Annex I: Cybersecurity

Purpose

Minimize business disruption via ransomware and extortion, resident harm, and data breaches by doing timely detection and training. Top five threats: email phishing attacks, ransomware attacks, loss or theft of equipment or data, insider, accidental or intentional data loss, and attacks against connected medical devices.

Health Industry Cybersecurity Practices (HICP) identifies ten best practices to mitigate the current threats: E-Mail Protection Systems; Endpoint Protection Systems; Access Management; Data Protection and Loss Prevention; Asset Management; Network Management; Vulnerability Management; Incident Response; Medical Device Security; and Cybersecurity Policies.

405(d) :: Knowledge on Demand (https://405d.hhs.gov/knowledgeondemand)

Internal Contacts:

- IT services:
- Administration/Public Affairs:

External Contacts:

- Local Emergency Manager:
  - County Emergency Managers
- Minnesota Duty Officer: (651-649-5451) duty.officers@state.mn.us

See Appendix C.2 excel spreadsheet for additional internal/external contacts

Be proactive for cybersecurity by:

- Installing antivirus and malware software and scanning for viruses.
- Using firewalls to stop unauthorized used from getting information.
- Updating apps, web browsers, and operating systems on all devices regularly.
- Keeping hard drives clean by reformatting and wiping them.
- Changing passwords and using multifactor authentication.

Email phishing attacks

E-mail phishing is an attempt to trick you, a colleague, or someone else in the workplace into giving out information using e-mail. An inbound phishing e-mail includes an active link or file (often a picture or graphic). The e-mail appears to come from a legitimate source, such as a friend, coworker, manager, company, or even the user's own email address. Clicking to open the link or file takes the user to a website that may solicit sensitive information or proactively infect the computer. Accessing the link or file may result in malicious software being downloaded or access being provided to information stored on your computer or other computers within your network

- How To Recognize and Avoid Phishing Scams | Consumer Advice (https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams)
- Malware: How To Protect Against, Detect, and Remove It | Consumer Advice (https://consumer.ftc.gov/articles/how-recognize-remove-avoid-malware)

Ransomware attacks

The HHS Ransomware Factsheet, available at FACT SHEET: Ransomware and HIPAA (https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf) , defines ransomware as follows: "Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) to receive a decryption key.

Loss or theft of equipment or data

Every day, mobile devices such as laptops, tablets, smartphones, and USB/thumb drives are lost or stolen, and they end up in the hands of hackers. Theft of equipment and data is an ever-present and ongoing threat for all organizations. From January 1, 2018, to August 31, 2018, the Office for Civil Rights received reports of 192 theft cases affecting 2,041,668 individuals. Although the value of the device represents one loss, far greater are the consequences of losing a device that contains sensitive data. In cases where the lost device was not appropriately safeguarded or password protected, the loss may result in unauthorized or illegal access, dissemination, and use of sensitive data.

Insider, accidental, or intentional data loss

Insider threats exist within every organization where employees, contractors, or other users access the organization's technology infrastructure, network, or databases. There are two types of insider threats: accidental and intentional. An accidental insider threat is unintentional loss caused by honest mistakes, like being tricked, procedural errors, or a degree of negligence. For example, being the victim of an e-mail phishing attack is an accidental insider threat.

Attacks against connected medical devices

The Food and Drug Administration (FDA) defines a medical device as "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part or accessory which is recognized in the official National Formulary, or the United

States Pharmacopoeia, or any supplement to them; intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease."

MN Executive Order 22-20

On October 13, 2022, the following message went out from MDH – Facilities/agencies need to decide for themselves what they need to do. The Executive order was attached to the email - EO 20-22 - Minnesota Fusion Center / Minnesota IT Services(https://mn.gov/mnit/government/policies/security/eo22-20-faq.jsp)

New Cybersecurity Requirements for State of Minnesota Critical Infrastructure Providers

On August 30 2022, Minnesota Governor Tim Walz signed Executive Order 22-20, directing state agencies to implement cybersecurity measures to protect critical infrastructure in Minnesota. Your business is part of the 16 critical infrastructure types.

MDH leadership, in partnership with Minnesota IT Services (MNIT) is following this order by continuing to monitor and help reduce cybersecurity risks to protect the life and safety of Minnesotans. All service providers rely on systems that are potentially vulnerable to cybersecurity threats and will be required to take actions to protect their system security, with more details in the future from MDH.

What needs to be done?

- MN Fusion Center at MNFC: Minnesota Fusion Center (MNFC) | Minnesota Department of Public Safety (https://dps.mn.gov/divisions/bca/bca-divisions/investigative-services/mn-fusion-center-mnfc)
- Report cyber-attacks using guidance at the EO 20-22 - Minnesota Fusion Center / Minnesota IT Services (https://mn.gov/mnit/government/policies/security/eo22-20-faq.jsp)
- Look for additional information in the future from MDH on materials to conduct a cybersecurity self-assessment. You may also choose to have an assessment completed by an outside entity.
    - After completing the cybersecurity assessment, your system will:
        - Certify completion with MDH.
        - Continue work in addressing potential security gaps; and
        - Annually certify that an updated assessment has been completed.
- **Minnesota Fusion Center (MNFC)** Questions can be directed to mn.fc@state.mn.us.
- Find general information on cybersecurity self-assessments?
- Free Cybersecurity Services and Tools | CISA (https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools)for additional guidance as it's available.