Pennsylvania Public Utility Commission

The utility-sector cyber threat: How to address cybersecurity vulnerabilities

Presented by: Michael Holko, Director of the Office of Cybersecurity Compliance and Oversight

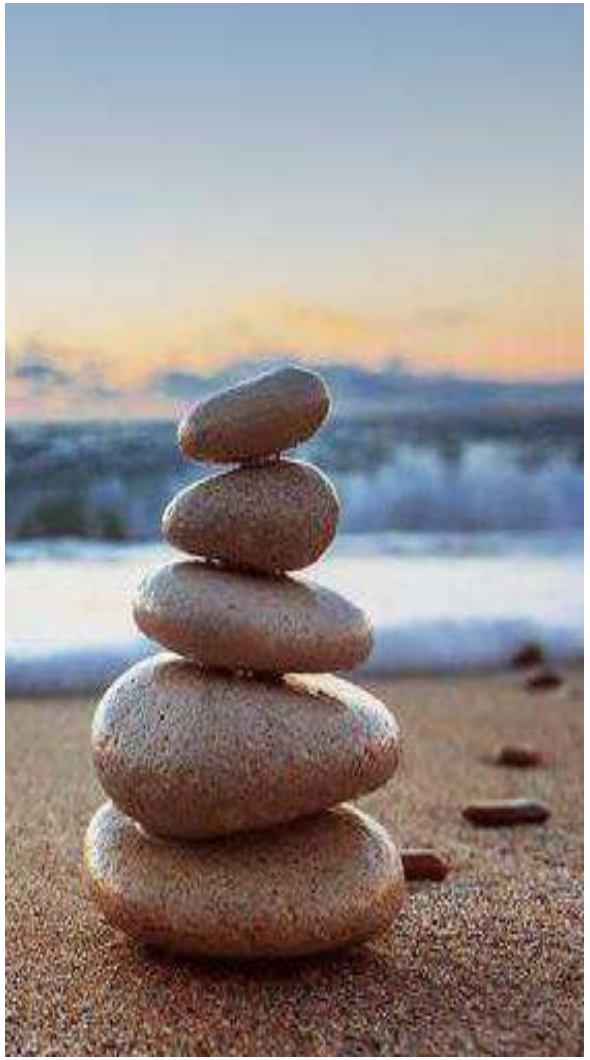
Agenda

- Cybersecurity Challenges Impacting Utilities
- Threats
- Recommendations
- Questions and Answers

Cybersecurity Challenges Impacting Utilities

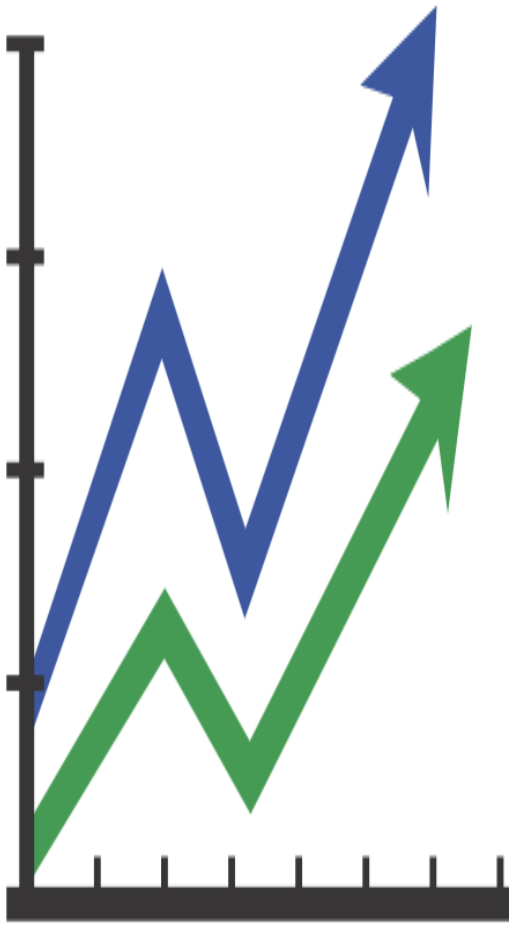
- **Expansive Attack Surface** – Arising from geographically dispersed critical infrastructure and the centralized nature of many organizations' IT and cybersecurity leadership.
- **Increased Number of Threats Actors Targeting Utilities** – Nation-state actors seeking to cause security and economic dislocation, cybercriminals who understand the economic value represented by this sector, and hacktivists out to publicly register their opposition to utilities' projects or broad agendas.
- **Supply Chain Threats** – Cyber attacks like SolarWinds and Log4J show that companies with the best security measures can be breached.
- **IT/OT Convergence** – Electric-power and gas sector's unique interdependencies between physical and cyber infrastructure make companies vulnerable to exploitation. U.S. companies are much more reliant on technologies to secure their critical infrastructure.
- **Lack of Cybersecurity Personnel** – According to Forbes, the number of unfilled cybersecurity jobs worldwide grew 350% between 2013 and 2021, from 1 million to 3.5 million. In April 2022, Cyber Seek (NIST) estimated the percentage of unfilled jobs was 35% nationwide and 54% in Pennsylvania.
- **Loss of OT Knowledge** – Many qualified OT staff are retiring, and they are taking their knowledge of the critical infrastructure with them.

Cybersecurity Challenges Impacting Utilities



- **Centralized Security Operations Centers** – In an attempt to address staffing shortages and retirements, many electric and gas utilities are using centralized SOCs to monitor the vast IT/OT infrastructures. This means that there are less cyber security staff member per employee and/or device which increases the risk of a breach occurring.
- **Outsourcing IT/Cybersecurity** – Many companies are hiring vendors to augment or replace some of the personnel they have lost. Many cybersecurity vendors can assist the utility from and IT perspective; but in many cases, they lack the OT experience/knowledge to secure the operations side of the organization.
- **Aging Infrastructure & Legacy Systems** – Many utilities are struggling with replacing or modifying systems that were built in the last century and managed by legacy systems that either outdated or jerry-rigged to work with newer technologies IT/IoT systems. Many of these systems are vulnerable to a cyber attack.
- **Increasing Information Technology Demands** – COVID 19, Telework, Customer Portals, Smart Meters, Help Bots, IoT, Artificial Intelligence, Smart Phone Applications, etc.
- **Mergers and Acquisitions** – Some utilities are acquiring other utilities to diversify their financial portfolios.

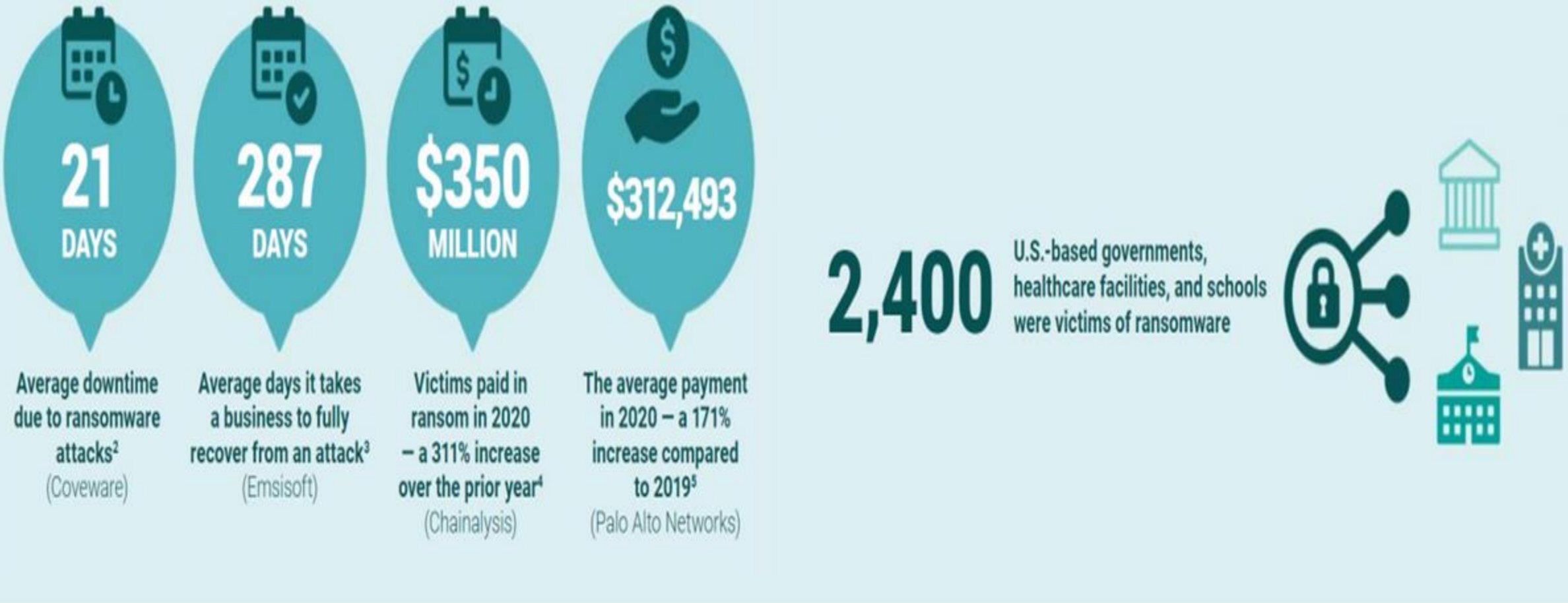
Threats - Cyber Trends



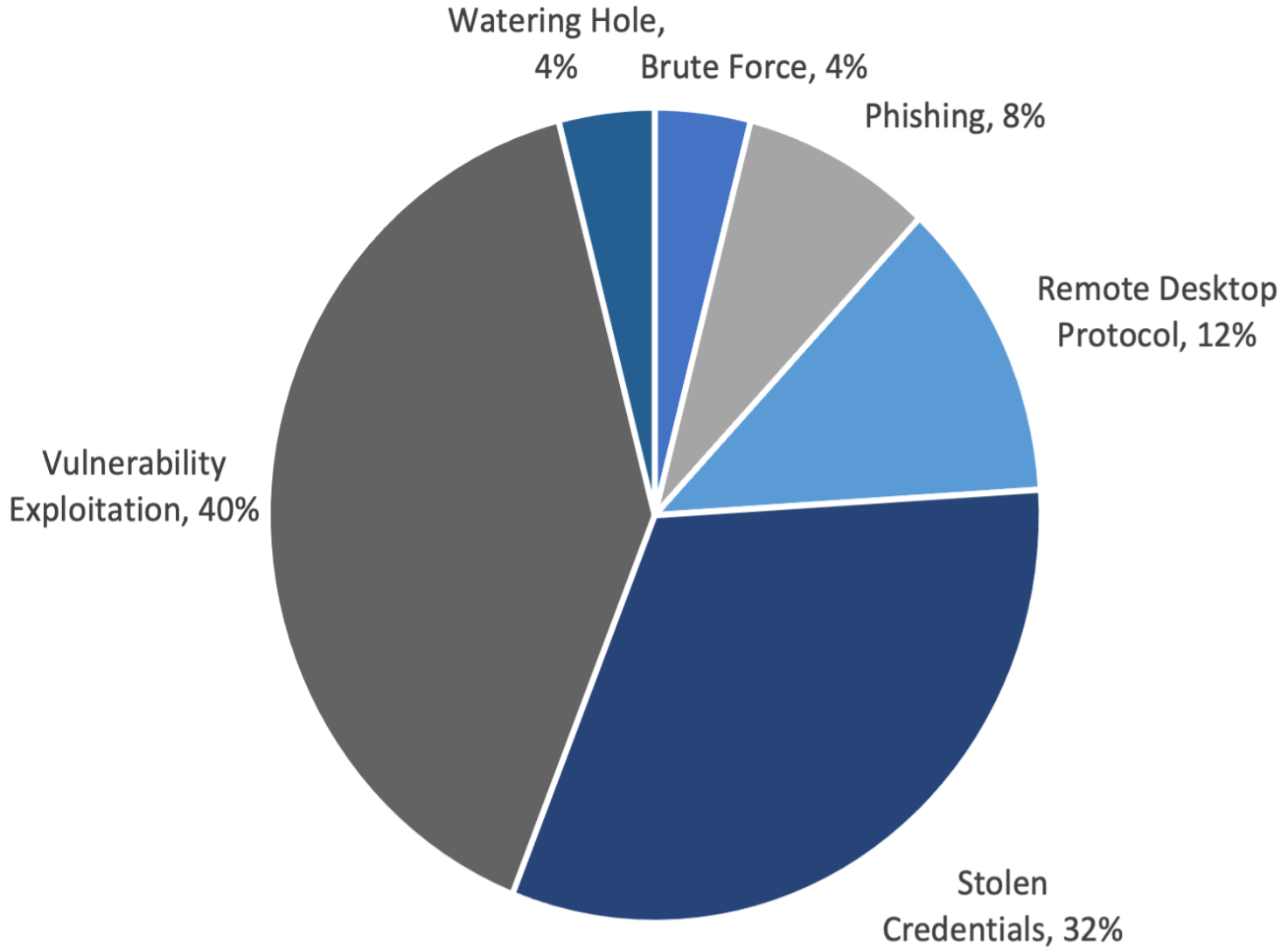
- **Phishing and Ransomware** – Phishing and ransomware continues to be the biggest threat to critical infrastructure organizations.
- **High-privilege Users Targeted** – Managers and executives make up **50% of the phishing attempts** and pose the most significant risk of causing a compromise.
- **Supply Chain Risk** – Over 80% of businesses surveyed reported they were attacked by a compromised supplier account.
- **Cloud Based File Hosting Vulnerabilities** – 35% of Microsoft OneDrive and Google Drive users have had their account compromised and experienced suspicious file activity after the breach, revealing that privilege-based risk widens as enterprises move to the cloud.
- **Cloud Based Web Hosting Vulnerabilities** – On average, approximately 10% of organizations surveyed reported they discovered at least one malicious application in their web hosting environment over the past year.
- **Smartphone Phishing Attacks (Smishing)** – Smishing attempts more than doubled in the US over the year. Cyber criminals initiated more than 100,000 smishing attacks per day.

Source: June 22, 2022, Proof Point Human Factor Report

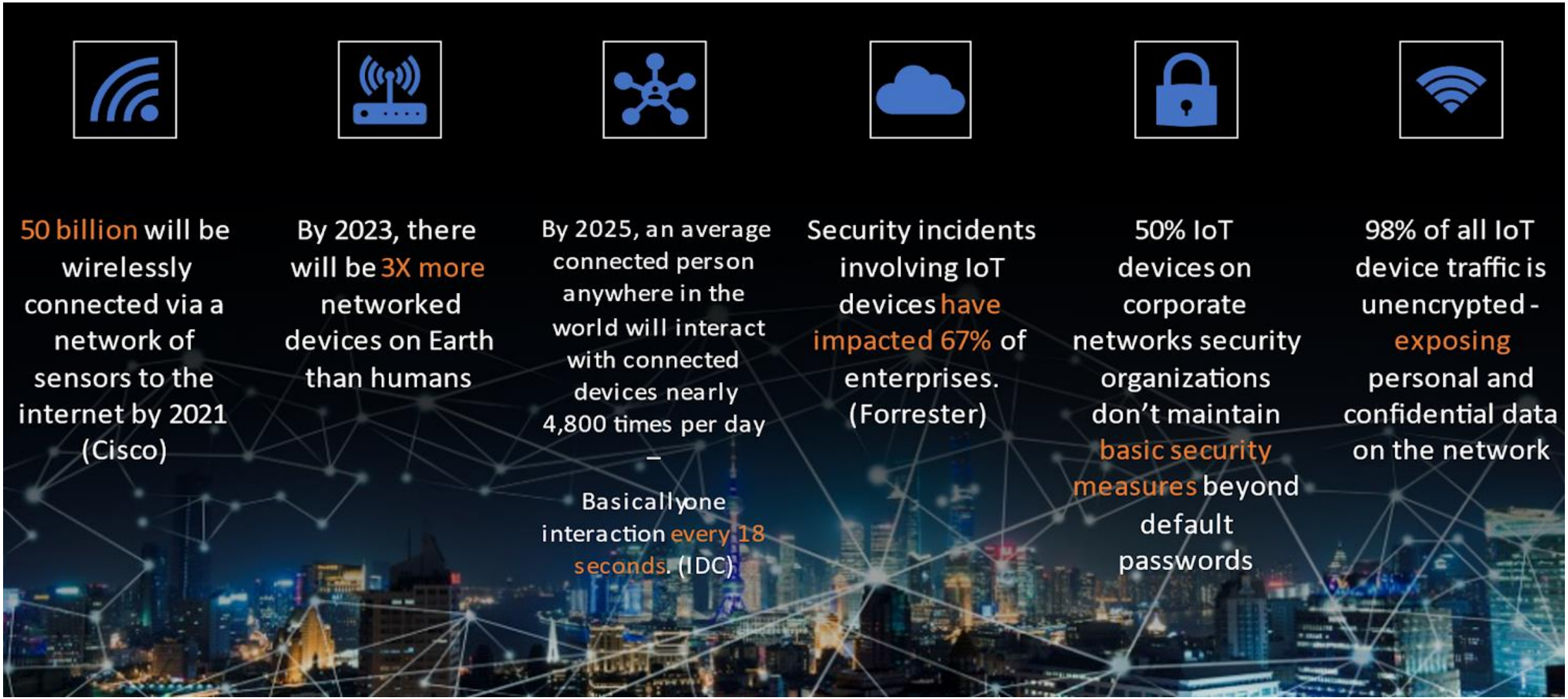
Threats - Ransomware



Threats - OT/Scada Attack Vectors



Threats - IoT



50 billion will be wirelessly connected via a network of sensors to the internet by 2021 (Cisco)

By 2023, there will be 3X more networked devices on Earth than humans

By 2025, an average connected person anywhere in the world will interact with connected devices nearly 4,800 times per day – Basically one interaction every 18 seconds. (IDC)

Security incidents involving IoT devices have impacted 67% of enterprises. (Forrester)

50% IoT devices on corporate networks security organizations don't maintain basic security measures beyond default passwords

98% of all IoT device traffic is unencrypted - exposing personal and confidential data on the network

Threats - Supply Chain

- Only 50% on U.S. small businesses have a cybersecurity plan in place.
- Of those, 32% haven't changed their cybersecurity plan since the pandemic forced remote and hybrid operations.
- Cybercrime cost U.S. small businesses more than $6.9 billion in 2021, and only 43% of businesses feel financially prepared to face a cyber-attack in 2022.
- Note: The most common attack vectors included phishing and ransomware.

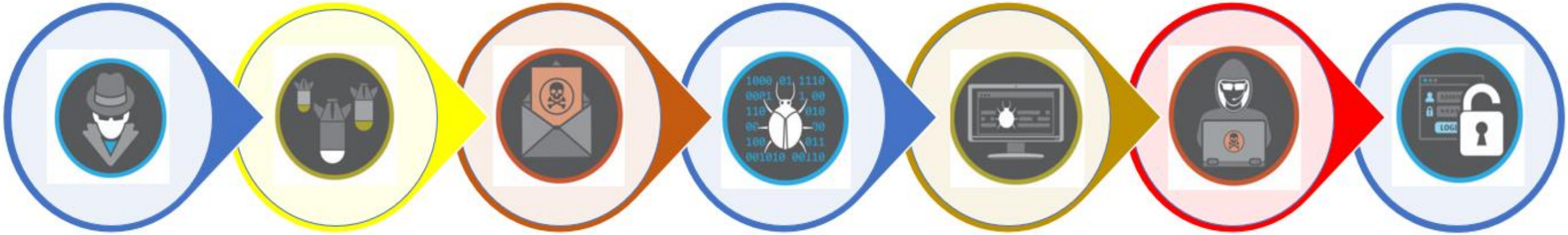
Takeaway: 2022 UpCity survey of 600 Small Business Owners and their IT staff.

Threats - Software Supply Chain Attacks

In February 2022, CSO Online surveyed of 428 executives, directors, and managers in IT, security, development, and DevOps and reported:

- Software supply chain attacks hit 60% of the companies.
- 30% were either significantly or moderately impacted by a software supply chain attack in 2021.
- Only 6% said the attacks had a minor impact on their software supply chain.
- 82% of the CIOs believe their software supply chains are vulnerable.

Threats - Advanced Persistent Threat



Reconnaissance:
Attacker probes for a weakness

Weaponization:
Create an Exploit

Delivery:
Deliver Exploit to Targeted System or Individual

Execute Exploit:
Create Backdoor

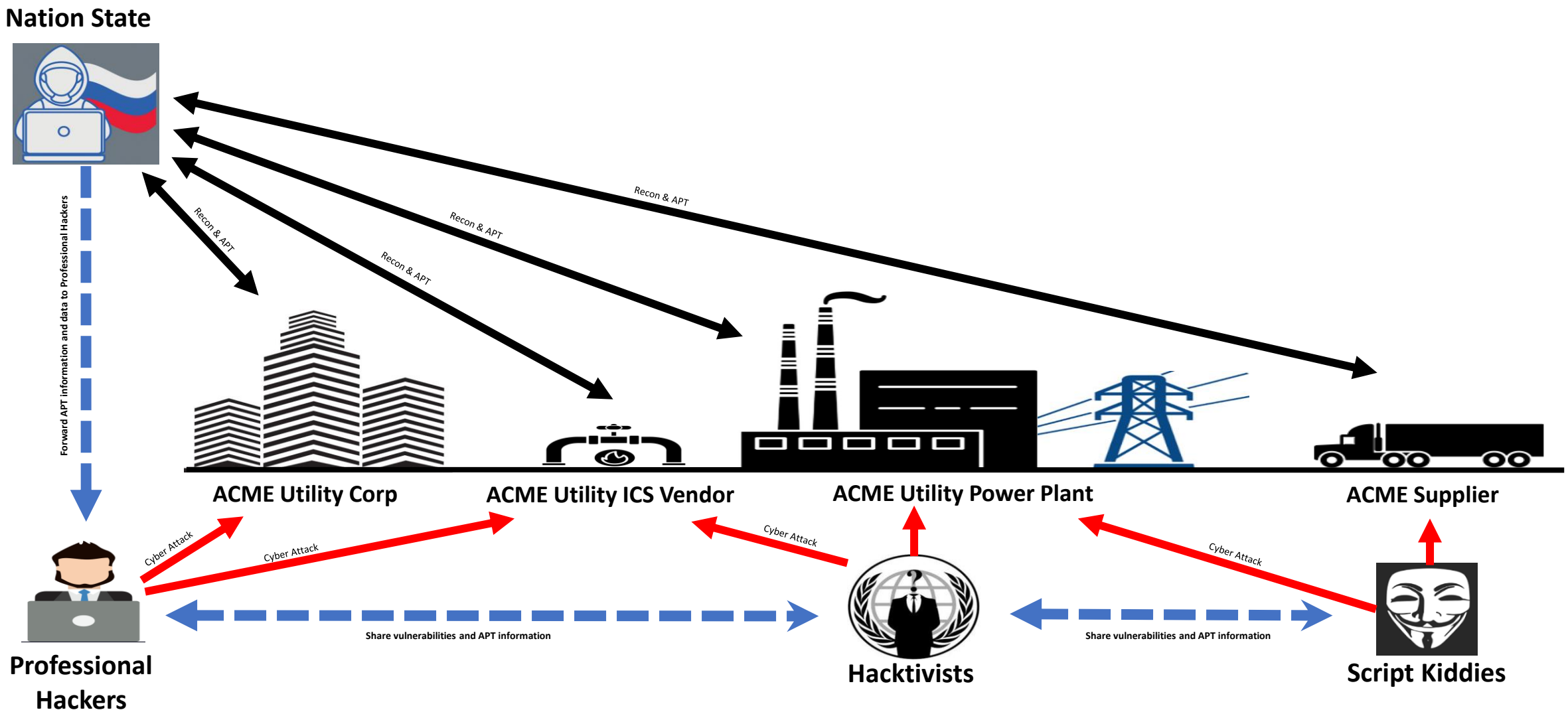
Installation:
Install Malware

Command and Control:
Takeover asset via secure channel

Actions:
Attacker Remotely Takes Over Systems, Networks, and Data

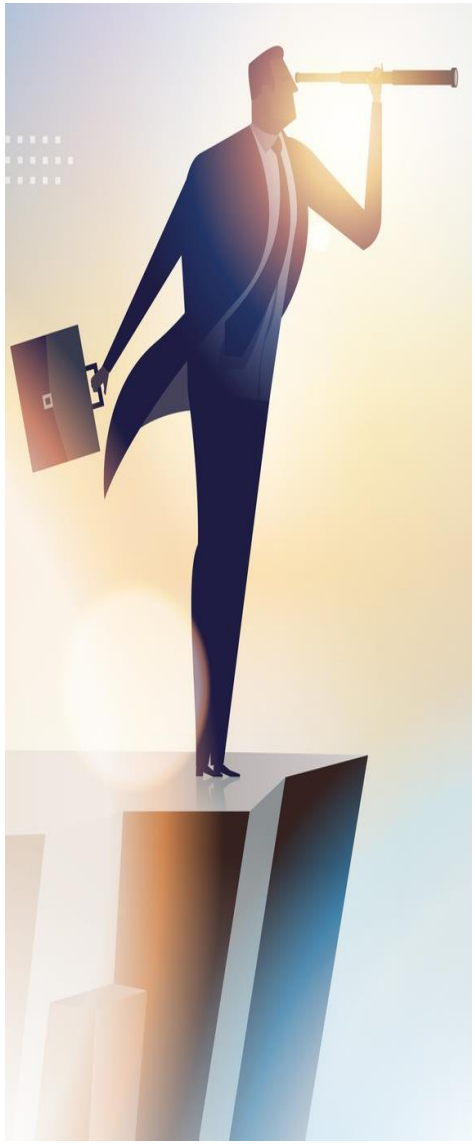
Advanced Persistent Threat (APT) is the most prevalent model used by advanced hackers to evade network security, antivirus, and malware detection tools and software.

Threats - Coordinated Cyber-Attack



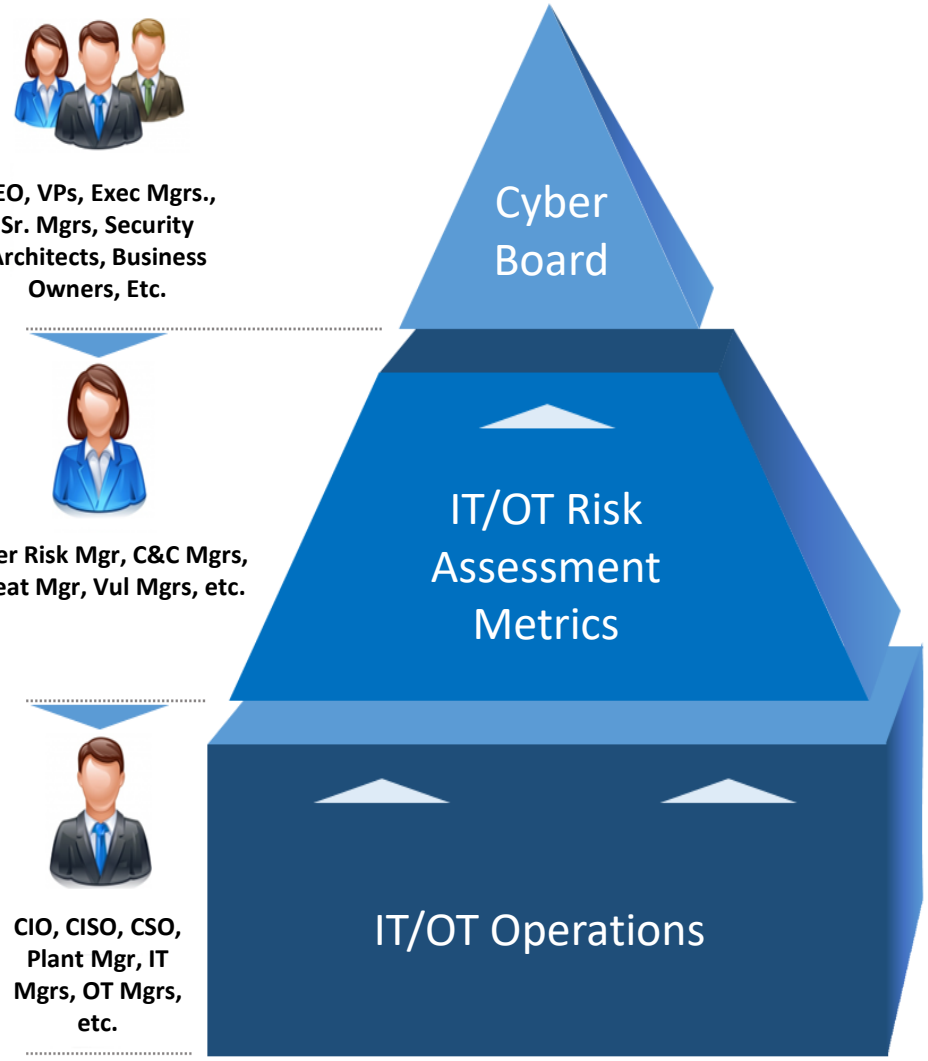
Takeaway: Utilities are constantly being scanned for vulnerabilities that can be exploited and this information is shared on the Dark Web.

Recommendations – Corporate Leadership



- 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.
- 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.

Recommendations – Cybersecurity Governance Board

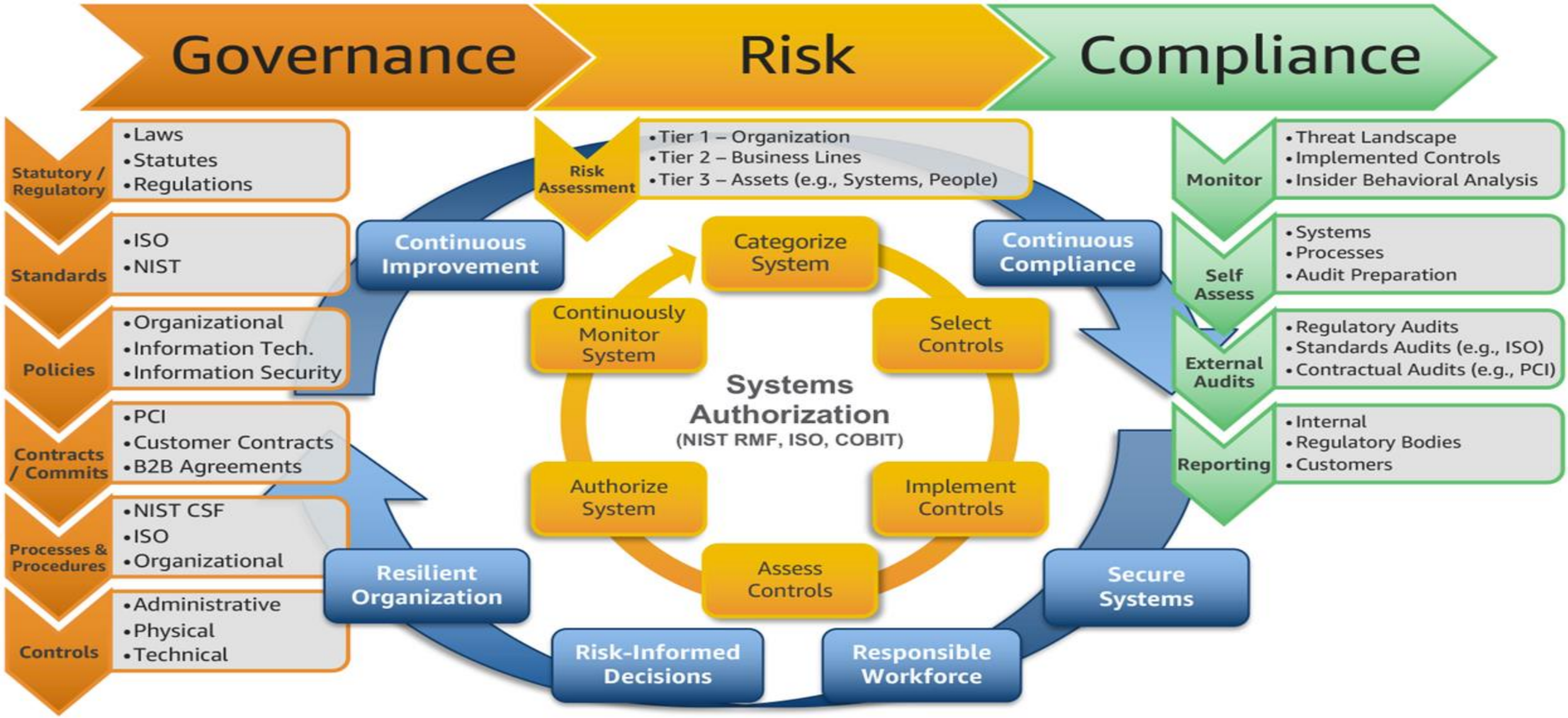


- Reviews new projects to make sure they comply with the company's cybersecurity architecture.
- Approves projects that identify and addresses vulnerable outdated systems.
- Creates and reviews policies, procedures, and standards to comply with their regulations.
- Reviews and approves configuration management requests.
- Reviews threat reports and vulnerabilities to determine the impact to their critical infrastructure and business applications.
- Works with Cybersecurity Risk Manager to:
  - Assign risk scores to known system and application vulnerabilities.
  - Approve risk management strategies, etc.

Recommendations - Governance, Risk, & Compliance

Governance, Risk, Compliance (GRC) – Governance, risk and compliance (GRC) refers to a strategy for managing an organization's overall governance, enterprise risk management and compliance with regulations. Think of GRC as a structured approach to aligning IT/OT with business objectives, while effectively managing risk and meeting compliance requirements.

Recommendations - Governance, Risk, & Compliance



Recommendations - NIST Cybersecurity Framework

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

- Designed with Critical Infrastructure (CI) in mind, it is extremely versatile and can be used by organizations which are just getting started in establishing a cybersecurity program or organizations with mature programs.
- Can be used by small organizations with a low cybersecurity budget, or a large corporations with a big budgets.
- Has built-in customization mechanisms (i.e., Tiers, Profiles, and Core all can be modified), the Framework can be customized for use by any type of organization.
- Outcome driven and does not mandate how an organization must achieve those outcomes and it enables scalability.
- Easy to adopt and use for assessing cybersecurity maturity and risk.
- Enables common cybersecurity and risk management terminology for leadership and technical staff.
- Built for future regulation and compliance requirements.
- Enables organizations to determine optimal levels of risk management.
- Illustrates compliance with NIST cybersecurity controls and identifies areas where improvements are needed.

Recommendations - Cybersecurity Evaluation Tool

- The Cybersecurity Evaluation Tool (CSET) is a **"free client-based application"** developed by the Cybersecurity and Infrastructure Security Agency (CISA) to assist organizations assessing risk to their critical infrastructure.
- CSET was developed under the direction of CISA, Idaho National Laboratory, and critical infrastructure cybersecurity experts.
- The tool can be downloaded to a PC or Laptop and is secured through the device's authentication and authorization protocols.
- CSET is very intuitive and guides users through a step-by-step process to evaluate their organization's IT/OT policies, procedures against industry frameworks and standards.
- Frameworks and standards include: NIST Cybersecurity Framework; NERC Critical Infrastructure Protection (CIP) Standards; INGAA Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry; NIST Special Publication 800-82; NIST Special Publication 800-53, etc.
- CSET provides users with built in executive summary templates, tables, graphs, and charts that help identify potential risk and compliance issues.
- More information about the tool be found at the CISA website located at: https://www.cisa.gov/

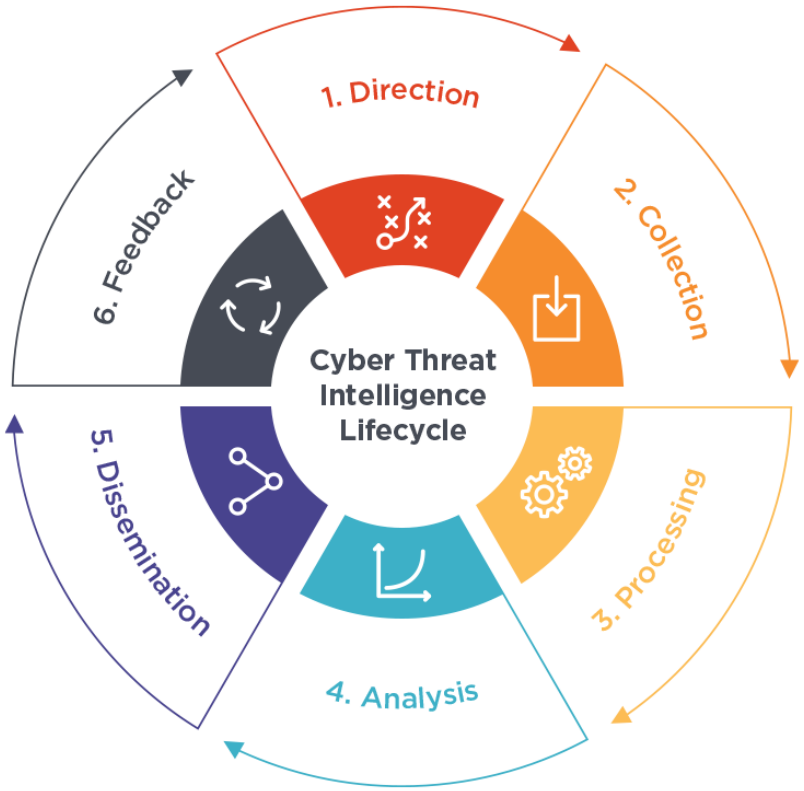
Recommendations - Free Vulnerability Assessments

- CISA conducts specialized security and resilience assessments on the Nation's critical infrastructure.
- These voluntary assessments assist CISA and its partners in better understanding and managing risk to critical infrastructure.
- The assessments examine infrastructure vulnerabilities, interdependencies, capability gaps, and the consequences of their disruption.
- Vulnerability assessments, combined with infrastructure planning resources developed through the Infrastructure Development and Recovery program, forms an integrated planning and assessment capability.
- This suite of capabilities, methods, and tools support the efficient and effective use of resources to enhance critical infrastructure resilience to all hazards.
- More information about these assessments can be found at: https://www.cisa.gov/critical-infrastructure-vulnerability-assessments

Recommendations – Information Sharing

- **Industry Information Sharing** – Join industry Information Sharing and Analysis Center (ISACs).
- **Federal Information Sharing** – CISA, FBI, NIST, ICS CERT, US-CERT, Etc.
- **State Information Sharing** – State Fusion Centers, State Emergency Operations Centers, State Agencies, etc.
- **Law Enforcement Information Sharing** – Create information sharing partnerships with federal, state, and local law enforcement.
- **Industry Information Sharing** – Create and maintain communications and collaboration between industry partners.
- **Information Consolidation** – Infuse intelligence information into your threat/incident management systems.

Recommendations – Threat Intelligence



- **Threat Analysis** – Understand your risks and vulnerabilities and compare that to the threat landscape.
- **Dark Web Analysis** – Hire/procure Dark Web Analysts/Services to scan the dark web for any threat information that could impact your organization.
- **Threat Intelligence** – Complete strategic intelligence on threats and actors before attacks on the network.
- **Threat Planning** – Develop security-minded plans to address “known/unknowns” as attackers continue to find and utilize new attack vectors.
- **Threat Detection and Prevention** – Enhance your IT/OT threat management capabilities (Incident Detection Systems (IDS), Incident Prevention Systems (IPS), Security Information and Event Management (SIEM), Advanced Persistent Threat Detection (APTD), etc..

Recommendations – Automated Threat Tools (ATT)

Planning & Direction

Planning and Direction Documents

- **Priority Intelligence Requirements**
- **Cyber Risks/Threats**
- **Intelligence Use Cases**
- **Threat Escalation Matrix**
- **Server and Desktop Targets**
- **Stakeholder Requirements**
- **Business Requirements**
- **Data Sharing Requirements**
- **Rules of Engagement**
- **Non-Disclosure Agreements**
- **Service Level Agreements**
- **Risk Management Agreements**
- **Automated Services & Bots**
- **SIS, Scada, ICS, IoT Services**

Data Collection

News Media ABC, BBC, CBS, CNN, Fox, NBC, Etc.	**Vulnerability Scans** Nessus, NexPose, Nmap, Tenable, etc.
Paid Threat Feeds AlienVault, Cyveilance, EmergingThreats, FireEye, etc.	**Data Leak Monitoring** Wikileaks, Darknet, Ransom Leaks, Pastebin, Etc.
Industry Reports Verizon, CISCO, E-ISAC, Gas-ISAC, FBI PINs, CISA Alerts, etc.	**Threat Sharing** Mandiant, LookingGlass, ThreatConnect, CrowdStrike, etc.
Cyber Media Bleeping Comp, Hacking News SANS, ICS, Dark Reading	**Social Media Monitoring** Facebook, YouTube, Instagram, etc.
Security Incidents Helpdesk Tickets, ISAC Alerts, etc.	**Darkweb Monitoring** Hacker Forums, Darknet Market Place, Darknet Chats, etc.
Phishing Intel PhishStats, PhishTank, OpenPhish, Email Spam Filters, Phishing Exercises, etc.	**Threat Gathering Intel** Honeypots, Tarpits, Deception Tech, etc.
Brand Monitoring Brand24, Google Alerts, Brandwatch, Hootsuite, etc.	**AppStore Monitoring** Monitoring Google Play and Apple Store

Processing, Analysis, & Products

Contextual Enrichment

Report Formatting

ATT Production IDS/IPS Alerting, Vulnerability Reporting, etc.

Quantitative Intelligence

Qualitative Intelligence

Data Aggregation & Enrichment

Analysis & Production

Quantitative Reporting

Qualitative Reporting

Intelligence Enrichment

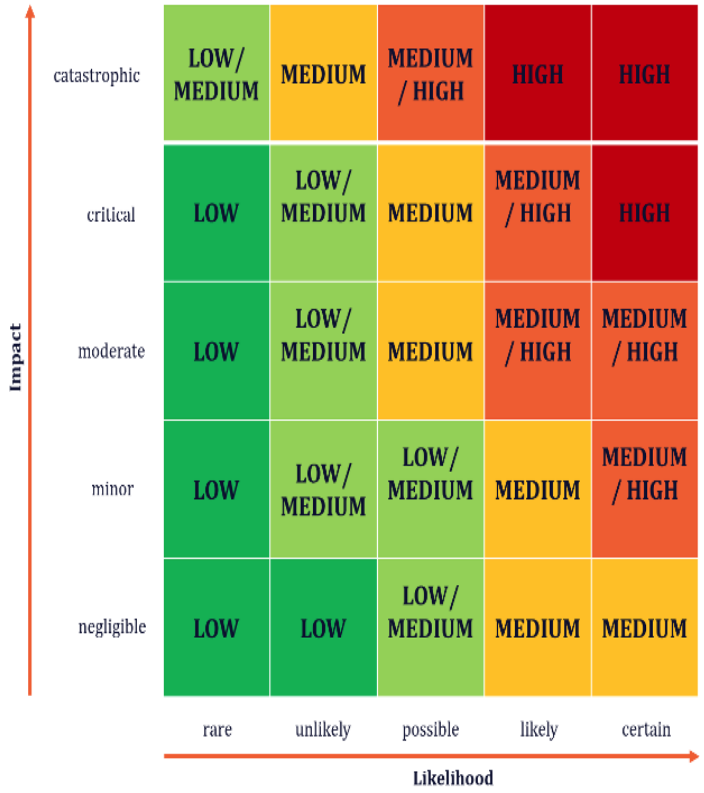
Work Flows

ATT Analysis Threat Actor Tracking, Threat Modeling, etc.

Integration & Dissemination

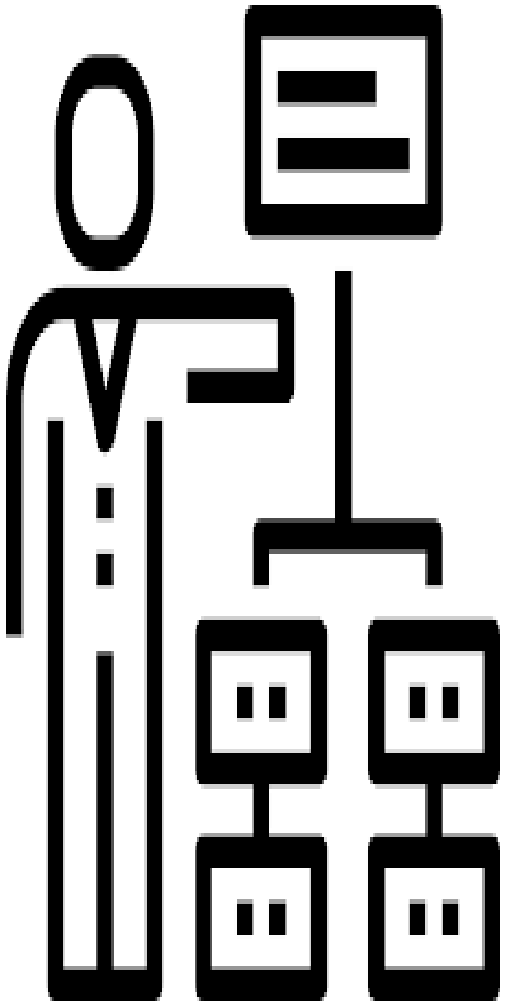
Quantitative Integration APTs, Yara, Sigma, Snort, Stix, IPs, Hashes, Domains, etc.	**External Stakeholders** ISACs, CISA, FBI, State Fusion Centers & EOCs, Supply Chain, Industry Stakeholders, etc.
Qualitative Reporting Dashboards, Strategic, Tactical, Operational, Daily, Weekly, Monthly, etc.	**Internal Stakeholders** SOC, NOC, OPS, CIRTs, CEO, CIO, CISO, Security Personnel, IT Staff, Managers, etc.

Recommendations - Risk Management



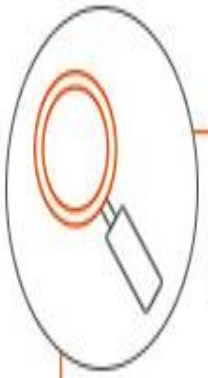
- **Create a Risk Register** – Document risks identified via audits, assessment, vulnerability/penetration scans, threat sources, physical inspections, etc.
- **Analysis** – Meet with business owners and stakeholders and rate each risk according to probability and impact. Conduct Business Impact Analysis and Cost Benefit Analysis to create risk management strategies and assign priorities and ownership for each risk.
- **Identify Risk Appetite** – Meet with the executives, governance board, business owners and stakeholders to identify how they want to address the risk that impact their organizations.
- **Risk Handling Strategies** – Define the response strategy (Accept, Remediate, Mitigate, or Transfer) and document and assign ownership of actions.
- **Dashboards and Reporting** – Develop dashboards and reports for executives, governance board, business owners, stakeholders, IT/OT Managers, supervisors, etc.
- **Briefings** – Hold regularly scheduled meetings with the organization's executives, governance board, business owners, and stakeholders to discuss the current risks and the handling status.
- **Continuous Monitoring and Improvement** – Monitor risk activities and update risk register and always look for ways to improve the process.

Recommendations - Incident Management



- **Establish a Team** – Even if your organization is small, take incident response seriously and establish a formal incident response body. If it is not possible to establish a full-time incident response team, create a virtual team with part-time staff, and give this team full authority and responsibility. This will dramatically improve your capability to respond when a cyber-attacks.
- **Create A Formal Policy** - This is a precursor to the incident response plan which lays out the organizational framework for incident response. The policy specifies what is considered a security incident, who is responsible for incident response, roles and responsibilities, documentation and reporting requirements.
- **Create a Plan** – An incident response plan is not merely a list of steps to perform when an incident happens. It is a roadmap for the organization's incident response program, including short/long-term goals, metrics for measuring success, training and job requirements for incident response roles.
- **Develop Procedures** – These are the detailed steps incident response teams will use to respond to an incident. They should be based on the incident response policy and plan and should address all five phases of the incident response lifecycle.

Recommendations - Incident Response Lifecycle

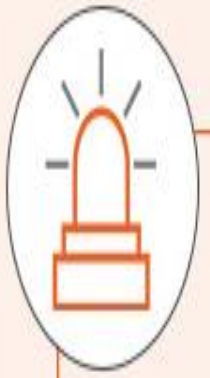


IDENTIFY

1. Asset Management
2. Business Environment
3. Governance
4. Risk Assessment
5. Risk Management Strategy

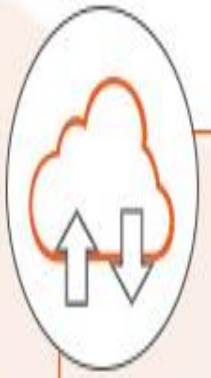
PROTECT

1. Access Control
2. Awareness and Training
3. Data Security
4. Info Protection Processes & Procedures
5. Maintenance
6. Protective Technology



DETECT

1. Anomalies & Events
2. Continuous Monitoring
3. Detection Process



RESPOND

1. Response Planning
2. Communications
3. Analysis
4. Mitigation
5. Improvements

RECOVER

1. Recovery Planning
2. Improvements
3. Communications

Recommendations - Reporting Cyber Incidents

On March 15, 2022, President Joe Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act. The act requires owners and operators of critical infrastructure to report certain cyber incidents to the Cybersecurity and Infrastructure Security Agency within 72 hours; and to report ransomware payments within 24 hours.

If your company has been the victim of a cybercrime, notify the appropriate regional FBI office. The FBI has two field offices in Pennsylvania, one in Pittsburgh and the other in Philadelphia. The FBI may be able to assist critical infrastructure owner/operators when there is a cyberattack or suspected cyber incident. The FBI regional offices are located in Pittsburgh and Philadelphia. The Pittsburgh Office number is 412-432-4000 and the Philadelphia Office number is 215-418-4000.

You can also report incidents to the Pennsylvania Criminal Intelligence Center (PaCIC). PaCIC is the primary All-Hazards Fusion Center for the Commonwealth of Pennsylvania. PaCIC coordinates the intake, processing and dissemination of intelligence and analysis concerning all threats and hazards to the commonwealth. You can contact PaCIC at 1-888-292-1919 or email at tips@pa.gov.

Cybersecurity Incident Reporting (52 Pa. Code § § 57.11(b)(4), 59.11(b)(5), and 65.2(b)(4)) – These regulations require jurisdictional electric, natural gas, water and wastewater 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. The PUC's AREP can be reached at 717-941-0003.

Questions and Answers

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
www.puc.pa.gov |Consumer Hotline 1-800-692-7380