CyberX

Trusted. Industrial. Cybersecurity.

Global ICS & IIoT Risk Report

A data-driven analysis of vulnerabilities in our critical industrial infrastructure

October 2017

www.cyberx-labs.com

Table of Contents

1. Executive Summary

It's clear from recent news that a number of adversaries are attempting to compromise our critical industrial networks. Their motives range from criminal intent to operational disruption and even threats to human and environmental safety.

At the same time, industry experts have been telling us for years that our Operational Technology (OT) networks are vulnerable — lacking many of the built-in controls we now take for granted in IT networks, such as automated updates and strong authentication — but we've never had the metrics to objectively evaluate the risk before.

To address this gap, CyberX used proprietary Network Traffic Analysis (NTA) algorithms to analyze traffic collected from 375 production networks over the past 18 months, across the US, Europe, and APAC[2]. The networks span all sectors including energy & utilities, manufacturing, pharmaceuticals, chemicals, and oil & gas. Although questionnaire-based surveys have been conducted in the past, this type of real-world network analysis has never been conducted before.

The data clearly shows that control networks are easy targets for current adversaries. Many are exposed to the public Internet and trivial to traverse using simple vulnerabilities like plain-text passwords. Lack of even basic protections like anti-virus enables attackers to quietly perform reconnaissance before sabotaging physical processes such as assembly lines, mixing tanks, and blast furnaces.

In fact, OT networks are, as some have observed, like M&M candies — "soft on the inside." But they're also not particularly "hard on the outside," either. Once attackers get into an OT network — either via the internet or using stolen credentials to access existing pathways between IT and OT — it's relatively easy for them to move around to perform cyber-reconnaissance and compromise industrial devices.

We don't want to be cyber Cassandras — but at the same time, we should have a realistic, data-driven view of the current risk.

Here are the top data points from our global ICS and IIoT risk analysis:

- **One-third of industrial sites are connected to the internet** — making them accessible by hackers and malware exploiting vulnerabilities and misconfigurations. This explodes the myth that OT networks don't need to be monitored or patched because they're isolated from the internet via "air-gaps."
- **More than 3 out of 4 industrial sites have obsolete Windows systems like Windows XP and Windows 2000**. Since Microsoft no longer develops security patches for legacy systems, they can easily be compromised by destructive malware such as WannaCry/NotPetya, Trojans such as Black Energy, and new forms of ransomware.

"They're testing out red lines, what they can get away with. You push and see if you're pushed back. If not, you try the next step."

Thomas Rid, Professor of War Studies at King's College London [1]

[1] "How An Entire Nation Became Russia's Test Lab for Cyberwar," Andy Greenberg, WIRED, June 20, 2017

[2] Similar to the methodology used for the Verizon DBIR, the analysis was performed on an anonymized and aggregated set of metadata with all identifying information removed. Rigorous attention was paid to preserving the confidentiality of sensitive customer information.

- **Nearly 3 out of 5 sites are have plain-text passwords traversing their control networks**, which can be sniffed by attackers performing cyber-reconnaissance and then used to compromise critical industrial devices.
- **Half aren't running any AV protection**, increasing the risk of silent malware infections.
- **Nearly half have at least one unknown or rogue device**, and 20 percent have wireless access points, both of which can be used as entry points by attackers. WAPs can be compromised via misconfigured settings or via the recently-discovered KRAC vulnerability, for example.
- **On average, nearly a third of all devices (28%) in each site are vulnerable**. CyberX characterizes devices as "vulnerable" when they have a score of less than 70%, where the score is determined by examining the severity of all published vulnerabilities for the device – such as buffer overflows – as well as configuration issues such as open ports.
- **82% of industrial sites are running remote management protocols** like RDP, VNC, and SSH. Once attackers have compromised an OT network, this makes it easier to learn how the equipment is configured and eventually manipulate it.

Most of these OT networks were built years ago, long before the proliferation of Internet connectivity and the need for real-time intelligence. The key priorities were performance and reliability rather than security. And it was assumed that OT networks were secure because they were "air-gapped" – that is, physically separated from the Internet and from corporate IT networks.

WannaCry and NotPetya showed how easy it is for adversaries to penetrate OT networks and disrupt production – causing hundreds of millions of dollars in losses – while the Ukrainian grid attacks showed how targeted attacks can disrupt critical infrastructure and impact large portions of the civilian population.

What can be done? It's unrealistic to expect asset owners to perform massive upgrades to their OT infrastructures in the short-term, which would cost their industries billions of dollars.

Section 6 describes a number of practical steps that organizations can take today to mitigate OT risk. This includes organizational initiatives like security awareness training for OT personnel and breaking down barriers between IT and OT teams.

It also includes technology initiatives such as using compensating controls and multi-layered defenses, including continuous monitoring with behavioral anomaly detection and threat modeling, to mitigate vulnerabilities that might take years to fully remediate. SANS describes this proactive approach as "Active Cyber Defense," which is the process of using security operations to continuously identify and counter threats.

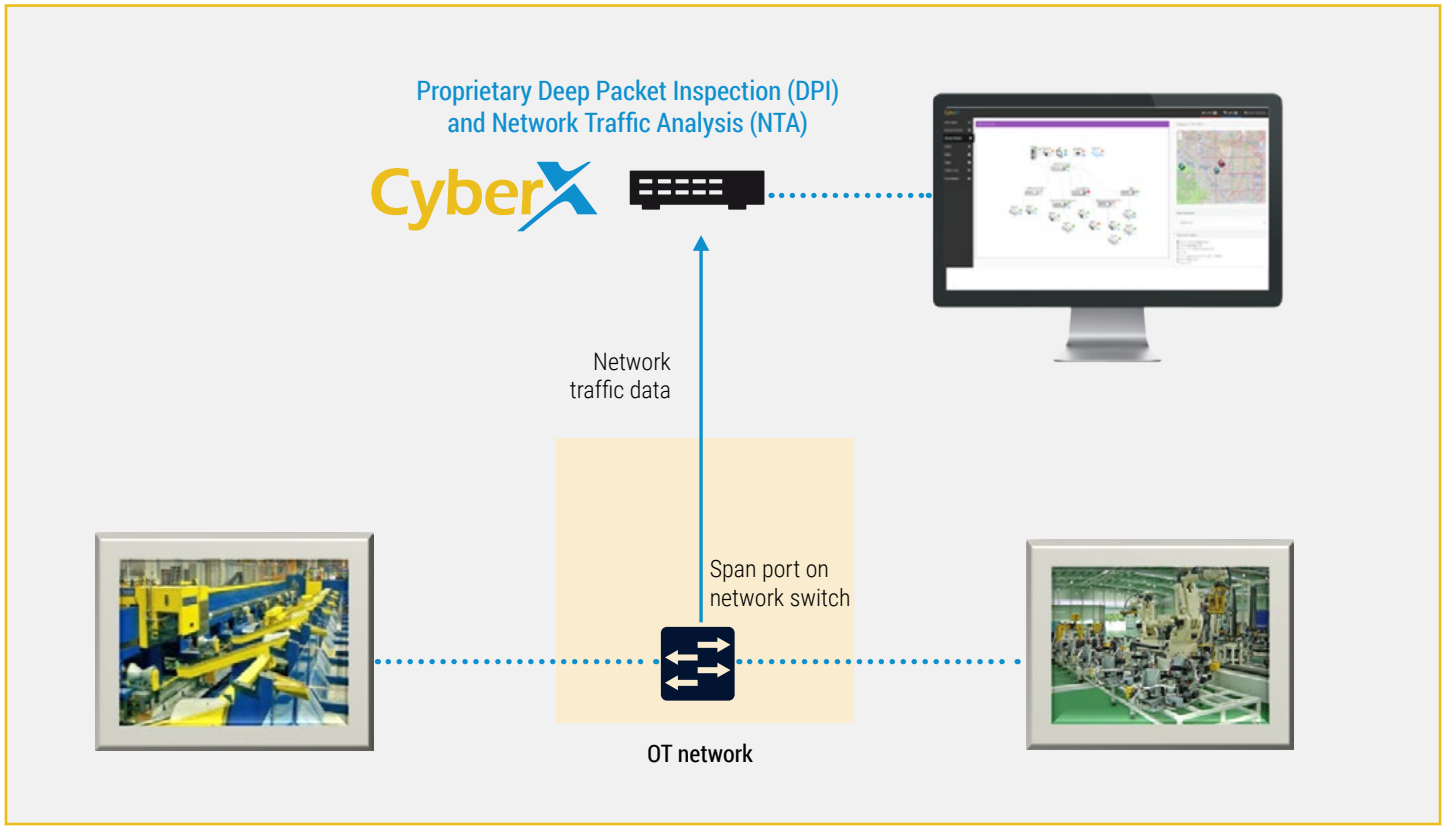
2. How Vulnerability Data Was Collected and Analyzed

The network traffic data was collected via passive (agentless) monitoring of OT networks. This entails connecting a CyberX collector appliance (physical or virtual) to the OT network via the SPAN port of a network switch, which provides a mirror of all network traffic, as illustrated in the diagram below.

The risk and vulnerability data was then compiled using proprietary Deep Packet Inspection (DPI) and Network Traffic Analysis (NTA) algorithms. DPI examines the data part and the header of all packets traversing the network, while NTA is used to deduce information from patterns in the communication.

The CyberX platform is 100% OT vendor agnostic, and our algorithms are designed to support all industrial automation protocols (Modbus, Siemens S7, GE SRTP, etc.) and devices (Rockwell Automation, Schneider Electric, GE, Siemens, etc.).

These algorithms are first used to perform an asset inventory of all devices on the network, as well as to discover the network topology. They are then used to identify all network and endpoint vulnerabilities that can be deduced from the traffic, including vulnerabilities for embedded OT devices such as Programmable Logic Controllers (PLCs).



CyberX collected traffic data from 375 production OT networks and then used proprietary Network Traffic Analysis (NTA) algorithms to analyze the traffic for vulnerabilities. The analysis was performed on anonymized and aggregated metadata, with all customer-identifying information removed.

3. Distribution of Industrial Protocols

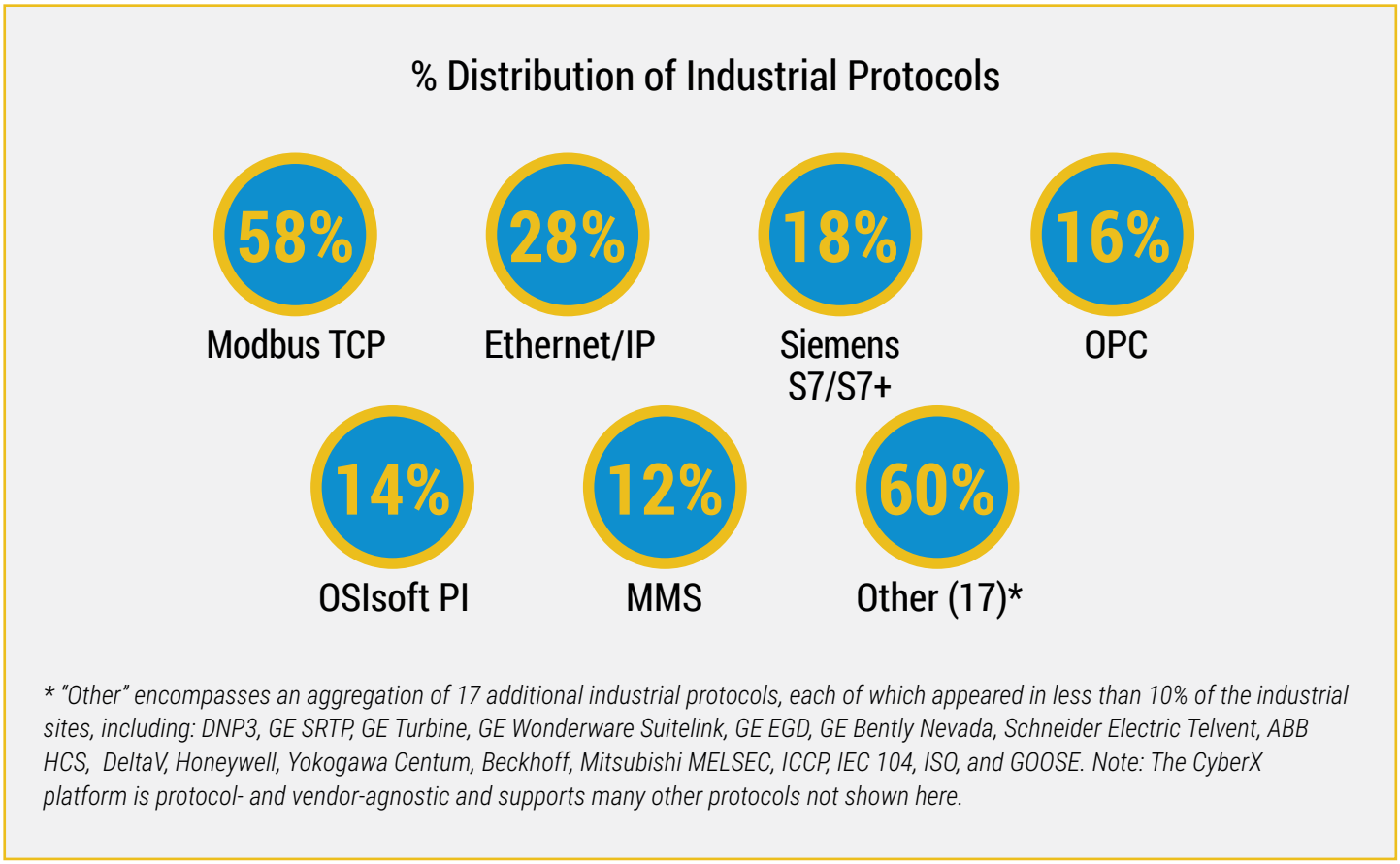
Industrial networks contain a complex mix of specialized protocols, including proprietary protocols developed for specific families of industrial automation devices. This heterogeneous mix complicates security for OT environments.

In addition, many protocols were originally designed when robust security features such as authentication were not even a requirement – because it was assumed that simply having connectivity to a device was sufficient authentication.

The most commonly-used protocol in our sample was Modbus, a serial communications protocol originally published by Modicon (now Schneider Electric) in 1979. Modicon invented PLCs, which are widely-used today to control physical processes such as motors and valves.

To further complicate OT security, industrial organizations have historically lacked any visibility into OT network activity and assets because monitoring tools designed for corporate IT networks are "blind" to OT-specific protocols like Modbus TCP.

In our automated risk assessments, we encountered standard IT protocols (HTTP, SMB, RDP, etc.) as well as a diverse mix of OT protocols shown in the graph below.



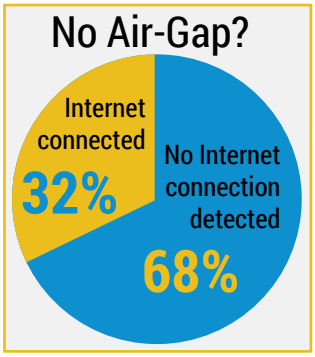
** "Other" encompasses an aggregation of 17 additional industrial protocols, each of which appeared in less than 10% of the industrial sites, including: DNP3, GE SRTP, GE Turbine, GE Wonderware Suitelink, GE EGD, GE Bently Nevada, Schneider Electric Telvent, ABB HCS, DeltaV, Honeywell, Yokogawa Centum, Beckhoff, Mitsubishi MELSEC, ICCP, IEC 104, ISO, and GOOSE. Note: The CyberX platform is protocol- and vendor-agnostic and supports many other protocols not shown here.*

4. Vulnerabilities Detected in ICS & IIoT Networks

4.1 Forget the myth of the air-gap

In theory, OT systems are air-gapped from the Internet, with no connection between the two. But we've known for a long time that the air-gap is a myth. In our sample, nearly 1 of 3 sites (32%) had industrial networks connected to the public Internet.

In 2014 the ICS-CERT issued an advisory stating they had "identified a sophisticated malware campaign that has compromised numerous [U.S.] industrial control system environments using a variant of the BlackEnergy malware. Analysis indicates that this campaign has been ongoing since at least 2011."



The advisory also reported that "Multiple [U.S] companies working with ICS-CERT have identified the malware on *Internet-connected human-machine interfaces (HMIs)*" (emphasis added). An evolved variation of the BlackEnergy malware was later used in the December 2015 Ukrainian grid attack.

The debate about air-gap security — and whether it really exists — has been going on for years. As far back as 2011, a Siemens executive was quoted as saying "Forget the myth of the air gap – the control system that is completely isolated is history."

So why do industrial organizations continue to have Internet-facing systems? There are various reasons, but most of them can be summarized by convenience:

- **Remote management:** Industrial automation vendors and other contractors often prefer to access systems from a remote location in order to manage and maintain them, rather than physically travel to remote sites.
- **Software updates:** It's often more convenient to have devices connect directly to Internet servers for automatic software updates, such as Adobe patches and updated anti-virus signatures.
- **Web browsing:** Few ICS networks allow email or web browsing from the OT network, but this is sometimes a difficult policy to enforce.

The air-gap is also sometimes defined as a barrier between IT and OT networks. But it's clear that this IT/OT boundary is also quite permeable, including via:

- **Stolen credentials:** The easiest way to compromise the OT network is to steal legitimate credentials from a control engineer, typically via phishing. For example, this approach was used in the first Ukrainian grid attack, where the attackers leveraged stolen credentials to pivot from the IT network to the OT network over a VPN connection[3].

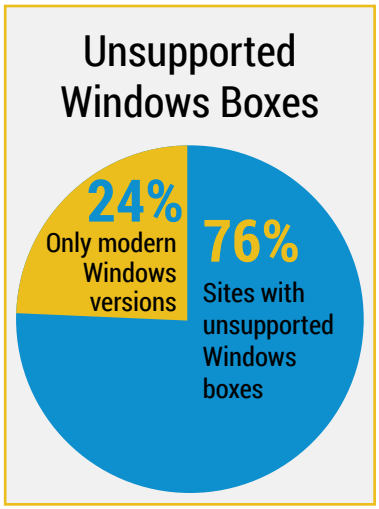
  This may also be North Korea's current strategy in attempting to compromise the US electric grid via recent phishing attempts against control engineers. Symantec (Dragonfly 2.0) and Cisco Talos also recently described how cyberattackers are targeting control engineers to steal their credentials, enabling them to bypass perimeter defenses and gain direct access to OT networks.
- **Infected laptops and USB drives:** In the Stuxnet attack, the OT network was compromised via infected laptops and USB drives that were connected directly to the OT network[4].
- **Supply chain compromise:** In the first wave of Dragonfly attacks against energy companies, the ICS-CERT reported that adversaries were attempting to compromise OT networks by infecting update installers with the Havex Trojan on at least three ICS vendor websites. This is similar to the way NotPetya spread via infection of Me.Doc updates.

4.2 Unpatchable Windows boxes - everywhere

More than 3 out of 4 industrial sites (76%) have obsolete Windows systems like Windows XP and Windows 2000 on their OT networks, which means these systems are no longer receiving security patches from Microsoft.

These systems can easily be compromised by older malware such as Conficker as well as by newer and more sophisticated malware such as ransomware, password-stealers and back-doors.

In addition, as legacy machines, they are typically unable to run modern endpoint detection and response (EDR) programs, which detect targeted attacks via real-time behavioral analytics on Windows endpoints.



WannaCry was a rare case of Microsoft issuing a security patch for some older versions of Windows like XP — but not for Windows 2000 — which illustrates the severity of the NSA EternalBlue exploit leaked by the ShadowBrokers. In fact, Microsoft wrote that it was "highly unusual" for them to provide a patch for unsupported versions of Windows. However, there are still hundreds or thousands of known vulnerabilities (CVEs) for older versions of Windows that will never be patched, making these Windows boxes ideal candidates for attackers to compromise.

[3] "Analysis of the Cyber Attack on the Ukrainian Power Grid" (page 6), March 18, 2016, SANS ICS.
[4] "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," November 3, 2014, by Kim Zetter, WIRED.

4.3 Weak authentication

Nearly 3 out of 5 sites (59%) have plain-text passwords traversing the network. These passwords can easily be sniffed by attackers performing cyber reconnaissance.

The next step in compromising these devices would be to log into the devices as an authorized user with the password that was just obtained. Depending on what privileges these users have, it could allow them to have full control of these devices, enabling them to manipulate critical control systems, such as shutting down assembly lines or closing valves in chemical or pharmaceutical plants.

4.4 No antivirus protection

Nearly half of the industrial sites we analyzed aren't even running basic antivirus (AV) protection on Windows endpoints. We've heard from customers that adding AV software to endpoints such as HMI workstations can sometimes void the warranty provided by their OT vendors. Vendors are concerned that the overhead of AV scanning software will impact the performance or reliability of their workstations.

Nevertheless, lack of AV protection increases the risk of having known malware on these systems — such as Conficker, WannaCry, and NotPetya — without even knowing about it.

Note that embedded devices such as PLCs aren't running any AV protection because they lack the CPU and memory resources to support scanning agents.

4.5 Unknown ("rogue") devices

44% of sites have at least one unauthorized or unknown device (rogue device). A rogue device can represent a simple gap in tracking new legitimate assets as they're added to your OT network — or it can represent a malicious device left behind by a malicious insider or 3rd-party contractor.

Security best practices suggest that you can't protect devices that you don't know you have. That's why most OT security initiatives start with a thorough asset discovery program to map all of your assets and how they're connected (network topology).

4.6 Known malware in the network

10% of the sites we analyzed were unaware they had known malware such as WannaCry, NotPetya, and Conficker in their industrial control networks.

While 10% seems like a relatively small number, it's a large number if you figure that — unlike in IT networks where the risk posed by an infected machine is typically loss of productivity as the machine gets rebuilt — in OT environments, these types of malware can have a material impact on your organization's financial results by disrupting production operations.

4.7 RDP & remote management protocols as attack vectors

82% of industrial sites are running remote management protocols such as RDP, VNC, and SSH.

This means that once an attacker has compromised the OT network, it's significantly easier for them to remotely access and control other devices on the network using standard administrative tools. As a result, remote access usage should be carefully monitored to ensure rapid detection of unauthorized or suspicious access.

Cyberattackers in the first Ukrainian grid attack used these types of tools to remotely control the Human Machine Interface (HMI) and open the circuit breakers. Additionally, RDP was recently used as a spreading mechanism by a new variant of the Petya ransomware.

4.8 Wireless Access Points (WAPs) as attack vectors

20% of sites we analyzed have at least one wireless access point. Poorly-configured or misconfigured WAPs increase the attack surface because they can be accessed by unauthorized clients, such as employee or contractor laptops and mobile devices. WAPs can also be compromised via the recently-discovered KRAC WPA2 vulnerability.

4.9 High number of vulnerable devices

On average, 28% of all devices in each industrial site are vulnerable. This includes non-Windows, embedded OT devices such as PLCs as well as standard Windows devices.

CyberX classifies devices as "vulnerable" when they have a security score of less than 70%, where the score is determined by examining the severity of all published vulnerabilities (CVEs) associated with the device, as well as configuration issues such as open ports.

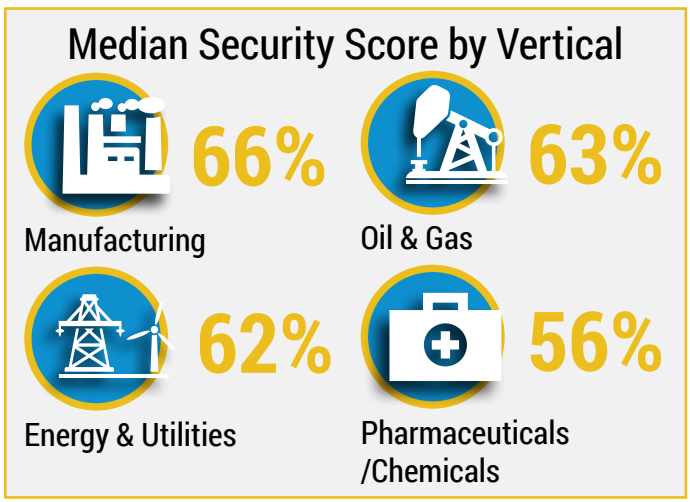
Vulnerable devices typically have critical CVEs representing high-impact vulnerabilities — such as buffer overflows — that provide attackers with complete control of the device. These vulnerable devices represent one of the weakest links in the security chain, and should be prioritized for remediation.

OT vendors have now incorporated Secure Development Lifecycle (SDLC) best practices and are typically quite responsive in patching known vulnerabilities. However, the challenges that OT end-user organizations face — of first testing patches, and then updating devices that often run 24x7x365, along with an absence of understanding the risk, combined with a false sense of security from years without any incidents — continue to prevent consistent patching of vulnerable OT devices.

4.10 Benchmarking ICS & IIoT risk across industries

The results show that there aren't wide variations in risk across various industry verticals, with all industries showing scores within +/- 5 percentage points of the median score of 61% across all sites in our sample.

But the main conclusion is that all industries have a long way to go, in order to approach CyberX's minimum recommended score of 80%.



5.0 Visualizing Attack Vector Chains

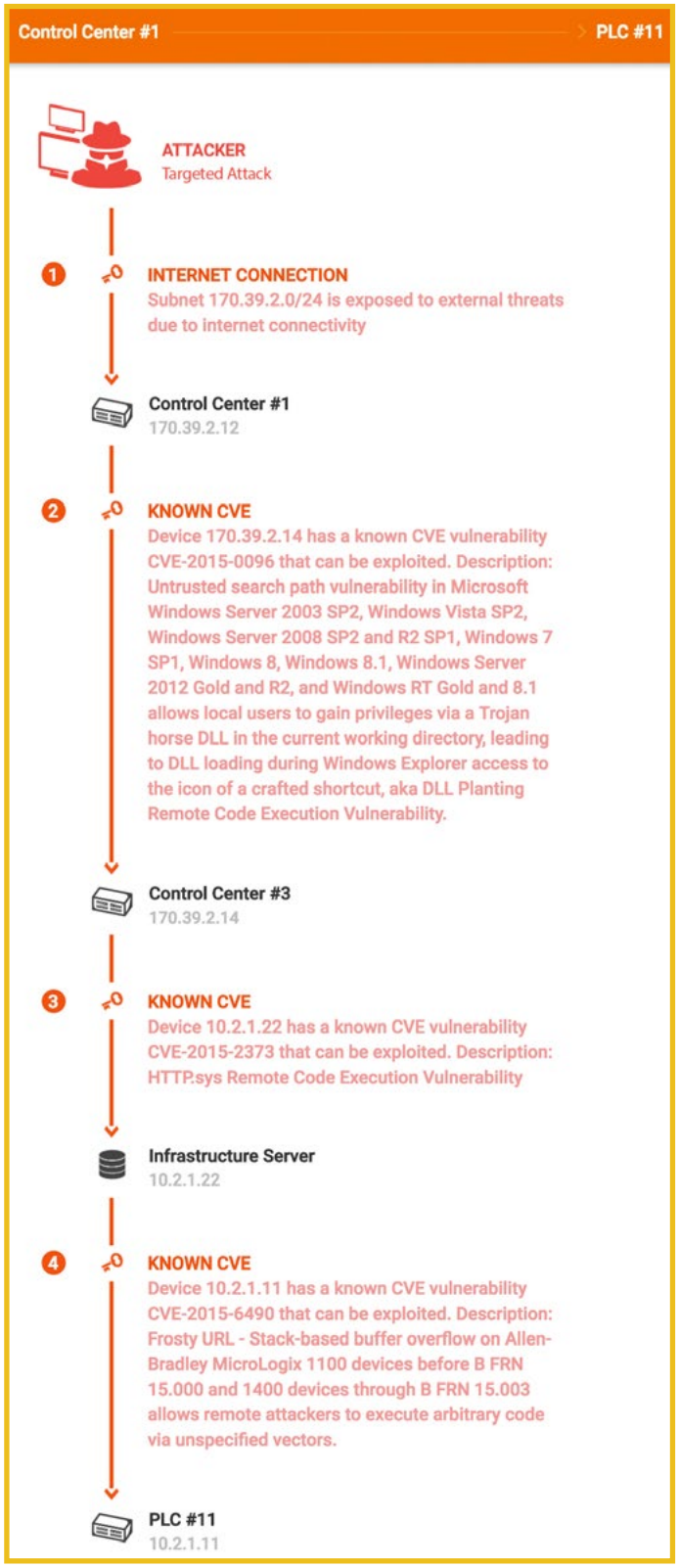
CyberX's ICS Attack Vector Prediction technology incorporates proprietary analytics and machine learning to continuously predict the most likely paths of targeted attacks on ICS/SCADA networks.

Understanding these paths and implementing mitigations for them, combined with continuous monitoring of their choke points, are primary aspects of mounting an Active Cyber Defense.

CyberX's Attack Vector Prediction uses the vulnerability data discussed in this report as input for a particular organization.

By generating a visual representation of all possible attack chains, it enables security teams to prioritize essential mitigations and simulate what-if scenarios to reduce their attack surface, such as "If I isolate or patch this insecure device, does it eliminate the risk to my most critical assets?"

In this example, Internet access on a particular subnet is used to gain initial access. The attacker then exploits a chain of known vulnerabilities to move laterally within the OT network, eventually compromising PLC #11.



6.0 Recommendations

Upgrading Windows systems and vulnerable devices environments is a lengthy and complex process. Many of these systems run 24x7 and have limited maintenance windows.

Also, many legacy Windows systems host SCADA applications that would need to be extensively tested or even re-written after an upgrade.

Here are 4 ways to address the complexity of securing legacy OT environments today, short of investing billions in infrastructure upgrades:

6.1 Implement a multi-layered defense with continuous monitoring

A multi-layered defense removes the reliance on perimeter security as the sole control, since perimeter security is no longer sufficient to protect against targeted attacks, sophisticated malware, and insider threats.

A key aspect of a multi-layered defense is continuous monitoring and anomaly detection, which helps defenders immediately identify unusual or unauthorized activity on their OT networks, such as adversaries performing cyber reconnaissance in preparation for an attack. In the December 2015 Ukrainian grid attack, for example, adversaries persisted in the environment for 6 months or more before executing their attack[5].

SANS refers to this multi-layered approach as "Active Cyber Defense." As defined by SANS, it's the process of using security operations to continuously identify and counter threats. The Active Defense Cycle consists of four phases that continuously feed each other to create an ongoing process: asset identification and network security monitoring; incident response; threat and environment manipulation (e.g., addressing vulnerabilities); and threat intelligence consumption.

6.2 Proactively address the most critical vulnerabilities

It's seldom practical to remediate or mitigate all vulnerabilities, but you can start by identifying your most critical assets — such as devices controlling your most important production processes — and then perform automated threat modeling to identify and address the most likely attack paths to those assets.

As shown in Section 5, some continuous monitoring systems automatically create simulations of all potential attack paths and then provide recommendations for the best way to break them. This can include deploying specific patches, eliminating plain-text passwords for particular devices, or implementing better network segmentation.

6.3 Educate plant workers and enforce strong corporate policies

As in corporate IT networks, raising awareness of risky behaviors can go a long way to reducing risk.

The first step is educating plant personnel about the risk of clicking on phishing emails, using Dragonfly 2.0, Cisco Talos reports, and recent North Korean attempts as examples. Other risky employee behaviors include:

- Plugging personal laptops and USB drives directly into the OT network.
- Sharing VPN credentials with third-party vendors and/or temporarily opening Internet connections to third-party vendors to facilitate remote maintenance[6].
- Dual-homing OT workstations between IT and OT, which adds an additional entryway from IT to OT networks.
- Installing unauthorized Wireless Access Points (shadow IT).

6.4 Break down the barriers between OT and IT

IT and OT teams have a lot to teach each other about their respective disciplines. Management needs to create a top-down culture that fosters a belief that "we're all in this together, so let's help each other."

Get people to understand that if malware or targeted attacks infect the plant, everyone suffers — downtime can lead to work stoppages, a decline in stock price, and slower growth and hence opportunities for career advancement.

One way to start is by integrating OT personnel into your Security Operations Center (SOC). Another is to assign IT security people to the OT organization for temporary assignments, so they learn first-hand how control systems work, and about the differences between IT and OT.

[5] "Analysis of the Cyber Attack on the Ukrainian Power Grid" (page 3), March 18, 2016, SANS.
[6] In fact, it's also a good idea to implement 2-factor authentication for VPN connections to protect against credential theft from employees and 3rd-party contractors.

Appendix

Appendix A: Methodology

CyberX analyzed production traffic from 375 OT networks worldwide across all sectors — including energy & utilities, manufacturing, pharmaceuticals, chemicals, and oil & gas — using its proprietary Network Traffic Analysis (NTA) algorithms.

Similar to the methodology used for the Verizon Data Breach Investigations Report (DBIR), the analysis was performed on an anonymized and aggregated set of metadata with all identifying information removed. Rigorous attention was paid to preserving the confidentiality of sensitive customer information.

We make no claims that the findings of this report are representative of all organizations at all times, but we found the results to be fairly consistent across our sample set and believe many of the findings are appropriate for generalization.

Appendix

Appendix B: About CyberX

CyberX provides the most widely-deployed industrial cybersecurity platform for continuously reducing ICS risk, enabling organizations to prevent costly production outages, catastrophic safety failures, and theft of corporate IP.

Founded by military cyber experts previously responsible for defending critical national infrastructure, CyberX is the only OT security firm selected for the SINET Innovator Award sponsored by the US DHS and DoD; the only one recognized by the International Society of Automation (ISA); and the only one selected by the Israeli national consortium providing critical infrastructure protection for the Tokyo 2020 Olympics.

CyberX addresses the need for robust industrial security with continuous ICS threat monitoring and asset discovery, combining a deep understanding of industrial protocols and devices with ICS-specific behavioral analytics, threat intelligence, and risk analytics. The company's platform is 100% vendor-agnostic and integrates seamlessly and non-intrusively with all OT environments and IT security tools.

With a long history of innovation, CyberX was the first OT security supplier to address all four requirements of Gartner's Adaptive Security architecture: Prediction, Prevention, Detection, and Response.

For more information visit CyberX-Labs.com
or follow @CyberX_Labs.