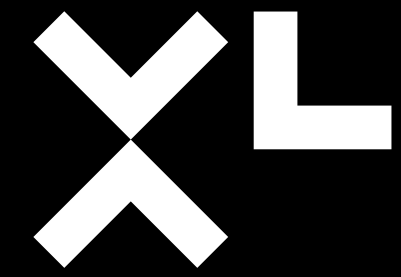
Environmental Risks: Cyber Security and Critical Industries

XL Group
Insurance



Environmental

Environmental Risks: Cyber Security and Critical Industries

Cyber security is an emerging threat to many critical industries. Cyber intrusions pose a significant threat for contaminant releases that can result in damage to human health and the environment. Cyber crimes have the potential to cause catastrophic spills, waste discharges, and air emissions that result in bodily injury, property damage, environmental remediation expense and significant legal liability claims.

Security for critical industries must now take into account cyber security as well as other "physical" aspects of security. Critical information infrastructures support vital services and goods such as: energy, transportation, telecommunications, financial services, energy production and transmission, and more. These are so essential that their unavailability may adversely affect the well-being of a company or a nation.[1] Recent federal action has included the compilation of a National Intelligence Estimate (NIE) for cyber crime and terrorism. President Obama has declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cyber security."[13] Federal Bureau of Investigation Director Mueller has stated that cyber attacks (of all forms) "...will eventually bypass terrorism as the biggest threat to national security."[39]

On February 13, 2013, President Obama issued an Executive Order to improve critical infrastructure cyber security. One of the salient activities in this order is to have the National Institute of Standards and Technology (NIST) develop a framework to reduce the cyber risks to critical infrastructure. Additionally, a cyber security bill was reintroduced in the United States Congress on the same day. The Cyber Intelligence Sharing and Information Act (CISPA) would allow private companies, intelligence agencies and the Department of Homeland Security (DHS) to share information about cyber threats with one another. The final version of the bill may also include cyber security provisions; however, it is uncertain if/when this will become law.

Recent news reports have contained an increasing amount of information about cyber security, cyber-sleuthing, and the potential for cyber warfare. The United States Naval War College's Weekly Maritime News Survey contains a cyber section that usually contains at least one item on cyber crime or cyber terrorism.[4] News topics have ranged from specific incidents involving the hacking of Twitter accounts or hacking of pipeline computer systems to broader issues involving the potential for serious international strife due to cyber espionage. This increased public awareness, along with recent Congressional and Presidential cyber initiatives, should make every critical industry acknowledge the risks and potential impacts associated with cyber security issues and a wide range of cyber attacks.

Cyber security is a growing threat. A variety of individuals and groups are using computer and network vulnerabilities to detrimentally affect the business world. Effects include: theft of assets/money; theft of company proprietary data, patents, and sensitive information; identity theft; impacts to business operations (distributed denial of services); and corporate spying/state espionage and terrorism. Cyber threats and the potential for cyber warfare exist and

sensitive industrial assets are prime targets. Malware has evolved from a nuisance into a criminal tool and a potential instrument of state-sponsored warfare and economic disruption.[3] The frequency of threats continues to escalate.

Even the United State's most secure computer networks are at risk as illustrated by the Moonlight Maze incident. Moonlight Maze refers to a previously highly classified incident in which U.S. officials accidentally discovered a pattern of probing of computer systems at the Pentagon, NASA, Energy Department, private universities, and research labs that began in March 1998 and continued for nearly two years. Sources told PBS's Frontline news program that the invaders were systematically searching through tens of thousands of files, including maps of military installations, troop configurations and military hardware designs. The Defense Department traced the trail back to a mainframe computer in the former Soviet Union, but the sponsor of the attacks remains unknown and the Russian Government denies any involvement. Moonlight Maze is still being actively investigated by U.S. intelligence agencies.

Who is performing cyber crime and cyber attacks? Many different agents including: hackers, competitors, company insiders, disgruntled employees, bored employees, organized crime, extremists, terrorists, spies and nation states.[10]

Any industry that relies heavily upon complex supervisory and control systems, such as energy, transportation, public service, and chemical manufacturing industries, is very vulnerable to cyber attack from a variety of sources.[7]

Security for critical industries must now take into account cyber security along with "physical" aspects of security.

What is the difference between Cyber Terrorism and Cyber Crime?

Cyber crimes are generally defined as: "Offenses that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as the Internet and mobile phones." In general, cyber crimes involve damage to a person's reputation or the stealing of assets or a person's identity, usually to obtain fraudulent access to computer systems to commit more crimes.

Cyber terrorism is generally defined as: "The use of Internet based attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses." In general, cyber terrorism is comprised of attacks on larger entities with the intent to cause property damage, or damage to human health and the environment that result in a large area of impact.[14]

Examples of the type of environmental, property, or theft damages that cyber crime and cyber terrorism can cause include:

- **Control of Hydro-Electric System** – In 1994, a hacker accessed the Salt River Water Project computers to gain control of water levels.[11]
- **Citibank Theft** – In 1995, millions of dollars were stolen from Citibank that ultimately resulted in very negative publicity to company.[9]
- **Airport Disruption** – In 1997, a hacker disabled the Worcester, Massachusetts Airport.[11]
- **Gas Pipeline Control** – In 2000, the Russian government announced that hackers succeeded in gaining control of the Gazprom pipeline network.[12]
- **Sewer Discharge** – In April 2000, a hacker caused the release of 800,000 liters of untreated sewage into waterways in Maroochy Shire, Australia.[8]
- **Nuclear Power Safety** – In January 2003, the safety monitoring system of Ohio's Davis-Besse nuclear power plant was offline for five hours due to the Slammer Worm.[12]
- **Server Code Theft** – In 2003, Cisco's IOS code was stolen by Huawei, a Chinese manufacturer of similar servers.[9]
- **CardSystem Secure Server Hacking** - In 2005, this credit card transaction processor, had their servers hacked. This affected VISA, Master Card, Amex and Discover, as well as their customers.[9]

- **Orbit Communications DDOS** – In 2006, this TV retailer used a distributed denial of services (DDOS) attack to cripple three competitors and cause over $2,000,000 in losses.[9]
- **Russian DDOS** – In May 2007, Estonia was subjected to a mass cyber-attack in the wake of the removal of a Russian World War II war memorial from downtown Tallinn. The attack was a DDOS attach in which selected sites were bombarded with traffic to force them offline; nearly all Estonian government ministry networks as well as two major Estonian bank networks were knocked offline.[8]
- **South American Electrical Power Disruption** – In 2008, electrical power generation in South America was damaged by a cyber attack by organized crime.
- **Attacks on Oil and Gas Platforms** – In 2009 an IT Contractor disabled leak detection alarm systems on three off shore oil rigs near Long Beach, California.[38]
- **Stuxnet** – In June 2010, this virus disabled Iranian centrifuges that were processing uranium into weapons grade uranium. The Stuxnet worm targeted nuclear industry software and equipment in Iran. Stuxnet impacted only clandestinely obtained Siemens control systems, which indicates a very narrow focus and a very capable originator.
- **Theft of Defense Secrets** – In 2011, many defense firms lost significant defense-related intellectual property in cyber attacks called "Nitro Attacks" which use a Trojan worm called "Poison Ivy".[38]
- **Theft of Secure Taxpayer Information** – In 2012, the South Carolina Department of Revenue was hacked and data from 3.8 million tax filers was removed. South Carolina has spent over $12 million in response and remedy costs to this data breach.[40]

This brief listing of cyber crimes and cyber attacks quickly illustrates that these incidents have been occurring for at least the past 20 years with a wide range of potential impacts.

Critical Industries

Many critical industries can be affected by cyber attacks, but some of the most common or higher profiles include: pipelines, refineries, petroleum terminals, marine, terminals, sewage plants, water plants, and chemical plants. Almost any industrial facility that stores or handles large amounts of chemicals and uses computer controls or monitoring is vulnerable to a cyber attack.

For critical systems, the major consequences of a cyber attack include: [10]

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 Attack System becomes inoperative or ineffective
Destruction of System	Destruction of system

Industries with environmental impact facing high risk for a cyber attack: pipelines, refineries, petroleum terminals, marine terminals, sewage plants, water plants and chemical plants.

Vulnerable Areas of Critical Systems

Pipelines

Pipelines are very vulnerable to cyber attacks due to their high reliance on SCADA (supervisory control and data acquisition) systems and computer networks. Oil and gas pipelines, globally, have been a favored target of terrorists, militant groups, and organized crime.[5] Pipelines are very vulnerable to cyber attack based on the extensive use of SCADA systems used to operate the pipeline, control inputs and outputs, and perform critical leak detection. A recent U.S. Department of Homeland Security (DHS) study noted that most SCADA systems are protected by very weak passwords that are easily compromised. Once in, a cyber attacker can gain control of the pipeline's SCADA system.[32] There is a search engine (Shodan) that cyber attackers can use to look for SCADA systems and support equipment. Note that this study also determined that many owners/ users of SCADA systems believed that their systems were not connected to the Internet, although a cyber attacker could access them via the Internet.

Pipeline operators have to be very cognizant about the continuously increasing number of port operational Information Communication and Technology (ICT) infrastructure elements (e.g. SCADA devices) connected to the Internet without appropriate security. Some systems have no real need to be connected to the Internet and are being unnecessarily subject to security threats. Threats to SCADA may come not only in the form of terrorism, but from general internet threats (e.g. worms and viruses), recreational hackers, errors resulting from ineffective training programs, or even disgruntled employees.

While not a petroleum pipeline, the cyber attack on the Maroochy Water System in Australia is very illustrative. In this case, a disgruntled job applicant used a wireless system to gain access to the Maroochy sewer system, and 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.[18]

Pipelines, oil production systems, refineries, manufacturing and chemical plants

Operations that make extensive use of Digital Control Systems (DCS) are also very vulnerable to cyber attack. The security of DCS systems will continue to grow as plant control systems become more integrated with corporate systems.[15] Control of a DCS system by an outsider can lead to severe consequences including fire, explosion or environmental release. Certain "high risk" chemical facilities present the potential for massive civilian and environmental impact from possible terrorist attacks. Release of chemicals

Most SCADA systems are protected by very weak passwords

can lead to a major catastrophe, such as the thousands of deaths that followed the leak of methyl isocyanate at a pesticide plant in Bhopal, India, in 1984.[22] By hacking into the computer networks behind the industrial control systems, an adversary could reprogram an ICS so that it commands the equipment to operate at unsafe speeds or the valves to open when they should remain closed. This is roughly the way Stuxnet was able to damage the centrifuges in Iran.[20] Care must be taken to prevent access by unwanted personnel as well as the physical security of the devices and the assets they are controlling or monitoring.[16] Any industrial or commercial organization that uses DCS systems are potentially vulnerable. This was highlighted by a cyber attack on the Saudi Aramco Network in August 2012 which was fortunately detected before any extensive damage occurred. It appears that one worm, the Slammer Worm, is the source of several incidents of process distribution and attacks on SCADA systems.[19]

Threats to pipelines continue to multiply. Supplanting the Stuxnet virus are the Duqu and Flames worms, both of which are targeted against industrial control networks.[38] Many operators of DCS systems believe that they are isolated from cyber threats as their DCS 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. Remember, Stuxnet was able to gain access to a highly secret and secure Iranian site, so if hackers want in, they can probably find a way.

Marine Systems

Maritime activity increasingly relies on ICT systems in order to optimize maritime operations. ICT is increasingly used to enable essential maritime operations, from navigation to propulsion, from freight management to traffic control communications, etc. A single tanker accident can result in a catastrophic release of millions of gallons of crude oil that causes long lasting environmental impacts. The vulnerabilities created by the security gaps in ICT systems within the maritime sector may affect not only the services supported by these systems, but also the commonly

shared infrastructure layers (e.g. databases, systems hosting sensitive information, etc.). Cargo tracking and cargo identification are increasingly subject to cyber security incidents resulting from cyber attacks or system failures.[1] During a strike in Venezuela in 2002, hackers were able to penetrate the SCADA system responsible for tanker loading at a marine terminal in eastern Venezuela. Once inside, the hackers erased the programs in the programmable logic controllers (PLCs) operating the facility, preventing tanker loading for eight hours.[19]

Water Systems/Utilities

An attack on the control and/or SCADA system used in a water treatment and distribution system can significantly alter the system's performance and negatively impact public health and safety.[31] In 2007 a faulty alarm at a water treatment facility in Spencer, Mass., caused release of excess sodium hydroxide into the water supply, ultimately injuring more than 100 people.[22] 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.

Other Systems

Other critical systems that can be severely compromised by cyber attack include building automation systems (HVAC, plumbing, water supply, sewer, electricity, etc.), traffic cams/traffic monitoring systems, red light cameras, and crematoria.[32]

Prevention and Guidance

In April 2007, the DHS, issued Chemical Facility Anti-Terrorism Standards (CFATS) that aim to ensure effective security at high-risk sites. The interim final rule (6 CFR 27) status of CFATS was reauthorized in October 2010 and the responsible subcommittee has recommended extending it further to 2015. Every affected facility 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 DHS published a RBPS guidance document in May 2009, to assist high-risk chemical facilities with selecting and implementing appropriate security measures as well as to help DHS personnel with evaluating RBPS compliance.[22] This plan emphasizes the need for:

- The appointment of a cyber security officer
- Managing access control to company computer systems (i.e., controls on what devices employees, vendors and other users can connect to the system)
- Effective password management
- Setting the appropriate level of system access for each employee

NIST is currently developing a framework to reduce cyber risks to critical infrastructure. Keep updated at: csrc.nist.gov

- Effective and recurring training and awareness
- System monitoring and incident management
- Life cycle and configuration management
- Layered computer security

As previously noted, NIST is currently developing a framework to reduce cyber risks to critical infrastructure. This framework will incorporate existing consensus-based standards in an attempt 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.

The NIST is expected to complete this work by February 2014. The Framework will be a series of voluntary standards. The Framework will be an evolving document, incorporating new standards/procedures as they are developed. Additional information on the Framework will be made available at: http://csrc.nist.gov/

How is Cyber Crime Performed?

Cyber Crime and Cyber Terrorism both take advantage of weaknesses in a company's computer systems and other security systems to gain access to the company's computer systems, networks, SCADA/DCS, and e-mail/chat. Access to any one of these pieces of computer equipment, can lead to a significant cyber crime event. A better understanding of the variety of techniques available to compromise company operations can assist in the preparation and prevention of damaging attacks. In general, attacks can be divided into Opportunist Attacks versus Targeted Attacks.

An opportunistic attack is when an attacker targets various different people or companies by using one or more generic, indiscriminant ways to attack in the hope that some will be vulnerable to attack by the means used by the hacker. 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. Most attacks on the Internet consist of opportunistic attacks rather than attacks targeted for some specific entity.[9]

Opportunistic attacks include the following:

- **419 Scams** – These are the e-mails from a "Nigerian Prince" or other individuals requesting funds in advance to assist with a financial problem.
- **Mass Mailing Worms** – These are worms hidden in e-mail attachments that are sent in mass mailings. These worms transmit themselves to other computers and replicate themselves on the new computer.
- **Trojan e-mails** – Similar to viruses, these are files that are run, usually inadvertently by the recipient of a mass e-mail. These Trojans can change a desktop PC, network, security settings, erase files, etc.
- **Scams involving well-known services such as Paypal or E-bay** – These are scams involving Internet purchasing of goods that result in funds being sent to a different account other than the one indicated on the website.
- **Mass scanning for vulnerable services/servers** – This is code written 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 malicious hacker are tailored. 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.[9]

Targeted Attacks may include the following:

- **Industrial Espionage** – This is using a cyber attack to obtain information from a company's computers. The most targeted industries are high tech or heavy industries such as aerospace, biotechnology, telecommunications, and computer companies.
- **Publicity Attacks** – This is a cyber attack on a firm to especially damage a firm's public reputation. This might be a cyber attack on a bank, insurance company, advertising firm, etc. to show that the firm does not protect their client's assets or information in an effective manner, thus causing the attacked firm to lose business or reputation.
- **Malicious Insider** – This is an employee that uses their access to the firm's computers to steal company proprietary information and sell it to others.
- **Person attacks** – This is the stealing and posting of a firm's or a person's sensitive information to cause damage to their reputation or embarrass them. Also may include cyber stalking.

Due to the increasing use of computers, cloud computing, e-mail and internet applications to perform business functions and communications, most organizations send and receive confidential e-mails and information via the Internet. Additionally, most firms engage in on-line shopping and financial transactions. This information is not to be shared with the public and financial transactions are intended to be very secure. Therefore, a company email address that initially doesn't seem to have any financial or strategic value suddenly becomes an email address that enables a hacker (with illegal access to the e-mail) to purchase products from online retailers, obtain financial information, or snoop into a firm's finances.[9]

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

Area	Description
Malware (computer viruses) (worms) (Trojan horses) (Spyware) (Adware)	Malware is software used or created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software
Wireless Connections	Gaps in wireless security allow hackers into an otherwise protected system. Usually hackers use a system such as mobile phone to gain access. Newer technology, such as: intrusion protection systems (IPS) that combines the features of firewalls, intrusion detection and anti-virus system, that record and trace intrusions and extend protection to network devices such as routers are needed to prevent and deter wireless cyber attacks.
Social Engineering (Phishing)	Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, financial institutions, online payment processors or IT administrators are commonly used to lure the unsuspecting public.[23]
USB Devices	A USB device can be used to infect a company's computers and networks. Malware is often delivered via an infected USB devices. According to the software security firm Avast, one out of every eight malware attacks originates via an infected USB device. These attacks target the Autorun function in Windows and plug-in USB devices. The infected USB device, such as mobile phone, mp3 player digital camera, or thumb drive starts an executable file and downloads the malware to Windows operating system prior to antivirus program starting up. This has the potential to replicate itself every time a PC is turned on with an infected USB device attached. According to Avast virus analyst Jan Sirmer, the danger of USB malware is more widespread than the Stuxnet attacks on corporate computers which was also spread via an infected USB storage device.[24]
Inappropriate computer network connections	Networks that allow Remote Desktop Protocol (RDP) connections without the most current security features have a high potential of allowing access by criminals to the computer network. Firms may wish to consider a Virtual Private Network (VPN) System with a strong two-factor authentication.[25] In addition, the physical security of all network assets and computers should be ensured.
Compromising Data Storage (Data Security)	Loss or theft of data is a large problem. McAfee, a software security company noted, after performing a 2009 survey of data losses and theft, that "The companies surveyed estimated they lost a combined $4.6 billion worth of intellectual property last year alone, and spent approximately $600 million repairing damage from data breaches. Based on these numbers, McAfee projects that companies worldwide lost more than $1 trillion last year."[26] A company's network should be separated from the public Internet by strong user authentication mechanisms and policy enforcement systems such as firewalls and web filtering proxies. Additional monitoring and security solutions, such as anti-virus software and intrusion detection systems, should also be employed to identify and stop malicious code or unauthorized access attempts. Encryption of data transmission and storage is also recommended. A firm must also ensure that physical security of computer backups, data tapes, etc, especially when it is moved off-site to remote storage locations. [25]

Cyber Security Programs and Awareness Training

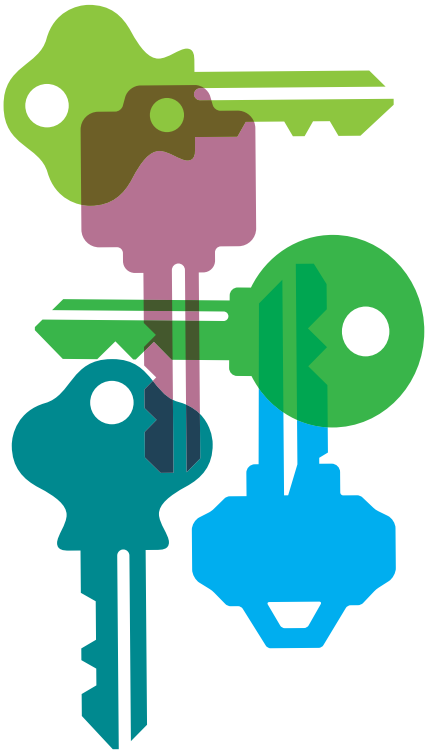
It is important to remember that cyber security, like all security, is a process, not a product. Cyber security must be an on-going action by all employees and contractors of a company/entity.

A limited number of sample plans are readily available (likely due to the sensitivity of the subject matter), but some public entities and organizations have developed templates and/or guidance. For example, a sample plan template can be obtained from the National Rural Electric Cooperative Association.[30] Additional sources, especially useful for protecting SCADA and DCS systems, are available from the International Society of Automation (www.isa.org) and Innominate Security Technologies (http://www.innominate.com/en). Information is also available from DHS National Cyber Security Division.[34] However, rather than developing a plan completely in-house, it is highly recommended that companies retain a qualified computer consulting firm with experience in cyber issues and 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.

In addition to a plan, companies need to develop and implement awareness training on company policies/procedures as these are developed. Refresher training is warranted to reinforce this training to employees. Systems also need to be in place to assess the effectiveness of plans and training.

At a minimum, a company's cyber security program should include:[21, 25, 27, 28, 29]

- 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



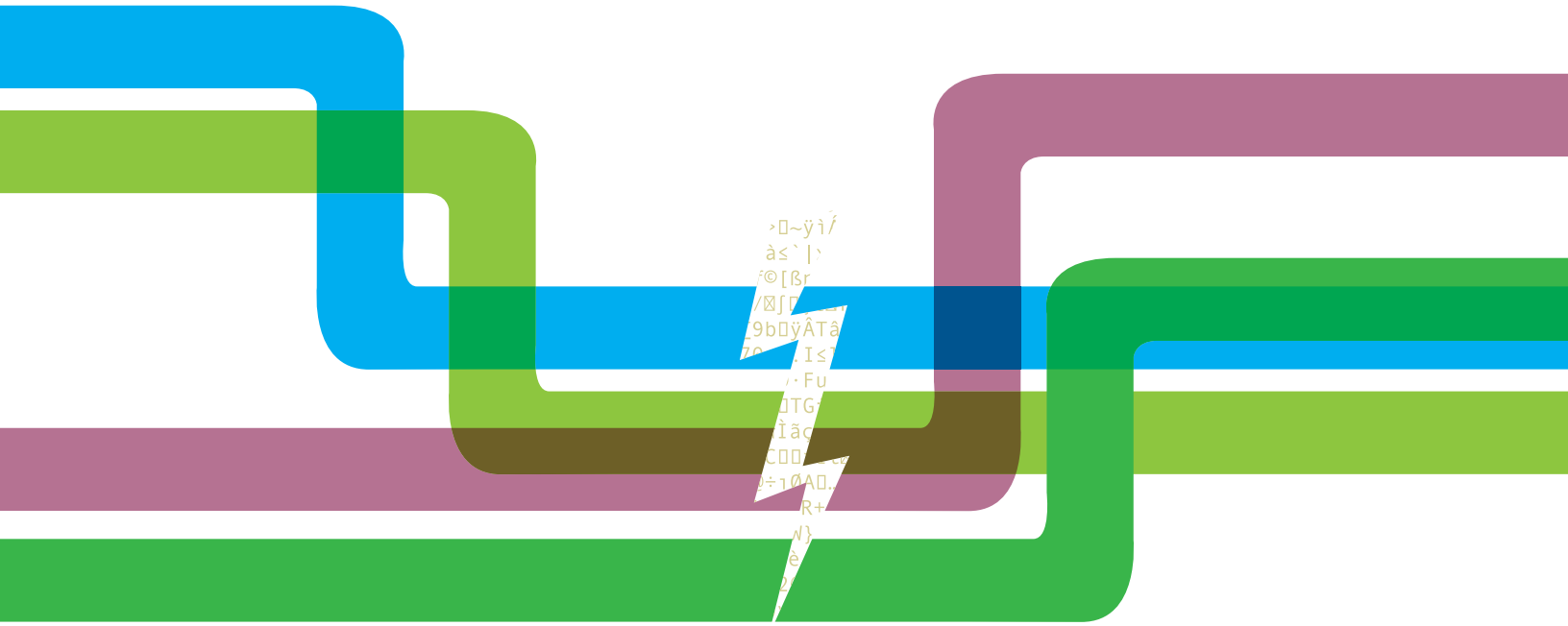
Conclusion

Industry and businesses must be highly cognizant of the detrimental and potentially devastating effects a cyber attack can have on an organization's assets. Catastrophic environmental impacts, fires, explosions and other consequences are possible from a single cyber attack. This can result in business interruption, reputational impacts, and significant financial loss.

The cyber security mindset for all industries must change from a 'it can't happen to us" attitude. 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 problem", but a problem for the whole company and everyone doing business with the company.[39]

There is no cook book or "off the shelf" prevention template with blanks to be filled in for critical industry cyber security. Only an in-depth analysis of the critical industry's operations, equipment, procedures, physical security and personnel will result in a security program tailored to deter and manage these 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 response.



References

1. Analysis of cyber security aspects in the maritime sector European Network and Information Security Agency (ENISA)
2. SCADA Security – Advise for CEO; IT Security Expert Advisory Group (ITSEAG); 2012
3. Russia's Top Cyber Sleuth Foils US Spies, Helps Kremlin Pals; *Wire Magazine* – Danger Room July 23, 2012: http://www.wired.com/dangerroom/2012/07/ff_kaspersky/4/
4. United States Naval War College Weekly Maritime News Survey: http://www.usnwc.edu/Departments---Colleges/Center-for-Naval-Warfare-Studies/Strategic-Research/Global-Maritime-Survey.aspx
5. Keeping America's Pipelines Safe and Secure: Key Issues for Congress – Paul W. Parfomak – Congressional Research Services; March 13, 2012
6. Moonlight Maze: http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/
7. http://www.securitymanagement.com/news/study-highlights-infrastructure-risks-0010178
8. *Wikipedia* entry on Cyberterrorism: http://en.wikipedia.org/wiki/Cyberterrorism
9. Targeted Cyber Attacks – The Dangers Faced by Your Corporate Network; GFUI White Paper
10. Protecting Organizations from Cyber Attack – Cliff Glantz and Guy Landine – Pacific Northwest National Laboratory; 2012
11. Cyber-Terrorism: Definitions, Background/History, Examples; VIGITRUST; July 2006
12. Cyber Attack Protection for Pipeline SCADA Systems; Tobias Walk, ILF Consulting Engineers; January 2012
13. Cyber Security: http://www.whitehouse.gov/administration/eop/nsc/cybersecurity
14. *Wikipedia* entry on Cyber Crime and Cyber Terrorism: http://en.wikipedia.org/wiki/Cyberterrorism
15. Experts Warn of PLC and DCS Cyber-Vulnerability; *Managing Automation*; January 1, 2005: http://www.managingautomation.com/maonline/news/read/Experts_Warn_of_PLC_and_DCS_Cyber_Vulnerability_12318
16. Control Systems Security Program (CSSP) – Overview of Cyber Vulnerabilities; US-CERT (United States Computer Emergency Readiness Team; 2012: http://www.us-cert.gov/control_systems/csvuls.html
17. 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
18. Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia; The Mitre Corporation (Abrahms, and Weiss); July 23, 2008: http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf
19. Cyber Security and the Pipeline Control System; Byres; Tofinosecurity; *Pipeline and Gas Journal*; February 2009: http://www.tofinosecurity.com/sites/default/files/Cyber_Security_and_The_Pipeline_PGJ_Feb_2009.pdf)
20. Stuxnet Raises "Blowback" Risk In Cyberwar; NPR; November 2, 2011: http://www.npr.org/2011/11/02/141908180/stuxnet-raises-blowback-risk-in-cyberwar
21. Guidance for Addressing Cyber Security in the Chemical Industry Version 3.0; American Chemistry Council's Chemical Information Technology Council (ChemITM) Chemical Sector Cyber Security Program; May 2006: http://trygstad.rice.iit.edu:8000/Policies%20&%20Tools/IndustrySpecificTools/CHEMICAL%20SECTOR%20-%20Cyber%20Security%20Program%20-%20Guidance%20Document.pdf
22. Strengthen Your Cyber Security; Chemical Processing.com; 2008: http://www.chemicalprocessing.com/articles/2010/088/
23. *Wikipedia* Entry on Phishing: (http://en.wikipedia.org/wiki/Phishing
24. Cyber Criminal Delivers Malware Via USB Devices; PC Optimization Secrets; November 7, 2010: http://www.pcoptimizationsecrets.com/cyber-criminal-delivers-malware-via-usb-devices/
25. Cyber Security Planning Guide; Federal Communications Commission; November 17, 2012: http://transition.fcc.gov/cyber/cyberplanner.pdf
26. McAfee, Inc Research Shows Global Recession Increasing Risk to Intellectual Property – Businesses Lose More than $1 Trillion in Intellectual Property Due to Data Theft and Cybercrime; McAfee; 2009: http://s3.documentcloud.org/documents/405722/mcafee-press-release.pdf
27. Cyber Security Programs for Nuclear Facilities; US Nuclear Regulatory Commission; January 2010: http://pbadupws.nrc.gov/docs/ML0903/ML090340159.pdf
28. Guide to Developing a Cyber Security and Risk Mitigation Plan; Cooperative Research Network; 2011: http://www.smartgrid.gov/sites/default/files/doc/files/CyberSecurityGuideforanElectricCooperativeV11-2%5B1%5D.pdf
29. An Introduction to Computer Security – The NIST Handbook (Special Publication 800-12); National Institute of Standards (NIST); October 1995: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
30. Cyber Security Plan Template; National Rural Electric Cooperative; 2012: http://www.nreca.coop/Pages/default.aspx

31. Protecting Water Industry Control and SCADA Systems from Cyber Attacks; Don Dickinson, *Phoenix Contact*; 2010: http://www.graybar.com/documents/phoenix-contact-protecting-water-industry-control.pdf
32. Important SCADA Systems Secured Using Weak Logins, Researchers Find; *CD0 Data Protection*; January 15, 2013: http://www.csoonline.com/article/726875/important-scada-systems-secured-using-weak-logins-researchers-find?utm_source=01.18.2013+News+Summaries+-+58th+Edition&utm_campaign=Weekly+News+Summaries&utm_medium=email
33. Shodan Search Engine Project Enumerates Internet-Facing Critical Infrastructure Devices; The Threat Post – *Kaspersky Lab Security News Service*; January 9, 2013: (https://threatpost.com/shodan-search-engine-project enumerates-internet-facing-critical-infrastructure-devices-010913)
34. U.S. Department of Homeland Security website – Cybersecurity; April 2013: http://www.dhs.gov/topic/cybersecurity
35. Jeep Hack Follows Burger King's – Who's Next?; February 20, 2013; *Chicago Tribune:* http://cyberfpn.advisen.com/fpnHomepagep.shtml?resource_id=193992643583282228&userEmail=jim.green@xlgroup.com#top
36. US Ready to Strike Back Against China Cyberattacks; *Washington Guardian*; February 20, 2013: http://www.washingtonguardian.com/us-ready-strike-back-against-china-cyberattacks-0
37. APT1 – Exposing One of China's Cyber Espionage Units; Mandiant; 2013: http://intelreport.mandiant.com/
38. Latest Threats to Pipeline, Production, and Process Management Systems – Hacking the Industrial SCADA Networks II; Frank Dickman – *Pipeline and Gas Journal*; February 2013, Volume 24- No. 2: http://pipelineandgasjournal.com/latest-threats-pipeline-production-and-process-management-systems?utm_medium=email&utm_campaign=PGJ+February+News&utm_content=PGJ+February+News+CID_c3c24093acc32ed137b5f3e149e933a4&utm_source=Email%20marketing%20software&utm_term=Latest%20Threats%20To%20Pipeline%20Production%20And%20Process%20Management%20Systems
39. Solving the Cybersecurity Puzzle; Dean Fox – *Pipeline and Gas Journal*; February 2013, Volume 240, No.2: http://pipelineandgasjournal.com/solving-cybersecurity-puzzle?utm_medium=email&utm_campaign=PGJ+February+News&utm_content=PGJ+February+News+CID_c3c24093acc32ed137b5f3e149e933a4&utm_source=Email%20marketing%20software&utm_term=Solving%20The%20Cybersecurity%20Puzzle
40. Judge Mulls Request to Dismiss SC Hacking Lawsuit; Associated Press; February 7, 2013: http://fpn.advisen.com/articles/article193233351-2140697918.html

Contact:

Environmental Risk Consulting Team

505 Eagleview Boulevard, Suie 100
Exton, PA 19341-1120
800 327 1414

xlgroup.com/insurance

3135_05/2013