WELCOME

PAPUC

Cyber Threats to the Electric Grid

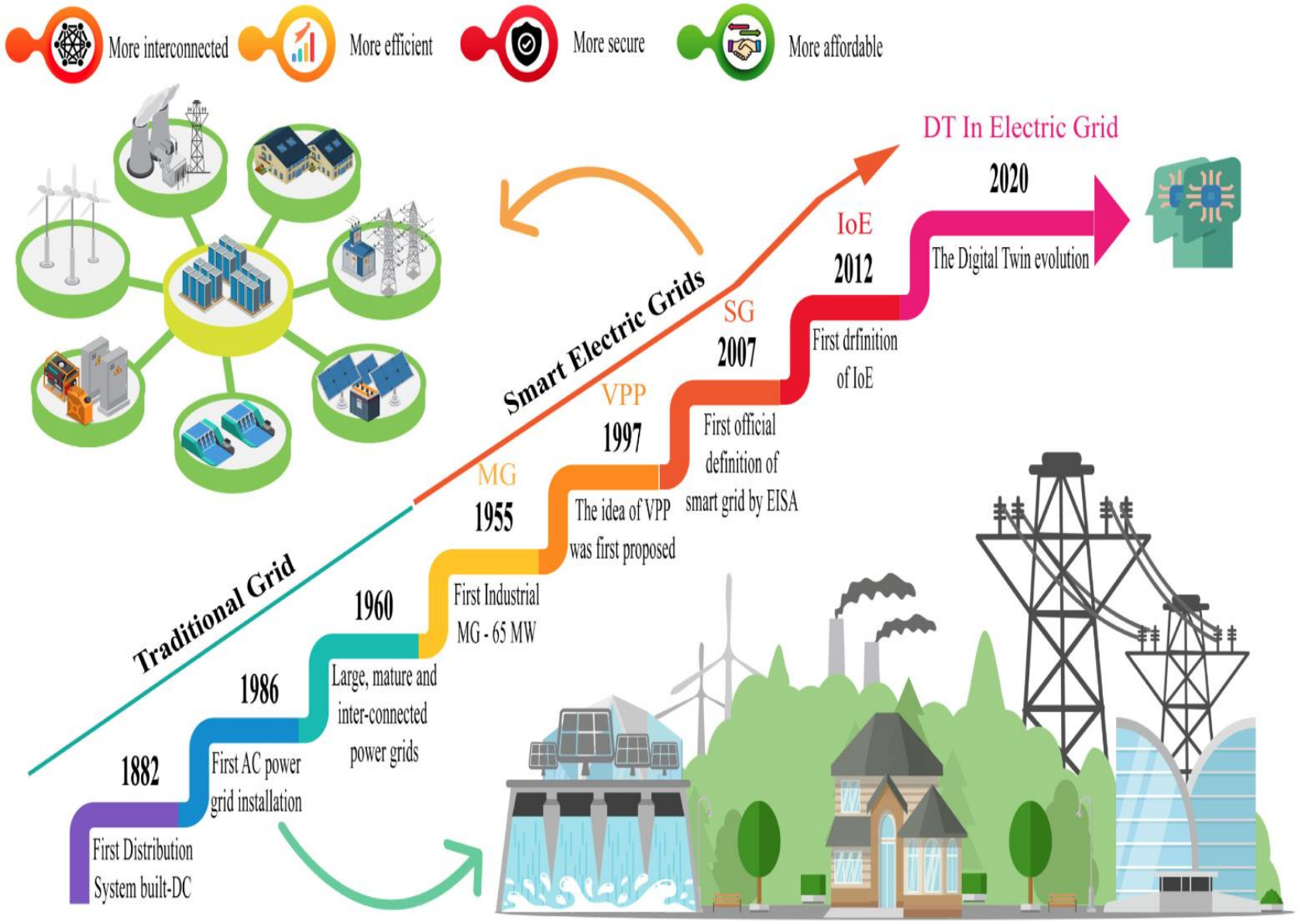
Michael Holko
Director of Cybersecurity Compliance and Oversight
Pennsylvania Public Utility Commission

Agenda

- Introduction
- Cyber Threats
- Incident Response
- Recommendations
- Conclusion
- Contacts

Introduction – Grid Transformation

The electric grid (grid) is an enormous network that allows power generation from a diversity of resources with a large number of producers and consumers. Using advance technologies, producers and consumers can be located far away from each other providing electricity at the cheapest amount with anticipated and unanticipated losses while meeting electricity demand. The grid transforms in various transformations Traditional Grid (TG), Smart Grid (SG), Microgrid (MG), Virtual Power Plant (VPP), and Internet of Energy (IoE).

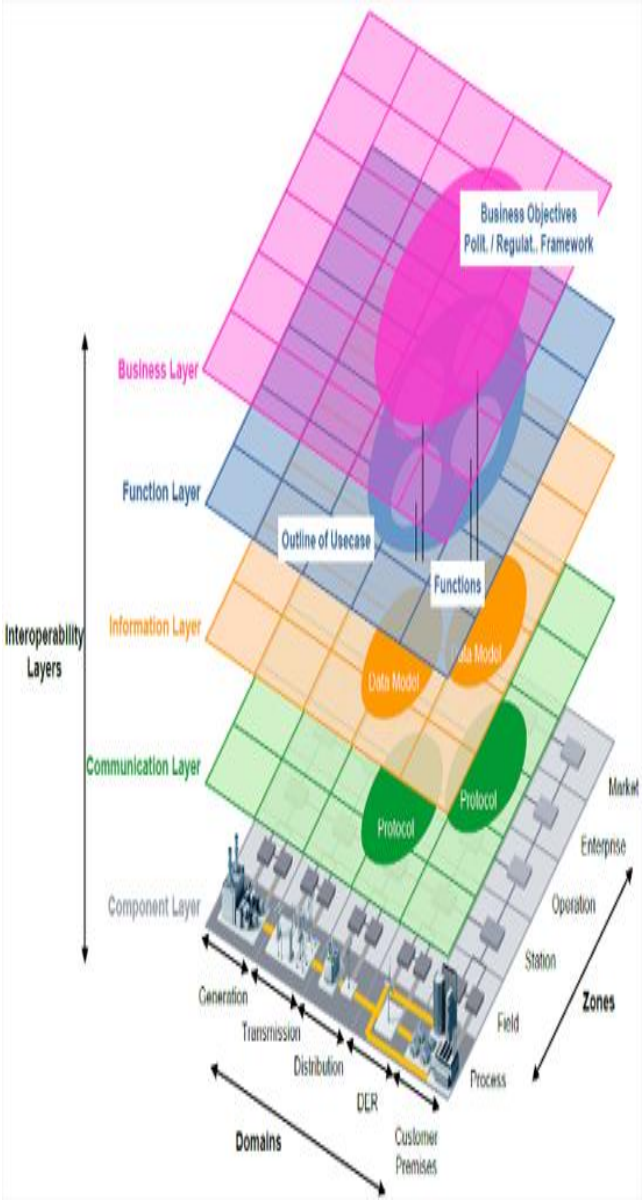


Cyber Threats – What is a Cybersecurity Incident?

- 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/OT infrastructure. This can involve unauthorized access, data breaches, malware infections, phishing attacks, or other forms of cyber threats.

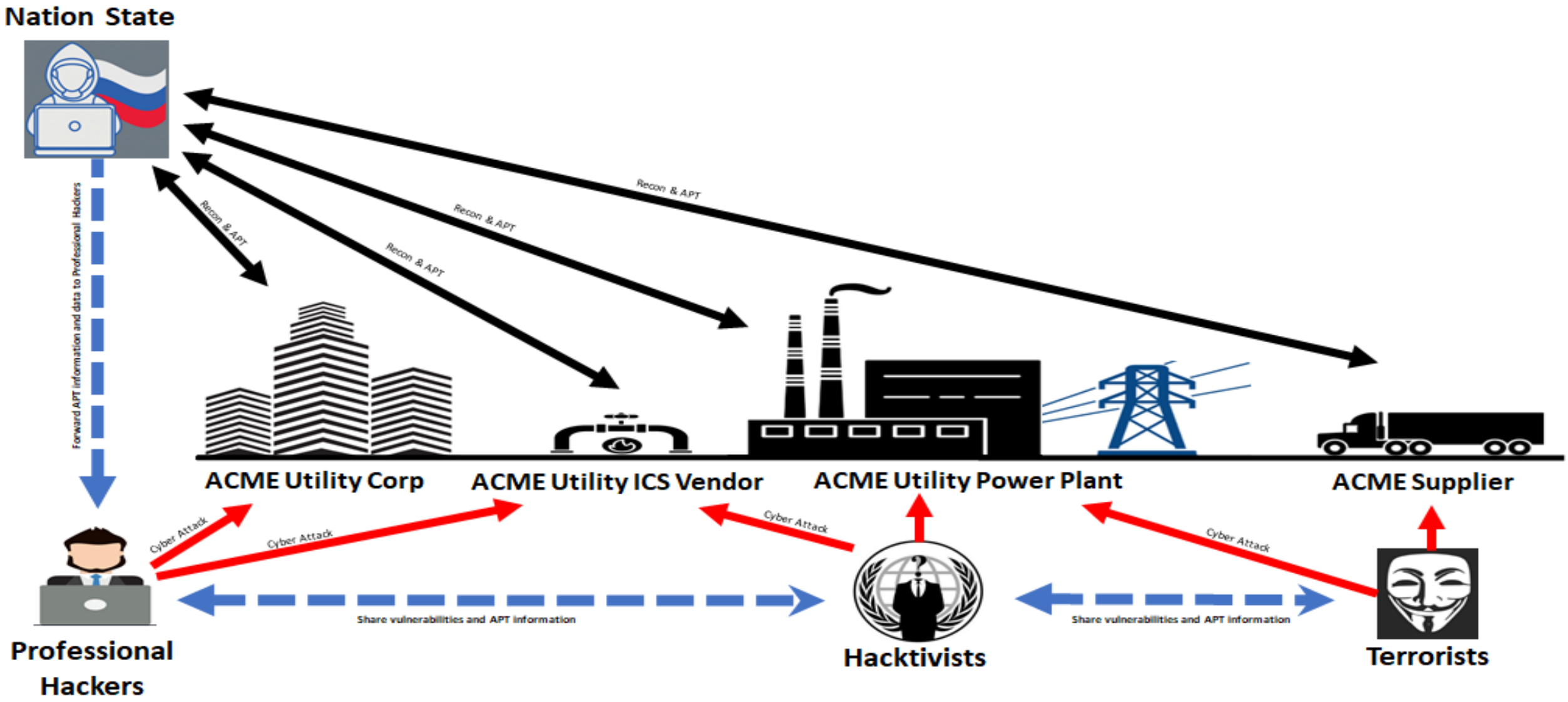
- Cybersecurity incidents can lead to financial loss, reputational damage, and legal or regulatory consequences for the affected organization, making prevention, detection, and response strategies critical to maintaining a secure environment.

Cyber Threats – Cybersecurity Risks to the Grid

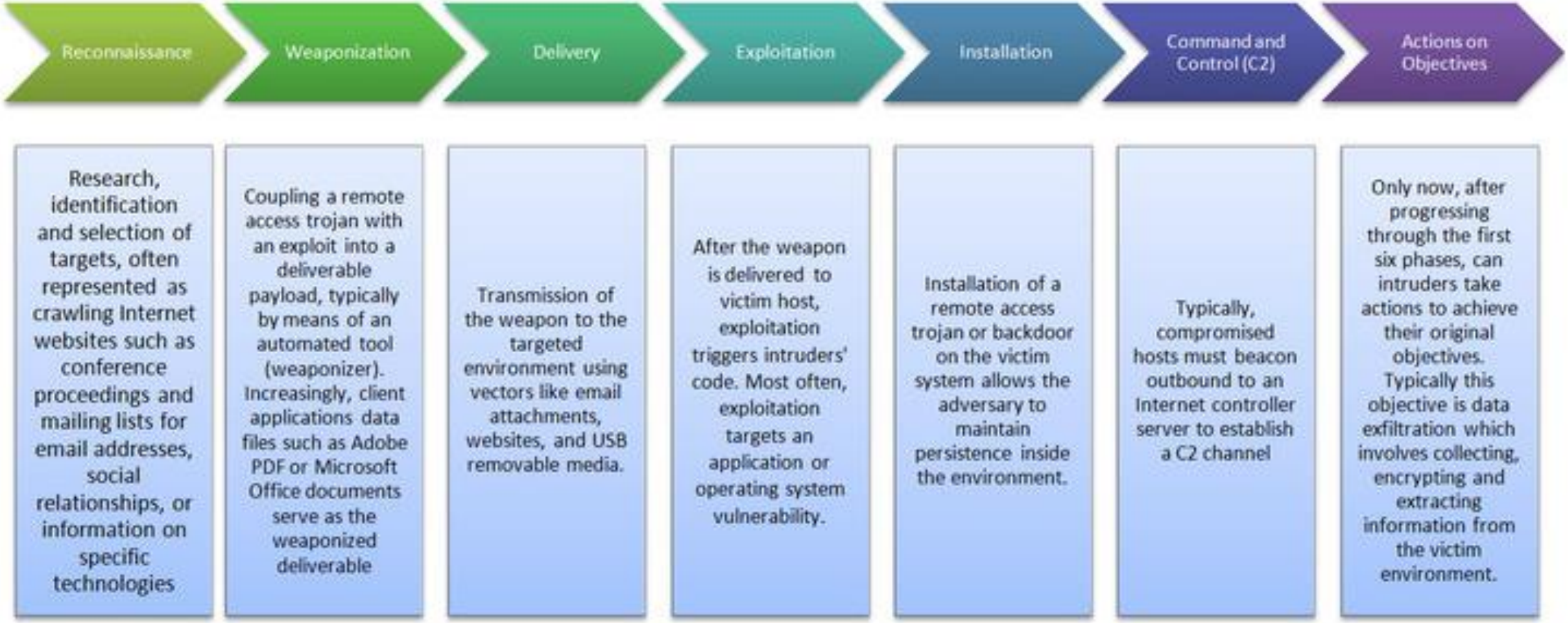


- The price of converting conventional grids to smart grids is high and could lead to cybersecurity vulnerabilities not being identified or addressed.
- Exposing legacy applications and software to the internet/cloud increases the risk of cyber attacks and data theft.
- Cybersecurity problems are more likely when a smart grid uses the internet for real-time information exchange.
- Centralized cybersecurity operations/monitoring can lead to potential security vulnerabilities and gaps.
- Retirement of security and technical staff can lead to the loss of institutional knowledge.
- Outsourcing of cybersecurity personnel can lead to gaps in security architectural knowledge and device knowledge and expertise.
- Customer portals expose utility databases, customer data, and usage to the internet.

Cyber Threats – Cybersecurity Risks to the Grid



Cyber Threats – Advanced Persistent Threat (APT) Model



APT threat model is the most prevalent model used by advanced hackers to evade network security, antivirus, and malware detection tools and software.

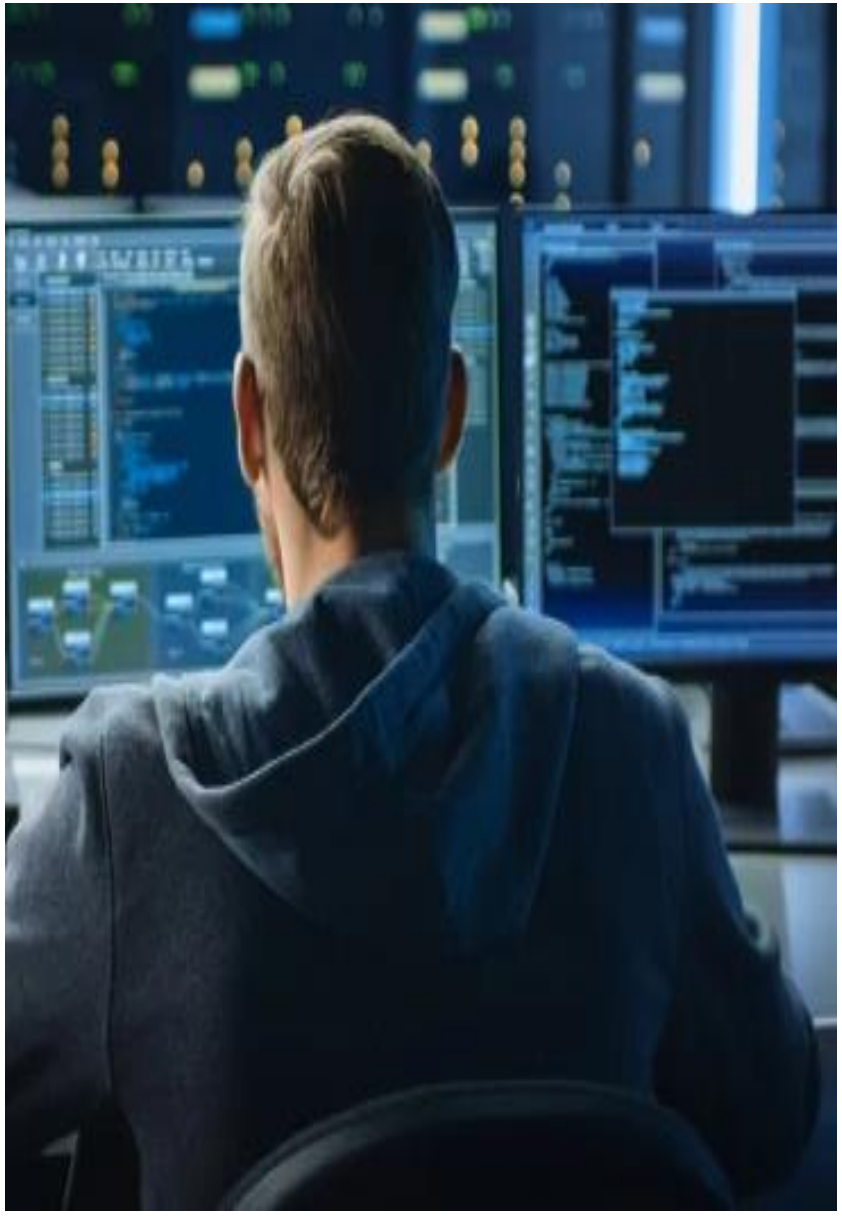
Cyber Threats – Most Common Threats to the Grid

- **Advanced Persistent Threats (APTs):** These are highly sophisticated and well-coordinated attacks often funded by nation-states. APTs aim to establish a long-term presence in the targeted systems to steal data or cause disruption.
- **Phishing Attacks:** Phishing is a common method used to gain unauthorized access to systems. Attackers send deceptive emails to trick recipients into revealing sensitive information or downloading malicious software.
- **Ransomware:** This type of malware encrypts a victim's files and demands payment in exchange for the decryption key. If the systems controlling the electric grid are compromised by ransomware, it could disrupt the delivery of power.
- **Distributed Denial of Service (DDoS) Attacks:** These attacks flood a system with unnecessary requests, causing it to slow down or crash. For the electric grid, a successful DDoS attack could disrupt monitoring and control systems.
- **Malware and Trojans:** These malicious software programs can be inserted into a system to steal data, monitor activities, or disrupt operations.
- **Supply Chain Attacks:** Threat actors target suppliers or service providers to gain access to their main target. By compromising software updates or hardware components, attackers can infiltrate primary electric grid systems.
- **Insider Threats:** Current or former employees, contractors, or business partners with access to the grid's systems and networks could intentionally or unintentionally facilitate cyber-attacks.
- **Unpatched Software:** Vulnerabilities in outdated software can serve as entry points for attackers. Regular patching and updates are essential for defending against known vulnerabilities.
- **Internet of Things (IoT) Vulnerabilities:** As the electric grid integrates more IoT devices for monitoring and control, it becomes exposed to vulnerabilities inherent to these devices.
- **Physical Attacks on Infrastructure:** While not strictly a cybersecurity threat, physical attacks on critical infrastructure components (like substations) can be coordinated with cyber-attacks for amplified impact.

Incident Response - What's the Importance of Incident Response?

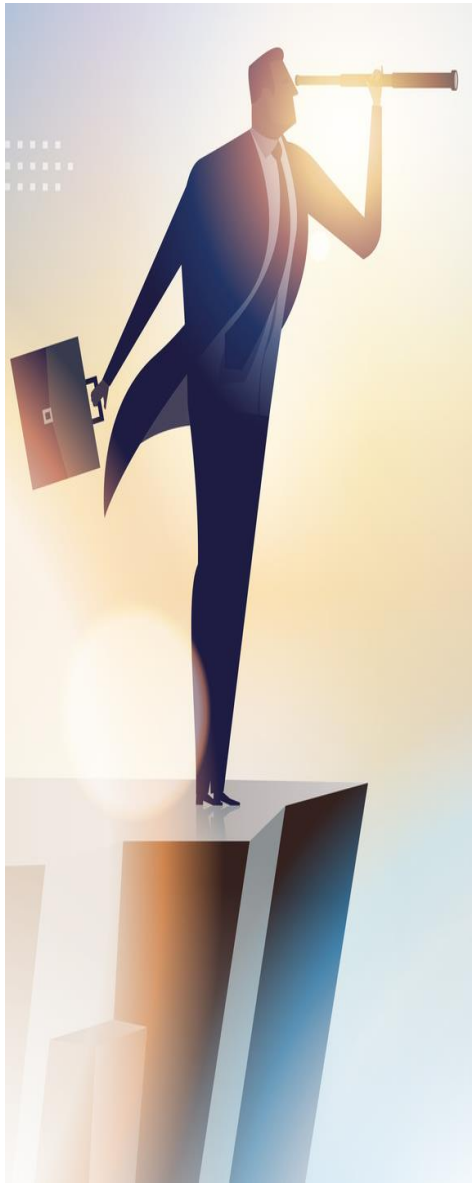
- **Minimizing Damage**: A prompt and effective incident response can help minimize the damage caused by a security incident. By quickly detecting and containing the incident, organizations can prevent further damage and limit the impact on critical systems and data.
- **Protecting Data and Systems**: 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.

Incident Response – Components



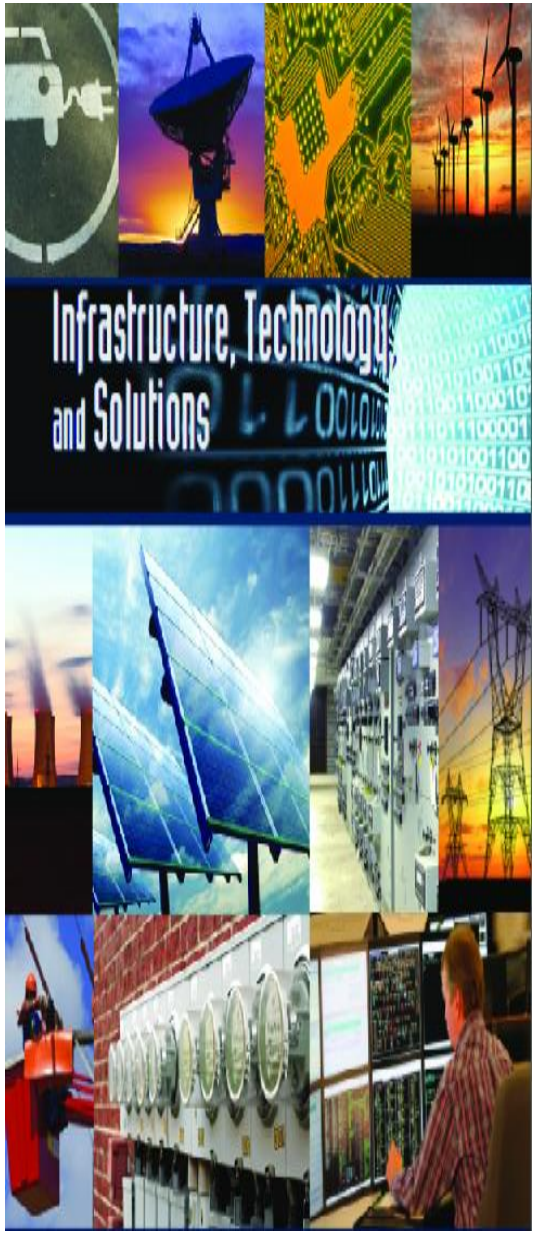
- **Preparation:** Establishing a team responsible for incident response, defining roles and responsibilities, identifying critical assets and systems, and establishing policies and procedures for incident response.
- **Detection and Analysis:** Establishing methods for detecting incidents, such as intrusion 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.

Recommendations – Corporate Leadership



- Create/support a cybersecurity governance board that ensures a company's security program aligns with business' objectives, comply with regulations and standards and achieve objectives for managing security and risk.
- Need to move beyond reactive measures and take a forward-looking approach to security that integrates the security function into critical decisions to reduce geographic and operational gaps in awareness and communication.
- Create a culture of security awareness by supporting their cybersecurity personnel and their efforts by providing them with the resources they need to do their jobs.
- Ensure the enterprise is aware of threats and have robust incident processes to report and respond to potential vulnerabilities and incidents.
- Get strategic intelligence on threats and threat actors before they launch attacks on their critical infrastructure.
- Develop flexible incident response plans to address the known vulnerabilities and are flexible to address the unknowns as well because threat actors are constantly changing their tactics.
- Create cybersecurity systems that provide their Security Operations Center with a common operating picture of sites across geographies and business units to detect coordinated attack and reconnaissance campaigns.
- Develop industry-wide collaboration to address the increasing convergence of physical and virtual threats; should engage in regular dialogue on how to secure their critical infrastructure.

Recommendations – Risk Mitigation



- **Architectural Reviews**: Ensure software and hardware purchases are properly vetted for potential vulnerabilities before integrating them into your critical infrastructure.
- **Risk Assessments**: Conduct comprehensive risk assessments to identify potential vulnerabilities, threats, and consequences. This will help utilities prioritize their cybersecurity investments and actions.
- **Implement Robust Security Standards**: Enforce industry standards such as the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards.
- **Security Audits and Penetration Testing**: Regularly test the grid's defenses by simulating cyber attacks. This helps identify vulnerabilities that might not be apparent during a risk assessment.
- **Network Segmentation**: Separate operational networks (those that control the grid) from business networks and the internet. This reduces the potential pathways for cyber-attacks.
- **Regular Software Patching**: Regularly update and patch software to defend against known vulnerabilities. Establish a regular schedule for system updates and ensure offline backups are maintained.
- **Multi-factor Authentication (MFA)**: Implement MFA, especially for systems that control critical parts of the grid.
- **Employee Training and Awareness**: Train employees to recognize and report phishing attempts and other cyber threats. Create a cybersecurity-aware culture.
- **Incident Response and Recovery Plans**: Develop and test comprehensive incident response and recovery plans. Ensure that roles and responsibilities are clear and that a communication strategy is in place.

Recommendations – Risk Mitigation

- **Threat Intelligence Sharing**: Collaborate with other utilities, government agencies, and industry groups to share threat intelligence. Platforms like the Electricity Information Sharing and Analysis Center (E-ISAC) help with this.
- **Physical Security**: Strengthen the physical security of critical assets and infrastructure. Cameras, fences, alarms, and on-site security personnel can deter or detect malicious physical acts that may accompany or facilitate cyber attacks.
- **IoT and Device Security**: Ensure that all devices connected to the grid, especially IoT devices, are secure by design, regularly updated, and monitored for anomalies.
- **Advanced Threat Detection and Monitoring**: Employ advanced analytics and machine learning to detect anomalies in system behavior that may indicate a cyber threat.
- **Backup Systems**: Maintain backups of critical systems and data in secure, offline environments. This is especially crucial in the event of a ransomware attack.
- **Supply Chain Security**: Ensure that suppliers follow strict cybersecurity protocols.
- **Public-Private Partnerships**: Engage in partnerships with government entities to leverage shared resources, knowledge, and threat intelligence.
- **Regulatory Compliance**: Stay updated and compliant with relevant regulatory guidelines that mandate specific cybersecurity practices.
- **Crisis Communication Plan**: Have a communication strategy in place for informing stakeholders, including the public, about cybersecurity incidents and the steps being taken to address them.

Conclusion

- Get involved with your organization's governance committee.
- 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.
- 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.

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)**
  - ELECTRICITY ISAC: www.eisac.com

Contact Information

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