Understanding the Hazard

Cyber Attacks

Human Element

As the number of cyber attacks increases, more companies will be exposed to financial loss and damage to their business reputations if they are not prepared to defend themselves and respond swiftly when breaches occur.

UTH topic categories:

- 🟧 Construction
- 🟪 Equipment
- 🟥 Fire Protection
- ▶ **Human Element**
- 🟦 Natural Hazards
- 🟩 Process Hazards

This series of publications is designed to help you understand the everyday hazards present at your company's facilities. For more information on how you can better understand the risks your business and operations face every day, contact FM Global.

FM Global®

The Hazard

Cyber risk is the new reality. It is no longer a matter of "if" but "when" your organization will experience a cyber attack. The number of cyber attacks reported annually is growing exponentially and is not expected to slow anytime soon. Media coverage of costly, high-profile cyber breaches is raising awareness that cyber risk is an enterprise concern, rather than exclusively an information technology (IT) problem. And, because these attacks have come from inside businesses as well as from outside, it is important to address both internal and external vulnerabilities.

Some cyber attack scenarios include a database of consumer data being breached by an unauthorized intruder with the intention of profiting from the information in these records. Or, a computer server failure, intentionally caused by excessive traffic, overwhelming a network and rendering websites and mobile applications completely inaccessible. Or, a hacker exploiting a weakness in the network and maliciously attacking power substations, causing outages for thousands, even millions, of customers.

Loss of key intellectual property and personal information assets are the most widely recognized risks associated with cyber attacks. However, physical damage to property is a very real risk, too. For example, hackers could intentionally make a turbine overspeed, causing significant damage to sensitive, high-value machinery. There are many other risks associated with cyber attacks that you may also need to address, including business interruption and subsequent loss of market share, heavy fines, increased regulation and, perhaps most damaging of all, long-lasting negative effects to your business reputation.

This brochure is made available for informational purposes only in support of the insurance relationship between FM Global and its clients. This information does not change or supplement policy terms or conditions. The liability of FM Global is limited to that contained in its insurance policies.

What you can do at your facility

Now:

- Determine what information security standard applies to your industry and base your cybersecurity framework on its standardized set of practices. Absent clear guidance from industry, we recommend the organization adopt the National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*.
- Identify and classify data based on business criticality, as well as sensitivity/confidentiality of data.
- Identify critical assets and physical/logical network access points at your facility, and determine how access is controlled. Prioritize actions to improve physical and remote access control for those identified assets and network access points. Contact FM Global and refer to FM Global Property Loss Prevention Data Sheet 9-1, *Supervision of Property*, for recommendations.

Soon:

- Create and maintain a documented incident response plan to prepare employees to respond accordingly during cyber events. The plan needs to be part of a complete risk management program, not just a document.
- Test the plan. Tabletop simulation exercises are very effective means of testing the adequacy of a plan and restoration time frames.

Science of the Hazard

Cyber attacks come in many forms, but two primary categories are virus/malware attacks and denial-of-service attacks.

Malware attacks usually involve the introduction of unauthorized computer code into the host system, either through a widespread virus infection or a targeted hacking attack. Such attacks can also lead to property damage (i.e., other than to data) and associated business interruption. Another emerging type of malware is ransomware. Ransomware is malicious software that restricts access to an infected computer system. Some forms of ransomware systematically encrypt files, making them impossible to open without paying a fee to receive the encryption key.

Denial-of-service (DOS) attacks are typically accomplished by overwhelming sending or receiving systems with outside requests, preventing the targeted system from functioning properly.

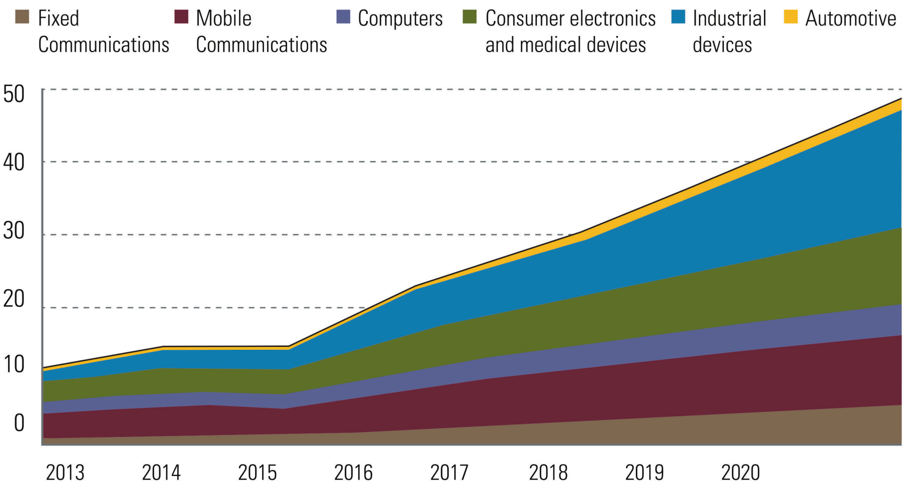
Network access is required to conduct any form of a cyber attack. Hackers can access a network both physically (for example, by inserting a flash drive in a computer port) and remotely (for example, over an Internet connection).

Loss Experience

According to a Global State of Information Security® Survey conducted by PricewaterhouseCoopers LLP, the number of cyber attacks in 2015 increased 38 percent from 2014. And, according to a 2015 Ponemon Institute study, the average cost of cyber crime worldwide on an annual basis now exceeds US$7.7 million per occurrence. In addition, Cisco Systems, Inc. reports that the number of Internet-connected devices worldwide will grow by more than 200 percent by 2020, greatly increasing cyber risk exposures.

The 50 Billion Question

Worldwide number of Internet-connected devices; forecast



Source: Cisco

*Includes military and aerospace

Illustrative Loss: Insider Threat

An employee tampered with a program involved in benchmarking the specifications for a very valuable proprietary computer system. The company spent a great deal of time trying to determine the cause of the difficulties they were experiencing. Finally, thinking the issues might be related to the room in which the testing was being performed, the entire project was relocated to a different facility. The employee was later found accessing another employee's computer, was confronted by management, and finally confessed to causing the problems. By then, however, several million dollars had been spent and a lot of time had been wasted.

But What About…

…the inevitability of a cyber attack? Why not just leave it up to our insurance company and law enforcement to deal with?

Due to the nature of the crimes and complications associated with enforcing the laws, hackers are rarely ever brought to justice and held accountable for their actions. At FM Global we believe that the majority of loss is preventable, including cyber attacks, and it is easier to prevent a loss than to recover from one. We work with clients to reduce their cyber-related exposures and mitigate cyber-related losses using tried-and-true loss prevention improvement principles.

…the fact that our organization doesn't have anything hackers would be interested in? Wouldn't our time and resources be better spent elsewhere?

It is true some industries are more likely to experience a cyber attack due to the nature of their business and the information they store. However, just because your industry might be at a lower risk right now does not mean you are immune from future cyber threats. As the Internet of Things (IoT) continues to grow and the number of Internet-connected devices increases, the likelihood of experiencing a cyber-related loss also grows. Hackers' motives are difficult to determine and some do it just because they can and, unfortunately, as their abilities and resources expand, so will their targets.

Definitions

Denial of service (DoS) attack: An attack specifically designed to prevent the normal functioning of a system and prevent access to the system by authorized users. Hackers can cause denial-of-service attacks by overloading the system's servers and preventing legitimate access to the service.

Encryption: The scrambling of data so it becomes unreadable to anyone not in possession of the "key" used to unscramble it.

Industrial control system (ICS): A general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), and other control system configurations such as skid-mounted programmable logic controllers (PLCs) that are often found in the industrial control sectors and critical infrastructures. An ICS consists of combinations of control and sensor components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).

Internet of Things (IoT): The network of physical objects—devices, vehicles, buildings and other items—embedded with electronics, software, sensors and network connectivity that enables these objects to collect and exchange data.

Malware: Malevolent software such as viruses, Trojan horses, spyware and malicious active content.

Ransomware: Software that encrypts the hard drive of an infected computer, enabling a hacker to demand money from the computer's owner in exchange for decryption software to make the data usable again.

Virus: A computer program that attaches itself to disks or files and replicates itself repeatedly, usually without user knowledge or permission. Some viruses just display symptoms, but very malicious viruses damage files and computer systems. Viruses use a variety of methods to infect computers. Some viruses wait until an infected file executes, while others infect files whenever the computer opens, modifies or creates files.

Don't Let This Happen to You…

A steel mill was subject to an industrial control system (ICS) attack. The hackers manipulated and disrupted control systems to such a degree that a blast furnace could not be properly shut down, resulting in significant damage.

Need more information?

Ask your client service team about the following:

- FM Global Property Loss Prevention Data Sheet 9-1, *Supervision of Property*
- 2016 Cyber Coverage Enhancements Sell Sheet
- 2016 Cyber Coverage Enhancements Video

Ordering Information

For additional copies of *Understanding the Hazard* publications, contact your FM Global engineer or client service team.

Additional FM Global brochures and educational material can be found in the FM Global Resource Catalog and ordered or downloaded online at fmglobalcatalog.com. Or, for personal assistance worldwide, contact our U.S.-based customer services team, Monday – Friday, 8 a.m. – 5 p.m. ET :

- Toll-free: (1)877 364 6726 (Canada and United States)
- By phone: +1 (1)401 477 7744
- By fax: +1 (1)401 477 7010
- E-mail: customerservices@fmglobal.com

FM Global

fmglobal.com

FM Insurance Company Limited
1 Windsor Dials, Windsor, Berkshire, SL4 1RS
Authorized by the Prudential Regulation Authority
and regulated by the Financial Conduct Authority
and the Prudential Regulation Authority