WHITE PAPER

ICS Cybersecurity

Updated for 2020: Insights for Safe, Secure and Reliable Operations

splunk> turn data into doing™

Executive Summary

The cybersecurity of industrial control systems (ICS) is both a control room problem and a boardroom issue. Awareness is vital as cyberthreats to ICS negatively impact the profitability and reputation of an organization, as well as the safety of employees, customers and the environment. Stakeholders demand that organizations are transparent about the rising number of severe cyber incidents and overall cyber risk, and CEOs and CISOs regularly answer tough questions about their ICS environments:

- What is the current security risk level and potential impact on the business?
- Are our employees aware of ICS cyberthreats, and are they appropriately trained and equipped to prevent and mitigate?
- Do we have documented incident response plans that span both IT and OT groups in place?

This paper describes how cyberattacks jointly affect IT and OT networks, documents many of the risks involved, and provides recommendations for preparing against cyberattacks on OT networks.

An Increasingly Interconnected World

From in-factory PLCs to network routers along a gas pipeline, industrial internet of things (IIoT) devices connect us with our operations, enabling the business to use data-driven decisions that improve productivity, reduce manufacturing and shipping delays, improve the availability of field and shop floor assets, and much more. These smart devices are changing how we work.

Traditionally, ICS exist in silos using proprietary processes, protocols, networks and technology. For example, an operator often needs to walk the plant floor and manually record variables such as temperature and pressure readings. Recently, modern ICS began to use more open architectures and standardized interfaces that connect to internal corporate networks, and in some cases, the internet.

With this modernization, the convergence of OT and IT is unavoidable. For one, it enables in-demand drivers of business value like preventive maintenance, asset and fleet optimization, and numerous other new connected services. With this advancement in technology and the resulting digital convergence comes more vulnerability and a heightened risk of both targeted and non-targeted cybersecurity threats. The ROI of IIoT ultimately depends on our ability to successfully manage and secure ICS or better yet, the entire OT environment.

How the Worlds of OT and IT Connect

IT and OT systems in industrial environments have been converging for years. Most facilities already use Windows PCs running a human machine interface (HMI) application to query conditions and send commands to field or factory equipment. While the idea of connecting devices, people and processes across the industrial enterprise is not new, harnessing the capability of connected applications and services is on the rise.

In a fully-converged OT and IT environment, intelligent devices on OT networks are connected to enterprise applications and infrastructure. This enables industrial companies to make smarter, data-driven business decisions. With all the variations in control systems and devices, however, many organizations solely rely on network segmentation policies to maintain separation between IT and OT networks which can be an obstacle to IIOT-driven outcomes.

Without full visibility and control of traffic entering and exiting OT networks, an attack can quickly move back and forth between IT and OT environments. If a control system or connected assets such as PLCs, operator workstations, and historian servers are compromised, malicious actors could bring about destructive physical consequences to critical infrastructure and services, the environment, and even human life.

OT Cybersecurity Challenges

According to SANS Institute's "Insights on ICS Security," threats are shifting, identifying attacks remains challenging, and basic security practices are regularly ignored. Part of the challenge stems from the fact that OT networks are traditionally un-managed from a cybersecurity perspective or are using OT-specific security tools, which only give a narrow view of the overall security posture.

Non-Stop Operations Running on Legacy Technologies

Despite the high-profile news coverage of recent attacks of unpatched systems, many organizations don't regularly apply patches or have patching policies or procedures in place for ICS. In many cases, these systems were developed years ago and are tied to older versions of Microsoft Windows. In the case of ransomware attacks like WannaCry, Microsoft issued a patch for Windows XP and other unsupported operating systems to limit the number of machines at risk from the attack. However, patching vulnerabilities is not an option in many industrial environments, as these systems need to operate non-stop.

Variations in Security Focus Across IT and OT Teams

The differences between IT and OT security strategies are clear. IT professionals operate in dynamic environments and are generally concerned with securing systems that house data such as financial and customer information, intellectual property and corporate data. They spend much of their time keeping up with the latest software and hardware technologies, patching, upgrading and replacing systems.

For the OT professionals, security is a lesser concern. They manage the critical plant floor, process automation, and production systems, and priorities are focused on the stasis, safety, and availability of their physical and digital assets. Disruption from updates and patching could cause production losses, and in some cases the failure of equipment could even be a matter of life and death.

The unfortunate irony is that choosing to forgo security best practices could very well harm system availability and performance — the very things OT staff care about most.

Lack of Security Expertise in OT Environments

New OT security tools, including those from several high-profile startups, provide a reasonable first step in increasing security awareness within the OT environment. Adoption of these tools provides better visibility into assets and OT networks but does not impart OT teams with the knowledge to detect, investigate, or mitigate unknown threats or to understand implications across the OT/IT divide.

This inability to accurately identify and immediately act on risks that impact business operations is one of the primary impediments to adequately securing ICS. This lack of security expertise within OT teams and often blind reliance on third-party vendors to provide SCADA/ICS security compounds the problem, as does granting external vendors with high-level access to those systems. All of these challenges combined have contributed to a bit of a "wild west" situation in the ICS security market.

Impact of Cyberattacks

As OT networks converge with the outside world, it is necessary to be vigilant and protect this critical technology from attacks. The following events show the magnitude of the situation and serve as a reminder to protect your business before it is too late. The following timeline includes highlights from a string of incidents related to industrial operations as reported by the Center for Strategic & International Studies. Complete information on these and other incidents are available online.

May 2020: German officials reportedly found a hacking group associated with the Federal Security Service (FSB) — a Russian government agency mainly focused on the state's security — gained access to the networks of energy, water and power companies in Germany by exploiting IT supply chains.

May 2020: Iranian hackers are believed to have carried out a cyberattack against air transportation and government actors in Saudi Arabia and Kuwait.

May 2020: Israeli hackers allegedly disrupted operations at an Iranian port for several days, causing massive backups and delays. Officials characterized the attack as retaliation against a failed Iranian hack in April targeting the command and control systems of Israeli water distribution systems.

May 2020: A cyberattack against Mitsubishi Electric might have compromised details of new missile designs and prompted an investigation by Japan's Defense Ministry.

May 2020: Two Taiwanese petrochemical stations were reportedly hit by malware attacks just ahead of the inauguration of Taiwanese President Tsai Ing-wen's second term.

April 2020: Iranian hackers were suspected of trying to hack the command and control systems of Israeli sewage systems,water treatment plants and pumping stations.

April 2020: American officials believed Chinese hackers were behind an attack of several U.S. Department of Health and Human Services, healthcare providers and pharmaceutical manufacturers working on a vaccine for COVID-19.

April 2020: Azerbaijan government and energy sites were reportedly hit by an unknown hacker group targeting SCADA systems of wind turbines.

March 2020: A nation state hacking collective was believed to be targeting Iranian industrial sector companies.

January 2020: A Ukrainian energy company featured in the U.S. impeachment hearings was allegedly hacked by a Russian collective.

December 2019: The National Oil Company of Bahrain, Bapco, was reportedly attacked by the Iranian wiper malware.

November 2019: An Iranian hacker group was implicated in a series of password-spraying attacks against thousands of organizations, including the U.S. grid.

September 2019: Hackers were believed to have targeted four Airbus subcontractors supply chains to steal commercial secrets.

July 2019: Chinese state-sponsored hackers were believed to have carried out a spear phishing cyberattack against several U.S. utility companies.

July 2019: Several major German industrial companies were reportedly attacked by Chinese state-sponsored cyberattacks. The companies targeted included Siemens, BASF and Henkel.

March 2019: The U.S. Department of Energy reported that grid operators in Los Angeles County, California and Salt Lake County, Utah, suffered a DDoS attack that disrupted their operations, but did not cause any outages.

March 2019: Thousands of people tied to more than 200 global oil and gas and heavy machinery companies were allegedly targeted by Iranian hackers. The attackers were reportedly trying to steal corporate secrets and then wipe data from compromised computers.

July 2018: A group of Iranian hackers was believed to have targeted the industrial control systems of electric utility companies in the U.S., Europe, East Asia and the Middle East.

December 2017: Schneider Electric revealed it had to shut down operation of one of its power plants in an undisclosed location after malware led to an attack on its industrial control systems. The attack was believed by many experts to have occurred in the Middle East.

October 2017: A DHS and FBI report warned of Russia-linked hackers targeting industrial control systems at US energy companies and other critical infrastructure organizations.

The U.S. Department of Homeland Security and the Federal Bureau of Investigation released a report warning that Russian hackers were targeting industrial control systems and other critical infrastructure of American government agencies, along with nuclear, water, aviation and energy companies.

Many of these attacks demonstrated a potential for colossal financial loss and risk to human safety, and they are becoming increasingly common. ICS-specific exploitation frameworks are on the rise, with many using asset-discovery strategies similar to those already used by standard "ICS security" tools. These attack toolkits, which may include ICS-specific malware and ransomware are generally available and are already in the hands of both outside and inside actors. Once deployed, scripts and applications built on these toolkits seek and destroy critical digital processes, and it can take months or longer to fully recover from the damage.

Preparing for the Future: Recommendations for ICS Security

Control systems are no longer isolated from corporate or other networks. Corporate security strategies that only focus on IT systems and ignore OT ignore the complete surface of attack, which outsider and insider threats will try to exploit. The attack surface continually increases with the level of convergence and digitization, and leaders should act now.

Here are some recommendations for managing the risk of cyberattacks on OT networks:

1. **Make your OT environment visible to corporate security teams.**

   Being aware of traffic in and out of OT systems and regular OT network activity helps to protect the enterprise. If you can't regularly patch old Windows machines and other legacy assets, you must watch them closely.

   Monitoring and securing ICS devices via the network is a critical first step. Leveraging the machine data from existing network technologies such as routers, switches, firewalls, and other technologies specific to industrial environments provides organizations with the ability to monitor and detect threats to their OT environment. For example, Splunk's OT Security Solution helps organizations apply our leading security monitoring, investigation, and analytics frameworks directly to OT environments, accelerating investigation efforts, drastically increasing visibility, and helping to reduce overall risks in ICS.

2. **Align IT and OT security goals and collaboration.**

   Business-level oversight and executive leadership help to establish a culture of collaboration between IT and OT for the common good of the business. Improving an organization's security posture depends on how effectively both sides can collaborate to improve mutual understanding and increase the reliability and security of critical infrastructure.

   This strategy becomes crucial in the years ahead as IT/OT convergence and investment in IIOT grows. The impact of these investments and the potential consequences of accidentally leaving the doors unlocked requires considerable and immediate attention.

3. **Think strategically about securing OT networks.**

   Make sure to implement critical, foundational cybersecurity controls such as access control, segmentation, and appropriate cryptography levels. Make sure OT networks are part of your governance and incident response plan. Ensure your security professionals can detect, investigate, and respond to ICS attacks like they can in their IT environment. Monitor for known and unknown threats by comparing OT network activity with credible sources of signatures and behavior. Use network traffic anomalies to anticipate threat activity before it causes significant damage to the environment and the business.

   When an organization suffers a breach, it must be able to react and remediate quickly. With Splunk's OT Security Solution, organizations can finally do so by bringing the data-driven nature of the Gartner-recognized leader in the SIEM market and security analytics platform to OT security challenges.

Want to learn how Splunk can help with cybersecurity for OT, IT and IoT? Click here.

20-14554-SPLK-ICS Cybersecurity-105-WP