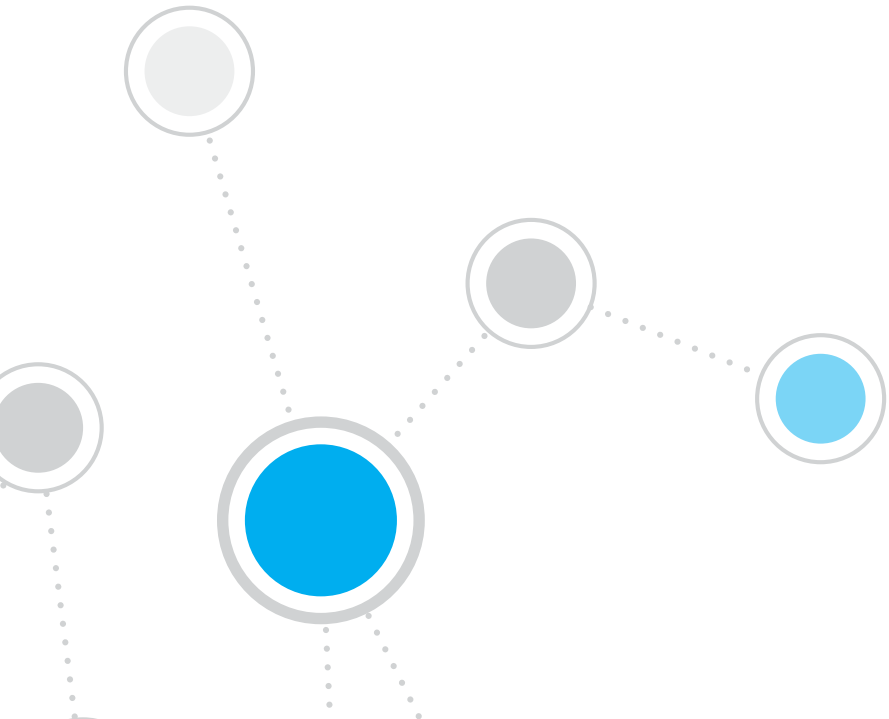
FORESCOUT

Gain Confidence in Protecting Critical Infrastructure from Cyberattacks

Knowing who—or what—is on your network is the first step to ensuring the security of critical infrastructure



Protecting Critical Infrastructure Is a Local and Global Imperative

Consider the services that society counts on everyday—everything from the electric grid, to utilities, to transportation systems, to communications networks, and more. Increasingly, these vital systems face potential disruption from both natural and man-made disasters. Protecting the connected services of the information technology (IT) and operational technology (OT) systems that keep critical infrastructure running 24/7 is a top local and global imperative.

In this white paper, we pay particular attention to the public and private critical infrastructure sectors that use OT as a part of their operations. Within that context, we lay out the cyber-risks that owners and managers of critical infrastructure are dealing with today. We list some of the most notable cybersecurity attacks on critical infrastructure in recent years and explain why traditional IT cybersecurity measures aren't successful in OT critical infrastructure scenarios. In addition, we introduce common regulations that govern security practices in these sectors. We elaborate on how network visibility and control are foundational components of a successful critical infrastructure cybersecurity strategy. Finally, we show why ForeScout offers a solution that can help you translate such a strategy into action.

The Department of Homeland Security (DHS) has named 16 different industry sectors that possess, manage or maintain critical infrastructure.[1] The assets and services provided by the organizations in these sectors are considered so important that destroying or impairing them would have "debilitating effect(s) on security, national economic security, national public health or safety, or any combination thereof."[2]

Common Sectors of Critical Infrastructure

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials & Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector

Challenges: Critical Infrastructure Already Under Cyberattack

The world has already seen examples of attacks and how risk to critical infrastructure can play out. Here are some examples of attacks on critical infrastructure that have raised awareness:

- In 2014, the "Energetic Bear" virus was found in more than 1,000 energy companies throughout 84 countries. Although the virus did not cause damage, it could have severely impacted important components in those facilities, including wind turbines, gas pipeline pressurization and transfer stations, port facilities and electric power plants. Because systems remained operational, researchers believe the virus was primarily being used for espionage, although some suggested that a nation-state had "pre-positioned it as an attack mechanism to disrupt national-scale gas suppliers" at some later date.[3]
- In 2016, seven cybercriminals from Iran were accused by the U.S. Department of Justice of successfully penetrating the computers that controlled the operations of a dam in Rye Brook, New York, approximately 25 miles north of New York City. The incident itself occurred in 2013, when the hackers infiltrated the dam's command-and-control system, but was not reported until three years later. The only factor that prevented the hackers from remotely unleashing water from the dam was that the sluice gate was disconnected for maintenance from automated computer controls at that particular time. Although a relatively minor incident, this represented a warning of how easily malicious cybercriminals and nation-states could attack critical infrastructure. "They were sending a shot across our bow," Senator Charles Schumer said at the time.[4]
- In 2017, a massive ransomware attack crippled hospitals in the United Kingdom, forcing patient appointments and operations to be canceled. The "WannaCry" ransomware locked down all the files on infected computers and demanded payment to regain control. At least 16 health service organizations in the National Health Service (NHS) were impacted.[5]
- In 2018, a distributed denial of service (DDOS) attack crippled the ticketing system of the Danish Railway. This is in addition to October 2017 DDOS attacks in Sweden that caused serious operational delays across its transportation network. By using a traditional attack method, the perpetrators were able to crash the IT system that monitors train locations as well as disrupt email systems, websites and traffic maps.[6]

So far, the world has been fairly fortunate in that the damage has been contained relatively quickly. But the potential for incurring high costs is immense.

In *Business Blackout*, a joint report by Lloyd's of London and the University of Cambridge's Centre for Risk Studies, researchers studied how a hypothetical cyberattack on the U.S. power grid would impact the country. Under this scenario, malware infected electricity generation control rooms in the Northeastern United States, taking control of 50 generators that possessed a specific technical vulnerability and causing them to overload and burn out. Economic losses were estimated to be $243 billion, increasing to more than $1 trillion in the most extreme version of the scenario. And this wasn't even considering aspects beyond the business impact. For example, what would the cost in human lives be if hospitals or first responders were put out of action due to a break in the energy supply?[7]

Lifeline Sectors: Certain Critical Infrastructure Sectors Must Be Secured

Maintaining the security of six critical infrastructure sectors is essential to prevent cascading effects on other sectors, on the global economy, and on societies in the event of successful cyberattacks.

Energy

The world cannot function today without a reliable supply of energy. If the energy sector ceases to function efficiently and effectively, other sectors will falter, too.

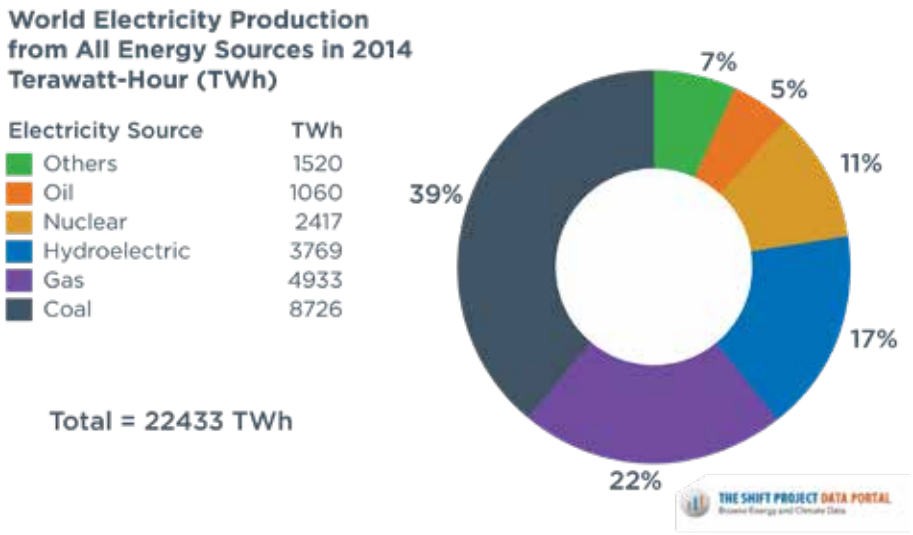


Figure 1: Global electricity production by energy source.[8]

To address cybersecurity in both IT and OT environments, ABI Research estimates that global spending on cyber protection of energy will total $8 billion in 2018 and $15 billion by 2023. The majority of cybersecurity spending will be focused on the electric power grid, specifically to secure generation, transmission and distribution as the most critical aspects of the grid.[9]

Non-Energy Utilities/Public Services

In addition to the electric grid, other utilities and public services are greatly at risk of cyberattacks. This broad sector includes public agencies that are responsible for providing clean drinking water, wastewater and sewage processing, and garbage collection and management. This category also includes emergency first-responder services, government activities that allow civic life to flourish, and a multitude of other services. These essential services for enabling citizens to go about their day-to-day lives around the globe have been particularly targeted in the past 12 to 18 months with malware/agents such as malicious Word documents embedded within PDF documents.[10]

Transportation

The U.S. Department of Homeland Security identifies seven key subsectors of the transportation sector, each of which has increasingly automated and digital infrastructure that must operate smoothly if societies and economies are to function: aviation, highways and motor systems, maritime transportation systems, mass transit and passenger rail,

pipeline systems, freight rail, and postage and shipping.[11]

Cyberattacks against transportation infrastructure—particularly airports—have been increasing recently. In September 2018, critical applications at the Bristol airport (UK) were taken offline due to a ransomware attack. In March 2017, the Atlanta airport—one of the busiest in the world—shut down its free Wi-Fi network and disabled some of its website's key functions after a citywide ransomware attack took down the city of Atlanta's network. Two Ukrainian airports were also affected by a variant of the Petya virus in 2017.[12]

Communications

Like energy, the DHS has named the communications sector as an "enabling function," as it is the foundation for the safe and secure operations of all businesses, public safety services and government operations.[13]

Globally, this is a highly diverse and extremely competitive segment that depends on earth-bound satellite and wireless transmission systems that are interconnected even as they are distributed throughout the world. Although largely privately owned, this sector is heavily regulated by governmental mandates, and communications operators must work closely with local, regional and even international governmental bodies to ensure that they operate in a way that benefits citizens, businesses and public organizations alike. Communications infrastructure is extremely vulnerable, as the data types it encompasses—photographs and videos as well as voice and text—are highly sensitive and affect the privacy of individuals, businesses and government agencies. As such, this sector is high on cyberattackers' lists of targets.

Healthcare

Healthcare is one of the industries at greatest risk of cyber intrusions. The list of successful cyberattacks is long.[14] Primarily, hackers are after patient or research data. However, as in Britain's NHS cyberattacks mentioned earlier, there is the real risk of the attack shutting down healthcare operations.

Healthcare organizations are aware of this, and are investing accordingly. Cybersecurity Ventures predicts global healthcare cybersecurity spending will exceed $65 billion cumulatively by 2021.[15] In the United States, the DHS' Healthcare and Public Health Sector-Specific Plan provides details on how this sector should protect itself.[16] The EU is working on a similar plan. But complicating the matter is the growing number of interconnected medical devices entering the market that are vulnerable. "White hat" hackers are exposing security weaknesses[17] and vendors are self-disclosing issues[18] in infusion pumps, EEG scanners and dispensing equipment, raising worries about intelligent devices that are both used in medical procedures and being implanted into human patients.[19]

Compliance: Regulations Enforce Cybersecurity Practices

Not surprisingly, governments and other regulatory bodies have stepped in to establish guidelines and regulatory mandates to protect critical infrastructure. Two regulations in particular that are having significant global impact and merit special attention are the EU-NIS and the U.S. NERC-CIP.

Below we explain these two important critical cybersecurity infrastructure regulations.

The European Union Network and Information Systems (EU NIS) Directive

The EU NIS directive 20 was first proposed in 2013 as a means of unifying the member states of the European Union in achieving a high common level of cybersecurity for critical infrastructure. It identified three key goals:

- Improve national cybersecurity capabilities
- Increase cooperation between EU member states
- Require "operators of essential services" (OES) and "digital service providers" (DSPs) to take "appropriate and proportionate" security measures, and notify national authorities of any serious incidents

The directive became law in August 2016. EU countries—including the United Kingdom, despite Brexit—had until May 2018 to translate the directive into national laws. They then have an additional six months to identify the organizations that own or manage critical infrastructure, and therefore must adhere to those laws. These entities include providers of electricity, transport, water, energy, transportation, healthcare and digital infrastructure services. Fines for noncompliance could be as high as £17 million or 4% of the erring organization's global turnover (or, according to a Dutch draft of the law, fines could reach as much as €5 million).[21]

In the UK, a National Cyber Security Centre has been created to provide proactive cybersecurity leadership and guidance on passing laws that meet the NIS Directive. The NCSC has further defined a set of guidelines under a Cyber Assessment Framework (CAF) for implementing strong security principles. Some EU countries are doing the same, but others seem to be taking a reactive, compliance-based approach that only meets minimum requirements.[22]

At the end of the day, much is going to be determined by the individual member states and how they choose to interpret what "appropriate and proportionate" security measures mean in terms of compliance and the security of their citizens and businesses.

North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)

In the United States, no single directive applies across all critical infrastructure industries. For each individual sector, there is either industry self-regulation or government regulations. However, the U.S. does have NERC CIP. The NERC CIP plan consists of more than 100 standards and requirements for protecting critical infrastructure assets in the nation's bulk electric systems and the systems that support those assets.[23] A complete list of covered functions and entities is available from NERC's compliance registry.[24]

CIP is just one of 14 NERC standards. But it is in the spotlight because it focuses on cybersecurity.

Not complying with NERC can be costly. Because NERC covers both the United States and Canada, the exact penalties vary. In the United States, the Federal Power Act permits NERC or regional entities to impose penalties of up to $1 million per day per violation.[25]

Although data integrity and privacy are both important, system availability is the most important factor for NERC CIP-affected as well as other critical infrastructure organizations. That priority alters the cybersecurity technologies techniques that should be used in critical infrastructures.

For additional information on global compliance, refer to articles such as, *"The protection of critical infrastructure against terrorist attacks: Compendium of good practices,"* compiled by Interpol and the United Nations Security Council.[26]

DFARS (Defense Federal Acquisition Regulations Supplement) /NIST 800-171

Recognizing the need to protect federal infrastructure, the Department of Defense (DoD) now requires all contractors that process, store or transmit Controlled Unclassified Information (CUI) to meet DFARS minimum security standards or risk losing their DoD contracts.

NIST 800-171 provides a framework for all companies that conduct business with the DoD to protect CUI. This includes prime contractors, subcontractors, research universities, chemical/pharmaceutical manufacturers, in fact, any company that has business interests with the DoD. For many companies, these contracts represent a large portion of their annual revenue.

Complexities: Why Securing Critical Infrastructure Isn't Straightforward

Whether attempting to comply with NERC CIP or EU NIS, or simply trying to improve your organization's cybersecurity status on your own initiative, the inevitable question arises: why haven't critical infrastructure organizations using OT found a comprehensive solution to these problems?

The answer? Because it isn't easy to come up with a uniform response.

Critical infrastructure has been built upon many different types of technologies over the years. Many systems are decades old—developed well before the Internet became mainstream. Many depend on hardware, software and operating systems that aren't compatible with today's technology. In fact, many of these systems use legacy proprietary operating systems, languages and protocols.

Operational technology assets that run critical infrastructure complicate matters considerably.

Most critical infrastructure facilities lack a complete, up-to-date inventory of their OT assets despite the need for safety, security and compliance. Ensuring 24x7 operations while maintaining diversity of technology, devices and protocols, not to mention the critical nature of the OT equipment, means extreme caution is needed to ensure that whatever security solutions are deployed do not put either physical safety or operational uptime at risk.

Previously, utilities and other organizations maintained cybersecurity by using "air gaps" to physically isolate secured operational computers, systems or devices from the non-operational part of the organization or unsecured networks, such as the public Internet. But significant efficiencies can be realized by interconnecting OT and IT systems, and critical infrastructure vendors have built these efficiencies into their technologies—with or without cybersecurity functionalities. A SANS survey found that 32% of IIoT organizations connect their critical infrastructure systems directly to the Internet,[27] which means they are ignoring security best practices and exposing their systems to potential threats.

Faraday rooms are also popular. These are "cages" designed to prevent electromagnetic signals from escaping. Some organizations even use both techniques, with air-gapped computers used for their most sensitive data also secluded in a hermetically sealed Faraday room. However, early in 2018, researchers from Ben-Gurion University demonstrated that a Faraday room and an air-gapped computer disconnected from the Internet, even when used together, do not prevent sophisticated cyberattackers from penetrating systems.[28]

Current IT Practices Not Up to the Task

Conventional IT security measures don't always work well for OT critical infrastructure. Take patching, for example. The *SANS Industrial IoT Study* shows that security patching is a top concern of organizations.[29] They know it's critical for safety—and even profitability—yet there are many difficulties inherent in doing it right. Chief among them: how to patch what needs to be patched without disrupting the rest of the critical infrastructure.

Indeed, rather than disrupt operations, many companies simply forgo patching and other important security measures. A recent Forrester Research study[30] revealed that 59% of respondents were willing to take medium-to-high risks with regard to their security practices, even in regulated environments.

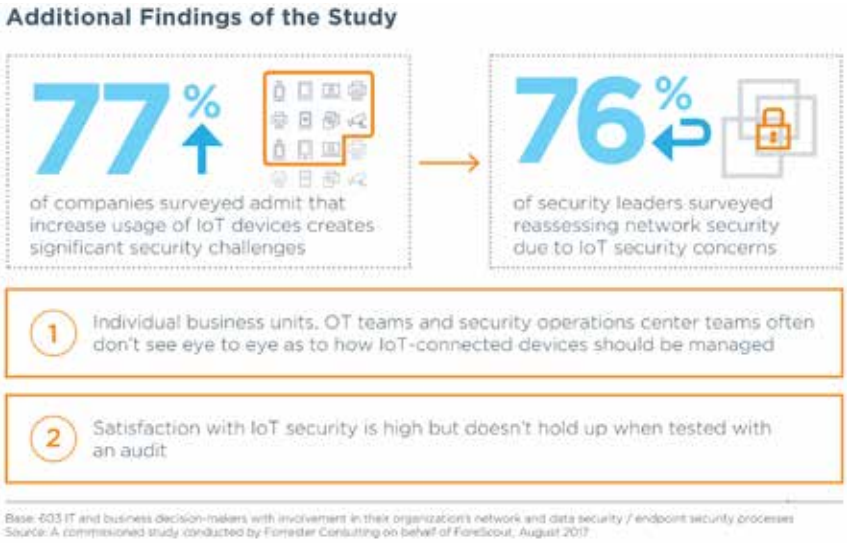


Figure 2: Global electricity production by energy source.[8]

Conventional network security monitoring and management tools are not always applicable in areas with automated equipment such as industrial control, and they tend to be less than effective in other ways when it comes to critical infrastructure using OT. Here are some of those weaknesses:

- **Offer limited visibility into OT and clinical assets**. Traditional network management tools do not easily detect, inspect or classify OT assets, leaving large blind spots in security defenses. Hackers use tools that inspect for unsecured Internet connections, so it is often the unknown devices or devices with unknown status that pose the greatest risk to organizations.
- **Rely upon active security measures.** Active security measures, in which a security solution not only detects an issue or potential threat, but also automatically takes remediation steps, can be very useful in a traditional IT environment. But in OT environments, active security techniques have the potential to disrupt control systems and could potentially impact business-critical operations. Any solution you deploy must first follow the adage: do no harm.
- **Aren't designed for critical infrastructure.** Legacy critical infrastructure equipment and operating systems weren't designed to accept the security software agents that most network management and monitoring tools require you to install on individual devices. Such agents require frequent updates in the form of patches to stay current, and that simply isn't possible in critical infrastructure environments where uptime is of utmost importance.

Analysis: The Source of the Problem Is Lack of Visibility

Visibility is a foundational requirement of critical infrastructure cybersecurity and compliance. If a particular network asset isn't identified (and effectively invisible), you can't protect it from hackers.

Traditionally, critical infrastructure organizations generally had two options in understanding the security posture of their assets: 1) to perform periodic, manual inventories using pen and clipboard, then input and track their network devices, or 2) use an agent-based solution that would quickly be out of date. The former was not only time-consuming, it meant that the inventory was subject to input errors. The latter required installing—and continuously updating—agents on each device on the network.

Agents don't work for OT devices and other non-standard equipment in critical infrastructure environments. In fact, the previously mentioned SANS IIoT study noted that security patching was identified as one of the greatest challenges in the next two years (see Figure 3).

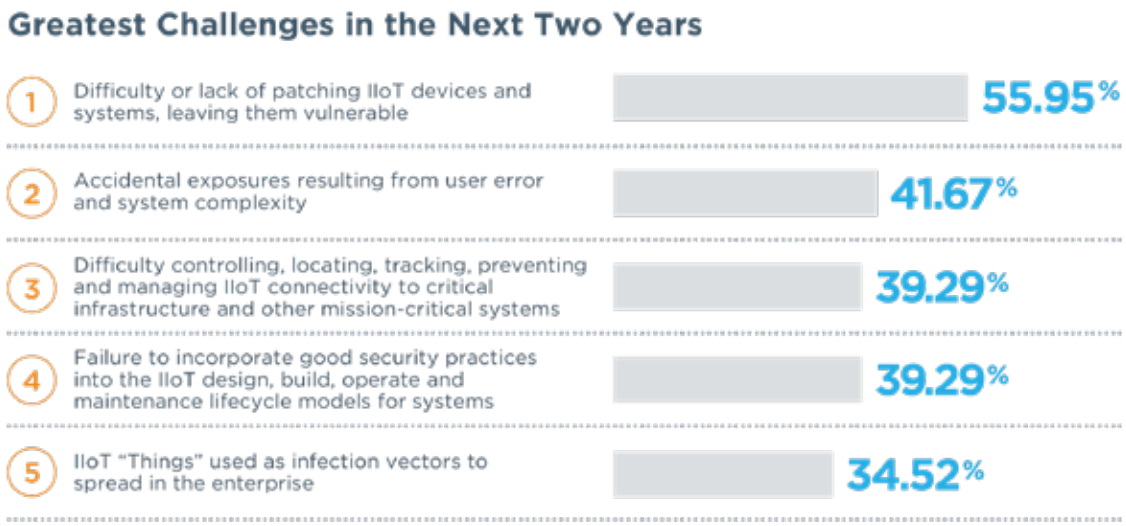


Figure 3: Challenges in making IoT devices compliant (Source: SANS IIoT survey).[31]

However, the critical infrastructure assets that are most vulnerable are not IoT devices but the outdated, unpatched pieces of traditional IT infrastructure mixed in with the OT critical infrastructure environment. In a recent SANS survey of hundreds of IT and ICS security professionals, 70% considered their traditional computer assets to be at greatest risk of compromise.[32] (see Figure 4)

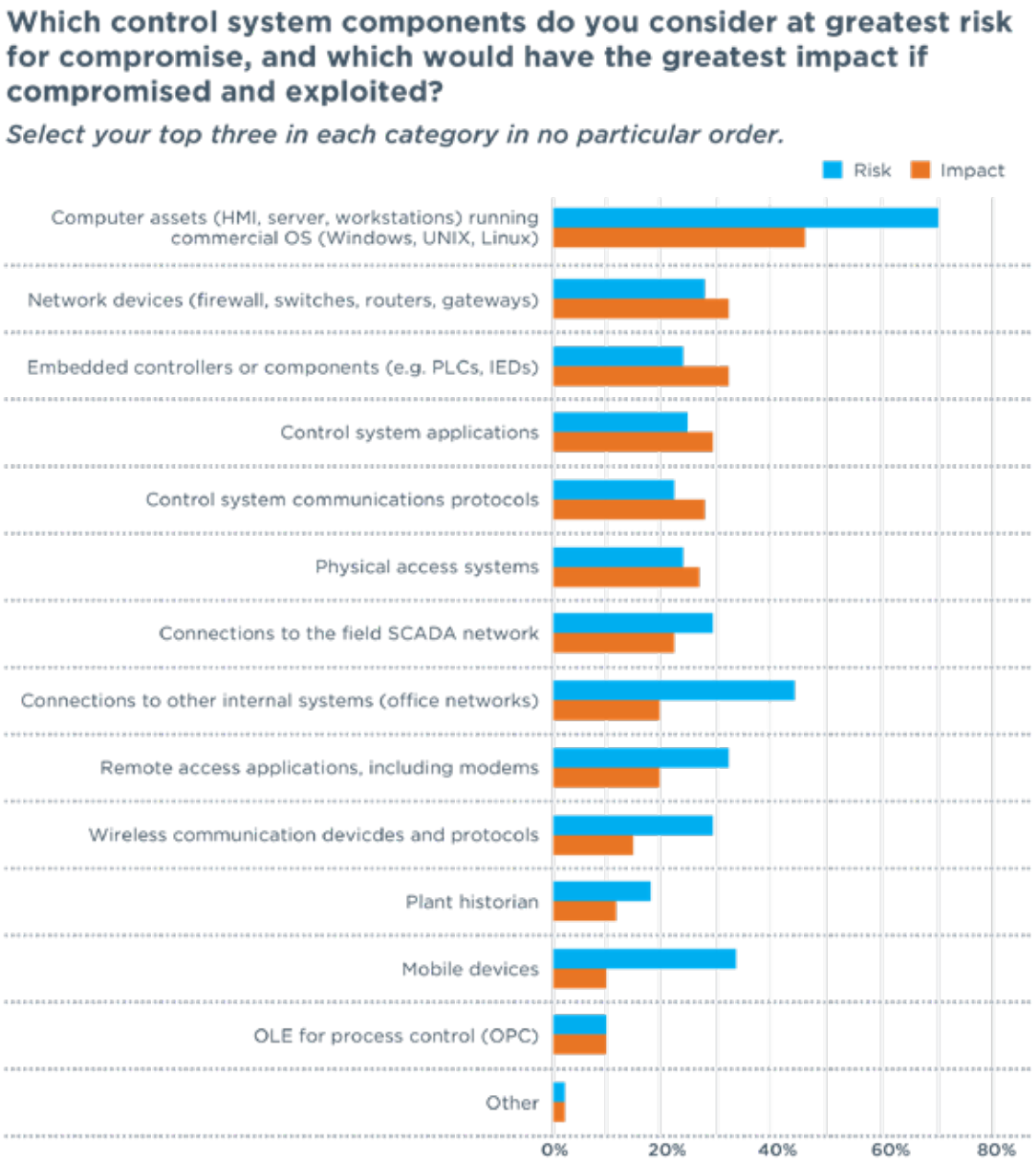


Figure 4: Network components that are most at risk (Source: *SANS Securing Industrial Control Systems-2017 survey*) [32]

Considerations: Building a Secure Critical Infrastructure

Some of the attributes to look for in cybersecurity solutions for critical infrastructure environments include:

Performs non-disruptive asset discovery

Critical infrastructure needs to be operational 24/7, so security measures that perform disruptive, active techniques that have the potential to take equipment offline cannot be used. You need solutions that give you the option of using passive techniques to perform asset discovery and classification to build an accurate, foundational inventory of asset intelligence.

Offers agentless, vendor-agnostic operations

Critical infrastructure environments have a heterogeneous mix of equipment from different vendors that offer varying levels of IT functionality, so security techniques that require uniform operating environments are difficult and costly to deploy. You need a solution that operates without agents, and that works across all types of devices from all types of vendors—even those devices that don't depend on the 802.1X protocol.

Focuses resources where most threats occur

As it turns out, most security risks for critical infrastructure lie within the IT layers of your network environment, such as IT-based controllers or embedded IT operating systems. This is the "messy" part of your IT environment, containing operating systems such as Windows 98 or other outdated or proprietary software that can't be patched by today's security tools. Even when attackers target industrial control system devices, they tend to go through IT layers to reach them.

Performs continuous monitoring

Be sure to choose a solution that continuously monitors the network so that device intelligence and status is always available in real time. Whenever a solution detects an anomalous or out-of-policy activity, it alerts and takes appropriate action based on outlined security policies.

Delivers risk-mitigating controls and compliance on demand

The solution should identify and classify a device from the moment it connects to the network, and should make sure that it complies with your security policies. However, it should do this without ever taking devices offline. This way, you ensure that you are following best practices for securing network devices while not putting the availability of critical systems at risk.

Can be integrated and orchestrated with other cybersecurity vendors' solutions

Most IT environments today are heterogeneous. As a result, a typical critical infrastructure organization will have as many as a dozen or even more vendors' security products operating in independent security management silos. This disjointed approach prevents coordinated, organization-wide security responses, allowing attackers more time to exploit system vulnerabilities. The manual, inefficient processes that are necessary in this scenario also can't easily scale.

Security solutions should orchestrate infrastructure-wide security management to make security products work together. To be effective, the number of partners the solution provider works with should be large and include leading cybersecurity vendors. A vendor that coordinates interoperability among all tools within one's security ecosystem enables

accelerated response, major operational efficiencies and superior security.

Scales to even the most demanding critical infrastructure environment

The numbers of IoT and OT devices on critical infrastructure environments are expanding day by day. To keep pace with this device growth, choose a solution that can scale to millions of devices in a single deployment.

Conclusion

Society today depends on a complex matrix of digital properties, products and services to function. From highway networks, water systems and transportation hubs to oil and gas distribution pipelines, smart power grids and wide-area information networks such as the Internet, we rely on critical cyber infrastructure to simply work so we can go about our daily lives. So important is this critical infrastructure that government organizations are busily creating regulations mandating that sufficient cybersecurity controls are put into place to keep it constantly operational.

But traditional IT security defenses won't work with OT critical infrastructures, as evidenced by increasing numbers of successful attacks.

ForeScout helps reduce risk. By giving you instantaneous visibility into every connected device, the ForeScout platform offers you control over who—or what—accesses your IT environment. As a pioneer and leader in innovative network security solutions, ForeScout provides you with unprecedented transparency—simply and cost-effectively. The instant any device attaches to your network, you know all about it—no software agent required. We continuously monitor to detect rogue or unsafe devices. And because we believe that collaboration and openness keeps us all safer, we work with other leading security vendors to keep your technology investments intact and your business compliant and secure. Today, almost 3,000 customers in more than 80 countries depend on ForeScout.

Additional resources

Implementing EU NIS with the Cyber Assessment Framework

Compliance Guide

OT Datasheet

Government Solutions Page

Compliance Web Page

Operational Technology Web Page

Healthcare Web Page

About ForeScout

ForeScout Technologies is Transforming Security through Visibility™ by providing Global 2000 enterprises and government agencies with agentless visibility and control of traditional endpoints, IoT devices, operational technologies, virtual instances and cloud workloads the instant they connect to the network. Our technology continuously assesses, remediates and monitors devices and works with disparate security tools to help accelerate incident response, break down silos, automate workflows and optimize existing investments. As of June 30, 2018 more than 2,900 customers in over 80 countries improve their network security and compliance posture with ForeScout solutions. See devices. Control them. Orchestrate system-wide threat response. **Learn how at www.forescout.com.**

[1, 2] https://www.dhs.gov/critical-infrastructure-sectors

[3] https://www.nytimes.com/2014/07/01/technology/energy-sector-faces-attacks-from-hackers-in-russia.html?_r=0

[4] http://time.com/4270728/iran-cyber-attack-dam-fbi/

[5] https://edition.cnn.com/2017/05/13/health/uk-nhs-cyber-attack/index.html

[6] https://www.transportsecurityworld.com/ddos-attack-cripples-danish-rails-ability-to-sell-tickets

[7] http://www.lloyds.com/-/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf

[8] http://www.tsp-data-portal.org/Breakdown-of-Electricity-Generation-by-Energy-Source#tspQvChart

[9] https://www.abiresearch.com/press/us8-billion-spend-secure-smart-utilities-inadequate-cyberthreats-utility-infrastructure-grave/

[10] https://engage2demand.cisco.com/LP=6449

[11] https://www.dhs.gov/transportation-systems-sector

[12] https://www.scmagazine.com/home/news/bristol-airport-hit-with-ransomware-attack/

[13] https://www.dhs.gov/communications-sector

[14] https://www.csoonline.com/article/3252343/cyber-attacks-espionage/why-healthcare-cybersecurity-spending-will-exceed-65b-over-the-next-5-years.html

[15] https://cybersecurityventures.com/healthcare-cybersecurity-report-2017/

[16] https://www.dhs.gov/publication/nipp-ssp-healthcare-public-health-2015

[17] https://www.theregister.co.uk/2015/10/13/brain_waves_security/

[18] https://ics-cert.us-cert.gov/advisories/ICSMA-18-233-01

[19] https://www2.deloitte.com/ch/en/pages/risk/articles/medical-devices-cybersecurity-vulnerable.html

[20] https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii/nis-directive

[21] https://www2.deloitte.com/nl/nl/pages/risk/articles/why-do-you-need-to-know-about-the-nis-directive.html#

[22] http://www.techcentral.ie/national-cybersecurity-strategy-can-help-ireland-cement-place-infosec-hub-within-europe/

[23] https://searchcompliance.techtarget.com/feature/What-is-NERC-CIP-and-ITs-role-in-critical-infrastructure-protection

[24] http://www.nerc.com/page.php?cid=3|25

[25] https://www.ferc.gov/about/ferc-does/ferc101.pdf

[26] https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-CIP-final-version-120618_new_fonts_18_june_2018_optimized.pdf

[27] https://www.forescout.com/2018-sans-industrial-iot-security-survey/

[28] http://in.bgu.ac.il/en/pages/news/faraday_cages.aspx

[29] https://www.forescout.com/2018-sans-industrial-iot-security-survey/

[30] https://www.forescout.com/iot_forrester_study/

[31] https://www.forescout.com/2018-sans-industrial-iot-security-survey/

[32] https://www.sans.org/reading-room/whitepapers/ICS/securing-industrial-control-systems-2017-37860

Learn more at
www.ForeScout.com

FORESCOUT

ForeScout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Fax +1-408-371-2284