What risks are lurking within your IoT?

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

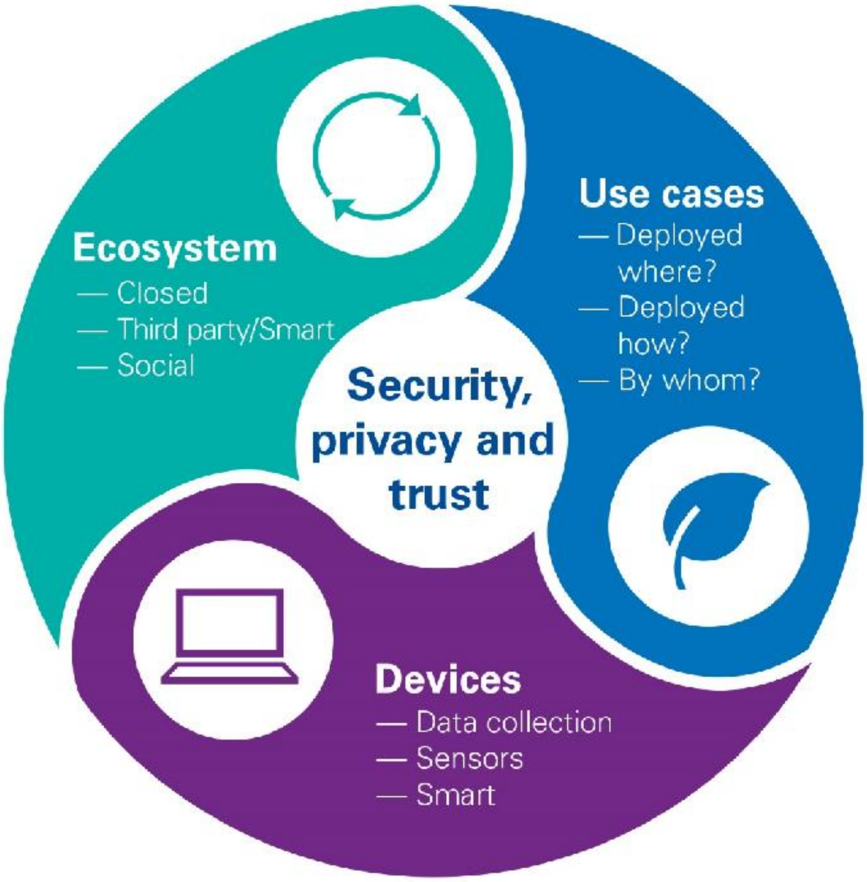
Much is being said about how the Internet of Things (IoT) is poised to unleash a 'big bang' of smart device connectivity — a wired galaxy of billions of internet products creating an endless array of data. IoT offers tremendous automation, intelligence, scale and efficiency benefits across the enterprise, and leverages cloud, data analytics, robotics and even machine-learning technologies.

At the same time, the security issues arising in the IoT environment cannot be overestimated and we believe that nowhere will this be more critical than among businesses. The typical enterprise has massive amounts of confidential data, intellectual property and competitive intelligence traversing the on-premise as well as off-premise IT ecosystem. This data faces a growing number of threats and vulnerabilities amid complex and rapidly changing processes and systems. Cyber security strategies will need to adapt to accommodate the deluge of connected devices and the entirely new security risks each could create.

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

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. This 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.

KPMG International's report, **Risk or reward: What lurks within your IoT?,** extends the dialogue and explores 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. It's crucial to realize how each of these three dimensions 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.



Devices

Many IoT devices may not enter the company via traditional technology (IT) purchase paths. 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 means considering the broader ecosystem in which all IoT devices are connecting through the enterprise network, including the use cases in which various devices are functioning.

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.

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.

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. 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 managed at all times.

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.

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 according to their level of complexity. Along the way, never assume any IoT device has effective security built in. Regularly update security software and implement antivirus programs and encryption.

Devices are the tip of the iceberg.

Look beyond to ecosystems and use cases to uncover sources of risk.

kpmg.com/iotsecurity

KPMG

Ecosystems

Beyond the daily workplace traffic of employees, the daily influx of third parties into your enterprise – clients, suppliers, messengers, maintenance workers and more – requires a proactive approach to overseeing who and what are entering your ecosystem. You are only as strong as your weakest link, so know who is using your system and ensure that every user understands their responsibility within it.

A simple ecosystem can consist of an IoT sensor sending data back to a single, centralized, internal server. In this closed, self-contained ecosystem, data may not face much risk. Conversely, 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 ecosystem involves multiple external service providers, each managing a different service. It's important to understand that enterprise suppliers or service providers are critical players in enterprise IoT security.

Use cases

The portability, flexibility, and intelligence of IoT offers boundless new possibilities and use cases. 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.

Telecommuting 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 all impact the level of risk involved. As devices enter the public domain, risk levels soar, especially if the device is being used for purposes or in locations for which it's not intended.

While IoT offers tremendous opportunities and benefits to the enterprise, identifying where the risks are coming from and understanding how to manage that risk will determine how successful the adoption of IoT will be.

KPMG

Risk or Reward: What lurks within your IoT?

Strategies to maximize IoT security in the enterprise

IoT security best practices in the enterprise

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.

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.

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.

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.

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.