sites with names or domains (".com," ".net," ".org," etc.) that are similar to trusted sites but with a small but key variation, such as ".net" instead of ".com" (e.g., "Google.com" vs. "Google.org"). The fake sites then install malware or capture sensitive information.



TECHNICAL TOOLS SECURE INTERNET BROWSING

Several technical tools can be used together to help prevent employees from encountering unsafe websites while in the scope of their work. These filters can prevent employees from visiting certain sites that are known or suspected to be fraudulent or malicious, and block popups or ads on websites.

SECURE WEBSITES

When entering private, valuable or sensitive information through an online form, such as for purchasing items, registering for events or providing sensitive data to a partner organization, **websites should be secure**.

A secure website encrypts and verifies information sent between the browser and the organization that owns the website.

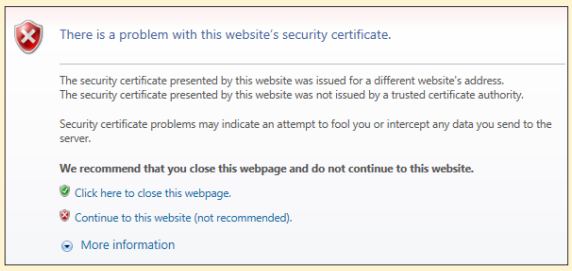
Organizations should have a computer use policy that **restricts employees from entering sensitive data on unsecured sites**.

To determine whether websites are secure, the user should:

- **Look for the presence of a padlock icon and an "https:" prefix** to the web address, as these show that the site is encrypted, and the encryption is current and functioning.
  - Every internet browser (the program used to access the internet, (e.g., Edge, Chrome, Safari, Firefox)) is different, and the padlock may be displayed in different locations.
  - If a site's prefix is "http:," it is not secure (note the prefix does not have an "s" at the end).

Employees should follow their organization's policy if they come across an unsecured site. They should be wary while browsing on unsecured sites and not enter any private or sensitive information.

- **Stop and consult with IT before proceeding to a site** when the user encounters a **warning that there is a problem with the site's security certificate** (see image for an example).



When users encounter a message such as the one above while navigating to a website, they should consult with IT before proceeding to the site.

RESOURCES

"UNDERSTANDING WEB SITE CERTIFICATES (" PRODUCED BY CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY: General resource intended for end users that summarize the importance, evaluation and identification of website certificates.

"TIPS TO STAY SAFE WHILE SURFING THE WEB, PARTS 1 AND 2" CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY: List of tips to help individuals identify and protect themselves from online threats, including resources for safe browsing. Intended for the end user.

QUICK TAKES ON DATA SECURITY PRODUCED BY MINNESOTA COUNTIES INTERGOVERNMENTAL TRUST (*MCIT.ORG*): Ready-to-use mini training scripts and employee handouts provide succinct information about specific data security threats and steps employees can take to keep information secure.

SAFE INTERNET BROWSING CHECKUP

Are employees trained about safe internet browsing and using secure websites per the organization's policy or best practices? ☐ YES ☐ NO	**ACTION ITEMS**
Is a plan in place to inform IT and others of any suspicious links or websites encountered during work? ☐ YES ☐ NO	
Are employees trained about the plan to report suspicious links or websites to IT and others? ☐ YES ☐ NO	

Training Employees and Officials

Despite sophisticated cybersecurity systems of firewalls, anti-malware software, sandboxes, security patches and the like, data compromises and breaches still happen.

One study indicates that unintentional or inadvertent user action is responsible for nearly 93 percent of data compromise incidents.* A survey of IT security professionals indicates that 84 percent of cyberattacks on their organizations was due in part to human error.** Therefore, a strong defense against data- and cyberthreats must include well-trained employees and officials.

FOSTER A CULTURE OF SECURITY

It is important for an organization to create an environment where **employees are encouraged to report suspected data compromises and cyberattacks as soon as possible**. It is to the organization's benefit to have problems identified immediately to minimize their effects on the system.

Employees may feel a sense of guilt, shame or fear that their jobs may be in jeopardy if they report data- or cybersecurity incidents due to their actions. As a result, these incidents may go unreported and relatively minor problems could grow to become serious or even catastrophic.

As threat actors become more sophisticated, it is likely that more individuals may fall for a data compromise or cybersecurity attack. Even the most vigilant person could be tricked, especially by AI-generated content from threat actors.

Creating a workplace culture where honest mistakes are understood to happen and are forgiven can go a long way in encouraging early reporting.

Keep in mind, though, that the employer may need to take disciplinary action against employees who violate computer use policies or who continually or willfully fall for data security or cyberattacks.

DEVELOP A TRAINING PLAN

Human resources professionals and other managers should create a plan that prepares staff and officials to understand data security threats and the actions they should take to prevent data compromises.

Human resources and management may want to partner with the IT staff to develop training content.

The training plan should consider these elements:

- **A regular review of policies and procedures**, including how to report suspected data compromises and cyberthreats.
  - When policies or procedures are changed, staff should be trained about the updates.
- **Remind employees about common data compromise and cyberattack threats**, and how they can help avoid them.
  - Making this an ongoing effort (e.g., monthly) is a particularly effective way to keep the issue front of mind for staff.
- Periodically **update employees about new threats**.
  - Share new phishing or social engineering scams that are circulating, for example.
- **Review data privacy laws** and compliance requirements.
  - Departments should consider making this discussion specific to the types of data they collect, create, maintain and disseminate to ensure that staff understand how the laws relate to their work.
- **Check for employee understanding**.
  - The employer can use a number of different approaches for this, including sending fake phishing emails, spot-the-problem quizzes, discussion questions at staff meetings, etc.
  - The checks can be developed in-house, or the organization could hire a service for them.
  - The employer should follow up with employees who do not demonstrate understanding and review data security threats and prevention methods with them.
  - Checks also identify whether the training is effective and areas that need to be improved.

EDUCATION RESOURCES

Quick Takes on Data Security

MCIT has developed Quick Takes on Data Security, a series of **mini training scripts and employee handouts that focus on targeted data compromise and cybersecurity issues**.

- Each discusses the threat and provides steps employees can take to combat it.
- Employee handouts are visually engaging to encourage staff to keep and post at their workstations.
- Quick Takes are written so that team leaders can modify the content to meet the particular circumstances of the group and align with the organization's policies and procedures.

Members can download Quick Take scripts and handouts from the Resource Library at *MCIT.org* at no charge.

Email Security Awareness

MCIT provides members with **digital images that address key steps that employees can take** to improve the organization's overall data security via email:

- Use strong, unique passwords and keep them secret.
- Identify phishing scams.
- Keep a clean email account.
- Be suspicious of requests in email, especially unsolicited ones.

Digital images can be used in a variety of ways, making these a flexible employee education tool.

Members can download email security digital images from the Resource Library at *MCIT.org* at no charge.

Coverage Information

Understanding how MCIT coverage applies to various situations can help an organization better manage its data security risks. MCIT offers a number of ways to learn about its coverage in the Resource Library at *MCIT.org*.

- **MCIT coverage videos:** Short videos explain coverage for data compromises and cyberattacks provided through MCIT to its members.
  - Videos address definitions related to cyber coverage, types of coverage and limits, conditions of coverage and coverage exclusions.
- **Coverage Summary:** A booklet that condenses details about coverage into plain language.

MORE NO-COST RESOURCES

Several credible organizations offer materials and tools that members can use in their employee training and awareness efforts around data security. The below is a short list, but others may be useful for members as well.

StopThinkConnect.org

Provides a number of free resources to help build cybersecurity awareness, including tip sheets, posters, videos, memes and graphics. The campaign was created by a coalition of private companies, nonprofits and government organizations.

CISA.gov

Website for the federal Cybersecurity and Infrastructure Security Agency. Its mission is to help organizations prepare for, respond to and mitigate the impact of cyberattacks.

FTC.gov

Website for the Federal Trade Commission, which provides small business resources around cybersecurity, many apply to local government operations as well.

The MCIT Coverage Document, which is mailed to members each December, **is the governing document for specific situations**.

Data Practices Training

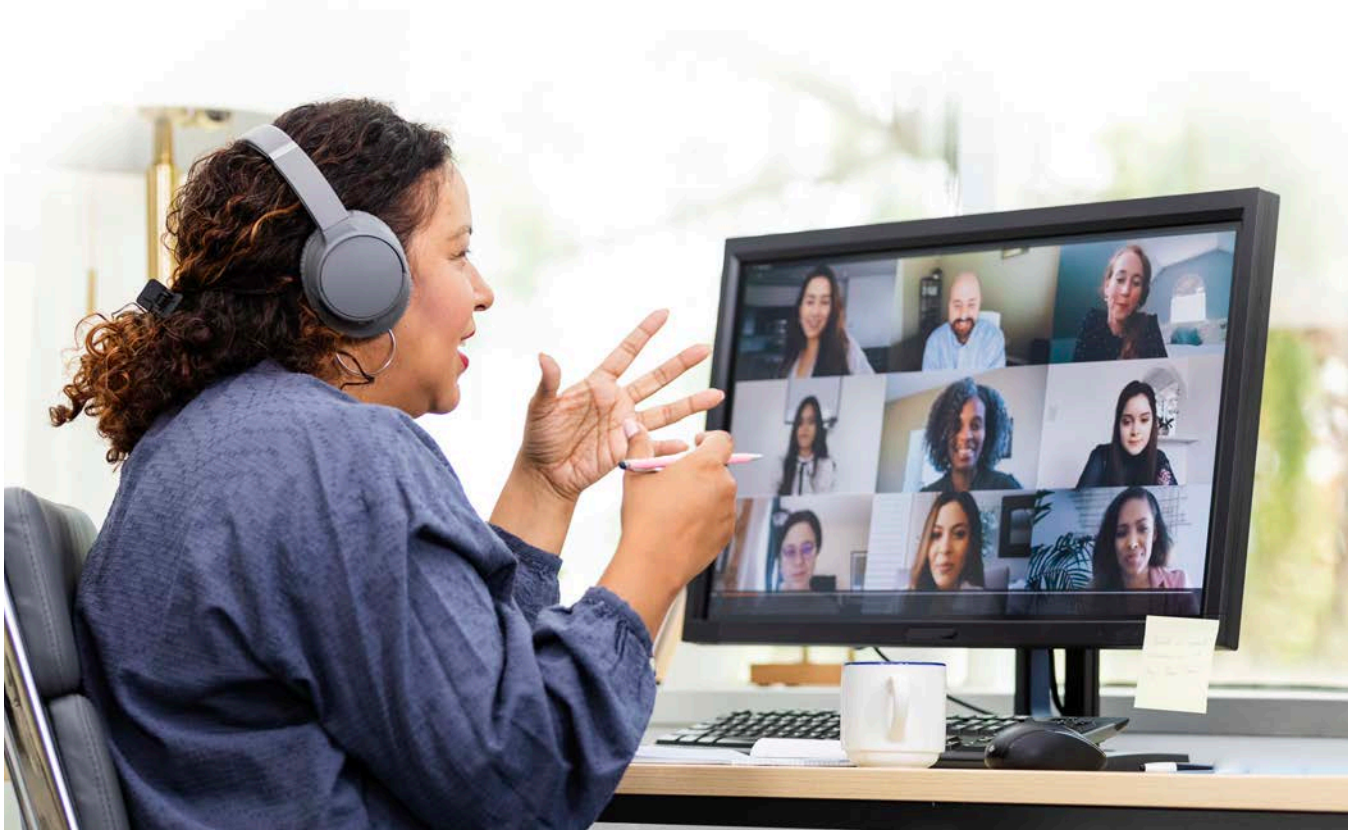
- **MCIT offers its members virtual or on-site training** for staff and officials related to the Minnesota Government Data Practices Act, as well as provides articles about the law. Members can learn more about training at *MCIT.org/services-programs* and access articles at *MCIT.org/resources*.
- The **Minnesota Department of Administration Data Practices Office provides a number of resources** to help educate staff and officials about the MGDPA, including handouts, presentations and videos, among other information. These are freely available at *MN.gov/admin/data-practices/resources/*.

Data Management Training

MCIT offers the training session "Manage Data to Manage Cyber Threats." The session acknowledges that public entities have an enormous volume of information that they collect to carryout their operations, but this means that their data security threat landscape is just as large. The session:

- Explains how reducing the amount of records maintained can help reduce the potential adverse consequences from a data security incident.
- Provides an overview of laws related to public entity data retention and management.
- Offers best practices for reducing an organization's retained data and how to ensure that those records are secure.

The training program can be delivered on site or virtually to MCIT member organizations as part of membership. Members can learn more about training at *MCIT.org/services-programs*.



eRiskHub.com

eRiskHub.com provides a wealth of data security tools and resources, including those to assist in training employees. MCIT offers its members access to this restricted site as part of MCIT membership.

- Individuals must **set up a site log in using the MCIT access code.** The code is provided to the MCIT primary contact. Members should **contact MCIT** (*info@mcit.org* or **866.547.6516**) **to request the code** if needed.

Fee-based Services

Some training vendors provide data- and cybersecurity employee awareness and education services. For varying fees, common services are:

- Simulated phishing and other social engineering attacks to assess percentage of users prone to these scams.
- Security awareness training content, which may include posters, videos, games, newsletters or interactive sessions.

If the training vendor has access to the organization's network or computers, security issues should be addressed in the contract. *See Chapter 4: Vendor Contracts*

*Source: "Data Indicates Human Error Prevailing Cause of Breaches, Incidents," The Privacy Advisor, International Association of Privacy Professionals Inc., Aug. 28, 2018.

**Source: "Security Professionals Name Top Causes of Breaches," Computer Weekly, Aug. 25, 2017, covering a survey of Black Hat security conference attendees.

NATIONAL CYBERSECURITY AWARENESS MONTH

Annually, October is National Cybersecurity Awareness Month. It is an opportunity for organization's to refocus on their cybersecurity risk management, including educating staff about the vital role they play in data security.

The National Cybersecurity Alliance (*StaySafe Online.org*) is the sponsor of the annual observance and offers employers ideas and no-cost materials to build their security awareness efforts.

TRAINING EMPLOYEES AND OFFICIALS CHECKUP

Are policies and procedures related to data security reviewed with employees and officials regularly and when changes are made? ☐ **YES** ☐ **NO**	**ACTION ITEMS**
Are employees and officials alerted to new data- and cybersecurity threats? ☐ **YES** ☐ **NO**	
Are data privacy laws and compliance reviewed with employees regularly? ☐ **YES** ☐ **NO**	
Are employees and officials trained to recognize social engineering attacks? ☐ **YES** ☐ **NO**	
Does the organization check for employee understanding of data- and cybersecurity threats, how to recognize them and how to report them? ☐ **YES** ☐ **NO**	

GLOSSARY

A

ACTIVE DIRECTORY: A centralized database and control system for managing users, computers and newtorks resources on a Windows-based network

ANTI-MALWARE (ANTI-VIRUS) SOFTWARE: A type of software program designed to prevent, detect and remove malicious software (malware) on IT systems or individual computing devices.

C

CLICKBAIT: A piece of web content with the main purpose of enticing users to click on a link to go to a certain web page. Clickbait often uses exaggerated or sensational headlines or pictures and is regularly paid for by advertisers. Social engineering attacks may use clickbait for installing malware.

CLOUD STORAGE: Data is stored on remote servers accessed through the internet. Cloud storage is available in two forms: private and public.

CRYPTOCURRENCY: A digital currency built with cryptographic protocols to make transactions secure and difficult to fake. Cryptocurrencies are typically not controlled by any central bank.

D

DATA BACKUP: A copy of files and programs made to facilitate recovery if necessary.

DATA LOSS PREVENTION: A tool used to screen information for potentially sensitive data to prevent data leaks. The term can also be used to help a network administrator control what data end users can release. It exists in different forms and can be included in email or various networks.

DENIAL OF SERVICE ATTACK: An intentional attack against the entity's computer system designed to overwhelm the capacity of the computer systems in order to deny or impede authorized users from gaining access to the system through the internet.

DISCOVERY REQUEST: A process that permits a party in a lawsuit to demand another party to produce or permit inspection of documents or tangible items in its possession, custody or control.

E

ENCRYPTION: Altering data to make it unusable to unauthorized users.

F

FIREWALL: Network security system that monitors and controls access to the system by blocking unauthorized web users or illicit software from gaining access to the network. It is the first line of defense in securing sensitive data. Firewalls are often understood to be about internet connectivity, but they also may apply in other network environments. Firewalls may restrict connectivity to and from internal networks used to service more sensitive functions, such as accounting or personnel data. Firewalls can prevent unauthorized access to systems and resources.

FLASH DRIVE: Also known as a jump drive or thumb drive, a small data storage device that plugs into a computer, printer or other device.

G

GOVERNMENT DATA: All data a government entity collects, creates, receives, maintains, disseminates that is recorded in some type of format.

GOVERNMENT RECORDS: State and local records, including all cards; correspondence; discs; maps; memoranda; microfilms; papers; photographs; recordings; reports; tapes; writings; optical disks; and other data, information or documentary material, regardless of physical form or characteristics, storage media or conditions of use, made or received by an officer or agency of the state and an officer or agency of a county, city, town, school district, municipal subdivision or corporation or other public authority or political entity within the state pursuant to state law or in connection with the transaction of public business by an officer or agency.

GOVERNMENT RECORDS EXCLUSIONS: Data and information that does not become part of an official transaction, library and museum material made or acquired and kept solely for reference or exhibit purposes, extra copies of documents kept only for convenience of reference and stock of publications and processed documents, and bonds, coupons or other obligations or evidences of indebtedness, the destruction or other disposition of which is governed by other laws.

H

HACKER (ALSO THREAT ACTOR): Person who attempts to gain unauthorized access to information (often to an electronic information system).

HACKTIVISM: A type of hacking where the motivation is political, religious or ideological, rather than criminal. For example, hacktivism goals may be to circumvent government censorship, take down government websites that pose a danger to politically active citizens, support citizen uprisings, disrupt corporate or government power, among other aims. Hacktivist methods include denial of service attacks, data theft, website defacement, deploying computer viruses and worms that spread protest messages, taking over social media accounts and stealing and disclosing sensitive data.

HEALTHCARE INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA): A U.S. law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers.

I

INDEMNIFY: To compensate for damages suffered.

INSTALLATION MANAGEMENT: software and hardware that includes processes and policies for installing, updating and removing software and hardware on an IT system and networks to ensure they remain secure, stable and compliant

L

LITIGATION HOLD: A written notice to employees, officials and other individuals instructing them to retain and not destroy any documents, data and other information related to an issue that likely will be involved in a lawsuit.

M

MALICIOUS CODE/MALWARE: A software program inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity or availability of the victim's data, applications or operating system, or of otherwise annoying or disrupting the victim. Viruses and ransomware are types of malicious code.

MINNESOTA GOVERNMENT DATA PRACTICES ACT (MGDPA): Minnesota statutes defining the responsibilities of government entities with regard to classification, security and dissemination of government data.

MINNESOTA RECORDS MANAGEMENT STATUTE: Provides that it is the duty of the governing body of each county, municipality and other subdivisions of government to establish and maintain an active continuing program for the economical and efficient management of the organization's records.

MULTIFACTOR AUTHENTICATION: A security enhancement that requires a user to present at least two pieces of evidence, or credentials, when logging in to an account, secure area or secure device.

N

NONPUBLIC DATA: Government data about businesses/organizations/inanimate objects that are available to the businesses/organizations but not to the public.

NOT PUBLIC DATA: Any government data classified by statute, federal law or temporary classification as confidential, private, nonpublic or protected nonpublic.

O

OFFICIAL RECORD: Item that documents a government entity's "official activities." An official record describes an entity's official functions, business activities and transactions.

OFFICIAL RECORDS ACT: Mandates that officers and agencies at all levels of government make and preserve all records necessary to a full and accurate knowledge of their activities.

P

PASSWORD/PASSPHRASE: A secret set of characters known only by the user to gain authorized access to devices, programs or locations. It is a secret that a person memorizes and uses to authenticate his or her identity. Passwords are typically character strings.

PATCHES/UPDATES: An update to an operating system, application or other software issued specifically to correct particular problems with the software. This is a frequent target for social engineering attacks, as many programs require regular updates.

PERSONALLY IDENTIFIABLE INFORMATION: Information that can be used to distinguish or trace an individual's identity (e.g., his or her name, Social Security number, biometric records, etc.) alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).

PHISHING: Tricking individuals into disclosing sensitive, valuable or private information through deceptive computer-based means.

POP-UPS: Web pages that open new browser windows or tabs that often interrupt browsing sessions. These are typically used for advertisements

and clickbait, and may contain links to malware or malicious websites.

PRE-ACTION SPRINKLER SYSTEM: A type of fire suppression system that requires the activation of both a smoke detector and sprinkler head to flow water. Although normal fire sprinklers are flooded with water until a fire activates a sprinkler head, a pre-action system consists of dry pipes and a smoke detection system. Activation takes place in two phases. If the smoke detector detects smoke, the pipes are flooded with water. Then the sprinkler head activates as normal. Therefore, the risk of an accidental activation is greatly diminished should a ladder or other item damage a sprinkler head.

PROTECTED HEALTH INFORMATION: Information relating to a person's past, present or future physical or mental health or condition; receipt of health care services; and past, present or future payment for the receipt of health care.

R

RANSOMWARE: A type of malware that encrypts data on the system, preventing users from accessing the information unless a fee is paid. Other forms of ransomware may prevent entire systems from working.

S

SANDBOX: An isolated environment that allows users to run programs or execute files (code) without affecting the application, system or platform on which they run. Potentially malicious software can be tested within the boundaries of the sandbox, which mimics the end-user's operating environment, without risking harm to the host device or network. This is particularly useful in detecting and combating previously unseen malware or stealthy attacks.

SECURITY INFORMATION AND EVENT MANAGEMENT (SEIM): A solution that collects, analyzes and correlates security data from across an organization's IT systems. It centralizes event information so IT can identify suspicious patterns, investigate incidents, streamline response efforts and meet compliance requirements.

SOCIAL ENGINEERING: Attacks using social skills or psychology to trick individuals into sharing sensitive, valuable or private information.

SPAM: Unsolicited bulk commercial email messages.

T

THREAT ACTOR: Person who attempts to gain unauthorized access to information (often to an electronic information system).

U

UNINTERRUPTIBLE POWER SUPPLY/BATTERY BACKUP: A piece of equipment that provides power to electronic equipment should power fail from a wall outlet. These work with on-board batteries and allow machines to shut down normally, thus preventing potential damage from unexpected shut downs. They are also effective in minimizing damage from power surges, and they allow users the opportunity to save data before losing it.

V

VIRUS: A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers or even erase everything on a hard drive.

VULNERABILITY SCANNING: automated process that uses software tools to find security weaknesses in computer systems, networks and applications before attackers can exploit them.