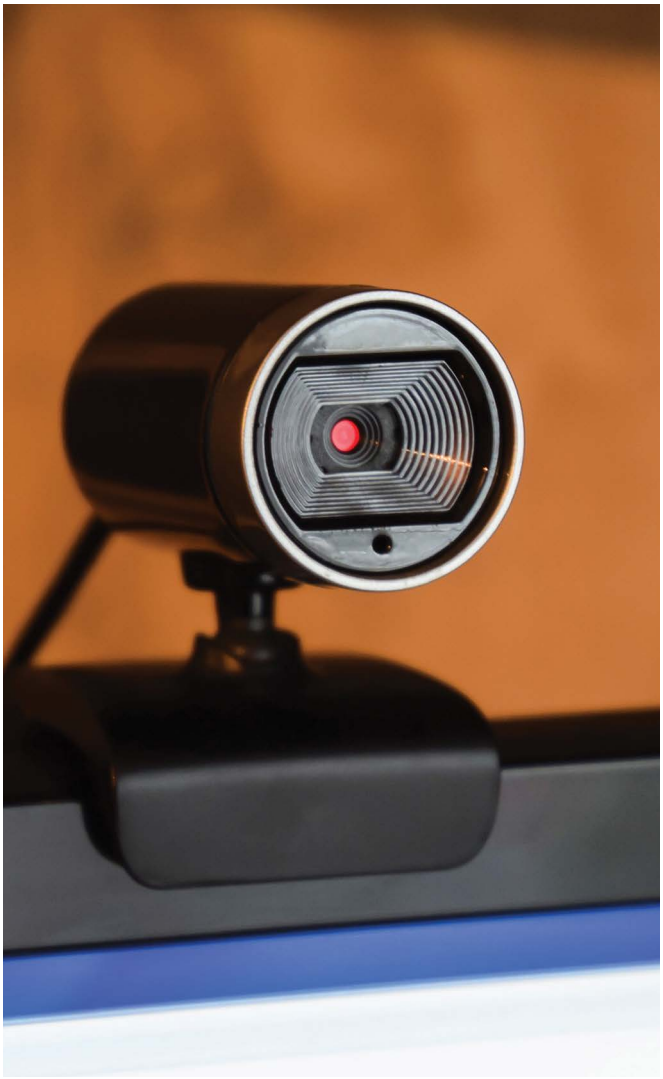
KPMG

Risk or reward: What lurks within your IoT?

Strategies to maximize IoT security in the enterprise

KPMG International

kpmg.com/iotsecurity



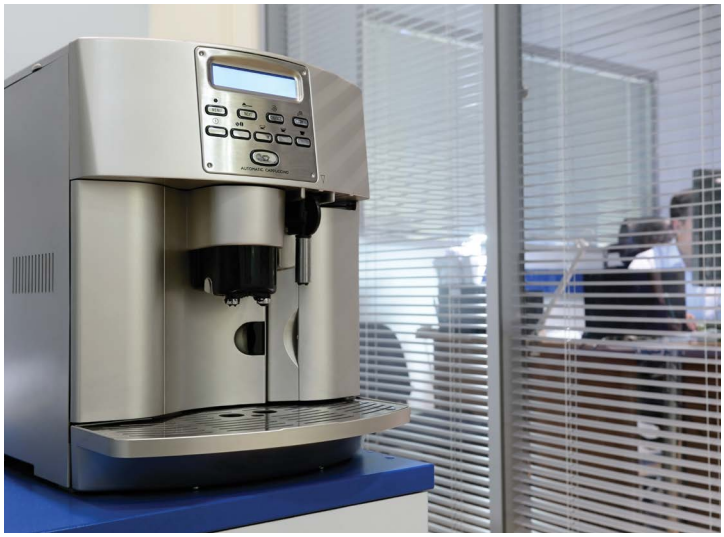


Table of contents

Foreword

Much is being said about how the Internet of Things (IoT) is poised to unleash a 'big bang' of smart device connectivity — a wired galaxy numbering billions of internet products radiating an endless array of data.

IoT offers tremendous automation, intelligence, scale and efficiencies across the enterprise. Many of these technologies leverage cloud, data analytics, robotics and even machine-learning technologies.

At the same time, the security issues arising in an IoT environment numbering an estimated 20 billion connected devices by 2020 cannot be overestimated and we believe that nowhere will this be more critical than among businesses.[1] Cyber security strategies will need to adapt to accommodate the deluge of connected devices and the entirely new security risks each could create.

The typical enterprise today has massive amounts of confidential data, intellectual property and competitive intelligence traversing the on-premise as well as off-premise IT ecosystem. All of this data faces a growing number of threats and vulnerabilities amid complex and rapidly changing processes and systems.

Adding to the volatile enterprise cyber-security picture is the comingling of personal data and corporate data into the enterprise network. Individual passwords, personal data and social networks are being used on PCs, laptops and various mobile devices across a range of locations that include the workplace, at home and in public settings. The enterprise IoT space represents some of the greatest overlap of risks and threats to your organization, employees and stakeholders.

[1] Source: Gartner Inc., 2017

As we evolve into a 'networked society,' enterprises need to address the advance of IoT as a business issue and not simply as the next 'cool tech' innovation. IoT will essentially transform the way we interact with our technology. From an enterprise perspective, this dramatic evolution will require new levels of awareness and responsibility, as well as support and governance from senior management to understand and accept the appropriate level of risks.

This KPMG International report, the second in a series of cyber-focused IoT reports, extends the dialogue by exploring the urgent and growing issue of IoT security within the enterprise. More specifically, how business leaders, IT and security teams should collaborate and look not only at the *devices* in use but also at IoT *ecosystems* — the level of connectivity and number of participants managing various connections — as well as the particular *use cases* in which these devices operate.

The goal of this report is to provide enterprise decision makers with a view of the significant new risks and threats that IoT poses to their businesses. We also provide a framework and best practices for effective security strategies that address the diverse challenges of adopting IoT in the enterprise. We believe that those organizations responding proactively today with holistic strategies will minimize IoT risks while maximizing its rewards.

IoT offers tremendous opportunities to automate processes and increase intelligence beyond expanded reach and efficiencies. Identifying where the risks are coming from and understanding how to manage that risk will have an immense impact on how successful the adoption of IoT will be in our rapidly emerging new world of connectivity.

Tim Zanni
Global Technology Sector Leader,
Chair of Global TMT Line of Business
KPMG International

Greg Bell
Co-Leader,
Global Cyber Security Services
KPMG International

Danny Le
Partner,
Cyber Security Services and IoT Security Lead
KPMG in the US

Alex Holt
Global Chair,
Media & Telecommunications
KPMG in the UK

The growing security threat of IoT in the enterprise

The Internet of Things (IoT)

The Internet of Things combines data, cloud, connectivity, analytics and technology to create a 'smart' environment, one in which everyday objects are embedded with network connectivity in order to improve functionality and interaction.

— An estimated 20.4 billion connected things will be in use worldwide by 2020. The number of IoT devices used by enterprises will more than triple to 7.5 billion. (Source: *Gartner Inc., 2017*)

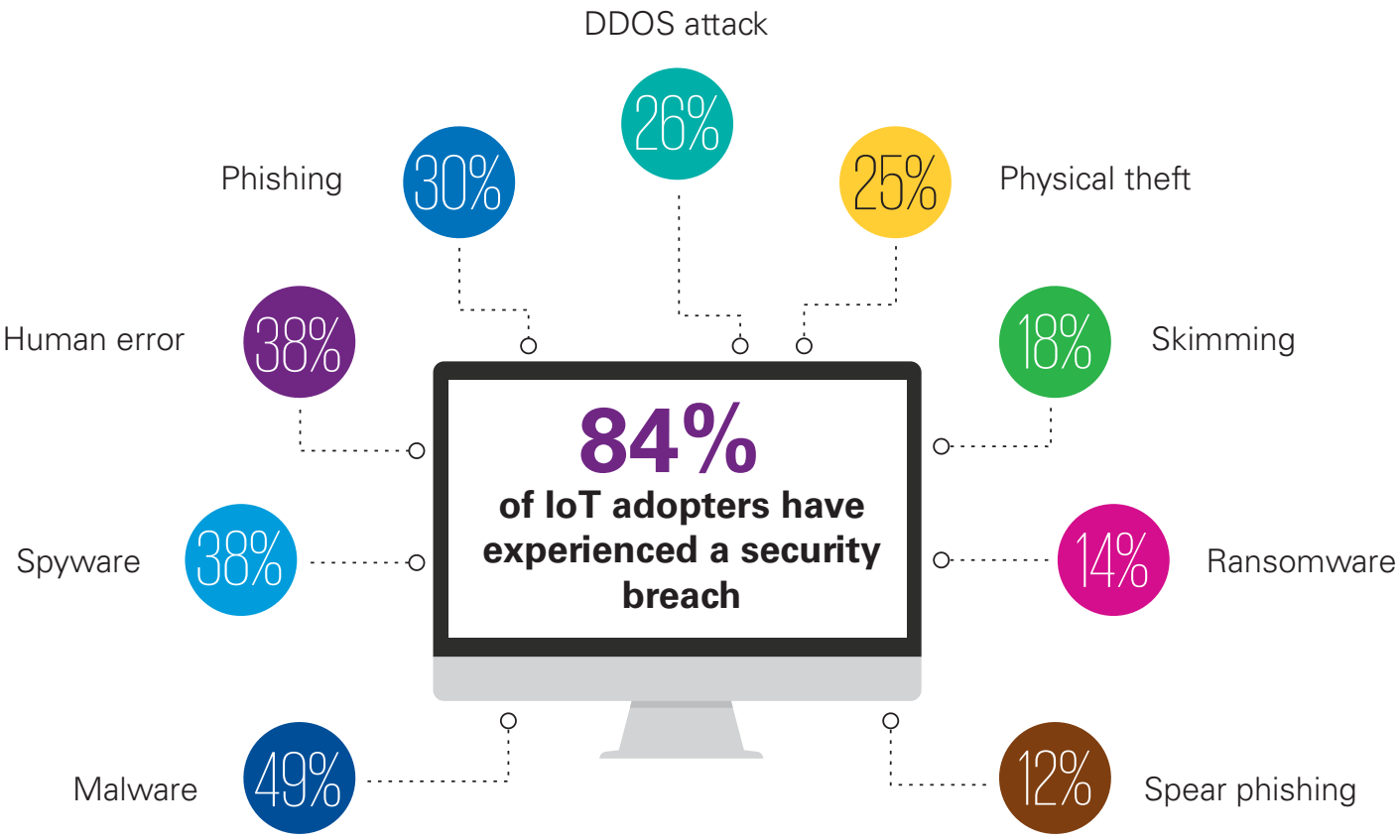
— Two-thirds of enterprises are expected to experience IoT security breaches by 2018. By 2020, more than 25 percent of identified enterprise attacks could be IoT-related — but IoT security accounts for only 10 percent of IT security budgets. (IDC *Worldwide Security Predictions, 2016*)

— Among 3,100 companies surveyed globally, just over half have implemented IoT — and 84 percent have already experienced a security breach as a result. (Aruba Networks — *The Internet of Things: Today & Tomorrow, 2017*)

— Cyber attacks on businesses globally cost between US$4 million and US$7 million on average last year. (IDC *Worldwide Security Predictions, 2016*)

— Among more than 5,000 enterprises surveyed around the world, 85 percent are, or will be, deploying IoT devices — yet just 10 percent feel confident about securing those devices against hackers. *(AT&T's Cybersecurity Insights Report, 2016)*

Security breaches hinder adoption



Source: Aruba, November/December 2016

> Cybercrime damages are expected to rise to US$6 trillion annually by 2021. This represents the greatest transfer of economic wealth in history and risks the incentives for innovation and investment.

AT&T's
Karthik Swarnam
VP Security Architecture

Exciting IoT innovations are emerging at an accelerating rate. New categories of IoT are being introduced and expanded as innovators pursue the next 'killer app' in a specific industry vertical (medical, automotive, consumer, etc.) or functional horizontal (IT, facilities, HR, etc.) that can provide a platform for growth and advancement. In corporate settings, IoT devices are being introduced via IT, HR, facilities management, office automation, specific product teams — or all of these at once.

In some cases, a new IoT innovation may be so compelling that the 'internet' aspect of the IoT goes unnoticed and the associated security risks ignored.

Traditional cyber security frameworks are likely inadequate for today's IoT. As IoT devices continue to multiply, the legacy hardware, software and processes are unable to keep up with the changing technology landscape. In some cases, these legacy systems — typically deployed before today's IoT invention — generally cannot be readily patched or upgraded to support modern security controls. As such, a broader view of risk is needed.

We are seeing the impact of sophisticated attacks and breaches that continue to earn global headlines, including the unprecedented Mirai malware attack that disrupted US internet traffic and brought down some of the world's busiest websites last year. Numerous major DDOS attacks to date have been attributed to the botnet Mirai — a Japanese word meaning 'the future.'

Bots and zombies need not apply!

You've no doubt heard of them and can be forgiven for mistakenly assuming they are players in a scary movie. A *bot*, or *web robot*, is a type of malware that allows a cyber attacker to take control of an affected computer. Bot-infected computers are referred to as *zombies* and collectively make up their own network, aptly named a *botnet*. Controlled by cybercriminals known as *botmasters*, botnets are a collection of thousands or even hundreds of thousands of zombie machines sitting on office desks and in homes across the globe, their owners unaware of any danger. The warning signs? A bot can cause your computer to slow down, display mysterious messages or crash. Bots sneak onto a person's computer by infiltrating the internet in search of vulnerable, unprotected computers or IoT devices. When they find access to an exposed computer, they quickly infect the machine and then report back to their master. Their goal is to stay hidden until instructed to carry out a task such as sending spam, viruses or spyware, stealing personal data, or launching denial of service attacks on business web sites. Scary indeed!

Source: Norton/Symantec Corp. https://ca.norton.com/botnet

Breaches and attacks ranging from malware to distributed denial of service (DDoS) attacks to simple human error continue to skyrocket amid the proliferation of vulnerable smart devices such as mobile phones, tablets, wearables such as smart watches and fitness trackers, vehicles, appliances, office equipment, and more. Many of these attacks did not come from weakness in the individual devices, but from the centralized services that connect to these devices.

IoT security breach statistics and predictions should be cause for concern for many enterprises today. That being said, many enterprises cannot play 'defense' and avoid the benefits of IoT. The key is to formalize the evaluation, understand the risks, and capture the benefits from IoT. Given the complexities of IoT, we recommend that enterprises use a holistic approach to understand its risks, perform a detailed analysis of the IoT cyber security framework and implement the relevant cyber security controls to mitigate risks identified.

> Today's enterprise is already quite porous from a cyber security perspective. Think about it — every moment of every day in countless locations around the world, a manager is connecting to cloud-based financial figures via restaurant Wi-Fi, a sales executive is accessing confidential growth data from an airport lounge or aircraft in flight, an HR person working from home or on a train is viewing confidential employee records. And on and on in an endless stream of connections and traffic that is about to expand exponentially. Businesses need to recognize the critical new risks they are facing.

Greg Bell
Co-Leader, Global Cyber Security Services, KPMG International

Three dimensions of enterprise cyber risks

Devices are the 'tip of the iceberg' *ecosystems* and *use cases* are also critical

Many IoT devices are built for specific use cases and may not enter the company via traditional technology (IT) purchases. As such, the business requirements and technology configurations are likely to differ from previous IT standards. While IT may not be deploying or using these IoT devices, it is important for the enterprise to support IT's efforts to centrally control and protect the enterprise network. Doing so effectively means taking into consideration the broader ecosystem in which all IoT devices are connecting through the enterprise network, including the use cases in which various devices are functioning or being used.

In many instances, companies are focused on the functionality that the IoT device provides. The connectivity to the internet and cloud services is seen as a utility. However, the increased connectivity via Wi-Fi, Bluetooth, cellular, among others, provides additional attack surface for threat agents. As more devices connect to the internet via Wi-Fi hotspots and the cloud, for example, opportunities will increase exponentially for hackers to come into the enterprise via other connections and service providers.

"We know that optimizing our security today is all about anticipating the unknown. Understanding and managing IoT complexity and risk as they proliferate within and beyond our enterprise requires a protect, detect and respond strategy," says Chief Cybersecurity Advisor Cyber Leader Michael Montoya, Microsoft. "We treat this security scenario as very dynamic, we must remain highly adaptive to changes in the threat landscape and pivot at any given moment if we want to fully ensure appropriate levels of safety and security. Basic approaches to hygiene with updated systems, ecrypted data and secure communications are essential to the foundation of IoT security."

Understanding cyber threats and vulnerabilities is a basic first step for all enterprises. *Threats* consist of different external and internal agents seeking to steal data, disrupt operations or use enterprise resources. *Vulnerabilities* are the weaknesses within the enterprise that various threat agents can exploit to achieve their goals.

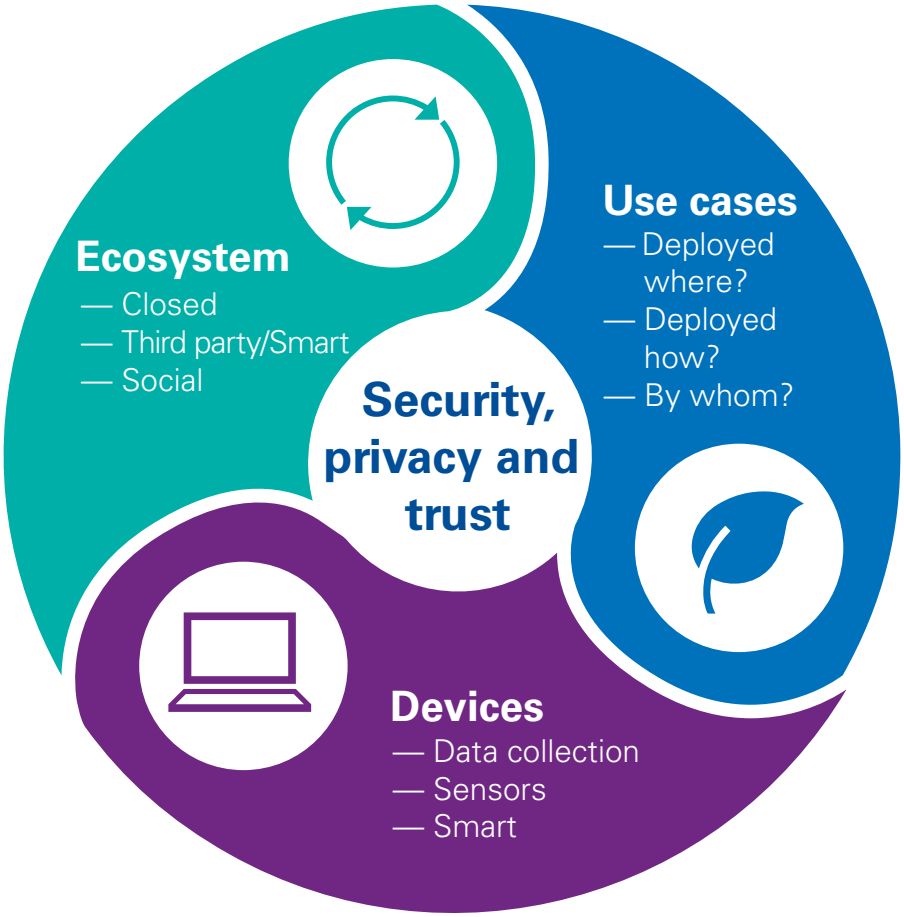
A possible example of the threat and vulnerability pair is an unethical competitor — as the threat agent — breaking into an organization's internet email system via weak password vulnerabilities and gaining access to confidential data. When high threats and high vulnerabilities align, the enterprise is exposed to critically high risks.

One approach to reducing cyber security risk is to remediate the vulnerabilities within the systems thereby reducing the attack surface available to threat agents. Companies traditionally have much more direct control over vulnerabilities than threats. Good vulnerabilities management practices are quite effective in reducing cyber security risks. "Because threat agents have different motivations, it is harder to reduce threats. Threat agents vary and are hard to anticipate as they include everyone from disgruntled employees, unethical competitors, nation-state actors, hactivists and even organized crime," says Henry Shek, Partner and Cyber Security Lead, KPMG in China. "Many clients do have formalized threats and vulnerability management programs in place to detect and mitigate these risks."

> "Managing and controlling IoT risk effectively goes far beyond simply controlling the device in your hand, office or enterprise. Devices represent just the 'tip of the iceberg' for IoT security. Businesses must understand the three dimensions of IoT cyber security — *devices, ecosystems* and *use cases,* each with diverse levels of complexity and impact on enterprise cyber security."
>
> **Danny Le**
> Partner, KPMG in the US

Devices, ecosystems and use cases — up close

Let's take a close look at how devices, ecosystems and use cases each present diverse levels of complexity, interaction and risk — and how enterprises can approach solutions to IoT risk from a holistic perspective that brings the three together.



Smart devices demand much smarter security

Consider the vast array of sensored and internet-enabled devices operating and collecting usage data in the typical business environment today: from printers, scanners, office phones, TVs and appliances to smart security cameras, lighting systems, doorways, elevators and much more. Any internet-enabled device can be hacked, allowing attackers to steal confidential business and personal data — usually long before businesses typically discover that they've been a target.

"It's safe to assume that most IoT devices possess vulnerabilities by default," says Akhilesh Tuteja, Co-leader Global Cyber Security, KPMG International. "When you bring any new IoT device into the enterprise, it's crucial to know how complex each device is in terms of how it functions and whether it has its own operating system. Are you placing a smart TV in your boardroom, for example? You should treat that TV like it's another computer on your network, because that's how it functions, including the need for regular updates of software and security measures."

Beyond the office environment itself, consider the number of people coming and going each day with personal connected devices of their own, including mobile phones, tablets, wearable devices and other IoT products possessing an array of internet applications — and risks. These individuals each represent potential risks as 'threat agents' — whether internal employees, those in transit and connected to the enterprise network, or outsiders such as hackers and competitors looking to access and steal data. Each of these use cases must be effectively managed at all times.

"There is no doubt today that organizations, employees and third parties, such as suppliers who have access to various enterprise devices and data, need a new set of business processes to ensure a reliable new level of security for IoT — and that is what we have tried to do for our organization," says Jaeyong Kim, Unit Director of PI & Information Technology Unit, LG Uplus. "An intelligent starting point for us was to become very aware of the various forms of IoT touching the organization every day, the risks they pose, and steps needed to prevent costly and potentially devastating attacks."

A simple office printer can open the door to data loss

Most offices have microcomputers that control printers. In some cases, these are adapted from low-cost consumer computers. Employees can send data to the printer through wireless connections and because the computer is internet-enabled, it is vulnerable to attack. Hackers can disrupt connected printers or, worse, steal access passwords and infiltrate the main office servers and confidential enterprise data.

Devices: Low, moderate or high complexity

There has been no agreement to date on an appropriate framework or reference architecture for IoT cyber security. IoT architectures differ across various industries and implementations, such as autonomous vehicles, robotic manufacturing, medical devices and more. For enterprise IoT, the key to understanding their potential threat is to map the level of *complexity* across the three cyber IoT dimensions: devices, ecosystems and use cases. Complexity can be evaluated on a broad scale based on a device's attributes, capabilities and functionality, ranging from 'low-complexity' sensors to 'moderate-complexity' embedded devices to 'high-complexity' smart devices. A simplified classification follows:

Data collection = low complexity

Low-complexity devices include relatively 'dumb' sensors producing no data and merely capturing information that's shared via Wi-Fi. These are devices such as light or heat sensors and fitness-monitoring wearables. While these devices are quite simple, they can gather a lot of specific data that must be evaluated for security purposes.

Sensors = moderate complexity

'Embedded' devices containing sensors are considered moderate in complexity. Sliding doors, heating and lighting systems and mail delivery robots are some examples. These standalone units possess on-board controls to monitor and control activity while producing active data. The risks these devices pose depend on their level of interaction and impact on the physical world in which they function. Turning off the lights in a home, for example, has limited impact when compared to the lights going out in a hospital, manufacturing facility or public transportation system.

Smart devices = high complexity

High-complexity devices include smart devices possessing sophisticated operating systems and various application capabilities. Unfortunately, it's easier for attackers to alter a smart device than an embedded device by detecting its operating system, installing malware to compromise the functionality of the control systems and accessing sensitive enterprise data. In today's BYOD (bring your own device) workplace, this presents a huge security challenge that's growing by the day. Devices may belong to the employee, a supplier or other outsiders and each must be monitored and managed to avoid a breach.

Security breaches traverse borders

Nearly a million users across Europe were cut off from the internet late last year as cyber criminals launched a cyber attack via internet routers. Security researchers said certain wireless routers provided to customers in Germany by internet service providers were vulnerable to botnet attacks. (*Wired Magazine* report, Nov. 2016) In another widely reported 2016 incident, five major Russian financial institutions were targeted in a cyber attack that overpowered their servers with fake requests — up to 660,000 per second — from more than 24,000 hijacked smart devices in 30 countries. A series of separate 2016 attacks saw hackers steal the equivalent of US$31 million from Russia's central bank and commercial banks using stolen customer credentials. (Kaspersky Lab statement, Nov. 2016)

> "Given the immense diversity and rapid proliferation of IoT devices, businesses should view security as a moving target demanding measures that are comprehensive, broad in scope and at all times up date to be truly effective. Devices need to be consistently secure and data needs to be protected as it resides in the cloud or traverses public or private networks."

Henry Shek
Partner and Cyber Security Leader
KPMG in China

Best practices: Secure your smart devices

Making the IoT work for you starts with knowing what is in and what is out in terms of devices that will be productive in your organization. If you see no clear advantage to a particular type of IoT device, move on. Here are some best practices on securing devices:

Asset management is critical. Establishing robust device controls begins with creating an inventory of devices entering your organization on a regular basis — such as personal phones, tablets and PCs belonging to employees, customers, suppliers, messengers and other visitors — and categorizing them by level of complexity. Beyond approved devices, monitor for unapproved or unfamiliar devices that should be subject to control protocols or entirely blocked from use while on the enterprise premises. The network management team can perform network traffic analysis to identify irregularities that may come from IoT devices, as well as identifying where internet traffic is going beyond the organization.

Know how it works — or doesn't. According to one study by tech giant HP, 80 percent of IoT devices tested failed to require passwords of sufficient complexity and length, and 70 percent did not encrypt communications to the internet and local networks (*Internet of Things Research Study,* HP, 2015). Some devices are designed for use only on networks that are isolated from external channels and these possess few access controls. Networked devices like printers and scanners, for example, may allow internet-based monitoring without passwords or user names. A widely reported attack in 2016 saw thousands of hijacked network printers in colleges across the US spewing out offensive flyers. (*Newsweek* report, March 2016)

IoT devices that can connect to business data should be accessible only to authorized users. To combat attacks on these devices, regularly update security software and implement antivirus programs and encryption. All hardware should be tamper proof and every device should be equipped to detect anomalous behavior or suspicious access attempts.

Create a vulnerability management program. A vulnerability management program will identify and fix device weaknesses that can emerge over time, perhaps through dated security software or operating systems. Consider this an ongoing 'health and fitness' program to maintain consistent, high-level performance throughout the IoT device's lifecycle. If the previous two practices are in place, this third recommendation will be much easier to achieve. Knowing the inventory of IoT assets and associated vulnerabilities positions an enterprise to allocate cyber security resources more efficiently.

Case Study: Secure by Design

To develop a cyber security governance framework, the goal is to integrate cyber security design and controls throughout the development of the products and services. This 'secure by design' approach integrates cyber assurance functions within the technology stack and throughout the product/service development lifecycle. Cyber security cannot be placed upon the IoT device once it has been developed.

Your ecosystem — do you really know who's in it?

Your enterprise IoT device is actually powered by an ecosystem containing various intermediaries that may be powering the cloud or processing data and analytics applications or providing a centralized console to manage the device remotely. The IoT ecosystem can be quite robust and complex, given its potential to identify and enhance the value of data gathered.

A simple ecosystem can consist of an IoT sensor sending data back to a single, centralized, internal server or service provider. In this closed, self-contained enterprise ecosystem, data may not face much risk. On the other hand, a business with smart lighting, printers or audio-visual equipment could be sending device data back to a main server owned by the device manufacturer or to a third-party maintenance company. In such cases, hacking the third-party service provider may provide the easiest path into the enterprise. This 'smart' ecosystem would need to be protected from hackers who could ultimately penetrate the larger enterprise network and create chaos.

The picture grows more complicated when IoT links involve multiple external service providers, each managing a different service. Currently, many organizations outsource facilities management in this way.

"It's crucial for enterprise to increase awareness of the countless interactions taking place among the people, devices, systems and data that are increasingly becoming part of their IoT environment," says Darren Yong, Senior Director Clients and Markets, KPMG Asia Pacific. "It could be an easy hack for someone to access one of these enterprise IoT devices. The impact could easily disrupt business and create security threats, not to mention the potential safety risk to employees and customers."

Beyond the potential risk that IoT devices pose, it's important to understand that enterprise suppliers or service providers who monitor and maintain enterprise facilities and devices are critical players in enterprise IoT security. Retailers, for example, are at risk of point-of-sale attacks in which customers' debit and credit card accounts could be accessed on the company's server by hackers using credentials stolen from a third-party service provider such as a store maintenance firm.

At the highest level of complexity are social networks that are vulnerable to attacks due to the minute-by-minute traffic of users accessing these sites via laptops, tablets and mobile phones.

Lights out in London

Some attacks demonstrate why we should never underestimate the cunning and resourcefulness of hackers. As media widely reported earlier in 2016, a hotel `guest' in London hacked into the light switch controls in his room. (*Information Age* report, March 2016) It was just a few steps from there for the hacker to access the hotel control systems for every floor and observe which hotel rooms had their lights off, indicating that guests were out and that the rooms were vulnerable to theft.

Best practices: Manage your ecosystem

Manage third-party access. Beyond the daily workplace traffic of employees, the daily influx of third parties into your enterprise — clients, messengers, service providers and more — requires a proactive approach to managing outside devices traversing your ecosystem. Some firms today use contracts requiring suppliers and service providers to protect enterprise confidentiality and to demonstrate sufficient cyber security within the third-party's own organization. Specialized consultants can help you develop a secure vendor-risk assessment and management program for this.

Use network segmentation to limit access. Beyond managing third-party access as noted above, it's important to separate network behaviors. It's possible to separate certain risky networked devices into discrete networks that feature additional monitoring and restricted access. For example, enterprise guests and business partners may log into a specific Wi-Fi network, while employees log into a different network that allows access to internal systems. Lastly, IoT may be isolated to a separate and closed network that monitors all data gathered. Segmenting the network enterprise effectively isolates the risks posed to certain parts of the IT infrastructure.

You are only as strong as your weakest link. The IoT ecosystem extends beyond the corporate environment in which the particular device is deployed. IoT typically involves being connected with other services in the cloud. As noted, different service providers may be participating in the ecosystem. As a result, the number of links needed to maintain cyber security becomes much larger and less transparent. Adopting IoT therefore requires a thorough vetting of the various participants throughout the IoT value chain. In addition, it's important to clearly define the roles and responsibilities of the participants in ensuring cyber security controls are effective. Is everyone in your IoT ecosystem equally invested in protecting the ecosystem and your data?

Case Study: The key to IoT

The use of encryption and public key cryptography will be critical to enabling and enforcing trust across the IoT ecosystem, whether that is to authenticate the digital identity of end points, authorize critical transactions, allow the secure exchange and processing of sensitive data across an open network, or validate the source and integrity of future software and firmware updates to a geographically dispersed community of devices.

Use cases pose unpredictable risks

The portability, flexibility, and intelligence of IoT offers new possibilities and use cases. Many uses of IoT may not have been initially envisioned. As such, we need to reevaluate the security architecture for each new use case. In today's mobile and connected world, it's critical to be hyperaware of just where and how access to business data is occurring and the risks posed by the many use cases through which personal or business devices linked to the enterprise's IT ecosystem are operating. Mobility and telecommuting allows us do business from any locale using any device we choose. With such convenience comes risk.

The telecommuting trend takes employee access to valuable business data from within the enterprise out into the external world, making it readily available anywhere and at any time. Threat agents are aware of this trend and can hack into sensitive data via an airport lounge or a hotel network, for example. When logging into public Wi-Fi networks, how do we know that we are logging into the right public network (SSID)? The device that we use, the network that we log into, even the location providing an internet connection is always questionable when we step beyond the four walls of the enterprise.

The use case becomes a question of *where* a device is being deployed, *how* it is being deployed and *by whom*. These factors will have a critical impact on the level of risk involved. Use cases can range from relatively simple, such as a proprietary phone app, to complex, such as a web-based login to the ERP. As devices enter the public domain, risk levels soar unpredictably, especially if the device is being used for purposes or in locations for which it's not intended.

"Be aware at all times of *how* your enterprise data and technology is being consumed, *where*, and by *whom*," says Leron Zinatullin, Security Architect, KPMG in the UK. "Do you want an executive, for example, to be looking at sensitive financial data while travelling in an unfamiliar city or foreign country? Certain data should only be accessible while in the enterprise, so firms need to manage this process to ensure security."

> "Be aware at all times of *how* your enterprise data and technology is being consumed, *where*, and by *whom*, and if it's appropriate to be used in a particular context."

Best practices: Control use cases

Streamline the amount of access based on use case: Each device has a particular use context for which it's designed and enterprises should restrict the amount of access and data available based on the intended use of the device. If the device is a sensor to detect customer traffic, for example, that device should not provide access to other systems or data. In addition, security controls, such as access and privilege, should be monitored in case a hacker gets into the device and tries to escalate access.

Before implementing IoT, companies should thoroughly evaluate associated use cases to determine what risks are present. This would include an evaluation of the various users, location of use, access level required, timing of use, etc. to understand the requirements and boundaries of the use case. Our recommendation is to restrict and streamline access to minimize exposure.

Understand the physical environment around the device: Most IoT have a physical aspect which requires us to consider physical safety regarding the device as well as the user and the environment that it is deployed in. This integration between cyber security and physical safety raises the need for new thinking and controls. In some cases, IoT may be harmful to the physical environment if taken over by a hacker. Even issues such as increased processing on the IoT device may create over-heating of the batteries or abnormal flashing of lights that can be distracting to nearby people.

Evaluate the environment in which IoT is being used. Is a public kiosk in use vulnerable to attacks from public users? Does the device in use need additional security to ensure that threat agents are not able to override security and access data through hardware connections?

Hold users accountable for their role in preserving security. As IoT provides greater convenience and functionality, the users of these devices must also be aware of their responsibilities, including use or sharing of passwords. In many instances, users become reliant and expect a certain level of security and protection. IoT device makers and service providers need to be clear on the limits of protect and service. In addition, users must be informed about the level of risk and the responsibility that they have in preserving an effective security control environment. This goes beyond the sharing of passwords and watching for "shoulder surfers."

With device mobility, users are increasingly working from home or in public places. Businesses need to clearly articulate the risks of the BYOD — bring-your-own-device — scenario and implement policies for the use of personal devices that access company networks and data. For example, employees should be aware of the risk posed and their responsibility for the co-mingling of corporate and personal data. While employees may use their own devices, they still have an obligation to utilize the latest antivirus and security monitoring software.

Case study: 'Bring a Burner'

Some executives travelling on business to other countries are leaving their normal mobile phones and laptops in the office. More often than not, the executive's devices hold more information than needed for a particular business trip. In some countries, it is prudent to bring a separate phone and laptop loaded with only the necessary data to prevent loss or theft of data. Some call these devices "burners" because they are easily wiped or disposed of once the use is completed. These devices are also loaded with additional security controls including VPN for encrypted communications.

Taking an integrated approach to security

"As digitization and the IoT continue to redefine business models and reshape marketplaces in every sector, businesses of every size need to recognize that digital represents not a trend but a revolutionary new way of doing business," says Tim Zanni, Global Chair TMT, KPMG International. "The sooner businesses take a strategic approach to adopting and securing IoT's unprecedented capabilities, the further ahead they will be."

While we've looked at various characteristics of IoT *devices*, diverse *ecosystems* and *use cases* in which devices operate, it's also crucial to realize how each of these three dimensions of technology use may present a *threat or attack vector* into the enterprise — essentially a gateway by which a hacker could invade a computer or server to inflict damage, chaos or the loss of critical business data.

The attack vector involves the alignment of a high threat to a high vulnerability, which creates a path for smart attackers to enter your enterprise ecosystem. In some cases, the threat is real and high, while in other cases, it's the vulnerability that's real and high. By linking these threat-vulnerability pairs or factors, enterprises can identify a threat vector with the highest risk. If the threat is high, but none of the identified high vulnerabilities are accessible, then the threat vector could be deemed a low risk. But to reach this equation, we must have an inventory of all threats and vulnerabilities across the enterprise's devices, ecosystems and use cases.

As we adopt IoT, we must ensure that traditional on-premises cyber security evolves to include a clear focus on devices, ecosystems and use cases. The IoT's convenience and capabilities come at a price, making security harder rather than easier.

Playing into this scenario is the need to also evaluate and prioritize the value of the business data and physical assets you need to protect. A review of enterprise data to prioritize its value provides a useful hierarchy of the various potential impacts that a cyber attack could pose. By understanding the value at risk, we can determine how much we can invest in appropriate cyber security controls. This ability to link cost and benefit makes the business decision much more transparent and effective.

The IoT wave is creating regulatory challenges

As the rapid advance of IoT technology and connectivity continues to unfold, there remains a need to develop common standards and regulatory guidelines for industry manufacturers, services and users.

With so many hybrid devices in office environments today, it's possible that more than one standard may apply to a particular device, which will challenge regulators to develop clear strategies regarding use and security. Diverse country standards are also sure to emerge and enterprises will need to become familiar with the various environments in which they are working globally to ensure consistent and optimal security. Regulators still have considerable ground to cover on the development of clear universal standards and policies governing IoT.

> "As digitization and the IoT continue to redefine business models and reshape marketplaces in every sector, businesses of every size need to recognize that digital represents not a trend but a revolutionary new way of doing business."

Tim Zanni
Global Technology Sector Leader
Chair of Global TMT Line of Business
KPMG International

Conclusion: IoT security best practices in the enterprise

Here are the five key takeaways for maximizing IoT security in the enterprise:

1. **Identify the business value proposition.** It's important to understand your IoT strategy and know which parts of it are at risk. Do a risk assessment that focuses on why you are implementing IoT and then evaluate the risk-reward equation that results — the benefits gained by the business versus the new risks being created via IoT enablement.

2. **Understand the complexity and risk.** Look across the three dimensions and plan your IoT security strategy accordingly. IoT devices are merely the tip of the iceberg when identifying potential risks and vulnerabilities. Devices, ecosystems and use cases related to your enterprise all interact to create various threats and risks, making it critical to take a holistic view on security.

3. **Embed cyber security controls within the corporate culture.** Users need to be aware of how they are responsible for maintaining your enterprise's IoT security. Develop a policy that illustrates everyone's role on cyber security. Users should be aware of risks raised and precautions required by various use cases, for example, when using a mobile phone to access enterprise data from a public place such as an airport.

4. **Maintain a health and fitness program.** Develop a strategy for revisiting your technology and business landscape on a regular basis to re-evaluate risk amid the ongoing changes in your business environment and innovations in technology. Revise your risk management strategy accordingly when changes impact risk.

5. **Prioritize IoT security as a key business issue.** IoT is a bigger business issue than it is a technology issue. Boards and senior leaders should be highly engaged on IoT security. Senior leaders also need to play a role as change champions on cyber security.

How KPMG can help

KPMG's Global Technology practice

KPMG's approach to serving the Technology sector is based on our detailed understanding of the issues affecting the companies in this dynamic industry.

In an industry defined by innovation and continual evolution, KPMG technology practice professionals understand the dynamic opportunities and challenges affecting global technology companies.

With professionals based in member firms around the world, KPMG member firms collaborate with clients to optimize business models, identify emerging opportunities, and address complex operational, compliance and risk-related challenges. KPMG member firms' professionals understand the issues affecting technology companies, including ever-shorter product cycles, sector consolidation, optimizing supply chains, and the importance of protecting the security and privacy of customer data.

KPMG's Global Cyber Security practice

KPMG brings together specialists in cyber security and business continuity, risk management, privacy, technology architects as well as specific industry business process experience. KPMG takes a business-driven approach to help clients achieve the incremental ROI on adopting IoT. Our IoT cyber maturity assessment methodology gives you a rapid assessment of your organization's readiness to adopt IoT, implement the necessary IoT controls, as well as manage the IoT to successfully realize the benefits.

Our capabilities extend well beyond the traditional technical assessments. KPMG member firms have been successful in assisting clients to design and engineer IoT solutions for their enterprise and the market. KPMG's global reach, technical depth and industry experience help the world's leading organizations work together to solve today's and tomorrow's biggest security challenges.

Contacts

Tim Zanni
Global Technology Sector Leader,
Chair of Global TMT Line of Business
KPMG International
E: tzanni@kpmg.com

Greg Bell
Co-Leader, Global Cyber Security Services
KPMG International
E: rgregbell@kpmg.com

Danny Le
Partner, Cyber Security Services
and IoT Security Lead
KPMG in the US
E: dqle@kpmg.com

Henry Shek
Partner and Cyber Security Leader
KPMG in China
E: hennery.shek@kpmg.com

Akhilesh Tuteja
Head of Technology sector,
Co-leader, Global Cyber Security
KPMG in India
KPMG International
E: atuteja@kpmg.com

Darren Yong
Senior Director,
Clients and Markets
KPMG in Asia Pacific
E: darrenyong@kpmg.com.sg

Alex Holt
Global Chair,
Media & Telecommunications
KPMG in the UK
E: alex.holt@kpmg.co.uk

kpmg.com/socialmedia

Designed by Evalueserve
Publication name: Risk or reward: What lurks within your IoT?
Publication number: 134287-G
Publication date: May 2017