The Importance of Strong Cyber Security in Industrial Environments

As equipment and processes become more interconnected, the lines between Information Technology (IT) and Operational Technology (OT) continue to blur. Although there are many benefits to the convergence of these areas, such as remote connections and superior access to information, there are also additional security risks that must be considered. Where OT had been a self-contained system in the past, connecting critical infrastructure to the IT domain through convenient Ethernet connections (e.g., switching from Serial connections to Ethernet-based Modbus TCP/IP or BACnet IP) has left entire networks at risk by providing an entry point for those wishing to do harm to the system. Industrial environments may not be uniquely vulnerable to cyber attacks, but the impact of an attack can extend well beyond the industrial plant itself. This is especially true for facilities that provide a service to the public, such as an electrical substation, which is why security considerations should never be an afterthought.

Consider the importance of cyber security in a water treatment plant. In February 2021, a malicious individual hacked into a such a facility in Florida that was responsible for supplying water to approximately 15,000 people in the local area. By penetrating the network though an unsecured TeamViewer account, they were able to remotely control an on-site computer to access sensitive controls within the facility and increase the amount of sodium hydroxide being added to the water supply. Also known as lye, sodium hydroxide is a corrosive compound that is added regularly to the water in small amounts to temper acidity. However, too much sodium hydroxide can cause numerous health issues to those exposed. Although the hack was detected before harming the public or causing any permanent damage, this incident highlights the critical importance of comprehensive cyber security policies in industrial environments.

> **“Electric utilities can be affected by cyberattacks across the whole value chain**[1]**”**
>
> *- McKinsey & Company*

Once inside an industrial environment, hackers may target any number of critical systems. Depending on the facility, they may attempt to control the opening or closing of circuit breakers or adjust system logic to prevent alarms from tripping. An attacker may also enter false input values into a SCADA system by emulating a power meter or other sensors. The SCADA system may react to the incorrect values, causing unnecessary shutdowns or equipment failures.

A cyber attack can have a direct financial impact as well as cause damage to equipment or infrastructure. Reduced productivity and unscheduled downtime can have lasting impacts on brand reputation and trust as a facility's quality of service degrades. In the case of service providers, cyber attacks will not only impact the facility directly but also the community being served. When it comes to the security of water or electrical systems, an attack is not only inconvenient, but can endanger the community at large.

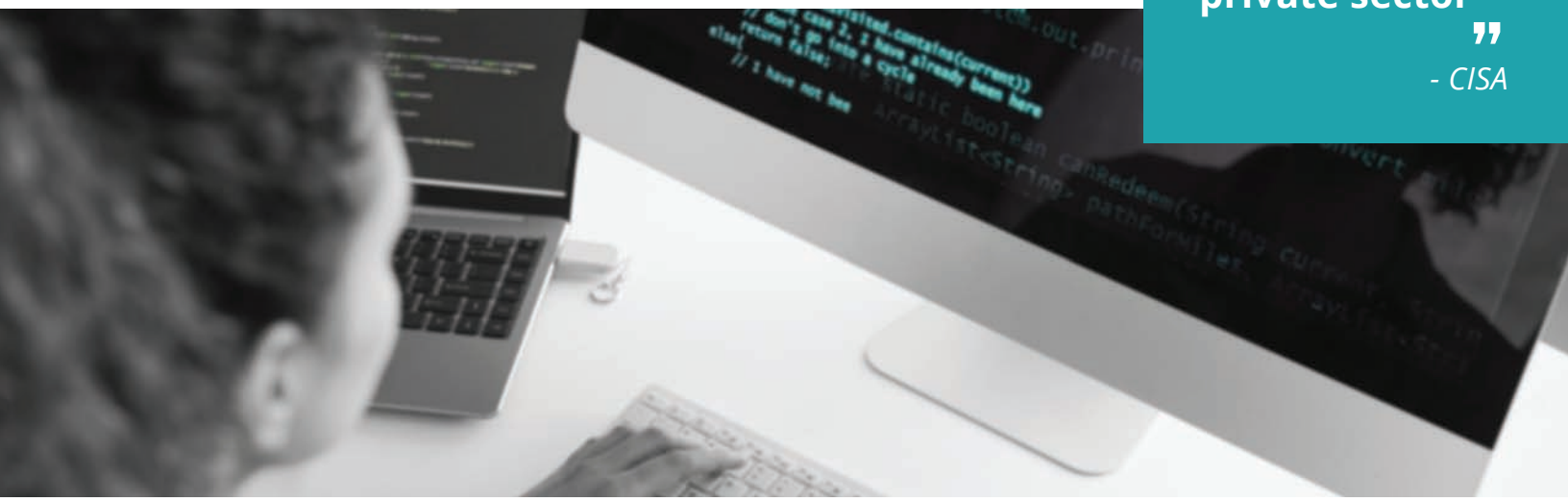
Unfortunately, simply acknowledging that strong cyber security in industrial environments is crucial is not nearly enough to prevent malicious attacks from happening. On top of that, industrial facilities often face major hurdles to securing their facilities including a lack of funding and inadequate training for on-site personnel. Hackers use several techniques to gain access to sensitive systems and networks, which is why a comprehensive approach that limits as many access points as possible remains crucial. Here are some common weaknesses exploited by malicious individuals to gain access to critical systems.

> **"48% lack adequate funding**[2]**"**
>
> *- Deloitte & Touche LLP*

Lack of Trained IT Personnel

Underfunded facilities struggle with the use of outdated, unsecured equipment and their financial shortcomings can also cause personnel shortages in key areas, including IT. It is not uncommon for only one or two IT professionals to be employed in an industrial facility. Their day-to-day responsibilities for computer maintenance and network troubleshooting may leave them with little time to address cyber security mandates, no matter how critical. In addition, they may lack the proper certification to understand how to cope with ongoing security concerns. Although these services could be outsourced to certified professionals, limited funding can be a roadblock to this strategy.

> **"More than 80% of the country's energy infrastructure is owned by the private sector[4]"**
>
> *- CISA*

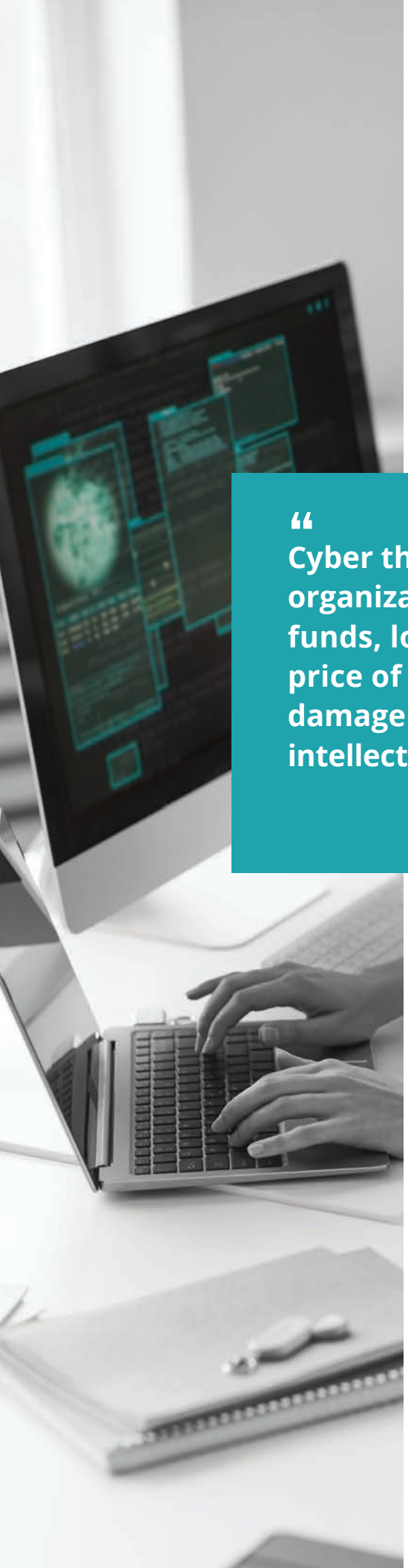


Inadequate Employee Training

Beyond IT personnel, other employees throughout a facility have a crucial responsibility to protect company assets. A common type of attack, known as "social engineering," includes strategies such as email phishing, malicious email attachments, or emails that include web links to viruses which are employed used by attackers to gain access to sensitive systems. Insufficient training leaves unsuspecting employees vulnerable to social engineering attacks and they may be unaware of any negative consequences until it is too late. A lack of funding for training, outdated anti-virus software, or a company culture that does not appreciate the serious nature of cyber threats can amplify the risk of social engineering attacks.

Insufficient Passwords

Weak passwords are another common vulnerability exploited by malicious individuals. Passwords that are too short, too simple, or left on the factory default setting (such as "admin" or "1234") can leave systems or devices open to intrusion. It is the responsibility of the IT or operations department to set policies that require strict password requirements. This is especially important for safeguarding key network hardware such as firewalls, managed switches, or servers but is also true for industrial systems and equipment, such as SCADA systems or power monitoring equipment.



Introduction of IP-Based Devices

Industrial environments have begun to shift away from sole reliance on industrial communication protocols, such as Modbus, and have started integrating IP-based devices. This shift has been a result of management and other stakeholders requiring real-time access to information used for critical facility decisions. Unfortunately, the increased interconnectivity as come at the expense of security. Although most traditional industrial protocols are not inherently safe, their relative obscurity offered a level of "accidental protection" against casual intrusion. IP-based devices can provide convenient remote access to critical facility data but can also be a liability if not secured properly.

> **"Cyber threat activity results in unwanted expenses for organizations, including the costs of ransoms or stolen funds, losses due to the disruption of operations, the price of securing and insuring networks, reputational damage and related loss of customers, and theft of intellectual property or confidential information."**[5]
>
> *- Canadian Center for Cyber Security*

Substandard Network Configuration

Attackers also look for improper network configuration settings to gain access to key industrial systems. Poor network architecture, such as unsecured remote access, or incorrectly configured firewalls can leave security gaps that can be exploited by hackers. Industrial environments that lack network segmentation are at an even greater risk as malicious individuals will also have access to sensitive industrial control systems. Substandard network administration practices, such as giving all system users full administrative access or not providing guest accounts for on-site visitors, can also leave networks vulnerable to intrusion. Especially for smaller facilities, proper network administration may be overlooked as being unnecessary and there may not be certified staff to undertake ongoing management responsibilities.

In addition, outdated network hardware or lack of security applications, such as anti-virus software, can also leave systems and equipment susceptible to intrusion. Unguarded systems can be quickly identified and exploited by attackers looking for an easy path into a sensitive system.

How to Reduce Cyber Security Risk

One of the most overlooked areas to bolster security is proper employee training. By teaching employees how to identify phishing attempts or malicious emails, it is possible to help lower the risk of a major cyber security vulnerability. Often, simple cues such as a mismatched sender and email domain can indicate that a message is not legitimate. In addition, pausing to get secondary confirmation before transferring any funds or releasing confidential information can prevent hackers from gaining the upper hand.

It is also important for management to implement standards for strong passwords and two-factor authentication, when available. Default passwords should always be changed, and key passwords should be updated regularly and be complex as well as unique. For critical equipment, such as SCADA systems, two-factor authentication should be implemented so that both a password and a second form of identification are used to make changes to the system. This is often a one-time password (OTP) with a unique code or a physical, USB-type device that is inserted during login to help prevent outside intrusion. Finally, management should ensure that security measures and user accounts are routinely audited. Not only should users have an access level appropriate for their position, but old or unfamiliar accounts should be regularly purged from the system.

> **"75% lack skilled resources**[3]**"**
>
> *- Deloitte & Touche LLP*

Despite high costs or other barriers, proper network configuration can prevent a wide range of attacks from casual intrusion to more serious, malicious attempts to damage a facility. In cases where on-site personnel are not properly trained, hiring a certified consultant to make network upgrades and recommendations is essential.

It is important for any facility to identify its key attack vectors so that a detailed cyber security plan can be implemented. A forward-thinking strategy can help mitigate ongoing threats by pinpointing current weaknesses to help reduce or eliminate vulnerabilities. By shifting from reactive responses to cyber threats to a proactive, comprehensive approach to security, industrial facilities can save time and money as well as protect those they serve.

1. *"Electric utilities can be affected by cyberattacks across the whole value chain."*
   Citation: Bailey, T., Maruyama, A., & Wallance, D. (2020, November 03). The energy-sector threat: How to address cybersecurity vulnerabilities. Retrieved March 04, 2021, from https://www.mckinsey.com/business-functions/risk/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities#
2. *"48% lack adequate funding."*
   Citation: Huelsman, T., Powers, E., Peasley, S., & Robinson, R. (2016). Cyber risk in advanced manufacturing. Retrieved March 04, 2021, from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-manu-cyber-risk-in-advanced-manufacturing.pdf
3. *"75% lack skilled resources."*
   Citation: Huelsman, T., Powers, E., Peasley, S., & Robinson, R. (2016). Cyber risk in advanced manufacturing. Retrieved March 04, 2021, from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-manu-cyber-risk-in-advanced-manufacturing.pdf
4. *"More than 80% of the country's energy infrastructure is owned by the private sector."*
   Citation: Energy sector. (n.d.). Retrieved March 04, 2021, from https://www.cisa.gov/energy-sector
5. *"Cyber threat activity results in unwanted expenses for organizations, including the costs of ransoms or stolen funds, losses due to the disruption of operations, the price of securing and insuring networks, reputational damage and related loss of customers, and theft of intellectual property or confidential information."*
   Citation: National Cyber Threat Assessment 2020. (2020). Retrieved March 04, 2021, from https://cyber.gc.ca/sites/default/files/publications/ncta-2020-e-web.pdf