FORESCOUT
Active Defense for the Enterprise of Things.

SECURING THE NEW, “SMART” NORMAL

Prepared by
Jill Klein, Senior Leader, IoT and Healthcare
and Kevin Rota, Principal Consultant
Sirius Computer Solutions, Inc.

with Elisa Costante, VP of Research
Forescout Technologies Inc.

December 2020

SIRIUS

Contents

Executive Summary

The integration of Internet of Things (IoT) technologies into work environments and business operations is creating a new, “smart” normal that is often built on—and sometimes forcing—the merger of information technology (IT) and operational technology (OT) systems. This integration, due to incompatible technologies, protocols, processes and even cultures, can sometimes introduce substantial risk into your environment.

The purpose of this Sirius/Forescout white paper is to educate senior leaders and engineering team members on security threats that can result from the collision between OT and IT, and to provide integration strategies that will help prevent security risks as you embrace the new, “smart” normal.

Emerging technologies are changing the definition of normal operations

Faced with business and resource challenges unprecedented in our lifetimes, organizations are investing in emerging technologies to help them optimize their resources and make their operations more resilient—investments that could also offer a competitive or operational advantage after the pandemic. These solutions often utilize new data sources that provide insights that can lead to additional cost savings. But that means interfacing with physical access control systems, edge gateways, storage systems, IP cameras and network management systems, all of which are referenced as potential risk points in a recent report by Forescout as discussed later in this paper.

For example: Safer workspaces through smart, integrated technologies

As organizations strive to ensure a safe environment for employees and customers during the pandemic, IoT technologies can provide insights that are critical to the health of employees and the safety of their workspaces. These technologies are capable of evaluating persons entering the building with elevated body temperatures, and can even trace where they have been and with whom they may have come in contact during their workday. Features like machine vision provide people-counting capabilities, and can also provide automated social distance monitoring, alerting employees when they fail to maintain a pre-set threshold of physical separation. And they can do it all without human intervention unless an alert is generated.

Effective back-to-work solutions require tight integration across a wide variety of technologies, manufacturers, protocols, and business units.

Challenges Caused by the Integration of IT and OT

As the need to share information across traditionally air-gapped boundaries of IT and OT increases, the complexities of IT-OT integration create new challenges:

The need for increased collaboration: Because IT and OT are traditionally siloed, these two environments must be configured to work more collaboratively—to move beyond simple connected domains into a fully converged digital environment.

Complex, heterogeneous environments: The introduction of operational technologies creates increasing complexity with more device types and interfaces. OT networks also introduce new protocols (e.g., BACnet and LonWorks) that might not be compatible with traditional IT tools. Managing these converged IT-OT environments requires process convergence as well as improved tools for monitoring and automation. Though some organizations may struggle with it, integrating previously siloed IT and OT departments is essential to managing newly converged technologies. Issues that must be addressed include:

- **Security:** Since OT environments were closed, air-gapped systems until IT-OT integration, OT department personnel tend to have limited knowledge and few concerns related to security. IT should work with their OT counterparts to change the culture, improve security profiles across the converged domain, and eliminate dangerous security gaps. The introduction of OT devices in a converged ecosystem expands attack surfaces, creating the need to take further precautions to protect enterprise systems.
- **Training:** Only recently have certifications like the Cisco Certified Network Associate Industrial (CCNA Industrial) been offered to help staff understand how OT technology intersects with networked technology. Organizations should focus on developing technical talent with a firm understanding of the technologies and standards used in both OT and IT environments.
- **Integration:** Because existing OT technologies and current IT systems may not always be fully compatible, organizations should build roadmaps to align the two and develop architectures that support the fully converged digital environment.

Security Discoveries and Challenges as the OT World Meets the IT World

According to research by Forescout, this complexity of IT-OT integrations has led to organizations implementing devices that can be considered "risky." Forescout, a leader in Enterprise of Things security platforms, recently produced a study identifying the riskiest devices by vertical market segment. The methodology used to produce this report is as follows:

Defining risk: Risk is classically defined as the likelihood of an incident happening multiplied by the impact of this incident. In cybersecurity, likelihood is usually measured in terms of vulnerabilities and threats. In contrast, impact is measured in terms of the loss of confidentiality, integrity or availability that usually leads to a negative financial impact.

Measuring risk: Risk is assessed both quantitatively and qualitatively. Good risk metrics should be consistently measured, easy to gather and relevant for decision-makers. Unfortunately, risk assessments are usually based on subjective estimations since obtaining exact values for every possible event's likelihood, and impact is rarely feasible [2]. The main challenges in measuring risk

typically include identifying metrics or factors, establishing how to measure metrics, and defining how to combine metrics and measurements in a reasonable risk-scoring formula.

For the study, Forescout defined a list of components that aggregate individual factors to create a risk score model for IoT devices. The risk for a device is calculated as a function of six different components: vulnerabilities, security events, services, connectivity, vendor and potential impact.

The Riskiest Devices

To determine the riskiest device functions, Forescout first calculated the individual risk score for each device, then aggregated this score by taking the average risk per device function.

The risk that a device poses to an organization is measured by aggregating vulnerabilities, assessing exploitability and remediation effort, matching confidence, counting open ports, estimating the potential for outbound communications and data exfiltration, gauging business criticality, and determining whether or not the device is managed. Note that the number of devices of a certain type or from a particular vendor does not impact the risk score. This is because the objective of the study was not to determine which popular devices are risky, but rather which devices are either inherently risky or risky because of their connectivity.

The analyses adhere to the Forescout model classification, which assigns a single vendor/model per device when searching for vulnerabilities in third-party sources. This is advantageous for devices that have low fragmentation of their software and hardware supply chains, with both software and hardware delivered by the same vendor (which includes most IoT devices and some networking equipment). For other devices, it is difficult to reliably map the knowledge base on publicly reported vulnerabilities to a specific hardware/software combination used by a vendor. Therefore, some vulnerabilities may go unreported in the search, and the final risk score should be adjusted accordingly.

Riskiest devices by vertical market 2020

The graphic below shows the ten riskiest device types in each vertical, and highlights the types of devices that security staff in each vertical should look at more carefully. As stated previously, several of these technologies are often integrated with smart connected devices.

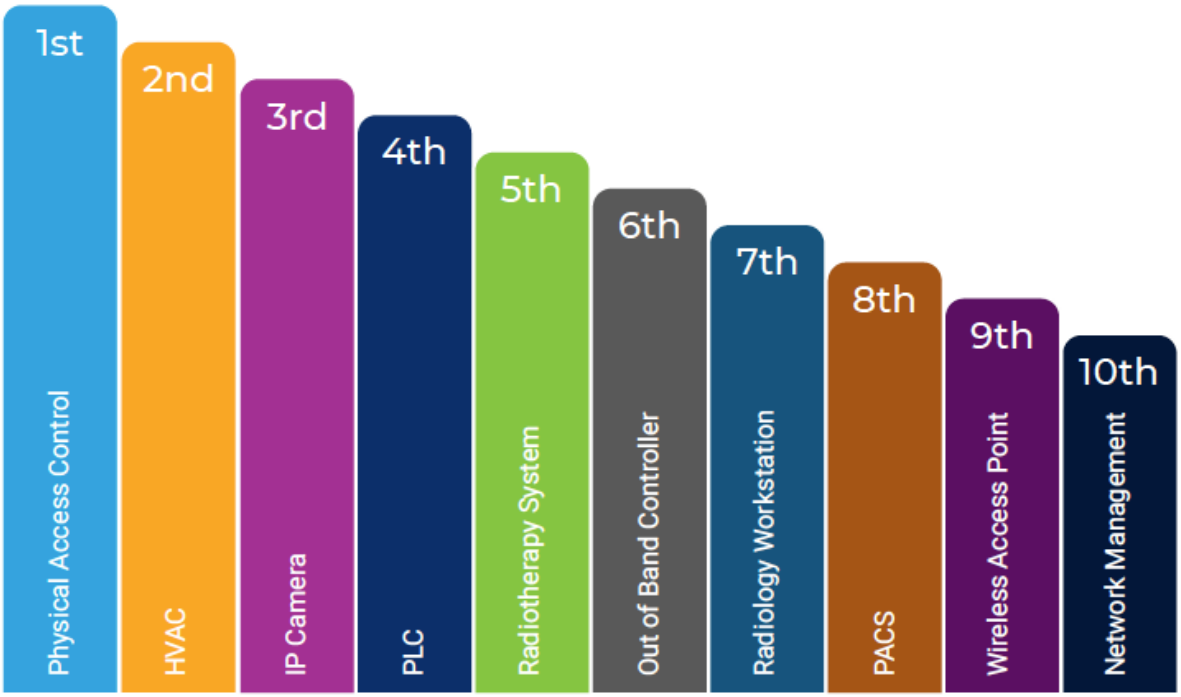
	Financial Services	Government	Manufacturing	Retail
1	Uninterruptible Power Supply	Physical Access Control	Uninterruptible Power Supply	Physical Access Control
2	HVAC	HVAC	Physical Access Control	HVAC
3	IP Camera	Emergency Communication System	Programmable Logic Controller	IP Camera
4	Programmable Logic Controller	IP Camera	IP Camera	Programmable Logic Controller
5	Network Management	Programmable Logic Controller	HVAC	Firewall
6	Firewall	Serial-to-IP Converter	Point of Sale	Out of Band Controller
7	Out of Band Controller	Lighting	Network Management	Wireless Access Point
8	Router or Switch	Out of Band Controller	Out of Band Controller	Video Conferencing
9	VoIP Server	Video Conferencing	Video Conferencing	Router or Switch
10	Printer	Network Management	Robots	Network Attached Storage

The types of devices that pose the greatest risk vary greatly depending on the industries where they’re deployed.

Top 10 riskiest device functions of 2020

Aside from analyzing the risk levels of device groups as well as device-group distribution within industry verticals, Forescout Research Labs also measured the risk associated with specific device functions and types from this same dataset. To identify device risk, Forescout first computed the individual risk score for each device, and then aggregated this score by taking the average risk per device model. As in the previous study, devices that had a model classification considered not granular enough (e.g., devices classified simply by device function) were then filtered out of the results. Vendor names and model numbers have been anonymized.

The graphic below lists the ten riskiest device functions over the whole data sample. These device functions are representative of the risky functions presented above, and provide examples of concrete vulnerabilities of typical network configurations (e.g., open ports and connectivity). They are by no means the only functions that should be monitored by security teams. Notice that all those devices are typically unmanaged.



Securing systems using smart devices includes increasing visibility by continuously monitoring, reducing attack surfaces, deploying endpoint management, and integrating real-time risk management strategies.

The Issue: Back-To-Work Technologies Come With High-Risk Profiles

Technologies that organizations are deploying to bring people back to work safely can pose security risks in multiple vertical markets. Some of the key back-to-work technologies being used include physical access control integrations such as building automation systems, edge gateways to connect thermal imaging devices, IP cameras, and network management of new "health safety" devices.

How to Keep Your Environment Safe and Secure

Forescout Research Labs analyzed more than eight-million devices deployed in the networks of organizations across five industry verticals, making the first Enterprise of Things Security Report the most comprehensive cybersecurity research endeavor of its kind to date. By leveraging the data in the Forescout Device Cloud, Forescout Research Labs provided the global cybersecurity community with detailed information about the types of devices present in enterprise networks, and the potential risks they can introduce to an organization.

The number and diversity of connected devices in virtually every industry vertical have presented new challenges for all organizations—and have indirectly made every business leader a cybersecurity stakeholder. According to a recent report by the Ponemon Institute, respondents from more than half of the organizations they surveyed are most worried about attacks involving OT and IoT assets.[1] At the same time, that report suggests that new approaches for measuring risk are needed. Cyberrisk is an interdisciplinary problem, and there are many ways to reduce cyberrisk in an organization.[2] Getting and sharing threat intelligence (e.g., by joining an Information Sharing and

Analysis Center) is one of them.[3] Applying security controls can also help reduce cyberrisk, with the advantage that security tools can automate technical controls. The Forescout platform is one such tool that reduces risks and increases the overall resilience of networks across the extended enterprise. By design, the platform:

1. **Increases visibility** by continuously discovering, classifying and assessing devices without agents or active techniques that could compromise business operations.
2. **Utilizes dynamic network segmentation** across the extended enterprise, reducing the attack surface and regulatory risk.
3. **Enhances endpoint manageability** with a single-pane-of-glass view of every network-connected device and unified asset, enabling compliance and risk reporting across the extended enterprise.
4. **Automates and enforces policy-based control** by enabling countermeasures to mitigate threats, incidents and compliance gaps.
5. **Highlights OT and IoT exposure** by continuously and passively discovering, classifying and monitoring network-connected OT and IoT devices, providing real-time risk management.

Summary

Even highly experienced professionals from the two worlds of operations and IT might not be able to anticipate the challenges and risks associated with integrating the two. Organizations rushing to implement new smart solutions often overlook broader implications to their overall security, risking not only a reduced ROI, but potential exposure.

As a systems integrator with extensive experience integrating these powerful new technologies, Sirius is here to help. If you have any questions about how back-to-work technologies can help your organization return to work safely, or how Sirius can help secure the technologies you already have in place, please don’t hesitate to reach out to your Sirius representative, contact us, or call 800-460-1237.

About the Authors

Jill Klein
Senior Leader, IoT & Healthcare, Sirius

Jill Klein has more than 25 years of experience in IT and business transformation consulting, serving in technical leadership roles at Fortune 500 companies including Inacom, Gateway, and ConAgra Foods. A tireless evangelist for innovative technology, Jill has been published in TechTarget, CRN and InfoWorld, and is a frequent presenter at universities and conferences focused on helping clients successfully integrate emerging tech. Jill continues to create industry-level thought leadership to assist with the advancement of emerging technologies and new business models as a member of the CompTIA IoT Advisory Council and the Tech Data IoT and Analytics Advisory Council.

As the senior leader for IoT at Sirius, Jill focuses on strategic growth opportunities and execution by leading new solution developments. Her teams strive to be the IoT solutions integrator of choice, delivering relevant solutions from current and future business partners.

Kevin Rota
Principal Consultant, Sirius

Kevin Rota has over 30 years of experience in IT strategy, operations and transformation. Prior to joining Sirius, Kevin served as the CIO for Dassault Systèmes and the VP of Project Management and Technology at Ness Technologies. His experience also includes leadership roles in global IT, management consulting, and business process reengineering at Cushman & Wakefield, Bellemead Development, and AT&T. As a principal consultant for Sirius, Kevin is focused on utilizing IT strategy along with process and operational improvements to help clients solve unique business problems.

Elisa Costante
VP of Research, Forescout

Elisa Costante is an expert in IoT and OT security. In her role at Forescout, she drives the execution of pioneering theoretical and experimental work addressing the cybersecurity challenges that IoT devices can pose to organizations. Her role involves generating original content to boost awareness and thought leadership and the identification, building and testing of prototypes for innovative products and services in line with Forescout’s overall product strategy.

Bibliography

[1] Ponemon Institute, “Measuring & Managing the Cyber Risk to Business Operations,” 2019. [Online]. Available: https://www.tenable.com/ponemonreport/cyber-risk.

[2] G. Falco, M. Eling, D. Jablanski, M. Weber, V. Miller, L. Gordon, S. Wang, J. Schmit, R. Thomas, M. M. T. Elvedi, E. Donavan and S. Dejung, “Cyber risk research impeded by disciplinary barriers,” Science, vol. 366, no. 6469, pp. 1066-1069, 2019.

[3] SANS, “CIS Critical Security Controls: Guidelines” [Online]. Available: https://www.sans.org/critical-security-controls/guidelines.