White Paper

The Internet of Things: A CISO and Network Security Perspective

By Jon Oltsik, Senior Principal Analyst

October 2014

This ESG White Paper was commissioned by Cisco Systems and is distributed under license from ESG.

© 2014 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Contents

Executive Summary 3

The Internet of Things (IoT) 3

IoT Considerations for Information Technology 4

IoT and Cybersecurity 4

IoT, Information Technology, and Operational Technology 6

Preparing for IoT Security 7

The Bigger Truth 9

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

© 2014 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Executive Summary

Industry visionaries have long written about globally connected intelligent devices arriving sometime in the distant future. With the "Internet of Things" (IoT) upon us, the future is now. In fact, numerous industries are already using IoT technology today, but this is just the beginning. This white paper concludes:

- **IoT will introduce unprecedented growth in devices and data. Various r**esearchers believe that there may be as many as 50 billion IP-connected devices by 2020, with the potential to generate ten times the amount of data produced today.
- **IoT will have a profound impact on enterprise IT**. IoT applications will demand ubiquitous connectivity across public and private networks, changing the enterprise IT paradigm in the process. Furthermore, the collection, processing, and analysis of IoT data will alter enterprise applications and infrastructure. As IoT matures, it will act as a catalyst for further and accelerated enterprise adoption of big data technologies for data analytics and information-as-a-service (IaaS) to help enterprises cope with widely varying workloads. IoT will also bring the information technology (IT) and operational technology (OT) worlds together, creating new challenges and opportunities. IT security tends to focus on data confidentiality and network penetration, while OT security centers more on physical security, safety, and maintaining continuous availability of critical systems.
- **IoT introduces new cybersecurity concerns**. IoT will add an army of heterogeneous devices, new protocols, and network traffic to the enterprise. These changes increase the overall enterprise threat surface and add new types of risks that go beyond IT assets and sensitive data. This will certainly exacerbate the threat landscape, leading to new types of breaches. Large organizations will not only have to manage these new risks, but also become more sensitive to how these threats are managed from both an IT and an OT perspective.
- **CISOs need an IoT plan.** Addressing IoT security won't be easy because it introduces new technologies, processes, and cultural changes. As IoT propagates, large organizations will need device-based identity and trust services, fine-grained network access controls, dynamic network segmentation, big data security analytics with integrated external threat intelligence, and a commitment toward automated remediation. Furthermore, enterprises will need to balance their existing IT-centric security philosophy with an OT-centric strategy.

The Internet of Things (IoT)

For years, technology pundits have discussed a future where a multitude of intelligent components collect and share data over global networks. This concept was dubbed the "Internet of Things" by British technology visionary Kevin Ashton in 1999, but has been part of IT discussions for much longer.

What once seemed like science fiction is fast becoming modern reality. In fact, there are more connected devices than people in the world today and this number will explode to over 50 billion connected devices by 2020. Government leaders and business executives are already exploring numerous ways to utilize IoT technology to benefit individual businesses, as well as society as a whole. For example:

- **Health care will move to 24/7 monitoring and treatment.** Hospital patients are regularly fitted with sensors to check vital signs like heart rate, blood pressure, and oxygen intake. IoT technologies will extend this type of monitoring for outpatient care. When patient conditions change, physicians can be immediately alerted, access real-time patient information for evaluation, and even administer remote treatment in some cases.
- **Smart cars will lead to improved automobile reliability and customized insurance plans.** Automobile manufacturers are installing IP-based sensors in cars to track components, collect data on automotive performance in various types of climates, and review automotive status prior to accidents. This data analysis will not only improve automotive reliability, but also align insurance rates with actual driving behavior rather than general population statistics.

© 2014 by The Enterprise Strategy Group, Inc. All Rights Reserved.

- **The public sector is already investing in IoT.** State, local, and national governments are already deploying IoT technologies for numerous applications. For example, the city of Barcelona (Spain) is in the process of moving most of its citizen services to virtual environments that use video and collaborative technologies to give residents round-the-clock access to services like water management, smart parking, waste management, and city bus service. Cisco Systems believes that IoT technology has the potential to save $4.6 trillion in government spending over the next decade.

IoT Considerations for Information Technology

Over the next decade, IoT will continue to evolve, altering business processes, personal services, and government programs along the way. At the same time, IoT will also have a profound impact on traditional enterprise IT. As CIOs plan for broad IoT adoption, they must consider specific IoT requirements including:

- **Massive scale.** As billions of connected devices swell to tens or even hundreds of billions, large organizations must be prepared for a quantum leap in IT scalability requirements. Network traffic will increase substantially as remote sensors and actuators modify their behaviors based on real-time data exchanges with applications. For example, ocean-based wind sensors may detect a sudden shift in the path of a hurricane, indicating that the storm is likely to track west toward New York City rather than proceed out to sea as originally thought. This new information could lead to a multitude of activity, as providers of bottled water and fuel, as well as utilities employees and emergency workers, are alerted to proceed toward New York immediately. IoT systems would then track the progress of supplies and emergency services in real-time. Clearly, this type of coordinated activity could generate an unprecedented amount of network traffic, database transactions, and data center workloads.
- **Data collection, transport, and processing.** At a 2010 technology conference, former Google CEO Eric Schmidt declared that we now create as much data every two days as we did from the dawn of civilization until 2003. As incredible as this assessment was, the amount of data created and collected as a result of IoT technology will be a quantum leap higher. Some researchers are predicting that the amount of global data generated will increase by a factor of 10x between now and 2020 as a result of IoT technology proliferation. This data will need to be collected, moved from place to place, and processed/analyzed in real-time.
- **Extremely variable workloads**. As IoT takes off, it will lead to lots of variability in terms of network traffic, processing, and storage needs. For example, an unanticipated refrigerator defect could start a flood of log data that would need to be distributed and analyzed by manufacturers, parts suppliers, and distributors simultaneously. The same scenario would be true for other events like a global pandemic, active hurricane season, or a water shortage. But despite this variability, network-based sensors will also enhance capabilities for capacity planning by collecting vast amounts of data for analysis. This analysis will result in pattern recognition that can help predict impending utilization spikes.

IoT and Cybersecurity

IoT will certainly have a profound impact on IT at large, but CISOs should be especially prepared for profound changes to current cybersecurity strategies and operations because:

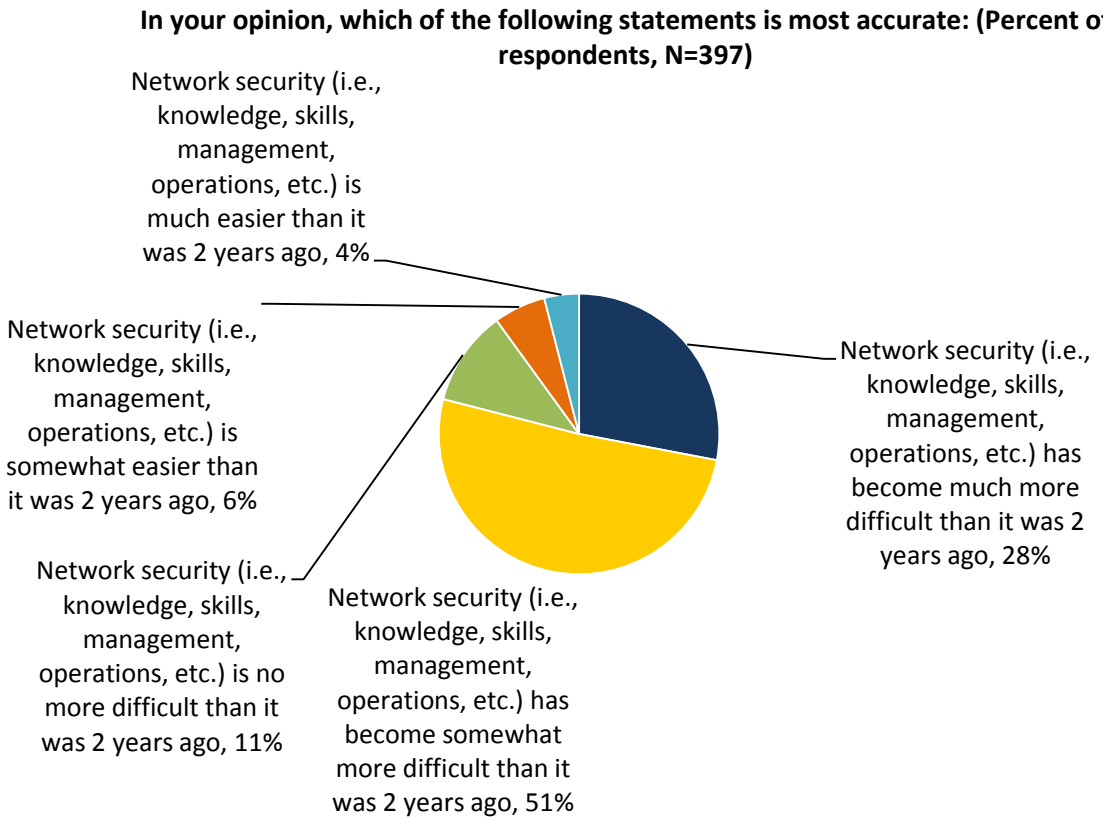
- **IoT introduces an avalanche of new devices, network traffic, and protocols to the mix.** Large organizations are still figuring out the cybersecurity implications of mobile devices, cloud applications, and BYOD policies. These initiatives will look like child's play compared with the scale, capacity, and variability of IoT. Why? As IoT devices proliferate, they will require secure access to data collection appliances and analytics applications from inside and outside the secure confines of the IT network. Furthermore, IoT is likely to be an extremely heterogeneous world featuring a multitude of raw devices and communications protocols that security professionals have little or no experience with. The security team will need the right skills and tools to identify IoT devices, secure IoT data and traffic, and recognize the difference between legitimate and suspicious communications.

© 2014 by The Enterprise Strategy Group, Inc. All Rights Reserved.

- **IoT applications demand data security improvements.** According to the Privacy Rights Clearinghouse, there have been 215 publicly disclosed security breaches in 2014 (as of this writing), exposing over 8.5 million personal records.[1] Data breaches continue to plague large organizations because they lack the right processes and oversight for data discovery, classification, and security controls. IoT could increase the number of data breaches for several reasons. First, IoT will increase the amount of operational data by a factor of ten, so data security controls and practices will need to scale accordingly. Second, IoT applications will consume assorted data from outside the network, thereby opening new threat vectors. Finally, the variety of IoT device types, locations, and security profiles will demand dynamic policy enforcement based upon the trustworthiness of devices and the integrity of IoT data.
- **IoT introduces physical and physiological risks.** At a base level, CISOs are responsible for the protection of IT assets and data today, but IoT introduces additional and somewhat frightening risks. As organizations monitor and take actions, IoT introduces both physical and physiological risks. For example, a cyber-adversary could use IoT to compromise automobiles, shut down transportation systems, destroy industrial components, or alter medical devices. These threats aren't theoretical: Stuxnet was used to disrupt atomic research in Iran; researchers demonstrated how to hack an Insulin pump at the 2013 Black Hat security conference; and hackers have proven that it is possible to take control of critical automobile mechanisms, including brakes and steering controls.

The addition of new devices, transport protocols, and network traffic to corporate and public networks may also be bad news for large enterprises as network security is already complex and cumbersome. In fact, ESG research indicates that 79% of security professionals believe that network security has become much more difficult or somewhat more difficult over the past two years (see Figure 1).[2]

Figure 1. Network Security Is Growing More Difficult



Source: Enterprise Strategy Group, 2014.

[1] Source: Privacyrights.org

[2] Source: ESG Research Report, *Network Security Trends in the Era of Cloud and Mobile Computing*, August 2014. All other ESG research references in this white paper have been taken from this research report.

© 2014 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Network security may become even more challenging as a result of IoT because:

- **Devices, users, and network traffic will skyrocket.** ESG research indicates that 36% of security professionals believe that network security is becoming more difficult as a result on an increasing number of overall devices with access to the network, while 23% believe that network security is becoming more difficult as a result of an increase in the amount of network traffic. With the onslaught of IoT devices and network traffic around the corner, this data should be of significant concern for CISOs in IoT-heavy industries like health care, transportation, utilities, and the public sector.
- **IoT makes the malware attack surface wider and deeper.** Nearly 40% of security professionals claim that network security is more difficult because malware can easily circumvent traditional network security controls (i.e., firewalls, IDS/IPS, etc.). This situation will be further impacted by IoT. For example, IoT devices will run embedded operating systems and applications with little if any malware detection/prevention capabilities. This could make it even easier for cyber adversaries to compromise the network. A vulnerable industrial controller, sensor, or thermostat could be compromised and then act as a beachhead for further malware proliferation.

Network security is also becoming more difficult due to the global IT security skills shortage. In this instance, 15% of enterprise organizations say they are understaffed for network security while 12% lack the right network security skills. Issues around network security skills will be further aggravated when organizations need security professionals with experience in both network security and IoT—these specialists will be extremely difficult to find.

IoT, Information Technology, and Operational Technology

Some CISOs see IoT as little more than a bigger footprint for today's cybersecurity strategies. In some regards, this is an accurate assumption since IoT introduces an army of new applications, data, devices, and network traffic that needs to be protected just like existing infrastructure. While this is true, IoT usage will be skewed toward the OT side of the house in many organizations.

Although IoT will converge IT and OT networks to essentially become different environments within the one extended network, security professionals must recognize that there are significant business, focus, security realm, and technology distinctions between the two (see Table 1):

Table 1. IT Versus OT

	Information Technology	Operations Technology
Business role	Supply technologies for revenue generation and cost control. Tends to be fairly common across industries.	Control technology used to supply a "product" (i.e., electricity, refining, logistics, etc.) or manufacturing process. Tends to be very specific to an industry.
Focus	Discrete IT assets (i.e., servers, storage, endpoints), or functional services (i.e., application development, networking, security, etc.).	Physical equipment or process focus, typically across a "system" of technologies.
Security realm	Data and IT assets.	People and physical equipment.
Technology	Mostly modern equipment with regular replacement cycles. Standard systems, tools, and protocols.	Can include older technologies with long lifecycles. Often use specialized equipment, tools, and protocols

Source: Enterprise Strategy Group, 2014.

When a security incident is detected, IT security professionals are trained to take immediate actions like quarantining a system and performing immediate system forensics. This rapid response mentality may not be

© 2014 by The Enterprise Strategy Group, Inc. All Rights Reserved.

appropriate for OT, however. For example, a utility company can't take a transmission station offline, even when the security team is certain of the presence of malware.

As IT and OT come together, CISOs will need policies and processes to work around the differences in order to apply the appropriate response for a multitude of cybersecurity requirements across both areas.

Preparing for IoT Security

In Figure 1, 28% of enterprise organizations claim that network security is much more difficult today than it was two years ago. As IoT flourishes over the next few years, it's likely that a much higher percentage of security professionals will share this opinion.

CISOs should anticipate big changes ahead, and smart CISOs can anticipate and address impending IoT challenges with sound planning and the right network security strategies. As IoT evolves, large organizations will need to bolster network security with:

- **Identity and trust.** As IoT propagates, security professionals will have to provide network access to an army of unmanaged heterogeneous devices. To be clear, CISOs should understand that IoT and mobile devices (BYOD) are different use cases. BYOD carries some additional requirements for user/device authentication, data/device security, and network access controls, but is simply a mobile adaptation of well-understood PC security best practices. Alternatively, IoT devices will come in all shapes and sizes, reside outside the network, and readily exchange data with corporate applications. Given the vast differences with IoT, there is a need for strong, non-reputable device identification. In other words, each device will have to announce itself to the network with some type of authentication that can be verified by some type of authority to establish trust. Enterprises will want to know details about the device type, location, activity, etc. Furthermore, all of this information will have to be captured, analyzed, stored, and shared among auditors, security analysts, and IoT system experts. It's likely that internal and external core routers and switches will be instrumented with X.509 certificates for trustworthy connectivity between public and private network backbones and cores as well.
- **Fine-grained access policies with real-time enforcement**. Fine-grained network access control policies will determine what devices are allowed to do on the network. Once again, the diversity in IoT device types, locations, and business functions demands more policy variety and granular enforcement rules than standard IT assets seeking network access. Device identity and behavior will determine how these network access policies are enforced. For example, untrusted devices or those exhibiting anomalous behavior may be denied network access, quarantined to particular IP domains, or closely monitored.
- **Dynamic traffic shaping and network segmentation.** In the IoT world, device type, transport protocols, or data/application sensitivity will trigger network segmentation policies. As IoT grows, CISOs should expect to see thousands of dynamically configured network segments at all times. Fortunately, this will not require VLAN tag configurations be applied to all network switches. It's likely that software-defined networking (SDN) technologies will combine with network identity and access policies to apply dynamic network segments on the fly for different traffic types.
- **Ubiquitous network encryption.** While large organizations already use encryption on internal networks, it's likely that IoT will drive more granular implementation. For example, SDN network segmentation may also trigger point-to-point/point-to-multi-point encryption based upon network segments, protocols, or network flows. As networking equipment and digital certificates come together, point-to-point encryption will be based upon some type of SDN/PKI amalgamation.
- **Greater network intelligence and data sharing.** IoT will add additional fuel to the need for big data security analytics as security analysts are called upon to investigate suspicious IoT traffic and IoT-based malware attacks. Within the enterprise, the security team will have to ramp up its ability to capture, process, and analyze distributed data, making full packet capture a network security staple. Furthermore, enterprises will use SDN and overlay management networks to route data to analytics engines in real-time. Keep in

© 2014 by The Enterprise Strategy Group, Inc. All Rights Reserved.

mind that intelligence sharing will demand automation for M2M traffic and require high performance and scale for real-time analysis. Finally, CISOs should expect to share massive amounts of threat intelligence with business partners, industry ISACs, government agencies, and security vendors. This requirement alone will drive standard security intelligence data formats and protocols like the DHS/MITRE standards (i.e., STIX, TAXII, CybOX, etc.).

- **Automated remediation.** Rather than just adding security components that work in isolation, IoT enables security solutions to be internetworked so that they work together to produce superior intelligence, thereby allowing rapid and often *proactive* response. IoT-enabled security solutions will generate vast amounts of data, making it impossible for human beings to keep up with threat intelligence and alerts, or adjust security controls in lockstep with real-time requirements. Therefore, these IoT-enabled security solutions need to support the communication and consumption of machine-to-machine intelligence for immediate, automated security control with no human intervention required. When security events are detected, the entire security network will need to consume the alert and take the appropriate action. For example, cameras can focus on the appropriate areas, doors in the affected areas can be locked, and access to critical systems can be disabled; meanwhile, alerts sent to security personnel can initiate the appropriate human response.

IoT security innovation won't happen overnight, but CISOs and the industry at large will need to embrace all of these changes over the next three to five years as they arrive. In the meantime, security executives should proceed by building a more integrated and scalable enterprise-class network security architecture in the short term. It's not enough to just add more security components to the network; it will be essential to truly *converge* the various components so that they work together. IoT takes billions of connected objects that produce data that is of little value alone and networks them so that the data can be shared and analyzed to produce business intelligence, and the same can be said about IoT security. By networking the various security components so that they can work together, IoT can take security data that is of only marginal value and produce comprehensive security intelligence that's actionable in real time. Security managers should also prepare themselves for impending business processes driven by IoT.

Smart CISOs will also recognize that IoT can actually help them improve cybersecurity protection and processes over time. For example, IoT will be a catalyst for unifying physical security, IT security, and industrial systems security. In fact, this *must* happen as IT and OT networks merge. As true cybersecurity expands its purview, it provides an opportunity to increase CISO value to the organization and ingrain cybersecurity best practices throughout the business.

© 2014 by The Enterprise Strategy Group, Inc. All Rights Reserved.

The Bigger Truth

As IoT becomes ubiquitous, enterprise IT will experience a paradigm shift in terms of scale, scope, and cooperation. The notion of an internal network will give way to global connectivity across extremely high-bandwidth public, private, and mobile networks.

For IT executives, this scenario is both daunting and breathtaking at the same time. IoT has incredible potential to change the world we live in, yet someone has to manage and secure a plethora of new requirements and technologies along the way.

Rather than panic, CISOs should prepare themselves for an inevitable IoT onslaught. This is especially important because IoT-enabled apps have the ability to consume the intelligence that's communicated by the network of connected objects, and dynamically change their behaviors based on that intelligence. This is the greatest value of IoT, yet is also one of the greatest security risks since these smart objects, which reside outside the network (security issues already discussed throughout), are sending petabytes of data through the network in order to populate the apps, which require that intelligence to function properly and add value. CISOs must make sure they understand IoT applications for the business so they can be directly involved in business process and IT planning for new IoT initiatives.

Aside from the applications themselves, CISOs should:

1. Assess their current strengths and weaknesses, especially in areas like identity, network access, network segmentation, and cybersecurity analytics.
2. Plan to build a converged IoT security architecture in which IT retains centralized command and control (i.e., provisioning, policy management, reporting, etc.), yet with the ability to enforce differentiated security policies to meet the specialized needs of each environment. IT and OT need to work together so that OT has significant input into security enforcement in its area, and IT gains a high level of understanding of the inherent differences between the two environments. In addition, this enterprise security architecture must also be extensible so it works with external parties like business partners, IT orchestration tools, and cloud service providers.
3. Closely follow technology innovations like SDN. It is also important to track the evolution of IoT threats and vulnerabilities.
4. Explore opportunities to use IoT initiatives to improve overall cybersecurity. For example, IoT may be a perfect vehicle to integrate physical, cyber, and industrial security into common standards, processes, and technologies.

Since IoT has the potential for massive business benefit, CISOs should become IoT cheerleaders and do all they can to support new applications and business processes. While CISOs will naturally continue to act as the voice of reason and caution toward IoT, they must also recognize that IoT is here today and can help their organizations in numerous ways that will have extraordinary positive impacts on the bottom line. Successful security executives will help their organizations benefit from IoT while maintaining an environment of strong security and privacy protection.

© 2014 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.esg-global.com