WELCOME

Cybersecurity Incident Response Handling

Michael Holko
Director of Cybersecurity Compliance and Oversight
Pennsylvania Public Utility Commission

Agenda

- Introduction
- Cybersecurity Incident Response Components
- Legal Considerations
- Incident Response Contact Information
- Conclusion

Introduction – What is a Cybersecurity Incident?

- A cybersecurity incident is an event or series of events that compromise the confidentiality, integrity, or availability of an organization's information assets or IT infrastructure. This can involve unauthorized access, data breaches, malware infections, phishing attacks, or other forms of cyber threats.

- Cybersecurity incidents can lead to financial loss, reputational damage, and legal or regulatory consequences for the affected organization, making prevention, detection, and response strategies critical to maintaining a secure environment.

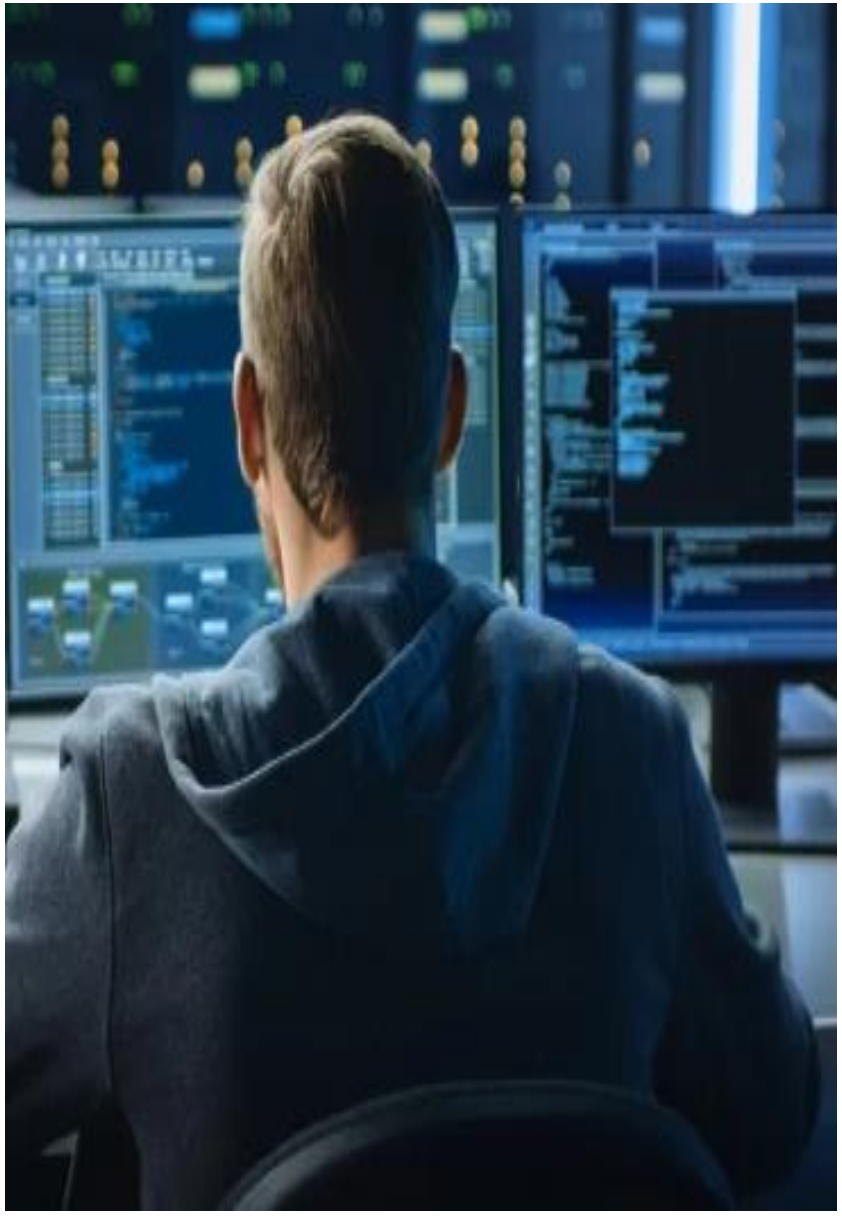
Introduction – What's the Importance of Cybersecurity Incident Response?

- **Minimizing Damage**: A prompt and effective incident response can help minimize the damage caused by a security incident. By quickly detecting and containing the incident, organizations can prevent further damage and limit the impact on critical systems and data.
- **Protecting Data and Systems**: A comprehensive incident response plan ensures that systems and data are protected from future attacks. It helps organizations identify vulnerabilities, implement appropriate controls, and improve their security posture to prevent similar incidents from happening in the future.
- **Compliance**: Many industries and jurisdictions have regulations and standards that require organizations to have an incident response plan. Failing to comply with these requirements can result in legal and financial consequences.
- **Reputation**: A security incident can damage an organization's reputation and erode customer trust. A well-executed incident response plan can help mitigate the damage and restore customer confidence.
- **Cost Savings**: Effective incident response can help minimize the financial impact of a security incident. By identifying and containing the incident early, organizations can avoid costly downtime, data loss, and remediation efforts.

Introduction – What are the Most Common Types of Cybersecurity Incidents?

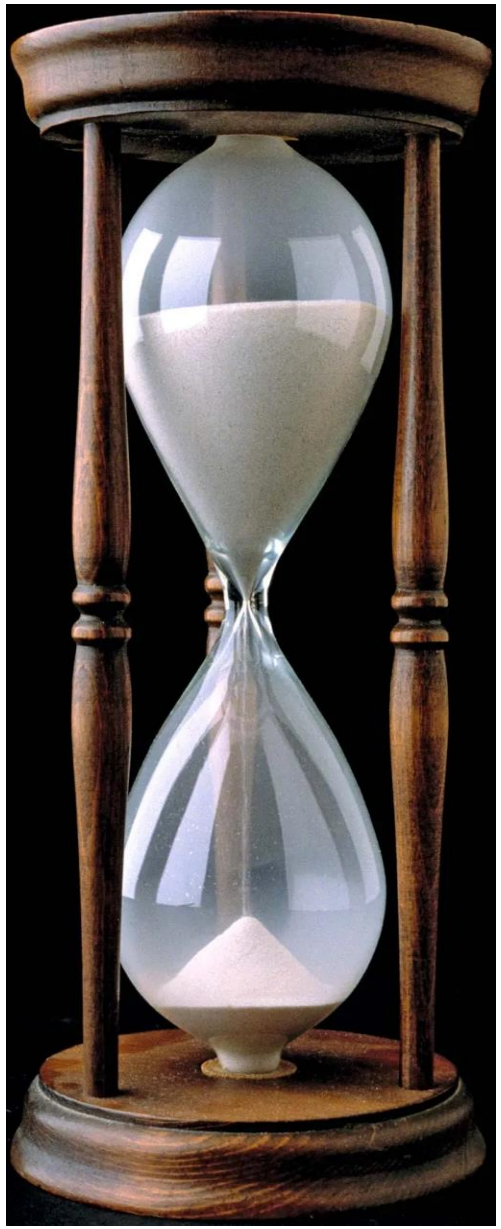
- **Malware**: Malware is software that is designed to damage, disrupt, or gain unauthorized access to computer systems. Examples include viruses, trojans, ransomware, and spyware.
- **Denial of Service (DoS) and Distributed Denial of Service (DDoS)**: These attacks involve overwhelming a network or website with traffic or requests to disrupt its normal operation, making it unavailable to legitimate users.
- **Man-in-the-Middle (MitM)**: In this attack, an attacker intercepts the communication between two parties to steal sensitive information or modify the communication without the parties' knowledge.
- **SQL Injection**: This attack targets databases by injecting malicious code into SQL statements to gain unauthorized access to sensitive data.
- **Cross-site Scripting (XSS)**: This attack involves injecting malicious code into a website to steal sensitive information from users or manipulate their web sessions.
- **Social Engineering**: This attack involves manipulating people into divulging sensitive information or performing actions that could compromise security, such as clicking on malicious links or downloading infected files.

Incident Response Components



- **Preparation:** Establishing a team responsible for incident response, defining roles and responsibilities, identifying critical assets and systems, and establishing policies and procedures for incident response.
- **Detection and Analysis:** Establishing methods for detecting incidents, such as intrusion detection systems, log monitoring, and user reports. The plan should also include procedures for analyzing the incident to determine its severity, scope, and impact.
- **Containment, Eradication, and Recovery:** Developing procedures for containing the incident to prevent further damage, eradicating the root cause of the incident, and recovering from the incident by restoring systems and data to a pre-incident state.
- **Reporting and Communication:** Establishing procedures for reporting the incident to internal and external stakeholders, such as senior management, law enforcement, and regulatory bodies. The plan should also include procedures for communicating with affected parties, such as customers, employees, and vendors.
- **Lessons Learned:** Conducting a post-incident review to identify areas for improvement, updating the incident response plan, and providing training to the incident response team.

Incident Response Components – Preparation



- **Incident Response Team:** Establishing an incident response team that includes representatives from various departments within the organization, such as IT, legal, human resources, and public relations. The team should have clear roles and responsibilities and be trained in incident response procedures.
- **Communication Plan:** Developing a communication plan that includes internal and external stakeholders, such as employees, customers, vendors, law enforcement, and regulatory bodies. The plan should include contact information and procedures for notifying stakeholders about a security incident.
- **Incident Response Plan:** Developing an incident response plan that outlines the procedures for detecting, analyzing, containing, eradicating, and recovering from a security incident. The plan should include predefined responses to common types of incidents and be regularly reviewed and updated.
- **Training and Awareness:** Providing regular training and awareness programs to employees, vendors, and other stakeholders on security policies, procedures, and best practices. The training should include simulated incident scenarios and be tailored to the needs of different roles and departments.
- **Asset Inventory:** Developing an asset inventory that includes all critical systems, applications, and data that need to be protected. The inventory should be regularly updated and used to prioritize incident response efforts.
- **Backup and Recovery:** Establishing a backup and recovery strategy that includes regular backups of critical data and systems, testing of backups, and procedures for restoring systems and data in the event of an incident.

Incident Response Components - Detection and Analysis

Continuous Monitoring of Systems, Networks, and Applications.

- Deploying intrusion detection systems (IDS), intrusion prevention systems (IPS), security information and event management (SIEM) systems, and other detection tools.
- Establishing a baseline of normal activity to help identify deviations and potential security incidents.

Incident Identification:

- Assessing security events or alerts to determine if they qualify as security incidents.
- Comparing the events against predefined incident criteria, such as the nature of the threat, the severity of the impact, and the likelihood of exploitation.
- Considering the context of the events, such as their relevance to the organization's assets and business operations.

Initial Analysis and Triage:

- Prioritizing incidents based on their potential impact on the organization, the urgency of the response needed, and the available resources.
- Performing an initial analysis of the incident, including gathering information about the affected systems, the nature of the attack, and the possible threat actors involved.
- Determining if the incident warrants escalation to a full-scale incident response.

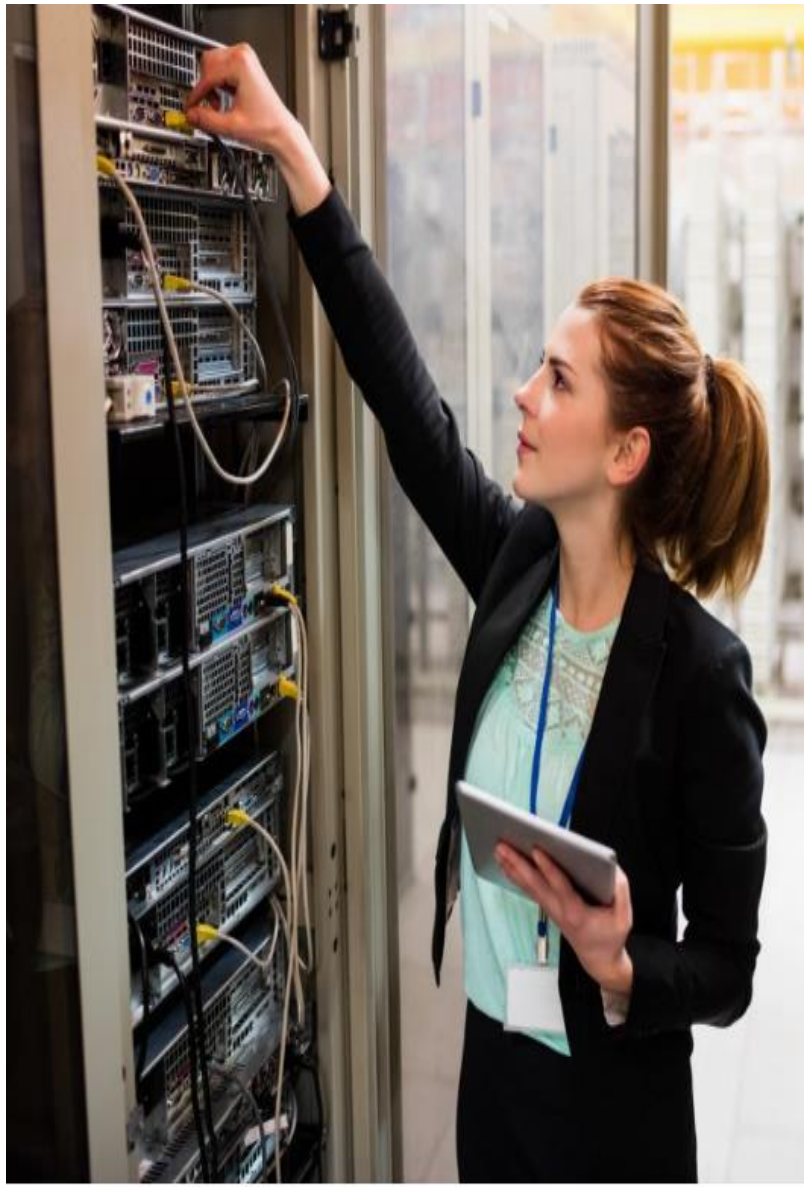
Incident documentation and tracking:

- Documenting all relevant information about the incident, including the details of the detection, analysis, and any response actions taken.
- Maintaining a central repository for incident data, such as an incident management system or ticketing system, to facilitate collaboration and information sharing among the incident response team.
- Keeping a record of the incident's timeline and any changes made to the affected systems to support forensic investigations and post-incident analysis.

Incident classification and scoping:

- Classifying the incident based on its type (e.g., malware, data breach, insider threat) and the affected assets (e.g., networks, systems, data).
- Identifying the scope of the incident, including the systems and data affected, the extent of the compromise, and the potential impact on the organization's operations and reputation.

Incident Response Components – Containment, Eradication, and Recovery



Containment:

- Isolating the affected systems or networks to prevent the spread of the attack and further damage.
- Implementing short-term containment measures, such as blocking malicious IP addresses, disabling compromised accounts, or disconnecting affected systems from the network.
- Developing and executing a containment strategy based on the nature of the incident, the organization's risk tolerance, and the potential impact on business operations.

Eradication:

- Identifying and removing the threat from the affected systems, such as eliminating malware, closing vulnerabilities, or revoking unauthorized access.
- Performing a thorough investigation to ensure all traces of the threat have been removed, including any backdoors, persistent threats, or indicators of compromise (IOCs).
- Updating and hardening the affected systems, including applying patches, updating software, and implementing additional security controls.

Recovery:

- Restoring affected systems and services to normal operations by rebuilding, reconfiguring, or recovering from backups, as needed.
- Ensuring the integrity and availability of data by validating backups and implementing data recovery procedures, if necessary.
- Conducting a phased return to normal operations, including monitoring the restored systems for any signs of recurrence or lingering issues.

Incident Response Components – Reporting and Communications

Internal Communications:

- Notifying relevant stakeholders within the organization about the incident, such as senior management, IT staff, legal, human resources, and public relations teams.
- Providing regular updates on the status of the incident, the progress of the response efforts, and any changes to the risk assessment or impact analysis.
- Establishing clear communication channels and protocols for the incident response team to ensure efficient collaboration and coordination.

External Communications:

- Reporting the incident to external parties if required, such as law enforcement, regulatory authorities, industry partners, or customers.
- Coordinating with external parties, such as cybersecurity vendors, third-party incident response teams, or legal counsel, to support the incident response process.
- Preparing public statements, press releases, or customer notifications, as needed, to inform the public about the incident and the organization's response efforts.

Incident Reporting and Documentation:

- Documenting all relevant information about the incident, including the detection and analysis phase, the containment, eradication, and recovery phase, and any post-incident activities.
- Maintaining a central repository for incident data, such as an incident management system or ticketing system, to facilitate information sharing and collaboration among the incident response team.
- Ensuring the accuracy and completeness of the incident documentation, including the incident timeline, the impact assessment, and any changes made to the affected systems.

Legal and Regulatory Compliance:

- Ensuring that the incident reporting and communication activities comply with applicable laws, regulations, and contractual obligations, such as data breach notification requirements or privacy regulations.
- Coordinating with the organization's legal and compliance teams to review and approve any external communications or disclosures related to the incident.
- Identifying any potential legal or regulatory risks arising from the incident and taking appropriate actions to mitigate those risks.

Incident Response Components – Lessons Learned

Post-Incident Review:

- Conducting a comprehensive review of the incident, including the detection and analysis, containment, eradication, and recovery, as well as reporting and communication phases.
- Analyzing the effectiveness of the incident response plan, the actions taken by the response team, and the coordination among different stakeholders.
- Identifying any gaps or shortcomings in the organization's security policies, procedures, infrastructure, or personnel that may have contributed to the incident or hindered the response efforts.

Identification of Lessons Learned:

- Assessing the root causes of the incident, such as vulnerabilities, misconfigurations, or human error, and determining if similar issues may be present in other parts of the organization.
- Identifying any opportunities to enhance the organization's security posture, incident response capabilities, or risk management practices.
- Documenting the key findings and insights from the post-incident review, including any areas for improvement, best practices, or lessons learned.

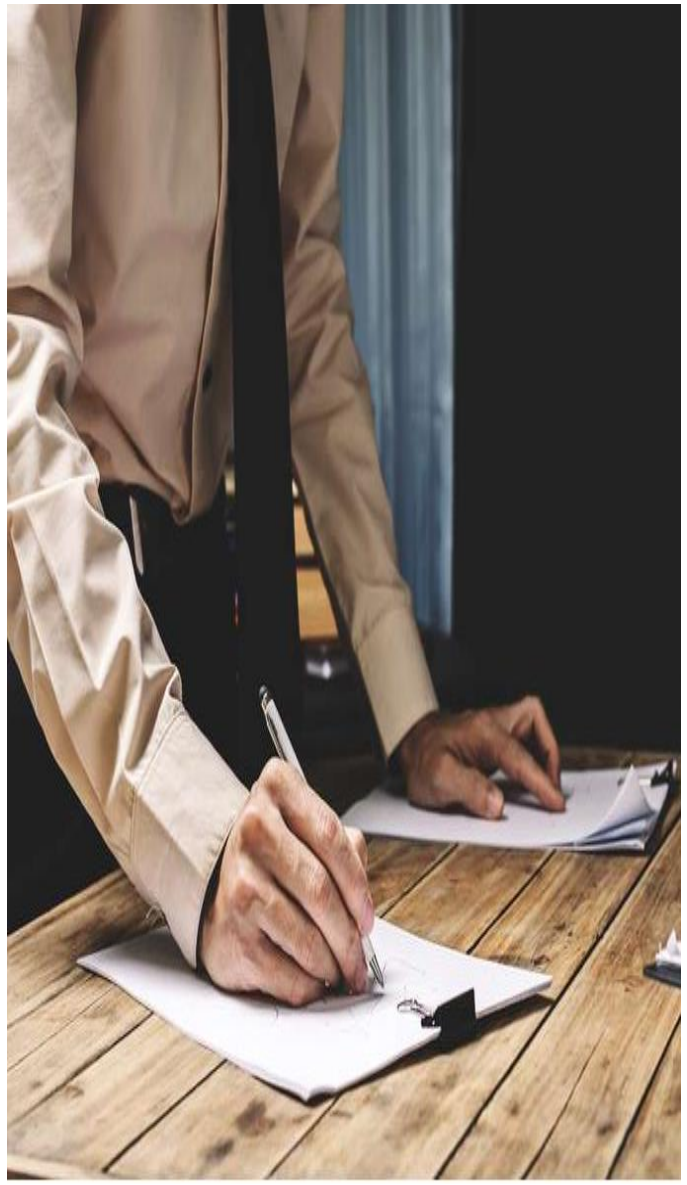
Implementation of Improvements:

- Developing an action plan to address the identified areas for improvement, including specific tasks, timelines, and responsibilities for each improvement initiative.
- Implementing the recommended changes to the organization's security policies, procedures, infrastructure, or personnel, such as updating the incident response plan, patching vulnerabilities, or providing additional training for staff.
- Monitoring the progress of the improvement initiatives and adjusting the action plan as needed to ensure the desired outcomes are achieved.

Knowledge Sharing and Collaboration:

- Sharing the lessons learned and best practices from the incident with relevant stakeholders within the organization, such as management, IT staff, and other business units.
- Collaborating with external partners, such as industry peers, cybersecurity vendors, or information sharing organizations, to exchange insights and enhance collective understanding of the threat landscape.
- Leveraging the lessons learned to inform the organization's broader cybersecurity strategy and risk management practices.

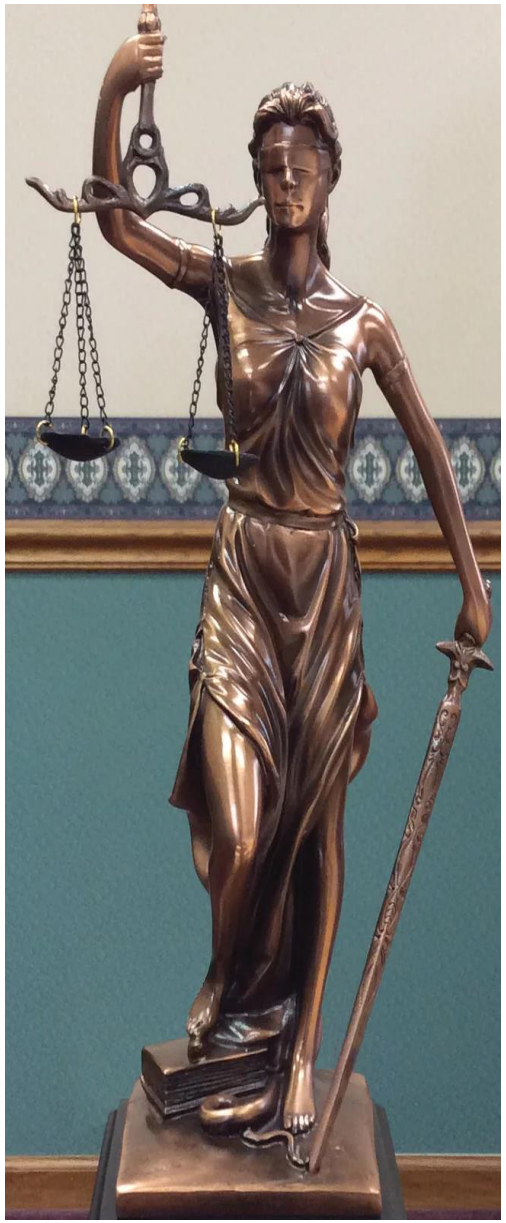
Legal Considerations – Overview



Engaging the law department or a law firm (legal counsel) to assist before or during a cybersecurity incident can help with the following products/services:

- Prepare incident response plans that can address how the company will respond and recover from a cyber incident or a data breach.
- Ensure that a company has an effective governance structure in place with respect to cybersecurity, which not only meets regulatory and legal requirements, but also helps ensure that key stakeholders are kept informed.
- Advise in scoping and obtaining cyber insurance coverage.
- Assist in the classification and protection of confidential information and/or privileged information.
- Retaining a forensics firm that can develop tools to monitor and assess threat levels, as well as respond to any suspected cybersecurity attack. Procure third-party vendors, including crisis communication firms, call center assistance, credit service providers, etc. Legal counsel also may partner with the company to help ensure that these vendors satisfy various regulatory and legal requirements.
- Terms and conditions for vendor contract management that obligate a vendor to maintain adequate information security safeguards, as well as allow the company to perform periodic inspections and audits of the vendor.
- Develop of training materials and exercises.

Legal Considerations – Risks and/or Impact



- **Civil Liability:** If a cyber-attack results in financial loss or damage to an individual or organization, the victim may be entitled to seek compensation from the perpetrator through civil litigation. The victim may also be able to pursue legal action against third parties who were involved in the attack, such as service providers or vendors who failed to adequately protect their systems.
- **Regulatory Violations:** A cyber-attack may result in violations of various laws and regulations related to data protection and cybersecurity. For example, if personal or sensitive information is compromised in a data breach, the victim organization may be in violation of data privacy laws such as the Pennsylvania Breach Act or the PUC's cybersecurity regulations. Failure to comply with such laws can result in fines, penalties, and reputational damage.
- **Criminal Charges:** If the cyber-attack is deemed to be a criminal act, the perpetrator may be subject to criminal charges and prosecution. Cybercrime is a rapidly growing area of criminal activity, and law enforcement agencies around the world are working to identify and prosecute cyber criminals.
- **Regulatory Investigations:** Regulatory (FERC, PUC, Etc.) bodies may investigate the victim organization to determine if any laws or regulations were violated and may impose fines or penalties if violations are found.
- **Reputational Damage:** A cyber-attack can cause significant reputational damage to the victim organization. This can result in loss of business, damage to brand reputation, and decreased customer confidence. The victim organization may also face legal action from affected customers or stakeholders.

Legal Considerations – Cyber Incident Reporting for Critical Infrastructure Act of 2022

- The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) was signed into law March 15, 2022, as part of the Consolidated Appropriations Act 2022. CIRCIA requires a "covered entity" to report a "covered cyber incident" to Cybersecurity and Infrastructure Security Agency (CISA) not later than 72 hours after the covered entity reasonably believes that the covered cyber incident occurs, and that a covered entity report a "ransom payment" as a result of a "ransomware attack" not later than 24 hours after the ransom payment is made. Covered entities include the following industries:
  - Chemical
  - Commercial Facilities
  - Communications
  - Critical Manufacturing
  - Dams
  - Defense Industrial Base
  - Emergency Services
  - Energy
  - Financial Services
  - Food and Agriculture
  - Government Facilities
  - Healthcare and Public Health
  - Information Technology
  - Nuclear Reactors, Materials and Waste
  - Transportation Systems
  - Water and Wastewater System
- A covered entity must also promptly submit an update or supplement to a previously submitted covered cyber incident report if substantial new or different information becomes available or if the covered entity makes a ransom payment after submitting a covered cyber incident report, until such date that the covered entity notifies CISA that the incident has concluded and has been fully mitigated and resolved.

Legal Considerations – Current CIRCIA Reporting Requirements

- CIRCIA Page 2,543 establishes some guidelines for what a substantial cyber incident is defined as:
  - Occurrences of substantial loss to confidentiality, integrity and availability of information systems, or serious impact to safety and resiliency of operational systems and processes.
  - Disruption of business or industrial operations.
  - Unauthorized access or disruption of business or industrial operations caused by third parties.
  - The number of people impacted.
  - Impacts on industrial control systems.
- CIRCIA Page 2,545 identifies the details the report should include:
  - Identification of systems impacted.
  - Description of the attack.
  - Dates and times.
  - Impact on operations.
  - Vulnerabilities exploited.
  - Threat actor tactics and techniques.
  - Information types impacted.
  - Contact information.
  - Etc.

Legal Considerations – CIRCIA Next Steps

The law is in effect, but some requirements are still pending making CIRCIA more of a guiding document for what must be addressed. The following is what CISA must address:

- CISA is required to publish a notice of proposed rulemaking (NPRM) not later than March 15, 2024, and to issue a final rule implementing CIRCIA not later than 18 months after publication of the NPRM, or by September 15, 2025.
- In the final rule, CISA must clearly define the types of entities that constitute covered entities and the types of incidents that constitute covered cyber incidents and consider potential impacts on industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers, among other statutory factors.
- CISA further must define the specific required content of a covered cyber incident report and a ransom payment report, the types of data to be collected, and how that data will be preserved and used by CISA and other federal agencies.

Legal Considerations – PA Public Utility Commission Cyber Regs

- **Public Utility Confidential Security Information Disclosure Protection Act (CSI Act) (35 P.S. § 2141)** – The CSI Act specifically defines Public Utility Confidential Security Information (CSI) to include, among other things, vulnerability assessments, emergency response plans, and security plans. The CSI Act directs the Pennsylvania Public Utility Commission (PA PUC) to develop filing protocols and procedures for public utilities to follow when filing CSI with the Commission, and to address challenges to the designations or requests to examine records containing CSI.

- **Cybersecurity Plans and Self-Certification Regulations (52 Pa. Code § § 101.1 - 7)** – These regulations require jurisdictional utilities to develop and maintain written physical, cybersecurity, emergency response, and business continuity plans. They also require utilities to submit a Public Utility Security Planning and Readiness Self-Certification Form on an annual basis.

- **Cybersecurity Incident Reporting (52 Pa. Code § § 57.11(b)(4), 59.11(b)(5), and 65.2(b)(4), 61.11, 61.45, and 65.2)** – These regulations require jurisdictional electric, natural gas, water and wastewater, and steam utilities to report an occurrence of an unusual nature that is a physical or cyber attack, including attempts against cybersecurity measures as defined in Chapter 101, which causes an interruption of service or more than $50,000 in damages.

- **Management Audits (66 Pa.C.S. § 516)** – The PA PUC's Bureau of Audits conducts Management Audits on the large (over $10 million in plant in service) electric, water, and natural gas utilities' cybersecurity, emergency preparedness, physical security, and business continuity plans. Any deficiencies identified during the audit are reviewed during a post audit review with the utility, and the PA PUC follows-up with the utility to ensure that corrective action is taken to address the deficiencies.

Incident Response Contact Information

- **Cybersecurity and Infrastructure Security Agency (CISA)**
  - 888-282-0870
  - Email: REPORT@CISA.GOV
- **FEDERAL BUREAU OF INVESTIGATION (FBI)**
  - Pittsburgh Office 412-432-4000
  - Philadelphia Office 215-418-4000.
- **Pennsylvania Criminal Intelligence Center (PaCIC)**
  - 855-772-7768
  - Email: SP-ProtectPA@pa.gov

Pennsylvania Public Utility Commission (PUC)

- PUC Agency Representative: 717-941-0003

- **Information Sharing and Analysis Centers (ISACs)**
  - COMMUNICATIONS ISAC: www.dhs.gov/national-coordinating-center-communications
  - ELECTRICITY ISAC: www.eisac.com
  - OIL & NATURAL GAS ISAC: www.ongisac.org
  - SURFACE TRANSPORTATION, PUBLIC TRANSPORTATION, AND OVER-THE-ROAD BUS ISACS: www.surfacetransportationisac.org
  - WATER ISAC: www.waterisac.org

Conclusion

- Get involved with your organization's cyber teams including preparation, response, and after-action reviews.
- Engage in the regulatory process to ensure robust discussion and rule/standard creation and monitor compliance requirements.
- Stay informed and participate in incident response conversations - IT and senior management are going to need your help.
- Work and advise on protocols and processes for internal notification, escalation, and artifact collection.
- Reach out to stakeholders and help drive the discussion.
- Continue learning. Cybersecurity changes daily so the only way to be effective is continual education on the topic.

You can find me at:

Michael Holko, Director
Office of Cybersecurity Compliance and Oversight
Pennsylvania Public Utility Commission
400 North Street, 3rd Floor North
Commonwealth Keystone Building, HBG, PA 17120
717-425-5327 | miholko@pa.gov