



 Insurance

Environmental risks: cyber security and critical industries

An environmental white paper



Imagine if you came into work Monday morning to discover your firm suffered an information security incident.

The company springs into action to minimize potential damages to customers, employees, shareholders and others. A quick, effective response helps you avoid negative publicity, lawsuits and regulatory inquiries.

This scenario is bad enough, but now imagine you are an operations or environmental manager and arrive at your job to find that an on-going pipeline release had been occurring undetected over the weekend because someone hacked your computer system and disabled your leak detection alarms. Your Internet-based systems could have detected and quickly stopped this release, but now it is an environmental catastrophe. Over the next few days you realize the far-reaching consequences of an unsecure computer server include emergency response and environmental remediation expenses, regulatory agency fines and penalties, third party bodily injury and property damage claims, and a public relations nightmare. Business interruption is projected to be significant because forensic cyber specialists must be hired to review your computer systems to help restore operations. The future of your company and your job hang in the balance.

Most people associate cyber incidents with identity theft, loss of assets/money, and theft of company proprietary data, patents, and sensitive information. However, today the business world and technologies advance so rapidly that threats continue to change and expand seemingly daily. Computer system hacking, denial of service attacks, malware, ransomware, data selling, identity theft,

and trading of sensitive information incidents continue to make headlines. These crimes can even extend to corporate spying, state espionage, cyberterrorism, and cyber warfare. This increased public awareness, along with government and regulatory cyber initiatives, should leave little doubt that many critical industries have existing and emerging risks and exposures.

Cyber security along with physical security is vital to critical industries such as: energy, transportation, telecommunications, financial services, energy production and transmission, public services/utilities, and chemical and manufacturing industries. Most businesses have some vulnerability to a cyber incident, but particularly if they rely on complex supervisory control and data acquisition (SCADA) systems.

This paper examines the various types of cyber intrusions and attacks and how they can pose a significant pollution liability risk. Cyber crime can result in loss of control of critical equipment and warning systems and has the potential to cause damage to human health and the environment from catastrophic spills, waste discharges, and air emissions. These events can cause fires, explosions and hazardous material releases that result in bodily injury, property damage, environmental remediation expense, and significant legal liability claims. The paper concludes with guidance on best management practices, risk management controls, prevention steps, and essential elements of a cyber security program.

Is it cyber crime or cyber terrorism? 2

Critical industries 3

Historic incidents 4

How are attacks performed? 5

Vulnerable areas of critical systems 6

Emerging risks 8

Prevention and guidance 9

Cyber security programs and awareness training 10

Conclusion 11

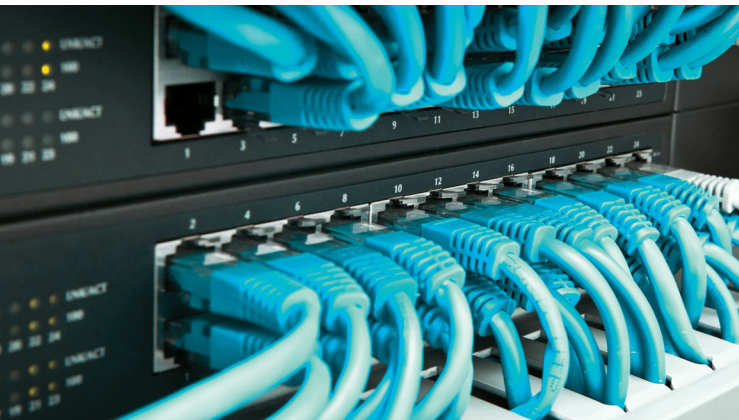
References 12

Is it cyber crime or cyber terrorism?

Terms such as cyber crime and cyber terrorism seem to be interchangeable and somewhat confusing. Providing some general definitions and examples will help with understanding these emerging and evolving cyber security threats.

Cyber crime is generally defined as a crime in which a computer is the target (hacking, phishing, spamming, etc.) or is used as a tool to commit an offense. Generally, cyber crimes fall into one of three categories depending on whether they involve, people, property, or the government.

One of the most common cyber crimes in the news these days are ransomware attacks, particularly on municipalities, where the criminal installs a virus that encrypts files or otherwise damages computer systems. To restore the system, the criminal requires an electronic payment by a deadline and often increases the ransom if the deadline is not met. A recent study cites an average cost of \$338,000 for ransomware attacks on municipalities, including estimated downtime costs that can be five to ten times the cost of the actual ransom.



Cyber terrorism has a variety of definitions. The FBI defines terrorism as the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. Cyber terrorism is defined more specifically as using computing resources to intimidate, coerce or otherwise harm others.

Broadly, cyber terrorism uses the internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation. Cyber terrorist activities can include deliberate, large-scale disruption of computer networks, especially of personal computers connected to the Internet, using tools such as computer viruses or worms, phishing e-mails, or insertion of malicious programming scripts, software or hardware.

A simple example of cyber terrorism could be hacking into a hospital computer system and changing a notable person's medicine prescription to a lethal dosage as an act of revenge. It sounds farfetched, but these things can and do happen.

Differentiating between cyber crime and cyber terrorism can be difficult, but both types of incidents can have devastating effects. Consider a cyber crime involving a ransomware attack on an industrial facility, but with the hacker also having the ability to use the same computer system to retaliate for a late ransom payment. Retaliation could include something as dramatic as causing a release of hazardous chemicals that threatens loss of life or causes pollution of the surrounding environment. This is a clearly a cyber crime, but if done in conjunction with a political ideology or to illicit a social response, it may be defined as cyber terrorism.

Critical industries

Almost any industrial facility that stores or handles large amounts of chemicals, including extremely hazardous substances, and uses computer controls or monitoring could be vulnerable to a cyber attack.

In 2018, the United States Department of Homeland Security (DHS) created the Cybersecurity and Infrastructure Security Agency (CISA) that cites protecting critical industries and infrastructure as one of its missions. DHS defines critical infrastructure as the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on physical or economic security or public health or safety. CISA identifies the following critical infrastructure sectors:

- Chemical
- Commercial facilities
- Communications
- Critical manufacturing
- Dams
- Defense industrial base
- Emergency services
- Energy
- Financial services
- Food and agriculture
- Government facilities
- Health care & public health
- Information technology
- Nuclear reactors, materials & waste
- Transportation systems
- Water

Within these categories, there are numerous types of specific facilities (refineries, bulk storage facilities, pipelines, power plants, wastewater treatment plants, etc.) that can have pollution exposures from a cyber attack.

CISA partners in their mission with both the public and private sectors to help organizations better manage risk and increase resilience using all available resources, whether provided by the Federal Government, commercial vendors, or their own capabilities. CISA notes that the current threats faced — digital and physical, man-made, technological, and natural—are more complex, and the threat factors more diverse, than at any point in history.

For critical systems, the ultimate consequences of a cyber attack generally involve one of the following four areas:

Area	Description
Loss of confidentiality	Loss of information, critical data, customer information, financial data, etc.
Loss of integrity	The critical system is in operation, but the company cannot control the system or the process; i.e., someone external to the company/entity is controlling the system
Loss of availability	Denial of Service type attack, where system becomes inoperative or ineffective
Destruction of system	Destruction of system with inability to restore

Historic incidents

Whether it is a cyber crime or cyber terrorism (intent to cause damage), attacks on larger entities have the potential to damage human health and the environment with wide reaching impacts.

Cyber vulnerabilities first began being prominently reported in the 1990s and 2000s as business and industry began relying more heavily on Internet based systems. As soon as widespread use of the Internet began, so too did attacks. Some of the early incidents reported involved loss of water distribution system controls, airport operations disruption, untreated sewage release, natural gas pipeline control room operations disruption, electric power generation failure, and oil rig leak detection systems.

The frequency and scope of cyber attacks and exploitation has continued to increase over the past ten years all around the world. More recent events include:

2014 <ul style="list-style-type: none">● A cyber attack against a German steel mill's industrial control system caused substantial damage to the blast furnace.	2015 <ul style="list-style-type: none">● A cyber attack against the power grid in Ukraine switched off 30 substations, leaving 230,000 people without power for up to six hours. The attack included seizing SCADA systems, disabling/destroying IT infrastructure components (uninterruptible power supplies, modems, RTUs, commutators), destroying hardware, and launching denial of service attacks on call centers.	2017 <ul style="list-style-type: none">● A cyber attack against a Saudi Arabian petrochemical plant, where the intention was to sabotage the firm's operations and trigger an explosion. Investigators said the only thing that prevented an explosion was an error in attacker's computer code that inadvertently shut down the plant's production systems.● Proof of concept cyber attack against dozens of US power companies, where data and critical systems were compromised to the point where they could have been sabotaged and had power shut down. Hacked systems details included company operations, engineering plans and equipment, and possible control of valves, pipes or conveyer belts. It is believed the purpose of the attack was to prove that whatever government or organization was behind the attacks was capable of having such potential impacts. It is the initial attacks that were launched using email phishing campaigns.	2018 <ul style="list-style-type: none">● A combined phishing and ransomware attack on the City of Atlanta occurred and was quickly recognized. The attack stopped people from accessing applications to pay bills and access court related documents. The city had to shut down many digital services such as its court system database and the Atlanta International Airport Wi-Fi.	2019 <ul style="list-style-type: none">● Employees at over 200 oil & gas machinery companies around the globe were targeted with attempts to steal corporate secrets and erase data from computers.
--	---	--	---	--

There are likely many more incidents that are not publicly reported. However, just this brief listing of cyber crimes and cyber attacks quickly illustrates the gravity of such events. Similar attacks have been occurring for over 20 years with a wide range of impacts.

Experts say that it is not a matter of "if" but "when" a successful cyber attack against a utility will cause widespread damage. In 2016, there were at least 245 cyber attacks against energy organizations. A recent survey of 400 executives and IT professionals in the energy, oil, gas, and utility industries found there is widespread agreement about the potential for cyber attacks. Of those responding, 94% indicated their organization has been a target of cyber-criminals, and 83% believed such an attack could cause serious physical harm.

How are attacks performed?

As previously noted, cyber crimes and terrorism are performed in various ways from spoofing to phishing to malware and denial of service. Cyber security experts know the subtle differences between these techniques, but in general it is helpful to think of them in terms of opportunist attacks versus targeted attacks. Most attacks through the Internet consist of opportunistic attacks rather than attacks targeted for a specific person or entity.

An opportunistic attack is when an attacker targets different people or companies by using one or more generic, indiscriminate ways to attack in the hope that some will be vulnerable.


In an opportunistic attack, an attacker will have a large number of targets and will not care who the victim is, but rather how many victims can be impacted. Methods include mass scanning for vulnerable services/servers. This involves written code designed to automatically search the Internet and find devices, services, or servers that are not adequately protected and can be accessed by a hacker.

A targeted attack is much more effective and damaging for the victim since the actions performed by the hacker are tailored to the intended target. This means that it is much more difficult to stop a targeted attack than an opportunistic one simply because the attacks themselves are not general. Targeted attacks may include the following: Industrial Espionage, Publicity Attacks, Malicious Insiders, and Personal Attacks.

Due to the increasing use of cloud computing and Internet applications to perform business functions and communications, companies have become more vulnerable to cyber security breaches.

There are several common areas where firms must be vigilant about their security in order to prevent or deter a cyber attack and these vulnerabilities include:

- Malware - hostile or malicious software used to create disruptions and gather sensitive information.
- Wireless connections with unsecured networks - gaps in or no security in public WIFI networks.
- Social engineering - phishing and e-mail based attacks
- USB devices - drives and devices with infected software that is downloaded onto an unsuspecting user's PC or network.
- Inappropriate computer network connections - clicking on unknown or unsecure web links to access company information instead of operating in a virtual private network (VPN), which is a widely used best practice.
- Data storage/data security – data compromises can occur from internal employee practices that create vulnerabilities to external stealing of unencrypted data.
- Physical security - a firm must ensure the physical security of computer backups, data tapes, etc., especially when it is moved off-site to remote storage locations.



Experts say that it is not a matter of “if” but “when” a successful cyber attack against a utility will cause widespread damage.

Vulnerable areas of critical systems

As the “Internet of Things” continues to expand, cyber security continues to grow more critical. Vulnerabilities highlight the need for environmental and operations staff to work together in identifying worst case scenarios and the operational systems that are most vital in preventing a pollution event. Only then can they work with IT security professionals to address the exposures. The following are some examples of key vulnerabilities and systems associated with several critical industries.

Pipelines and oil & gas production

Pipelines can be very vulnerable to cyber attack based on their extensive use of SCADA systems to remotely operate the pipeline, control inputs and outputs, and perform critical leak detection. Threats to SCADA may come not only in the form of physical terrorism, but from general Internet threats, (phishing, hackers), errors resulting from ineffective training programs, or even disgruntled employees.

Pipeline operators must be cognizant about the continuously increasing number of operational Information Communication and Technology (ICT) infrastructure elements (e.g. SCADA devices). Pipeline system equipment and monitoring systems are often connected to the Internet, but may lack appropriate security such as strong password protections. Some systems have no real need to be connected to the Internet and are being unnecessarily subjected to security threats.

While not a petroleum pipeline, the Maroochy Water System cyber attack clearly illustrates the potential impacts from a pipeline and treatment system. This Australian utility was the target of a disgruntled job applicant, who used a wireless system to gain access to the Maroochy sewage system. This hacker caused 800,000 liters of raw sewage to spill into local parks, rivers and even the grounds of a Hyatt Regency hotel. “Marine life died, the creek water turned black and the stench was unbearable for residents,” said a representative of the Australian Environmental Protection Agency.

Refineries, manufacturing and chemical production

These industries make extensive use of Distributed Control Systems (DCSs) and Programmable Logic Controllers (PLCs) that can be vulnerable to cyber attack. Control of DCSs and PLCs by an outsider can lead to severe consequences including fire, explosion or environmental release. Care must be taken to prevent access to both the industrial equipment computer systems as well as to ensure the physical security of the devices and assets being controlled or monitored. Further, increased security measures are needed as plant industrial control systems (ICSs) become more integrated with other potentially vulnerable corporate computer systems.

Certain “high risk” petrochemical facilities present an opportunity for massive civilian and environmental impacts from domestic and foreign terrorist attacks. This includes cyber attacks. The world knows all too well that loss of operational control can lead to airborne release of extremely hazardous substances. One of the most notorious air emission catastrophes, the devastating 1984 methyl isocyanate release in Bhopal, India, led to worldwide re-evaluation of process safety management and release risk management plans.

Many operators of DCS systems believe that they are isolated from cyber threats as these systems are not connected to the Internet but this is often not so. Cyber criminals can use Remote Access Tools (RATs) to gain access to DCS systems that were thought to be secure. By hacking into the computer networks behind ICS’s, an adversary can potentially reprogram commands for the equipment to operate at unsafe speeds, valves to open when they should remain closed, or allow temperatures and pressures to move into unsafe ranges.

Any industrial or commercial organization that uses DCS systems is potentially vulnerable. This was highlighted by a cyber attack on the Saudi Aramco Network in August 2012, which was fortunately detected and their internal network shutdown before any extensive damage occurred. The hackers attacked this state-owned oil company with a virus intended to erase 75% of data on its corporate personal computers. Once the virus had effectively damaged the internal network, it was designed to force the company to cut Internet connections to oil rigs, terminals, and pipelines.

Marine systems

A single tanker accident can result in release of millions of gallons of crude oil that causes an environmental disaster and long lasting natural resource damages. Maritime activity has long relied on GPS technology, but is also increasingly relying on ICT to meet the demands of customers and provide transportation safety. ICT is used to deliver and optimize operations that include ship propulsion, navigation, freight management, traffic control, predictive maintenance and communications.

The vulnerabilities created by security gaps in ICT systems within the maritime sector can also introduce risk to other commonly shared infrastructure and systems. Ship to shore pipelines and bulk storage systems can also be exposed. Systems used to manage and treat oily bilge water can also be vulnerable.



A simple example, although it did not result in a pollution incident, occurred during a labor strike in 2002 in eastern Venezuela. Hackers were able to penetrate the SCADA system responsible for tanker loading at a marine terminal. Once inside, the hackers erased the programs in the PLCs operating the facility and prevented tanker loading for eight hours.

Water/waste water and electric utilities

An attack on the SCADA system used in water treatment and distribution systems can significantly alter the system's performance and negatively impact public health and safety. In 2007 a faulty chemical control system and alarm at a water treatment facility in Massachusetts caused a release of excess sodium hydroxide into the water supply, ultimately injuring more than 100 people. Wastewater treatment facilities are vulnerable to cyber attacks that could cause releases of raw sewage or inadequately treated effluent.

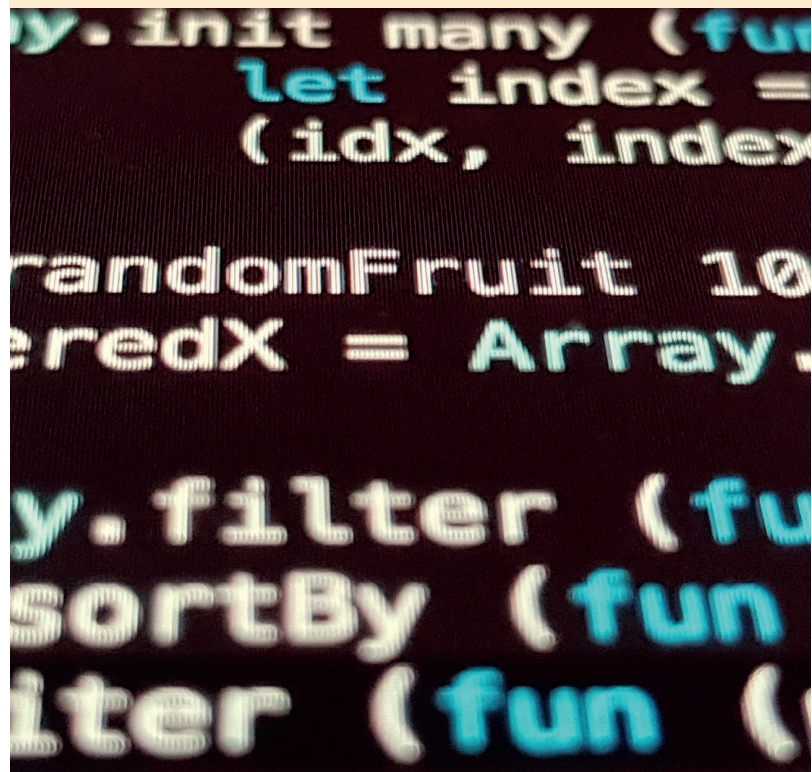
Electric utilities are also prime targets because of the high visibility and wide-ranging impacts associated with power outages. The US national power grid as a whole has known significant potential weaknesses. These vulnerabilities can result in loss of power at industrial facilities with critical systems. As noted, lack of emergency power and/or uninterruptable power supplies can lead to pollution events.

Transportation and other systems

In addition to marine transportation, air transport has also proven to be vulnerable to cyber security breaches. Airports continue to assess their security needs beyond passenger screening as noted in the US Transportation Security Administration Roadmap for Aviation Cybersecurity. Other critical transportation systems that have the potential to be compromised by include highway and rail cameras, signals, and monitoring/control systems.

There are many other systems present in most modern buildings with electronic controls that can be vulnerable to a cyber attack. These include utility systems such as HVAC, plumbing, water supply, sewer, electricity, as well as electronic security systems. These systems present exposures that could result in accidents and releases of hazardous materials.

Vulnerabilities highlight the need for environmental and operations staff to work together in identifying worst case scenarios and the operational systems that are most vital in preventing a pollution event.



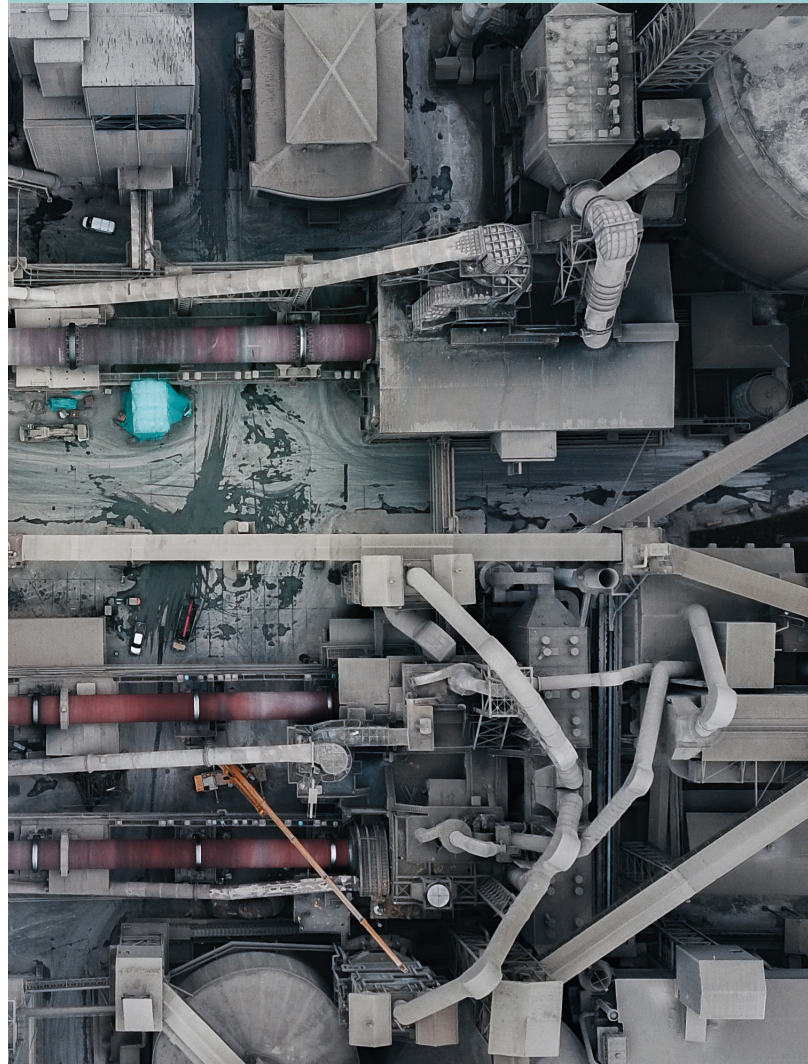
Emerging risks

Cybersecurity exposures for all businesses will continue to evolve and increase over time. Some of the emerging risks that are likely to become more prominent include:

- **5G technology** – New 5G digital networks have already been installed in some areas and are anticipated to be built out in additional market areas in ways that will transform the world. Standards and processes for acceptable 5G system cybersecurity are still being established. Risks will continue to emerge from the unintended introduction of network vulnerabilities in development of new software applications and updates. These larger networks will also be more at risk since more devices will be connected under 5G and the impacts could be more widespread. Also, there is a risk of legacy vulnerabilities in 4G LTE networks that will initially be integrated with 5G networks.
- **Cloud services** – Data security management whether in transmission or at rest in storage is critical. Adequate encryption of data at all times along with penetration testing is essential.
- **Autonomous vehicles and drones** – These technologies are heavily dependent on automation and will present important cyber security concerns and require advance controls.
- **Artificial intelligence** – Advances in, and maturing of, AI use may result in increases in vulnerability to attacks. Defense of facility systems and operations will need to include both software and hardware that rely on AI.
- **Internet of Things (IoT)/Industrial Internet of Things** – Internet capable devices are projected to increase from an estimated 11 to 13 billion in 2013 to 200 billion in 2020. Various organizations are evaluating this area and need to develop additional standards. This includes the energy, manufacturing, healthcare, and transportation sectors.

Recent cyber security statistics from 2019 highlight some important trends and vulnerabilities:

- IoT attacks up by 600% in 2017
- 350% increase in ransomware attacks annually
- 65% of companies with > 500 employees have staff, who have never changed their password
- 95% of cybersecurity breaches are due to human error
- 31% of organizations have experienced cyber attacks on operational infrastructure
- 75% of the healthcare industry was infected with malware at least once
- Approximately 50% of the cyber security exposure risk can be attributed to using multiple security vendors, equipment, and services



Prevention and guidance

In April 2007, the DHS issued Chemical Facility Antiterrorism Standards (CFATS) that comprised the first US regulatory program focused specifically on security in a high risk sector: chemical facilities. CISA now manages the CFATS program, which has been extended at least through mid-2020. They work with facilities to ensure security measures are in place to reduce the risks from certain hazardous chemicals and prevent them from being exploited in a terrorist attack.

Facilities subject to CFATS must conduct a security vulnerability assessment and implement security measures that meet risk-based performance standards (RBPS), which cover such areas as perimeter security, access control, personnel authorization and cyber security. The program emphasizes the need for:

- Appointment of a cyber security officer
- Managing access control to company computer systems (i.e., controls on what devices employees, vendors, and customers can connect to the system)
- Effective password management
- Setting appropriate levels of system access for each user
- Effective and recurring training and awareness
- System monitoring and incident management
- Life cycle and configuration management
- Layered computer security

More recently, CISA developed a Cyber Security Advisor (CSA) Program to provide coordination and outreach in the protection of cyber components of critical infrastructure. CISA also developed Cybersecurity Framework Function Areas and sector-specific guidance for all six critical infrastructure sectors that the DHS has responsibility for: Chemical, Commercial Facilities, Critical Manufacturing, Dams, Emergency Services, and Nuclear. Their regional advisors are available to help the public and private sectors secure their networks.

Their guidance provides the following general outline for development and implementation of a cyber security program:

- **Identify** – establish the organizational structure to manage cyber security risk to systems, assets, data, and capabilities
- **Protect** – create safeguards to ensure delivery of critical infrastructure services
- **Detect** – perform activities to identify the occurrence of a cyber security event
- **Respond** – develop actions in the event of a detected cyber security event
- **Recover** – implement activities that maintain plans and enhance resilience and restore impaired company capabilities or services

Staying informed, sharing information and acting on general industry cyber vulnerabilities as they are discovered is another key component of a prevention program. CISA is also charged with coordinating reports and disclosure of cyber vulnerabilities with affected suppliers of industrial control systems and information technology products. They help prioritize and develop appropriate timeframes for mitigation based on the potential for on-going active exploitation, threat level, and other situations. Sharing cyber vulnerability information must take into account the following:

- Whether the vulnerability has been publicly disclosed
- Severity of vulnerability
- Potential impact to critical infrastructure
- Possible threat to public health and safety
- Immediate mitigation actions available
- Vendor/supplier responsiveness
- Feasibility of creating an upgrade or patch
- Time required for technology users to obtain, test and implement a patch

These risk factors should be embraced by industry as they attempt to quantify their own company's exposure. Once cyber security issues are identified, CISA outlines five key steps for vulnerability remediation: Detection/Collection, Analysis, Mitigation Coordination, Application of Mitigation and Disclosure. CISA helps coordinate this final critical disclosure/sharing step with end users of vulnerable technologies via multiple channels.

Cyber security programs and awareness training

It is important to remember that cyber security, like all security, is a process, not a product. Cyber security must be an on-going action by all employees and contractors of a company/entity. Many companies have internal IT security departments, training, and vendor assisted programs to raise awareness of the potential types of cyber attacks and to provide clear guidance on reporting suspicious activity. Further, there are now cyber security journals, training programs, college degree programs, and government information available as resources that can help industry stay current with trends and threats.

A literature search reveals a limited number of readily available cyber security sample programs (likely due to the sensitivity of the subject matter). However, some public entities and organizations have developed templates and/or guidance for their membership. For example, a sample plan template can be obtained from the National Rural Electric Cooperative Association. Additional resources, especially useful for protecting SCADA and DCS systems, are available from industry associations such as the International Society of Automation (www.isa.org) and other manufacturers of industrial control systems.

The Cyber Readiness Institute (CRI) is another resource that was launched in July 2017 by senior leaders in government, industry, and cyber security. They provide information and resources to small and mid-level companies to assist with cyber security. Cyber security prevention guidance has been created by the National Institute of Standards and Technology (NIST) Computer Security Resource Center, who has created a Cyber Security Framework (CSF) and various other cyber security publications. The CSF program incorporates existing consensus-based standards to:

- Identify existing cyber security standards, guidelines, frameworks, and best practices that will increase the security of critical infrastructure
- Specify high-priority gaps where new or revised standards are needed
- Collaboratively develop action plans to close these cyber gaps.

This guidance is intended to evolve by incorporating new standards/procedures as they are developed. Additional information is available at: <http://csrc.nist.gov/>

Further, CISA also developed a Critical Infrastructure Cyber Community Voluntary Program (C3VP) to support cyber resilience, increase awareness of exposures, and provide a framework for improving critical infrastructure cyber security. This public-private partnership provides existing resources to assist with implementation of the NIST Cyber Security Framework as part of a comprehensive enterprise risk management program. Companies should take care to verify the accuracy of cyber security related information and any Internet provided guidance. It is best to have direct interaction with vendors, suppliers and outside consultants to better evaluate capabilities and experience.

For an independent evaluation, it is highly recommended that companies retain a qualified cyber security consulting firm with relevant industry experience prior to developing and implementing a new cyber security program. These firms are more likely to be able to identify vulnerabilities and emerging threats than in-house efforts.

In addition to a plan, companies need to develop and implement awareness training on company policies and procedures as these are developed. Refresher training and system tests/response (i.e. fake phishing drills, etc.) are warranted to reinforce computer security concepts. Systems also need to be in place to assess the effectiveness of plans and training.



Conclusion

An attitude of “it can’t happen to us” can be very detrimental to a company, its employees, and stakeholders. All industries and businesses, especially critical infrastructure and other sensitive industries, must continue to be highly cognizant of the detrimental and potentially devastating effects a cyber attack can have on an organization. This includes catastrophic environmental impacts, fires, explosions and other consequences that are possible from a single cyber attack and can result in business interruption, reputational impacts, significant financial loss, and regulatory actions/enforcement.

Businesses must ask the questions: When will it happen? Has it already occurred? and How do we prevent it? Firms also need to recognize that cyber security is not just “an IT Department problem”, but a problem for the whole company and everyone doing business with the company.

There is no cook book or “off the shelf” prevention template with blanks to be filled in for critical industry cyber security. In-depth analysis of the critical industry’s operations, equipment, procedures, physical security and personnel must be performed to develop a security program tailored to deter and manage exposures.

To combat or minimize potentially negative outcomes, each firm needs to take cyber security seriously and develop and implement robust cyber security measures. This should include initial and periodic vulnerability assessments, awareness training and on-going prevention and monitoring programs. Much like any safety or security program, a penny of prevention may be worth millions in a cure.

An attitude of “it can’t happen to us” can be very detrimental to a company, its employees, and stakeholders.

At a minimum, a company’s cyber security program should include:

- Program management
- Planning
- Awareness training/
procedures training/
notification training
- Configuration management
- Firewalls
- Content filtering
- Intrusion prevention systems
- Patch management systems
- Penetration testing and
security auditing
- Quick response/
quick response team
- Security assessment
- Risk assessment
- Physical protection of
assets and personnel
- Contingency planning
- Security system management/
oversight programs
- Connectivity (protection
of businesses, systems,
and control systems
with the Internet.)
- Vulnerability assessment
- Implement action plan

References

- 15 Alarming Cyber Security Facts and Stats; Cybint; September 23, 2019; <https://www.cybintsolutions.com/cyber-security-facts-stats/>
- An Introduction to Computer Security – The NIST Handbook (Special Publication 800-12); National Institute of Standards (NIST); October 1995; <https://csrc.nist.gov/publications/detail/sp/800-12/archive/1995-10-02>
- Attacks Targeting Oil and Gas Sector Renew Questions About Cybersecurity; Hutchins – Hunton Andrews Kurth; April 13, 2018; <https://www.pipelinelaw.com/2018/04/13/attacks-targeting-oil-and-gas-sector-renew-questions-about-cybersecurity/>
- Can Taxpayers Spare \$338,700? That's the Price of a Public Sector Ransomware Attack, Joel Berg, October 7, 2019. <https://riskandinsurance.com/can-taxpayers-spare-338700-thats-the-price-of-a-public-sector-ransomware-attack/>
- Chemical Facility Anti-Terrorism Standards; CISA; November 2019; <https://www.dhs.gov/cisa/chemical-facility-anti-terrorism-standards>
- Chemical Sector Cybersecurity Framework Implementation Guidance; Department of Homeland Security; 2015; https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/chemical-framework-implementation-guide-2015-508.pdf
- CISA Vulnerability Disclosure Policy – CISA; 2019; <https://www.us-cert.gov/vulnerability-disclosure-policy>
- Control System Security Meets Modern Threats; Pipeline & Gas Journal; October 2015; <https://pgjonline.com/magazine/2015/october-2015-vol-242-no-10/features/control-system-security-meets-modern-threats>
- Cyber Defense Magazine; July 2019; <https://www.cyberdefensemagazine.com/>
- Cyber Security and the Pipeline Control System; Byres - Tofinosecurity; Pipeline and Gas Journal; February 2009; https://www.tofinosecurity.com/sites/default/files/Cyber_Security_and_The_Pipeline_PGJ_Feb_2009.pdf
- Cyber Security Planning Guide; Federal Communications Commission; November 17, 2012; <http://transition.fcc.gov/cyber/cyberplanner.pdf>
- Cyber Security Programs for Nuclear Facilities; US Nuclear Regulatory Commission; January 2010; <http://pbadupws.nrc.gov/docs/ML0903/ML090340159.pdf>
- Cybercrime and Utilities: Preparing for an Attack; Pipeline and Gas Journal; February 2016; <https://pgjonline.com/magazine/2016/february-2016-vol-243-no-2/features/cybercrime-and-utilities-preparing-for-attack>
- Cybersecurity - Solving the Complex Puzzle; Dean Fox - URS, 2013; <https://southernegas.org/index.php/section-main-page-transmission/921>
- Cyber-terrorism; Jimmy Sproles & Will Byars; 1998; <http://csciiwww.etsu.edu/gotterbarn/stdntppr>
- Entertainment Security: Managing Third Parties; ASIS International; October 2019; <https://www.asisonline.org/security-management-magazine/articles/2019/10/entertainment-security-managing-third-parties/>
- Guide To Developing A Cyber Security And Risk Mitigation Plan Template; National Rural Electric Cooperative; 2011; <https://www.smartgrid.gov/files/CyberSecurityGuideforanElectricCooperativeV11-21.pdf>
- Guide to Developing a Cyber Security and Risk Mitigation Plan; Cooperative Research Network; 2011; <https://www.smartgrid.gov/files/CyberSecurityGuideforanElectricCooperativeV11-21.pdf>
- In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back; New York Times; Nicole Perloth; October 23, 2012; <https://riskandinsurance.com/can-taxpayers-spare-338700-thats-the-price-of-a-public-sector-ransomware-attack/>
- Industrial Security; Siemens; January 2019; <https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security.html>
- Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia; Abrahms, and Weiss - The Mitre Corporation; August 2008; <https://www.mitre.org/publications/technical-papers/malicious-control-system-cyber-security-attack-case-study-maroochy-water-services-australia>
- New Technology, New Risk: Cyber Concerns For Industrial Control Systems; FM Global/Advisen; circa 2018; <https://www.advisenltd.com/wp-content/uploads/2017/07/cyber-concerns-for-industrial-control-systems-paper-2017-07-26.pdf>
- Pipeline Cybersecurity Road Map: Key Points; TSA; January 2019; <https://www.hklaw.com/es/insights/publications/2019/01/tsa-pipeline-cybersecurity-road-map-key-points>
- PLC and DCS: How do they differ & How did they come about?; Mondri Anderston; October 8, 2018; <https://www.automation.com/automation-news/article/plc-and-dcs-how-do-they-differ-how-did-they-come-about>
- Protecting Organizations from Cyber Attack; Cliff Glantz and Guy Landine – Pacific Northwest National Laboratory; 2012; https://conferences.wsu.edu/forms/emergencyprep/presentations12/F5_Cliff%20Glantz.pdf
- Protecting Water Industry Control and SCADA Systems from Cyber Attacks; Don Dickinson - Phoenix Contact; 2010; https://www.automation.com/pdf_articles/WaterIndustryCyberSecurity_final.pdf
- Rural Cooperative Cybersecurity Capabilities (RC3) Program; National Rural Electric Cooperative; 2017 and 2018; <https://www.cooperative.com/programs-services/bts/rc3/Pages/default.aspx>
- Securing The Industrial Internet of Things Draft; NIST; May 2019; <https://csrc.nist.gov/publications/detail/white-paper/2019/05/06/securing-the-iiot-scenario-based-cybersecurity-for-energy-sector/draft>
- Significant Cyber Incidents; Center For Strategic And International Studies; June 2019; <https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents>
- Solutions For Security By Design Page 6; VDMA Mining; 2019; https://mining.vdma.org/documents/105698/30836548/BoG%20VDMA%202019%20full%20issue_1554296211901.pdf/a943fd43-efb5-3272-3583-31add9895d9e
- Strengthen Your Cyber Security; Andrew Ginter - Chemical Processing; April 27, 2010; <http://www.chemicalprocessing.com/articles/2010/088/>
- Stuxnet Raises "Blowback" Risk In Cyberwar; NPR; November 2, 2011; <http://www.npr.org/2011/11/02/141908180/stuxnet-raises-blowbackrisk-in-cyberwar>
- The Value of ICT in the Maritime Industry; Silje Moan; October 16, 2019; <https://www.dualog.com/blog/the-value-of-ict-in-the-maritime-industry>
- TSA Needs To Improve Pipeline Cybersecurity GAO Says; Law360; May 2019; <https://www.law360.com/articles/1155700/tsa-needs-to-improve-pipeline-cybersecurity-gao-says>
- TSA Roadmap For Aviation Cybersecurity; Law360; December 2018; <https://www.law360.com/articles/1111007>
- US Offers \$25 Million Cybersecurity Grant After Pipeline Attacks; Collins -Bloomberg; April 17, 2018; <https://www.bloombergquint.com/business/u-s-offers-25-million-cybersecurity-grant-after-pipe-attacks> USDHS – CISA; 2019. <https://www.cisa.gov/infrastructure-security>
- What Are The Three Types Of Cyber Crimes?; Swier Law Firm; 2019; <https://www.swierlaw.com/faqs/what-are-the-three-types-of-cyber-crimes-cfm>
- Who is Responsible for the Saudi Aramco Network Attack?; INFOSEC Island; August 29, 2012; <http://www.infosecisland.com/blogview/22290-Whos-Responsible-for-the-Saudi-Aramco-Network-Attack.html>



Contact

Environmental Risk Consulting team

505 Eagleview Boulevard, Suite 100, Exton, PA 19341 USA
Phone 800 327 1414

First Canadian Place, 100 King Street West, Suite 3020
Toronto, ON M5X 1C9 Canada
Phone 416 928 5586
axaxl.com

This document shall not be construed as indicating the existence or availability under any policy of coverage for any particular type of loss or damage. The provision of any service does not imply that every possible hazard has been identified at a facility or that no other hazards exist. AXA XL Insurance does not assume, and shall have no liability for the control, correction, continuation or modification of any existing conditions or operations. We specifically disclaim any warranty or representation that compliance with any advice or recommendation in any document or other communication will make a facility or operation safe or healthful, or put it in compliance with any standard, code, law, rule or regulation. Save where expressly agreed in writing, AXA XL Insurance and its related and affiliated companies disclaim all liability for loss or damage suffered by any party arising out of or in connection with our services, including indirect or consequential loss or damage, howsoever arising. Any party who chooses to rely in any way on the contents of this document does so at their own risk.

AXA XL is a division of AXA Group providing products and services through three business groups: AXA XL Insurance, AXA XL Reinsurance and AXA XL Risk Consulting. In the US, the AXA XL insurance companies are: AXA Insurance Company, Catlin Insurance Company, Inc., Greenwich Insurance Company, Indian Harbor Insurance Company, XL Insurance America, Inc., XL Specialty Insurance Company and T.H.E. Insurance Company. In Canada, coverages are underwritten by XL Specialty Insurance Company - Canadian Branch. Coverages may also be underwritten by Lloyd's Syndicate #2003. Coverages underwritten by Lloyd's Syndicate #2003 are placed on behalf of the member of Syndicate #2003 by Catlin Canada Inc. Lloyd's ratings are independent of AXA Group. Not all of the insurers do business in all jurisdictions nor is coverage available in all jurisdictions. Information accurate as of January 2020.



axaxl.com