The Economist Intelligence Unit

A report from The Economist Intelligence Unit

Securing the internet of things

The conversation every CIO needs to have with the CEO

The internet of things (IoT) presents the ultimate scenario of technology disruption. In industries ranging from door locks to auto, from sports apparel to heavy manufacturing, the IoT is upending business models, restructuring organisations and redefining the very nature of information technology (IT).

But recent research by The Economist Intelligence Unit finds a dangerous contradiction. A majority of large companies are building-out IoT businesses, yet data security continues to be a low priority for the C-suite and board of directors. Are companies putting their business and customers in danger?

Building-out the IoT will require leadership from many parts of the organisation, but its security will rest with the CIO and the company's security team. The following article, sponsored by Hewlett Packard Enterprise, presents key points that concerned CIOs should make to their CEOs and boards of directors. This is a conversation that needs to happen, and happen soon, in thousands of enterprises.

Background

An increasing number of firms have made a strategic commitment to the internet of things. Senior management and boards of directors recognise that this is a multi-trillion dollar opportunity that customers, competitors and shareholders will not allow them to ignore. As a result, many firms now have multiple IoT initiatives in various stages of development across the enterprise.

But just as the IoT presents unprecedented opportunity, so it presents unprecedented risk. Cyber-security is not keeping pace with cyber-criminals. It is urgent that companies understand the dangers to the firm, and adopt a comprehensive strategy and framework for managing them.

Sponsored by

Hewlett Packard Enterprise

The following is an analysis of the growing risk of cyber-attacks in the internet of things, followed by a six-step strategy for managing this risk. This strategy can form the basis for CIO recommendations to CEOs and boards of directors across multiple industries.

The IoT: a quantum leap in cyber-risk

In adopting the IoT, companies are facing significantly higher levels of risk. Here are the reasons why:

There are more cyber-criminals, they are better funded and they are becoming smarter

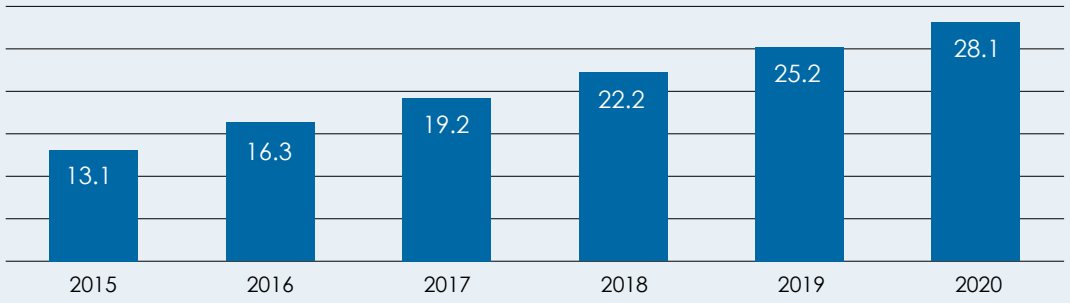
The cyber-threat to all companies is escalating. Cyber-specialists are being recruited as criminals. Powerful new players—organised crime, sovereign governments and extremist political movements—have entered the arena. Proceeds from successful scams are funding criminal innovation. A criminal marketplace has been created that supports a thriving business of theft, blackmail and corporate espionage.

These criminals are using sophisticated techniques to identify weaknesses and vulnerabilities. The concern is that the IoT—if not properly secured—will expand their opportunities.

A dramatic increase in new attack vectors

The sheer size of the IoT is increasing global vulnerability to cyber-attack. The number of IoT sensors is expected to approach 30 billion within five years—and each unit is a potential entry point for cyber-criminals.

Projected number of IoT connected devices: 2015-2020
(billions)



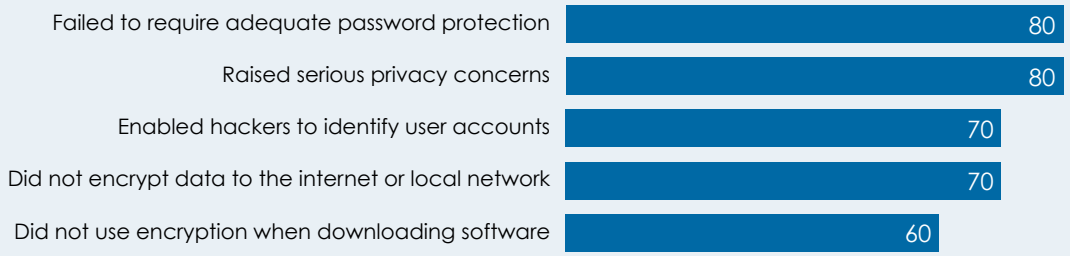
Source: IDC, *Worldwide and Regional IoT Forecast*, 2015

Many of these will operate outside of traditional firewalls, but will nonetheless connect directly to networks and applications. This presents a quantum leap in the attack surface of the enterprise—and a quantum leap in potential vulnerability.

Lower security thresholds

Even more alarming is that billions of these devices can be expected to *lower* industry security standards. Low energy consumption requirements and limited processing power can reduce the security capacity within individual sensors. A recent

Percentage of devices displaying vulnerabilities to cyber-penetration



Source: Hewlett Packard Enterprise Security Research, 2015 report. Devices came from manufacturers of TVs, webcams, home thermostats, remote power outlets, sprinkler controllers, hubs for controlling multiple devices, door locks, home alarms, scales and garage door openers. All devices used mobile connections, and the majority were connected to a cloud service.

examination of ten of the most popular devices in some of the most common IoT niches revealed an alarmingly high average number of vulnerabilities per device.

Firms cannot just expect to use current technologies and remain secure. They will need to proactively set a high standard now, to build security for the future.

Partners need to come under the security umbrella

The promise of the internet of things extends beyond the borders of a single enterprise. For example, the IoT could provide transparency into the product flow from a supplier's warehouse through the production line and into the retail outlets of customers. But this also requires that these partners—suppliers, contractors, customers—be brought within the firm's firewall, so they must be brought up to a common and rigorous standard of security.

Difficult to retrofit security

Another concern is that many companies have self-starters in the lines of business who are even now experimenting with IoT capabilities. However, once deployed, it can be extremely difficult to retrofit security on thousands of installed and deployed devices. These initiatives need to be brought quickly under an effective, unified security strategy.

Cyber-risk increases regulatory and legal risk

Even as risks rise, a company's ethical and legal commitments remain. A firm can be subject to regulatory action if there is a breach of regulatory data. It can be subject to legal action if it does not protect the privacy and security of customers. Furthermore, a protracted and public legal action can seriously harm the brand and customer franchise.

IT resources are limited

In virtually every firm, IT and security personnel are already stretched to manage current levels of cyber-attack and security risk. Even without the IoT, cyber-attacks are

escalating almost twice as fast[1] as security budgets[2]. The shortage of qualified security personnel is a chronic bottleneck to increased security capability.[3]

In other words, the IT department must do more with less just to manage the current threat level. But the current level of cyber-risk is expected to be child's play compared to what is coming in the IoT.

The dark side—the potential consequences of a cyber-breach in the IoT

The greatest cyber-danger of the IoT lies in the potential consequences of a successful breach.

Today, cyber-thieves generally target customer lists and financial assets. But within the internet of things, they can crash vital operations or directly harm customers. Here are some recent examples:

- In 2012, attackers calling themselves the Cutting Sword of Justice attacked 30,000 substations of Saudi Aramco. Production was reduced for a week before they could be brought back on line.
- In late 2014, the German government acknowledged a successful attack on a German steel mill, in which hackers gained control of a smelting furnace and caused it to overheat, resulting in substantial damage to the furnace and interruption of the mill's business.
- Medical devices company Hospira chose to update its pumps by replacing the cables with internet-connected switches. The company bolted on wireless, internet-connected switches to send commands to subcutaneous pumps. But, unmindful of cyber-security risks, the vendor failed to add appropriate defences, such as passwords that kept unauthorised users from accessing the controls. In April 2015, the US Food and Drug Administration issued an advisory calling for hospitals to stop using the pumps, a sobering result for any company.

The consequences of these kinds of attacks for the enterprise are clear. The IoT, for all of its promise, can put a company's assets and reputation at risk. Operations can be slowed or brought to a halt. Legal liability, harm to the brand and the triggering of regulatory action could conceivably lead to catastrophic harm to the firm, let alone its customers or employees.

1 PwC, *The Global State of Information Security® Survey 2016*
2 Economist Intelligence Unit survey, *Cyber-security: The gap between the board-C-suite and the security team,* 2016
3 US Bureau of Labor Statistics, 2015

What the enterprise needs to do—six steps

The following are six recommendations for immediate action that CIOs can make on securing the IoT:

1. **Adopt a comprehensive framework and strategy for digital security**: Reactive, stand-alone perimeter defences won't work in this world of escalating cyber-threat. Firms need a proactive, enterprise-wide strategy for securing the IoT. This strategy will require the active support of the CEO and board to succeed.
2. **Conduct a full audit of current and likely risks within IoT initiatives**: Companies need to conduct a full security audit that assesses the complete IoT deployment being proposed. This includes not only IoT devices, but also the network infrastructure and all mobile, web and cloud touchpoints. This should include the identification of risk by regulatory, legal and brand exposure.
3. **Bake security into devices and processes early**: Many companies have IoT products in development that are not meeting security standards. At best, it will be challenging to secure them after deployment. At worst, this exposes the firm to serious cyber-attacks. Security needs to be instilled into these projects now.
4. **Mobilise the larger workforce around IoT security**: The IoT is not just another IT project. It will extend sophisticated technology deep into product design, the supply chain, production and other traditional parts of the organisation. The employees of these functions will need to be part of the enterprise effort to keep it secure.
5. **Bring partners up to rigorous security standards**: In an IoT environment, security will only be as good as its weakest connection. Firms need to ensure that partners—customers, suppliers and others—adhere to standards of security that are as rigorous as their own.
6. **Rethink the role of IT**: The IoT will cause the IT department to change the role of IT from a service provider to becoming a valued partner in virtually every part of the business. This will demand new organisation, skills and lines of authority. Just as the IoT will change the business, so it will change IT.

The internet of things may be the greatest technology disruption that firms will face. The opportunities are so great that they have no choice but to participate. But in doing so, enterprises will have to take clear, strategic steps to make it secure for customers, operations and the enterprise. These are recommendations for securing the future in the internet of things. ■