Cybersecurity and the Impact on Operational Technologies

WHAT IS CYBERSECURITY?

Cybersecurity is the broad term given to technologies and processes designed to protect networked equipment, software and data from unauthorized access, attack or damage.

As the world becomes more interconnected, networked equipment, software and data are increasingly susceptible to security breaches. In the past, the protection of such equipment, software and data was the sole responsibility of information technology (IT) teams. However, as more devices are introduced and more operational technology (OT) takes advantage of IT networks, the attack surface becomes more difficult to control and monitor. The attack surface is a point of vulnerability such as a port, device or software interface where an unauthorized user could attempt to enter or extract data from a network. Now, IT and OT teams must work together to assess areas of risk that have not been considered in the past.

WHAT IS OPERATIONAL TECHNOLOGY?

Operational technology can be hardware or software that controls physical devices or processes in specific environments, such as buildings, factories and utilities. In the past, OT systems operated in closed networks creating an "air gap" where they were segregated from the corporate IT network and the external internet. Today, OT systems are becoming increasingly interconnected and integrated with other IT systems.

One example of OT is a building's video surveillance subsystem. What was once a closed-circuit television (CCTV) system that did not interact with any other devices or networks now uses the IT infrastructure for data transportation, storage and monitoring.

The attack surface within video surveillance systems has changed virtually overnight. This rapid shift to the IT network has allowed technology advancements in endpoints – such as network cameras – to outpace the network security policies and procedures required to protect them and an organization from being targets in cyberattacks. According to IHS Markit, more than 66 million network cameras were shipped globally in 2016.[1] Many of these units are installed using a mix of wired and wireless networks without network security measures in place to protect them. As cyberattacks on IT networks increase and more integrations of OT systems occur, vulnerabilities are multiplying, drastically increasing the attack surface of OT networks.

While there are similar strategies for securing IT and OT systems on a network, there are also major differences between the two and confusion about who is responsible for securing what. Collaboration on a consistent security strategy across both IT and OT is imperative with the continued rapid growth of connected endpoints.

One major example is the availability requirements of OT systems. Downtime for software upgrades, patches or firmware updates are generally accepted in the IT environment, but can be very disruptive and costly in some OT systems. For example, within physical security subsystems, a simple firmware upgrade can break system integrations, rendering the system inoperative. However, a worst-case scenario is running an outdated software or firmware version with known security vulnerabilities, which can lead to increased risk of attack by a potential adversary. Considerations need to be taken to properly maintain OT systems to minimize downtime, otherwise lack of routine maintenance will increase the potential for a cyberattack.

As more and more operational functions take advantage of the capabilities that IT networks offer, the attack surface – or number of devices that are no longer in the controlled IT environment – expands. The manufacturers of these devices must provide users with the ability to protect not only from tampering of the device, but also the software used and the data collected by the device.

The Internet of Things (IoT) provides us many examples of challenging devices to protect. For example, utilities want to use IT networks to transmit process control data from substations and monitoring points. These areas are not easily physically protected and the question of component manipulation along with the data that is being collected becomes susceptible to inaccuracies. This attack surface provides unpredictable results unless protective measures are instituted.

	Information Technology (IT)	Operational Technology (OT)
Equipment	This includes switches, routers, cable, servers, storage and other general use equipment for networking.	This includes the edge devices, such as network cameras, sensors, meters or smart objects, that collect specific information.
Software	This can sometimes be characterized as firmware or the software needed to help the devices perform their function.	Includes the specific processing software to meet the application requirement. Video management software, process control systems, analytic software, etc.
Data	This is the information that is maintained by the operating system to identify events that may impact the operational data. Data logs give information used in analysis of performance of the overall system.	Includes the raw information collected and in what format: open or closed.

WHAT ARE SOME OF THE TYPES OF ATTACKS?

Virus

This is a programming code that reproduces itself and can be transmitted via email, download, or other transfer method. It can be benign or malicious depending upon the programmer's intent.

Malware

Malware is short for malicious software. This encompasses many cybersecurity threats, but is specifically code that is intended to harm other code or data. On October 21, 2016, Mirai, an open-source malware strain that scans the internet for IoT devices protected only by the factory-default passwords, hacked 150,000 devices to power a massive 1 TBps Distributed Denial of Service (DDoS) attack that brought down popular sites, including Twitter, Netflix and Amazon.

Botnet

This is the result of a hacker gaining control of multiple unprotected devices across the internet. The hackers use this botnet army of devices to attack victims with the intent of harming the victims' systems.

Denial of Service (DoS)

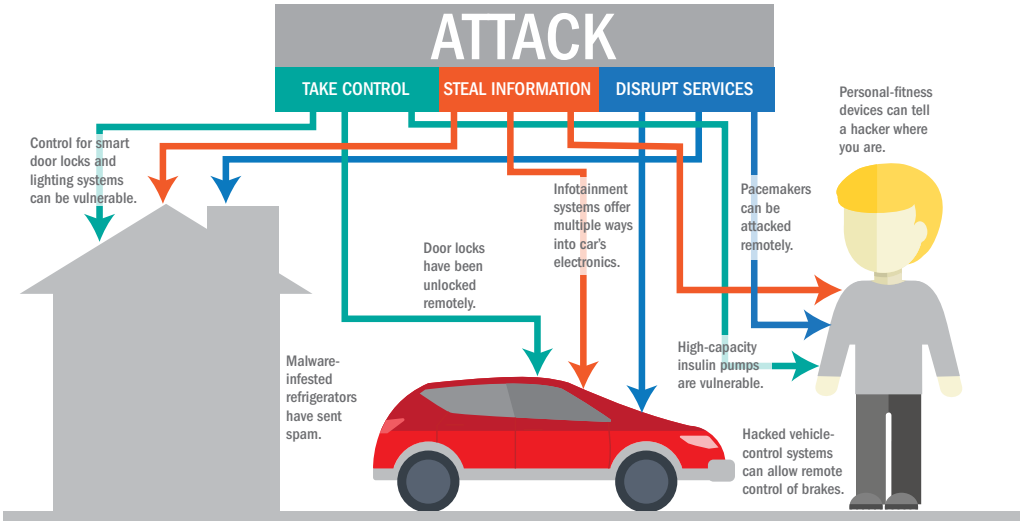
The network components become overloaded with processing requests such that they cannot perform their designed function and shut themselves off. A DDoS attack is when the processing requests come from innumerable remote devices to cause the shutdown. These are often caused by botnets.

Theft

The individual components or sensors and the corresponding software and data are physically removed from their intended environment.

Social Engineering

The individuals with approved access to sensitive information are manipulated by deceit to divulge the target data.



Backdoors

Software is left with an entry point that is not realized by legitimate users and the attacker gains access to data.

Direct Access Attack

By having physical access to a portion of the system, attackers can use mobile storage devices, such as USB drives, to insert malicious software or copy data files.

Eavesdropping

The monitoring of unencrypted conversations between devices with the intention of gaining sensitive information.

Financial gain remains the primary motivation for cyberattacks. The estimated global annual cost of malicious cyber activity ranges from US $300 billion to US $1 trillion[2] and is expected to greatly increase to $2.1 trillion by 2019.[3]

HOW CAN YOU PROTECT THESE SYSTEMS?

Follow manufacturer recommendations

- The first and most important thing you can do is look at any component that will be connected to a network and determine how to implement the manufacturer's cybersecurity recommendations. Follow the hardening guide that the manufacturer offers.

What is in the hardening guides for devices?

- Password - Delete default user IDs and passwords and set passwords that are difficult to guess. In 63 percent of confirmed data breaches, a weak, default or stolen password is at fault.[4]
- Firmware - Keep firmware up to date so that any known deficiencies are addressed.
- User permissions - Monitor which users have rights to perform specific tasks. Among all insider breaches, 55% are caused by misuse of privileged accounts.[5]
- Review/reconfigure basic network settings - Know where your vulnerabilities are so that you can monitor them closely.
- Disable features as applicable - Disable any unused feature in the device so you can identify if it is tampered with in the future.

- Enable encryption/SSL certificates - Encrypt the data output.
- Monitor accounts - Keep track of who has access and why.
- Disable IT functions - Don't give management rights to users who do not need them.
- Set address filters - Set up control filters for IP or MAC addresses.
- Configure SNMP - Configure any messaging required in your system.

Network protection - IT organizations have numerous options and tools to use, including but not limited to:

- Intrusion detection
- Log monitoring
- Network behavior monitoring
- Network inspections
- Whitelisting
- Firewall

Penetration testing

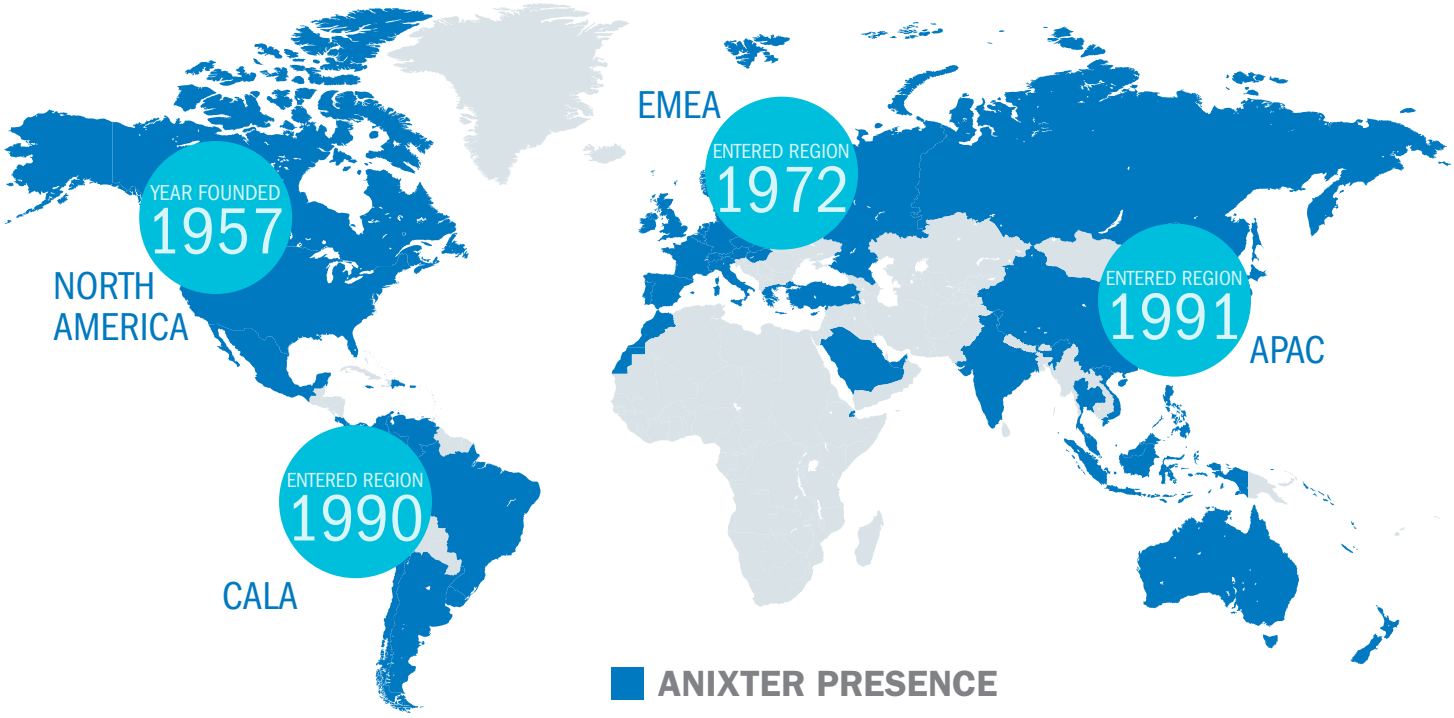
- Hire a company to test your cybersecurity and offer you advice on known and unknown vulnerabilities.
- Implement changes based upon penetration tests.

Sources

1. https://technology.ihs.com/api/binary/572252
2. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf
3. https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion
4. http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf
5. https://msisac.cisecurity.org/whitepaper/documents/1.pdf

Contact the device manufacturer for cybersecurity recommendations for specific devices.

Corporate Snapshot



Global Reach. Local Advantage.

With Anixter, you get a true local partner around the world. No other distributor of our kind can claim an in-country presence in approximately 50 countries and in over 300 cities.

We do business in more than 35 currencies and 30 languages, which means we are uniquely positioned to help facilitate your project in the local environment, reduce risks and keep costs down.

- YEAR FOUNDED 1957
- APPROXIMATELY 8,700 EMPLOYEES
- APPROXIMATELY 50 COUNTRIES
- OVER 125,000 CUSTOMERS
- APPROXIMATELY 320 WAREHOUSES/ BRANCHES
- OVER $1.1 BILLION INVENTORY
- IN OVER 300 CITIES
- STOCK SYMBOL AXE
- OVER 450,000 PRODUCTS
- FORTUNE 500 COMPANY

About Anixter: anixter.com/aboutus
Legal Statement: anixter.com/legalstatement

Anixter Inc. World Headquarters
2301 Patriot Boulevard
Glenview, Illinois 60026
224.521.8000