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

Nontechnical Tools and Strategies for Data Security

MCIT

MINNESOTA COUNTIES INTERGOVERNMENTAL TRUST

Presented by:

Nick Lindberg

MCIT Loss Control Consultant

866.547.6516 or *nlindberg@mcit.org*

Data and Cyber-security

- What is data and cyber-security?
- Common incidents
- Methods to prevent incidents
- Resources
- Action Items

3

What is Data and Cyber-security?

4

What Are Data and Cyber-incidents?

- Sending personal information to the wrong recipient
- Others viewing unattended work files
- Phishing attacks
- Hacking
- Mobile device, file theft
- Misplacing equipment containing private data

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

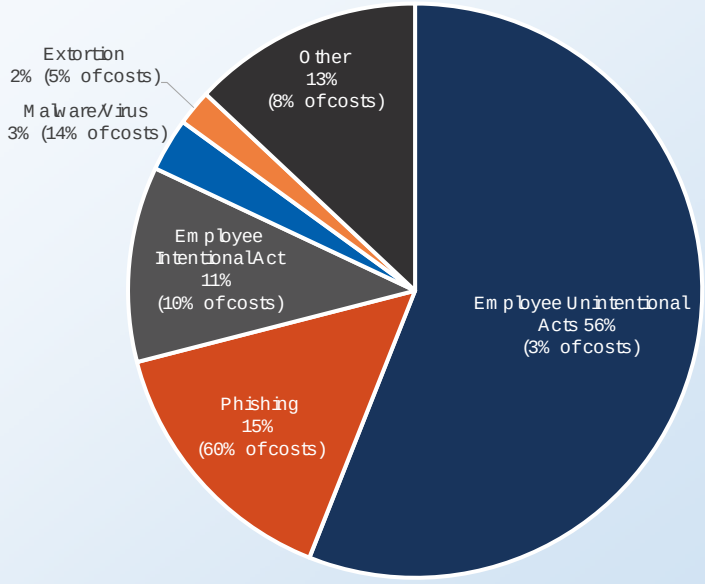
8 misdirected payment claims

Minnesota county has **ransomware** claim

7 million+ SSNs exposed in U of M data breach

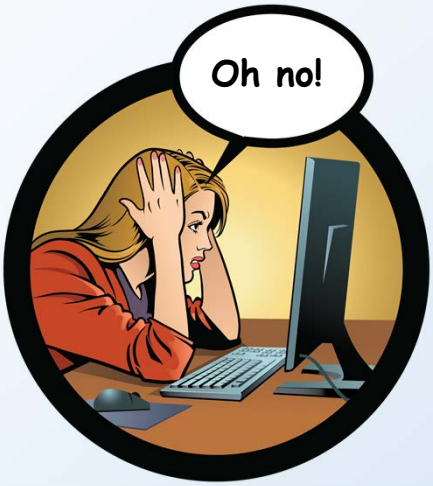
6

Causes of Data and Cyber-incidents



7

Employee Unintentional Acts



- 56% of claims
  1. Misaddressed emails
  2. Incorrect attachments or documents sent
  3. Postal mail sent to incorrect address

8

Employee Intentional Acts

- 11% of claims
  1. Accessing information without work assignment that reasonably requires access.
  2. Sharing private information with those who have no need
  3. Stealing/theft of data or equipment

9

Phishing

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

- 15% of claims
- Includes
  1. Misdirected payment scams
  2. Mass emails from compromised users
  3. Introducing malware

10

Phishing Example of Misdirected Payment Fraud

- Joe Smith Construction had a contract
- Hacker emailed instructions to change Joe's bank
- $300,000+ was transferred to fraudulent account
  - Account closed upon receipt of funds
  - Bank notified entity
  - Reverse transfer requested

- No one asked Joe
  - Double check using normal channels

11

Case Study: Email Compromise Phishing Incident

- Clicked link
  - Employee email had volumes of personal information
  - Years of data
- Mass emails from compromised account

12

Malware

Malicious, often covert, software introduced to system that may compromise:

- Data confidentiality, integrity
- Operating system and/or applications
- 3% of claims
- Most malware comes from phishing
- Ransomware is a type of malware

13

Ransomware

Extortion via a malware that encrypts system data, preventing users from accessing information unless pay a fee

- 2% of claims
- Other forms of ransomware may prevent entire systems from working

14

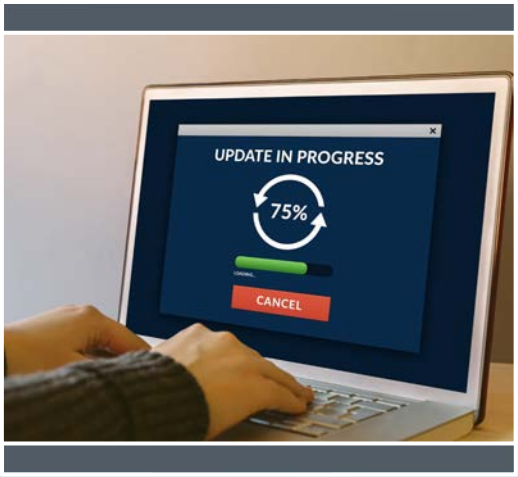
Ransomware Example

- Employee clicks a phishing link
- Malware spreads through network, encrypting data
- People are locked out of computers
- Demand for $5 million ransom appears
- System down for long period
- Costly and reputation at risk

15

Incident Prevention Best Practices: 4 Key Areas

- Strong password policy
- Multifactor authentication
- Recognize, report phishing
- Update software, ensure endpoint protection



16

Incident Prevention Best Practices: Policies

- Incident response plans
- Data retention/ destruction
- Vendor policies

17

Incident Prevention Best Practices: Training

- Data privacy laws
- Incident response plan
- Reporting

18

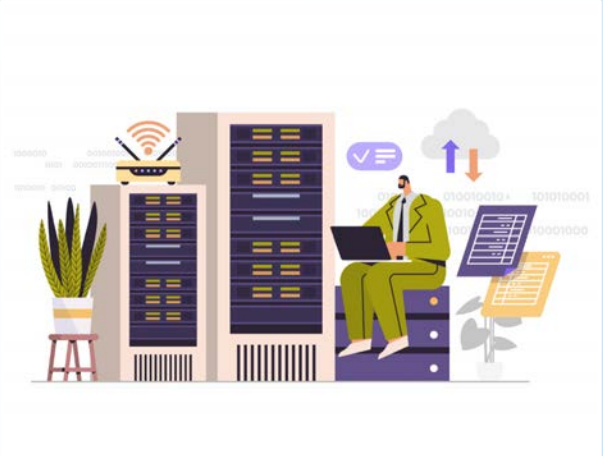
Incident Prevention Best Practices: Reporting

- Mistakes
- Attacks
- Culture of open communication

19

Incident Prevention Best Practices: Infrastructure

- Segmented networks
- Data backups



20

Department Head, Supervisor Action

- Review organization and department policies
- Training
  - Employee role: security guard for data
  - Data privacy laws
  - Phishing, other data security threats
- Encourage reporting
  - Culture of open communication
- Enforcement

21

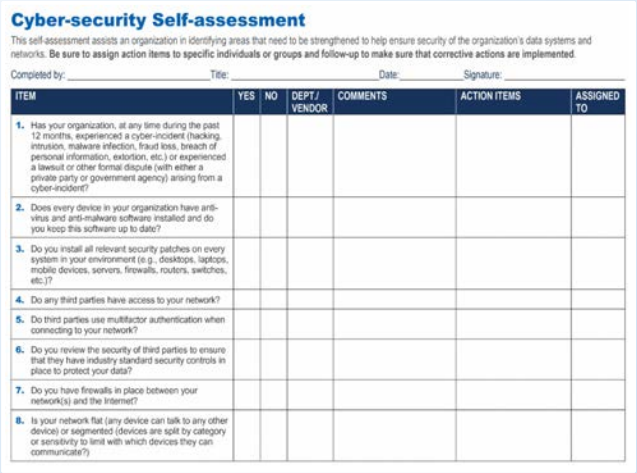
‘Essentials of Data Security for Public Entities’

- Coverage
- Threats
- Best practices
- *MCIT.org/resources/*

22

Cyber-security Self-assessment

- 32 detailed questions
- *MCIT.org/ resources/*



Cyber-security Self-assessment

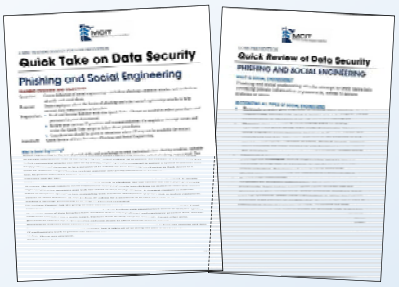
This self-assessment assists an organization in identifying areas that need to be strengthened to help ensure security of the organization's data systems and networks. **Be sure to assign action items to specific individuals or groups and follow-up to make sure that corrective actions are implemented.**

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?)						

23

Quick Takes on Data Security

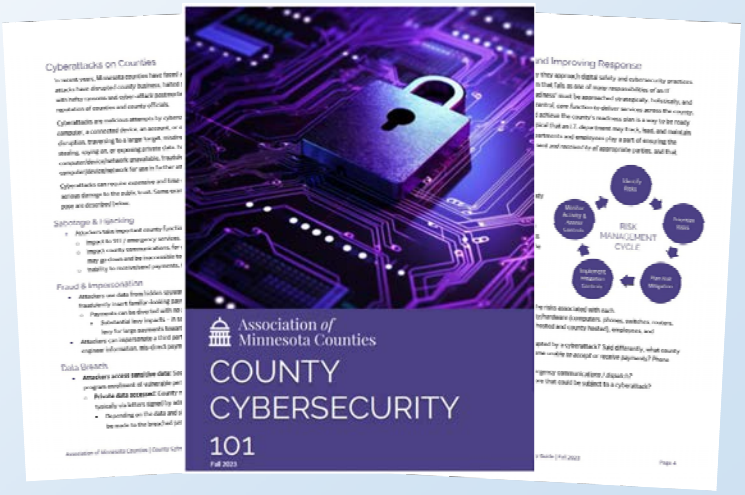


- Phishing
- Safe browsing
- Secure destruction
- Passwords
- Mobile devices
- Customizable script & employee handout
- *MCIT.org/resources/*

24

‘County Cybersecurity 101’

- Collaboration/Call to action
  - Policymakers
  - Administrators
  - IT
- Policies
- Procedures
- Infrastructure
- *MNCounties.org*



25

eRiskHub

- *eRiskHub.com/MCIT/*
  - Response plan development
  - Practice exercises
  - Sample policies: cyber and data security
  - Training tools: employee awareness
- Contact *info@mcit.org* for access code to set up eRiskHub account

26

Phishing Training Vendors

1. KnowBe4
2. Goldphish
   - Simulated Phishing
   - Training
   - Reports
3. Ninjio
   - Video training

27

Cybersecurity & Infrastructure Security Agency

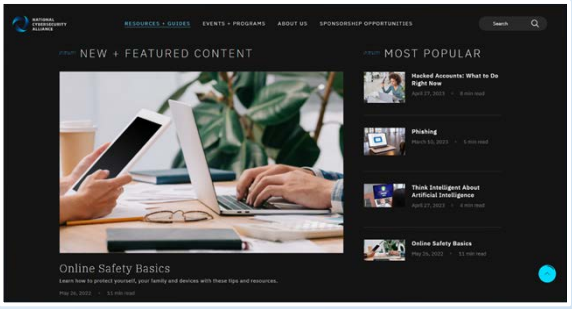
DEPARTMENT OF HOMELAND SECURITY

- Best practices
- Posters/awareness
- Cybersecurity scenarios
  - Local government
  - Elections
- *CISA.gov/cybersecurity/*

28

National Cybersecurity Alliance

- Nonprofit organization
  - Partners to create Cybersecurity Awareness Month
  - Resources, guides, articles
- *Staysafeonline.org*



29

Action Items

- Create, implement policies and procedures:
  - Cross-departmental communication
  - Collaborate with IT, policymakers, department heads, administration
- Train staff
  - Threats
  - Best practices
  - Reporting
  - Policies

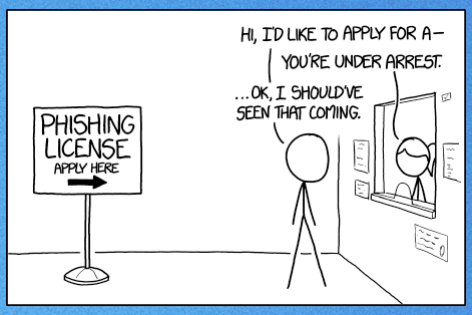
- Document trainings, protocols, enforcement
- Internal reporting system and procedures

30

Culture of Open Communication

- Fact finding, *not* fault finding
- Methods:
  - Safety/security committee
  - Intranet
  - Training
  - Policies
- Emails, articles, posters
- Learning management system
  - Tracking
  - Documentation and acknowledgement

31



Discussion

ASK QUESTIONS, SHARE EXPERIENCES


MCIT
Thank you!
MCIT Loss Control: 866.547.6516
MINNESOTA COUNTIES INTERGOVERNMENTAL TRUST