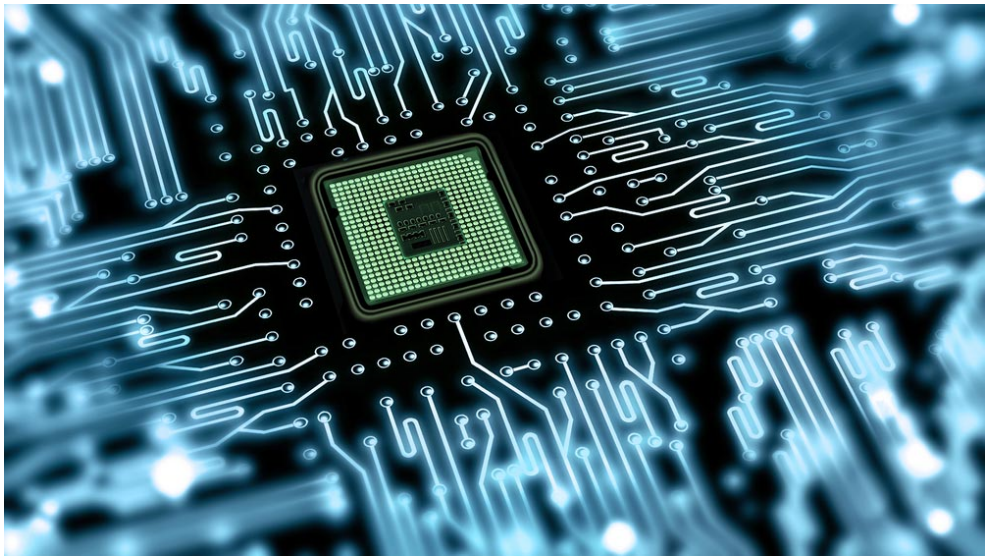
THE one BRIEF
AON EXPLORES THE WORLD'S MOST PRESSING BUSINESS ISSUES



RISK & INNOVATION

Cyber And Physical Threats Collide

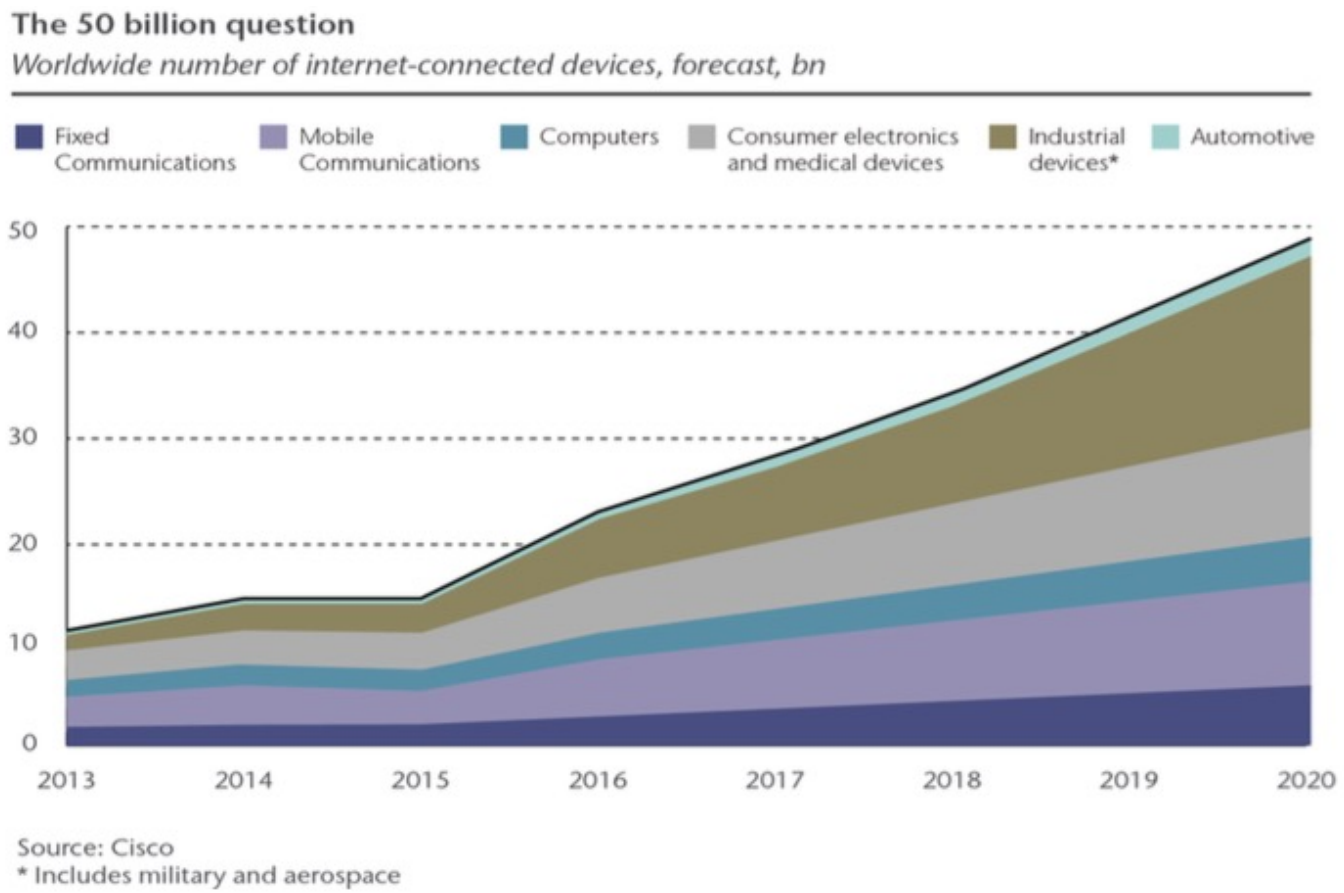
January 21st, 2016

OVERVIEW

A quarter of a century after the worldwide web began to transform the Internet into the indispensible tool we all rely on today, we're now entering a new digital revolution. Over the next four years, the number of connected devices is expected to grow to as many as 50 billion, according to the 2015 Ponemon Global Cyber Impact Report, sponsored by Aon. Business is expected to make up a far larger percentage of Internet of Things (IoT) usage than Consumer – this is more about smart factories and computer-controlled office system than it is shiny gadgets like smart watches and fitness trackers.

What's more, the risks are becoming physical. Some of these new devices could cause serious real-world damage. We've already seen manufacturing plants seriously damaged by cyber attacks and electricity grids and automobiles shut down by hackers. It's only a matter of time before such threats become more common – and more physically dangerous to both people and property.

With the rise of new technology comes fresh opportunity for business, but also new risk. In the workplace, every new connected device represents a new link in the IT chain. With the age of the Internet of Things upon us, what are the new risks, and what do business leaders need to know to be prepared?



Source: 2015 Ponemon Global Cyber Impact Report, sponsored by Aon

IN DEPTH

New Technology Big Opportunities

The benefits of Internet connectivity are hard to understate. For businesses, the Internet of Things offers the promise of quantified everything. Employers will be able to track productivity and leverage metrics to uncover new efficiencies. With connected sensors underpinning every square inch of an organization's footprint, once siloed data sets can be integrated, correlated and cross-referenced, identifying new efficiencies and delivering new value.

The benefits are immense – but so, potentially, are the risks.

"As we move into having smart workplaces and offices, you're really talking about a technology backbone that's driving an organization," says Stephanie Snyder Tomlinson, a cyber insurance expert at Aon. "What impact can that have on a business? What are the potential losses to an organization if you have a network security breach that results in property damage or bodily injury?"

Digital Threats Turn Physical

An unfortunate side effect to some of the most high-profile recent cyber breaches is that many have come to regard cybercrime as solely a privacy issue. It can be far more complex than that.

"If there is a failure of network security or systems," warns Snyder Tomlinson, "there could be a resultant business income loss. It could be intangible loss in terms of loss of data information assets or, especially as we move into relying more heavily on technology and the Internet of Things, it could be tangible loss as well."

You don't need to look very far to get a sense of the potential risks to property and other physical assets when the Internet of Things

You don't need to look very far to get a sense of the potential risks to property and other physical assets when the Internet of Things begins to help run a workplace. As organizations grow increasingly dependent on technology to run their businesses and offices, the attack surface for cybercriminals increases dramatically. Each new device represents an additional access point for hackers.

These scenarios can sound like something out of a science fiction film:

- Does your building have computerized entry or elevator systems, with employees issued smartcard keys for access? Hackers could take control and lock down your building, trapping employees and visitors inside.
- Computer-controlled electricity or water supplies can be shut down, rendering working impossible.
- Connected thermostats are becoming increasingly common – these could be taken over, shutting off heating in winter, air conditioning in summer, or driving temperatures to unbearable levels, making your office unusable.
- Logistics servers managing orders and deliveries could be hacked into, with real orders cancelled, false orders placed, or essential supplies redirected to the wrong locations, disrupting your supply chain.
- Factory robots could be set to destroy rather than create your end products.
- HVAC systems in a company data center could be overridden, causing a rise in temperature that could render network servers inoperable.
- Fire alarm systems can be turned off just as real-world arsonists attack.

This may sound far-fetched, but it has already become a reality. A cyber attack on a German steel mill in late 2014 caused immense physical damage after hackers installed malware on the network. "It caused the blast furnace to be unable to be shut down, leading to massive property loss," says Snyder Tomlinson. "The property loss arose from a network security breach. It's a perfect example of the potential risks when you have companies that are relying on technology to run their business."

Understanding the level of risk

"There's always going to be some type of access point into a network, in one way, shape, or form," says Snyder Tomlinson. "You can have the best network security possible but as everybody says, 'It's not if, it's when.'"

Consequently, many companies are revisiting their approach to cyber security. Organizations previously concerned only with safeguarding client privacy and personally identifiable information are suddenly contemplating a broader spectrum of loss.

"We're seeing more interest in cyber insurance from manufacturers and critical infrastructure companies, because they recognize that their exposure isn't necessarily just about private information or the liability arising out of a breach," says Snyder Tomlinson. "We're going to continue to see growth in the breadth of cyber coverage over the next several years, where we're getting into the true property space, because there is the potential to have a property loss arising out of a network security breach or a systems failure."

This is why businesses need to take a holistic view of their cyber vulnerability, says Snyder Tomlinson. "Cyber risk flows through an entire organization." A good cyber risk management framework has three key elements, she says:

1. **Preparation** – Identify and quantify your cyber risk exposures. Develop a breach response plan and business continuity plan. Consider taking out a cyber insurance policy, which can assist with the potential balance sheet impact of a breach.

1. **Practice** – Speed of response can be vital to limit damage in the event of a breach. Identify the key stakeholders within the organization and perform a tabletop scenario exercise to ensure that everyone knows the role they need to play should an incident occur.

3. **Execution** – Engaging with appropriate vendors is critical to successful execution. An organization should have relationships with defense lawyers, a public relations firm and a computer forensics firm, so that they can work with them to mitigate loss in the event of a breach.

With the rise of the Internet of Things, cyber crime is no longer simply about loss of information. Increasingly, you need to consider the possibility that cyber could be just as physically disruptive to your business as a natural disaster or a terrorist incident. This is no longer simply a data issue – today, property and potentially even lives could be at stake.

TALKING POINTS

TALKING POINTS

"IoT is all about connectivity, but connectivity is also the biggest vulnerability that could bring it all to its knees." – James King, Oberthur Technologies

"There have been safety regulations for many, many years, of course, but they rarely consider how a logical attack might affect a physical result. We've seen the start of these 'kinetic cyberattacks' with Stuxnet and the German steel mill, but the [Industrial Internet of Things] drives a growing attack surface. The equation simply isn't the same as it has been for IT security, and we'll need to adapt." – Tim Erlin, Director of Security, Tripwire

"Security is not a feature that will emerge on its own. Past results have shown that adding security after systems are designed and deployed, i.e., 'bolting security on,' is challenging at best and at worst can have catastrophic consequences." – U.S. Department of Homeland Security

"The benefits of deploying connected devices ecosystem are game changing in nature compared to the risks involved. The ecosystem has to evolve around standardization and interoperability with integrated security at the heart of every solution." – Satash Jadhav, Director, IoT, Embedded Sales Group – South Asia, Intel

FURTHER READING

- The Most Innovative And Damaging Hacks Of 2015 – PCWorld, December 28, 2015
- For The First Time, Cyber Attack Causes Widespread Electricity Blackout – Fast Company, January 5, 2016
- Systemic Risks And The Internet Of Things – JDSupra Business Advisor, December 18, 2015
- What Is The Internet Of Things? Everything You Need To Know About IoT – TechWorld, December 7, 2015
- Building Regulations Will Drive IoT In Offices – Computer Weekly, December 7, 2015
- Internet Of Things Data Deluge Could Lead To Security Concerns, Warns Report – Computing magazine, December 8, 2015
- Internet Of Things: Many Uses But What About Rules? – EU Observer, December 2, 2015
  The Hidden Risks Of Bringing The Internet Of Things Into Your Home – Mashable, December 10, 2015
- 10 Data Security Trends That Will Impact You In 2016 – Information Management, December 16, 2015
- Underrated Threats: Research Into The Evolving World Of Risk – Aon report

AON
Empower Results®