Cyber Preparedness and Response for Public Entities

Nontechnical Tips for Leaders

MCIT

MINNESOTA COUNTIES INTERGOVERNMENTAL TRUST

Presented by:

Paul Hajduk

MCIT Risk Management Consultant

866.547.6516 or *phajduk@mcit.org*

Coming Cyber Training Opportunities

"What You and Your Employees Can Do to Prevent a Cyber Incident" webinar

- Oct. 25, 11 a.m.
- Department heads and managers
- Register: *MCIT.org/events*

"Don't Be the Breaking News" keynote address

- Dec. 5, 8 a.m.
- AMC annual conference
- County commissioners and administrators
- Register at *MNCounties.org*

"What Leaders Need to Know to Improve Cyber-security in Their Organizations" webinar

- Dec. 13, 10 a.m.
- Follow-up to "Don't Be the Breaking News"
- Elected leaders, administrators, executive directors
- Register: *MCIT.org/events*

How Well Is Your Organization Prepared for a Cyber-attack?

- Exposures
- Coverage
- Action plans
- Resources
- Claims process

‘County Cybersecurity 101’

- Current cyber-threats to Minnesota local governments
- Strategies to manage risks
- Download at *MNCounties.org*

Cyber/Data Incident Process

- Preparation
- Response
- Recovery

Reasons to Prepare for an Incident

$1 million Minnesota nonprofit suffers hacking loss

106 local government **ransomware attacks** in 2022

Minnesota **county** has **data breach**

11 misdirected payroll check claims

Member **Facebook page taken over** by hacker

8 misdirected payment claims

Minnesota county has **ransomware** claim

7 million+ SSNs exposed in U of M data breach

MCIT Cyber Coverage

- Theft, loss or **unauthorized disclosure** of or **access** to personal information … whether such … information is … electronic, paper or another format
- Violation or **failure of computer system security**, including:
  - Unauthorized access or use
  - Denial of service attack or receipt
  - Transmission of malicious code.

MCIT Cyber Coverage

- Theft, loss or **unauthorized disclosure** of or **access** to personal information … whether such … information is … **electronic, paper or another format**
- Violation or **failure of computer system security**, including:
  - Unauthorized access or use
  - Denial of service attack or receipt
  - Transmission of malicious code.

Annual MCIT Coverage Limits

	Limit	Deductible
All MCIT	$10 million	NA
County Members	$500,000	$10,000
Noncounty Members	$250,000	$5,000

Privacy or Security Event Examples

- Laptop theft
- Misplacing a flash drive
- Others viewing unattended work files
- Sending personal information to the wrong recipient

- Phishing attacks
- Hacking
- Cyber-extortion

Incident Example: Hacked Email

- More than 5,000 phishing emails sent worldwide
- Email server placed on multiple blacklists
- Still determining if data was accessed

What Is a Breach? (Per Minn. Stat. § 13.055)

Requires notice when all of the following apply.

- A person:
  - Views or takes private or confidential data
  - Without permission or statutory authority and
  - With the intent to use the private or confidential data for nongovernmental purposes

Case Study: Phishing Incident

- Employee clicked a malicious link in an email
- This allowed the hacker access to the email history
  - What is in your email record?
- The history had volumes of personal information

Is this a breach?

MCIT Coverage for Expenses

- Response expenses
  - Forensic IT
  - Legal counsel
  - Public relations
  - Cyber-extortion ($50,000 sublimit/annual aggregate)
- Third-party expenses
  - Settlement costs
  - Defense costs
  - Regulatory proceedings and penalties
  - Payment card industry data security standards (PCI-DSS) assessments

Misdirected Payment Fraud and Computer Fraud

	Limit
County Members	$25,000
Noncounty Members	$10,000

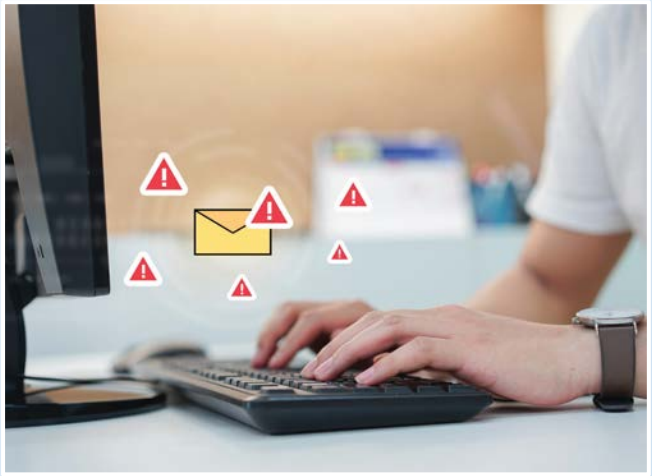
- Criminal deception
- Criminal manipulation

MCIT Coverage Review Videos

- Cyber Coverage Definitions
- Types of Cyber Coverage and Limits
- Cyber Coverage Conditions
- Cyber Coverage Exclusions
- Misdirected Payment Fraud and Computer Fraud

Case Study: Phishing Incident

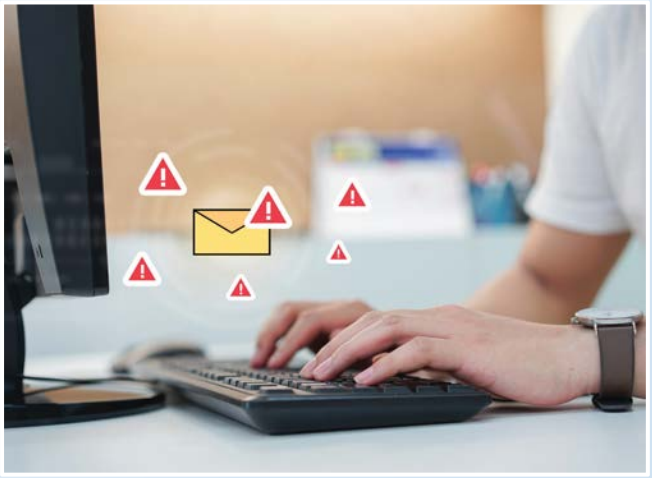
- Hacker gained access to all entity email addresses
- Hacker phished all of them



Case Study: Phishing Incident

- Hacker gained access to all entity email addresses
- Hacker phished all of them

This is a breach.



Your Entity's Incident Response Plan

- Responsibilities
- Claim reporting
- Investigation
- Business continuity
- Threat removal
- Recovery

Response Plan: Responsibilities

- Responsibilities
  - What has to be done (submit the claim)
  - Who is assigned the tasks
  - Internal/external partners
- Identify primary, secondary, team roles
- Tailor to type of incident
- Document and train
- Review and practice

Best practices:

- Response leader/ coordinator
  - Outside of network contact information

Case Study: Phishing Incident

- Who discovers the hack?
  - Hacker sent phishing emails from the employee's account
  - How is it reported to you?
    - Internal and external email recipients let you know
  - How does the incident response leader get notified?

Incident Example: Unusual Employee Email Sign-in

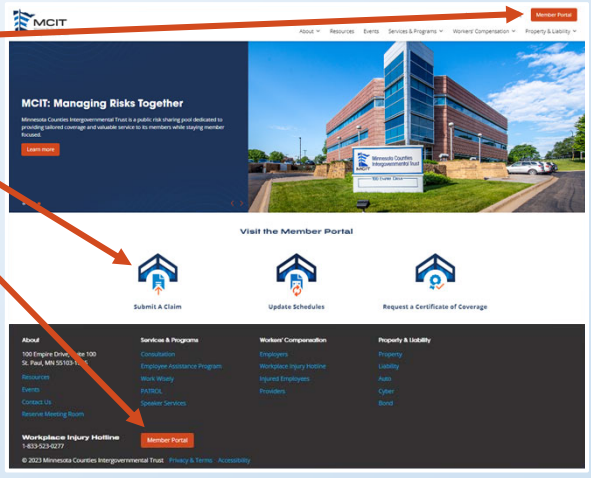
- Originated in Texas, but employee had not been to Texas
- Employee had clicked on email and entered credentials, including multifactor authentication
- System alert flagged incident
  - Employee did not initially report it
  - Personal health information may have been accessed

Best practice: Encourage employee reporting of potential issues

Response Plan: Notify MCIT

- Notify MCIT immediately
  - Primary
  - Backup
- Activates response resources
  - Breach counsel
- Preserves coverage

Best practice: Use outside system for reporting



Response Plan: Investigation & Threat Removal

- Investigation
  - Forensic IT
  - Law enforcement
- Threat removal
  - Ransomware
  - Malware
  - Hacker access/ credentials

Best practice: Have law enforcement (e.g., sheriff, FBI) contact information before an incident

Case Study: Phishing Incident

- Forensic investigation
  - Employee email had volumes of personal information
  - Years of data
  - No policy on retaining data (duration, location)
    - Data destruction
  - No procedure for securing data

Response Plan: Business Continuity & Recovery

- Business continuity
  - Activate the plan
- Recovery
  - Your system or hosted?
  - Host for others?
  - Backups/redundancies
    - Verify in advance
  - Restore systems
  - Modify procedures

Best practice: Restore after investigation is complete

Case Study: Phishing Incident

- 100s of notifications
- Credit monitoring
- Public relations coaching
- Recovery
- Modify procedures
  - Personal information: Not retained in email

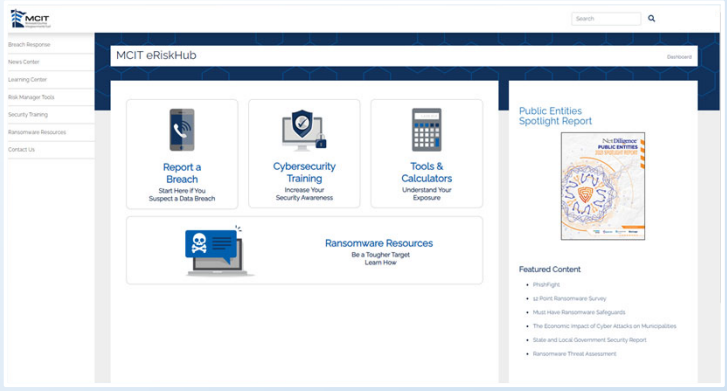
Incident Example

- Joe Smith Construction had a contract
- Hacker created fake invoice to change Joe's bank
- $300,000+ was transferred to a fraudulent account
- No one asked Joe

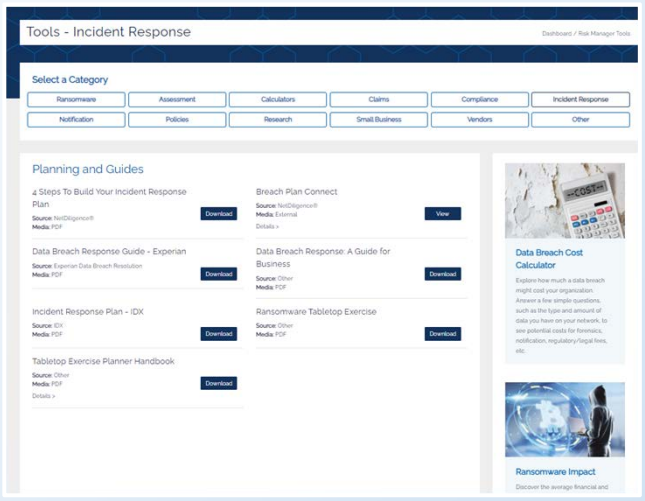
Best Practice: Double check using normal channels

eRiskHub

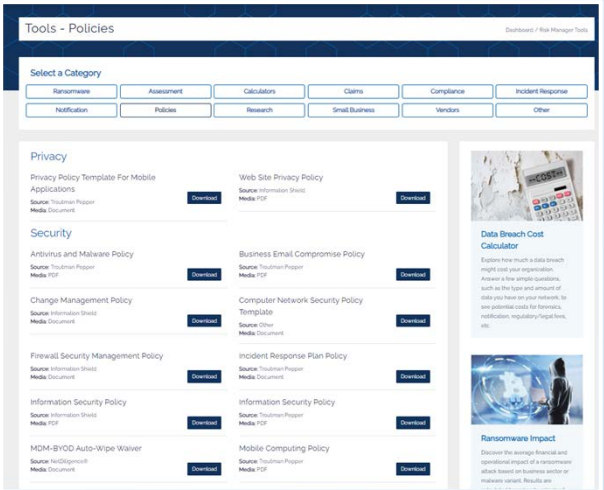
- *eRiskHub.com/MCIT/*
- Request access code at *info@mcit.org*



Incident Response Resources

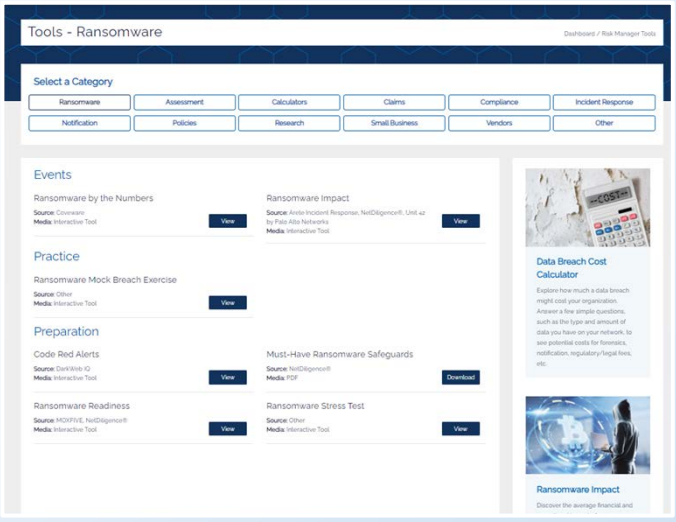


Sample Policies



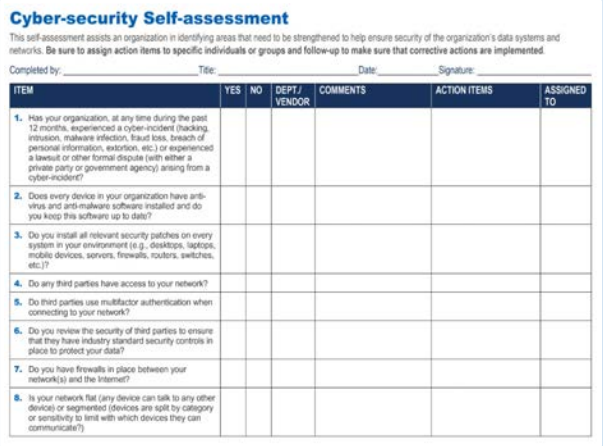
Training Tools

Ransomware



Cyber-security Self-assessment

- 32 detailed questions
- Best practices for data security
- Download at *MCIT.org/resources/*



Cyber-security Self-assessment

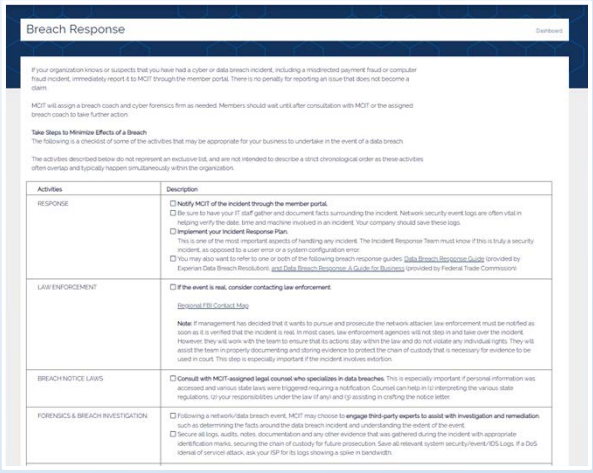
This self-assessment assists an organization in identifying areas that need to be strengthened to help ensure security of the organization's data systems and networks. **Be sure to assign action items to specific individuals or groups and follow-up to make sure that corrective actions are implemented.**

Completed by: _____ Title: _____ Date: _____ Signature: _____

ITEM	YES	NO	DEPT./ VENDOR	COMMENTS	ACTION ITEMS	ASSIGNED TO
1. Has your organization, at any time during the past 12 months, experienced a cyber-incident (hacking, intrusion, malware infection, fraud loss, breach of personal information, extortion, etc.) or experienced a lawsuit or other formal dispute (with either a private party or government agency) arising from a cyber-incident?						
2. Does every device in your organization have anti-virus and anti-malware software installed and do you keep this software up to date?						
3. Do you install all relevant security patches on every system in your environment (e.g., desktops, laptops, mobile devices, servers, firewalls, routers, switches, etc.)?						
4. Do any third parties have access to your network?						
5. Do third parties use multifactor authentication when connecting to your network?						
6. Do you review the security of third parties to ensure that they have industry standard security controls in place to protect your data?						
7. Do you have firewalls in place between your network(s) and the Internet?						
8. Is your network flat (any device can talk to any other device) or segmented (devices are split by category or sensitivity to limit with which devices they can communicate?)						

Cyber Claims Process

- Report to MCIT via the member portal (*MCIT.org*)
  - Breach counsel
  - Forensic IT analysis
  - Notification consultation
- Involve law enforcement
- Plan to participate and cooperate



Breach Response

Dashboard

If your organization knows or suspects that you have had a cyber or data breach incident, including a misdirected payment fraud or computer fraud incident, immediately report it to MCIT through the member portal. There is no penalty for reporting an issue that does not become a claim.

MCIT will assign a breach coach and cyber forensics firm as needed. Members should wait until after consultation with MCIT or the assigned breach coach to take further action.

Take Steps to Minimize Effects of a Breach

The following is a checklist of some of the activities that may be appropriate for your business to undertake in the event of a data breach.

The activities described below do not represent an exclusive list, and are not intended to describe a strict chronological order as these activities often overlap and typically happen simultaneously within the organization.

Activities	Description
RESPONSE	☐ **Notify MCIT of the incident through the member portal.** ☐ Be sure to have your IT staff 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. Your company should save these logs. ☐ **Implement your Incident Response Plan.** This is one of the most important aspects of handling any incident. The Incident Response Team must know if this is truly a security incident, as opposed to a user error or a system configuration error. ☐ You may also want to refer to one or both of the following breach response guides: Data Breach Response Guide (provided by Experian Data Breach Resolution) and Data Breach Response: A Guide for Business (provided by Federal Trade Commission)
LAW ENFORCEMENT	☐ **If the event is real, consider contacting law enforcement.** Regional FBI Contact Map **Note:** If management has decided 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 any individual rights. They will assist the team in properly documenting and storing evidence to protect the chain of custody that is necessary for evidence to be used in court. This step is especially important if the incident involves extortion.
BREACH NOTICE LAWS	☐ **Consult with MCIT-assigned legal counsel who specializes in data breaches.** This is especially important if personal information was accessed and various state laws were triggered requiring a notification. Counsel can help in (i) interpreting the various state regulations, (2) your responsibilities under the law (if any) and (3) assisting in crafting the notice letter.
FORENSICS & BREACH INVESTIGATION	☐ Following a network/data breach event, MCIT may choose to **engage third-party experts to assist with investigation and remediation**, such as determining the facts around the data breach incident and understanding the extent of the event. ☐ Secure all logs, audits, notes, documentation and any other evidence that was gathered during the incident with appropriate identification marks, securing the chain of custody for future prosecution. Save all relevant system security/event/IDS Logs. If a DoS (denial of service) attack, ask your ISP for its logs showing a spike in bandwidth.

Cyber Claims

- Clicking on a phishing attempt
- Sending information in error
- Losing a flash drive

Best practice: Encourage reporting

  - The sooner you know

Cyber Claims Process Expectations

- This is not an auto claim
- It takes significant time
  - Administrator/coordinator
  - IT director
  - Internal legal counsel
  - Department head(s)

Claim Process Roles, Responsibilities

MCIT and Partners

- Breach counsel
- Forensic IT
- Notifications
- Public relations coaching and expenses
- Negotiator/investigator

Member Organization

- Document
- Cooperate
- Participate
- Collaborate
- Recover
- Modify procedures

Best Practices

- Preparation
  - Incident response plan
    - Backups, coordinator contact outside the system
  - Business continuity plan
  - Practice, modify plans
  - Budget dollars
- Data security policy
  - Data destruction procedure followed
  - Confirm requests (e.g., financial changes) through verified contact
- Employee responsibilities
  - Empower employee reporting
- Resources
  - MCIT specific
  - eRiskHub
  - Cybersecurity and Infrastructure Security Agency (CISA)
- Claims commitment
  - Cooperation/collaboration
  - Time

Discussion

ASK QUESTIONS, SHARE EXPERIENCES

Coming Cyber Training Opportunities

"What You and Your Employees Can Do to Prevent a Cyber Incident" webinar

- Oct. 25, 11 a.m.
- Department heads and managers
- Register: *MCIT.org/events*

"Don't Be the Breaking News" keynote address

- Dec. 5, 8 a.m.
- AMC annual conference
- County commissioners and administrators
- Register at *MNCounties.org*

"What Leaders Need to Know to Improve Cyber-security in Their Organizations" webinar

- Dec. 13, 10 a.m.
- Follow-up to "Don't Be the Breaking News"
- Elected leaders, administrators, executive directors
- Register: *MCIT.org/events*