CYBER SECURITY

Shifting Behaviors - How to make everyone guardians of Cyber Security

Reduce risk by empowering your workforce by deploying simplified and intuitive cyber security tools designed for industrial systems and users.

Summary

Today's evolving threat landscape requires cyber security solutions that protect industrial systems without compromising reliability. Increased interconnectivity between operational technology (OT) and information technology (IT) and the adoption of remote technologies accelerated by the global Covid-19 pandemic mean systems are increasingly more vulnerable to cyber-attacks.

Two incidents in 2021 illustrate this fact. In the first, a hacker gained access to a water treatment plant in Florida via outdated remote access software and poor password policy. Three months later, the ransomware attack on the Colonial Pipeline that disrupted fuel supplies from Gulf Coast refineries to key markets on the US East Coast was carried out using a single password and a VPN connection[1].

Despite high-profile attacks such as these, many organizations in the industrial space still do not approach cyber security as a business priority. The World Economic Forum (WEF) Global Cybersecurity Outlook 2022 reveals three main perception gaps between chief information security officers (CISO) and their CEOs: prioritizing cyber in business decisions; gaining leadership support for cyber security; and recruiting and retaining cyber security talent. The WEF survey found that 59% of all respondents would find it challenging to respond to a cyber security incident due to the shortage of skills within their team.

Rather than just recruiting external cyber security personnel, organizations are well advised to invest in training their existing staff in cyber security, processes and carefully selected technologies, so that cyber security becomes a fundamental element underpinning the business, alongside existing deep domain expertise in their internal IT systems. Yet there is an incorrect perception that OT cyber security is somehow complex, resource-intensive, expensive and less important. It is easy to forget where the revenue comes from: namely, the production controlled by OT systems.

The result is that an overarching OT cyber security strategy is often missing, leading to siloed cyber solutions, each solving a single problem and each with its own interface and workflow. This, paired with the time it takes to monitor and maintain these disconnected solutions once implemented, can make such programs challenging to sustain and perpetuate the illusion that maintaining good cyber security is convoluted and confusing.

When cyber security controls are perceived to be complex or intimidating to operate and manage, one of two things happens: 1) Implemented security controls get neglected, significantly reducing their efficiency. 2) Security is viewed as a hassle and is never implemented. A customer's investment in security controls is wasted if those tools are not implemented, operated and maintained correctly.

This article challenges the presumption that cyber security threats are complicated and that security solutions always require experts. It also addresses the impact this misconception can have on organizational behavior, how to simplify security and make everyone part of cyber security efforts.

Finally, we describe how one of the most up-to-date security solutions on the market, ABB Ability™ Cyber Security Workplace, offers a simplified user experience and a unified, scalable approach to OT cyber security, resulting in optimal use of implemented security controls and improved uptime.

Cyber attacks and solutions are not always complex

A common misconception is that both cyber attacks and cyber security controls are sophisticated and complex. In fact, the methods criminals use to infiltrate industrial networks are often relatively straightforward. Therefore, it follows that protection measures also often do not need to be overly convoluted, especially when implemented in line with a defined strategy based on a risk assessment and managed by a user-friendly application that enables everyone to be part of cyber security efforts.

Cyber criminals may gain access to a facility through insecure remote login software by exploiting disclosed vulnerabilities in the software or sending phishing emails to employees, who open them on a system connected to the plant network. Attackers may then take control of the mouse on an individual workstation and perform malicious tasks undetected in the guise of a control system engineer performing their typical job but remotely.

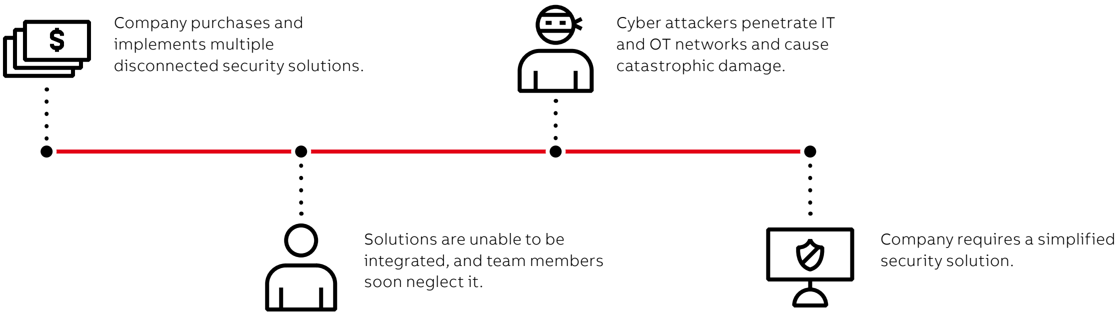
While controls such as patching, malware protection and system backups offer essential protection from cyber-attacks, they need a solid foundation. Suppose an industrial system is built on a poorly designed, indefensible network, where all devices are separated from the internet by a single firewall. In that case, additional risks are added to the mix and may even offset the benefit from the implemented security controls. Combining this with an ageing distributed control system relying on unsupported Windows computers makes it much easier for attackers to find and infiltrate the operation without using sophisticated methods.

Implementing and maintaining even the most basic security controls upon a solid architecture significantly reduces the risk of being compromised. Over time, when the assessed threat changes, one may need to add more security to stay ahead and aligned with the company's strategy and risk appetite.

According to the SANS 2021 OT/ICS Cybersecurity Report[2], 48% of the organizations surveyed did not know whether their industrial control system (ICS) had been compromised. That statement by itself is rather disturbing but even more so when coupled with the evidence that most systems already are or have been compromised.

This illustrates that the urgent need to secure operational environments is matched only by the need for cultural change. Leadership must understand and support OT cyber security efforts and instigate an organizational cultural shift to prioritize training and action. Without culture and behavioral change, it is unlikely that any investment in technology/software will lead to long-term protection.

A typical sequence of events



Company purchases and implements multiple disconnected security solutions.

Solutions are unable to be integrated, and team members soon neglect it.

Cyber attackers penetrate IT and OT networks and cause catastrophic damage.

Company requires a simplified security solution.

The human factor: empower existing staff to become cyber security guardians

The WEF report reveals that security-focused executives perceive their ability to respond to a cyber attack with adequate personnel as one of their main vulnerabilities, with 61% of respondents citing employee training as a solution to the increasing threat of ransomware attacks. Operational and IT teams therefore need to be prepared and equipped to face evolving threats, defend and adapt within budget and – most importantly – commit to ongoing training to ensure skills are retained and updated.

A well thought out strategy implemented throughout the organization, coupled with security tools designed for the people that already work in the organization, motivates each team member to do their part to keep the operation on track and make everyone feel responsible for cyber security rather than intimidated by it. Partnering with a trusted technology provider with proven deep domain knowledge is a considerable benefit, ensuring that personnel in the operational environment understand the threat, the cyber security solutions and what to do if something happens.

Organizations must also beware of technologies that promise much but deliver little. Many cyber security solutions are designed for cyber security experts working on the system 100% of the time, making them prohibitively expensive, reliant on external expertise – and ultimately pointless. Industrial operators can end up investing significantly in a flashy security solution and, in return, get a treadmill that they use as a coat rack. Why? Because they partnered with a company that promised the world with no contextual knowledge and ultimately invested in a system that does not address their organization's specific needs.

Every security strategy should be rooted in a risk assessment and match the individual operation's risk appetite. What is the likelihood of a cyber-attack? What would the impact be to the business if someone targeted a specific system? How much risk is acceptable, and is it worth it? The answers to these questions can differ markedly depending on the specific industry sector, a company's strategy and where they are on their cyber security journey.

So, a risk assessment looks at the production systems as one unit, how each component fits into the overall operation and what will happen if a component is compromised. Each component is analyzed for its criticality in the system and the likelihood of it being compromised. The goal is to identify which components are critical to the production and ensure they are protected.

The WEF report recommends that security executives communicate talent shortages and risks with leadership and drive initiatives for organic growth of security staff and skills within the business. This should begin with training existing OT and IT personnel in foundational cyber security controls, in partnership with a technology vendor, so that everyone – from plant managers to maintenance engineers – is cognizant of the threat and empowered to play a part in the overarching solution.

Risk versus cost

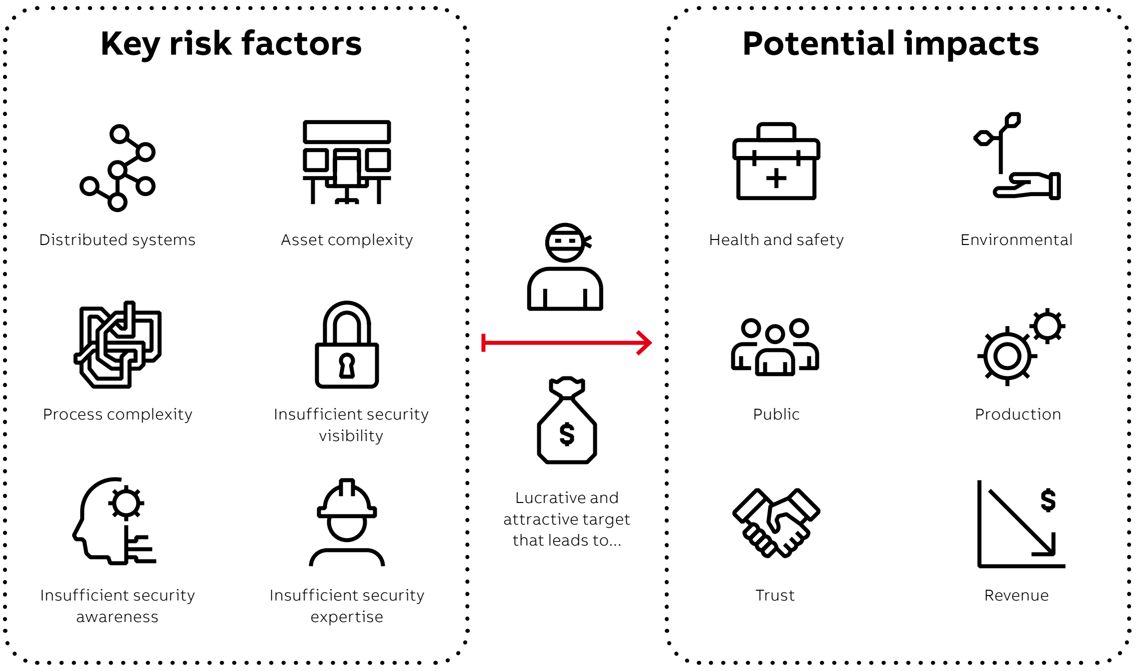
Why is this investment in human capital necessary? The threat posed by cyber-attacks on the industry regarding financial loss, production downtime and reputational damage cannot be underestimated.

A total of 61% of factories report that they have experienced a critical cyber security incident[3], while 75% say an incident has halted production[4]. The average cost of OT-specific malware attacks for organizations is $2.6m5. Ransomware attacks – carried out by criminals for financial gain – account for around eight out of ten attacks. Industrial companies are viewed as easy, high-value targets whose OT systems may be outdated, unprotected and exploitable, maybe even via the internet, making an attack even easier.

So, the question industrial companies should be asking is not: 'can I afford to implement a cyber security strategy', but rather 'can I afford not to'. Viewed in terms of business criticality, protecting internal systems from hackers is now a business priority, particularly when it comes to critical public infrastructure such as electricity or fuel and water supplies, as in the two examples cited earlier.

Defining ROI from cyber security is never easy, because you are effectively buying risk insurance, rather than tangible increases in revenue and production. However, companies are increasingly aware that security is not just about protecting critical assets: it is also about answering to investors and protecting their right to operate by complying with international best practices and standards.

Keep in mind that the yearly cost of implementing a robust cyber security strategy and controls – which can be upgraded to respond to evolving threats to OT production assets – in partnership with a trusted service and technology provider works out far less than the cost of an insurance policy. A well-implemented cyber security strategy may reduce the insurance premium to partly or fully fund the cyber efforts.



Key risk factors

Distributed systems

Asset complexity

Process complexity

Insufficient security visibility

Insufficient security awareness

Insufficient security expertise

Lucrative and attractive target that leads to...

Potential impacts

Health and safety

Environmental

Public

Production

Trust

Revenue

A simplified view: ABB Ability™ Cyber Security Workplace (CSWP)

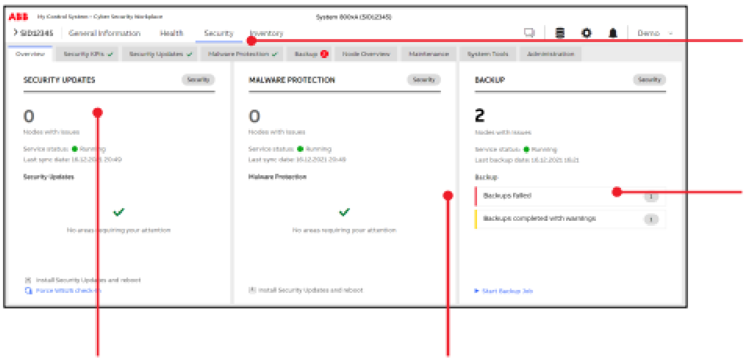
As discussed, making cyber security an enterprise-wide priority by training the existing workforce to recognize the evolving threat, be vigilant about potential vulnerabilities within OT systems and implement and maintain foundational cyber security controls requires a cultural change within an organization. Equally important are simplified, intuitive, user-friendly security tools that give employees the power to manage cyber security in industrial environments confidently.

ABB Ability™ Cyber Security Workplace (CSWP) simplifies the process of monitoring and maintaining foundational security controls by collecting security-relevant data from implemented cyber security solutions and forwarding it into a consolidated application. Operators can seamlessly monitor the status of basic security controls such as patching, malware protection and system backup, perform standard security tasks and receive alerts with actionable insights to remediate weaknesses and reduce risks – all from a single, easy-to-use dashboard.

This makes maintaining your cyber security easier, quicker, and critically, less daunting. CSWP is scalable, meaning it can be updated with new security features to keep up with evolving threats and support regulatory compliance without a lengthy learning curve.

For example, an industrial plant may have McAfee malware protection software, Windows Server for patching and separate software for backup, all of which can be complex to operate and maintain. CSWP makes this both standardized and configurable and consolidates all security controls into one view so that staff do not have to access multiple applications. Equipping front-line workers with the tools to secure the operational environment also reduces labor and operating costs.

Another feature requested by many is the power to isolate the OT and IT environments by a click of a button and prevent IT network intrusions and external actors from affecting the OT systems and potentially harming people, assets or the environment. CSWP also reduces the risks associated with remote access by managing user accounts and authentication, notifying staff6 when someone remotely accesses the systems, and letting operators activate and terminate remote sessions at will.



- Designed to **scale with your security program** so you benefit from advanced controls without the lengthy learning curve
- **Stoplight-like KPIs** provide early detection of increased risk
- **Simple and intuitive user interface** built for any and everyone
- **Flexible & customizable design** you fine-tune to fit your workflow

Conclusion

This article has explored some misconceptions around industrial cyber security and why protecting health and safety, processes and data requires a fresh approach to managing foundational security controls. This should be built around educating and training employees to feel empowered to monitor and maintain security solutions as part of their everyday responsibilities.

Organizations should no longer have to depend solely on experts for foundational cyber security. Instead, OT security must be based around clearly defined best practices, collaboration between industry, technology providers and their experts, and technology solutions that offer a simplified user experience. The result: fortified operations that support uninterrupted optimized operations and commercial success.

Sources

1 https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/

2 https://new.abb.com/process-automation/process-automation-service/advanced-digital-services/cyber-security/abb-cyber-security-reference-architecture

3, 4 The State of Industrial Cybersecurity. Trend Micro. May 2021 - https://new.abb.com/process-automation/process-automation-service/advanced-digital-services/cyber-security/abb-cyber-security-reference-architecture

5 The Cost of OT Cybersecurity Incidents and How to Reduce Risk. Nozomi Networks. 2020 - https://new.abb.com/process-automation/process-automation-service/advanced-digital-services/cyber-security/abb-cyber-security-reference-architecture

6 ABB Ability™ Cyber Security Workplace PDF

—

ABB Ltd.
Operating in more than 100 countries

Patrik Boo
Commercial Portfolio Manager
Cyber Security

abb.com/cybersecurity/workplace