Gerry Kane
Cybersecurity Segment Director, Risk Engineering, Zurich Services Corporation

The internet of things: An argument for cyber resilience

Many companies are unprepared for changing digital infrastructure and need to recognise threats and prioritise solutions

The internet as we have known it until recently has been a global network that allows individuals and organisations to connect with one another and to vast sources of information; any time, from anywhere there is an internet access point.

One notable feature of this network is that it has been used to connect people via the computing devices that they own, i.e. there has been someone at a keyboard entering information or executing scripts in order to 'dialogue' with other devices or humans similarly connected to the internet.

The internet of things (IoT) is a similar concept with the key difference being the removal of the human from the information exchange. Now the dialogue involves devices without human intervention. Devices such as security systems and HVAC systems in commercial properties or a home, flow controllers in pipelines, performance monitoring sensors in automobiles and health monitoring medical devices. The IoT, then, is simply an extension of the internet as we have always known it, with many more connectable devices – perhaps as many as 50 billion by 2020.

Benefits of internet of things – the good news

This explosion in growth of connected devices is happening for very simple reasons – these devices may bring benefits to those who use them and profits to the companies who make them. These benefits may come in the form of productivity, safety, convenience, efficiency or even quality of life. In our personal lives, we are already seeing 'wearables' that monitor our health and contribute to our well-being.

We are becoming accustomed to smart homes with refrigerators able to sense when they are getting empty and order groceries on their own. We read about vehicles that are either self-driving or are able to sense dangerous conditions and react accordingly without driver action. Farms are becoming more efficient by having sensors that monitor soil moisture and nutrient levels and begin irrigation and fertilisation only when it is needed and only where it is needed. An oil rig can inform a computer that it's a month away from needing repairs.

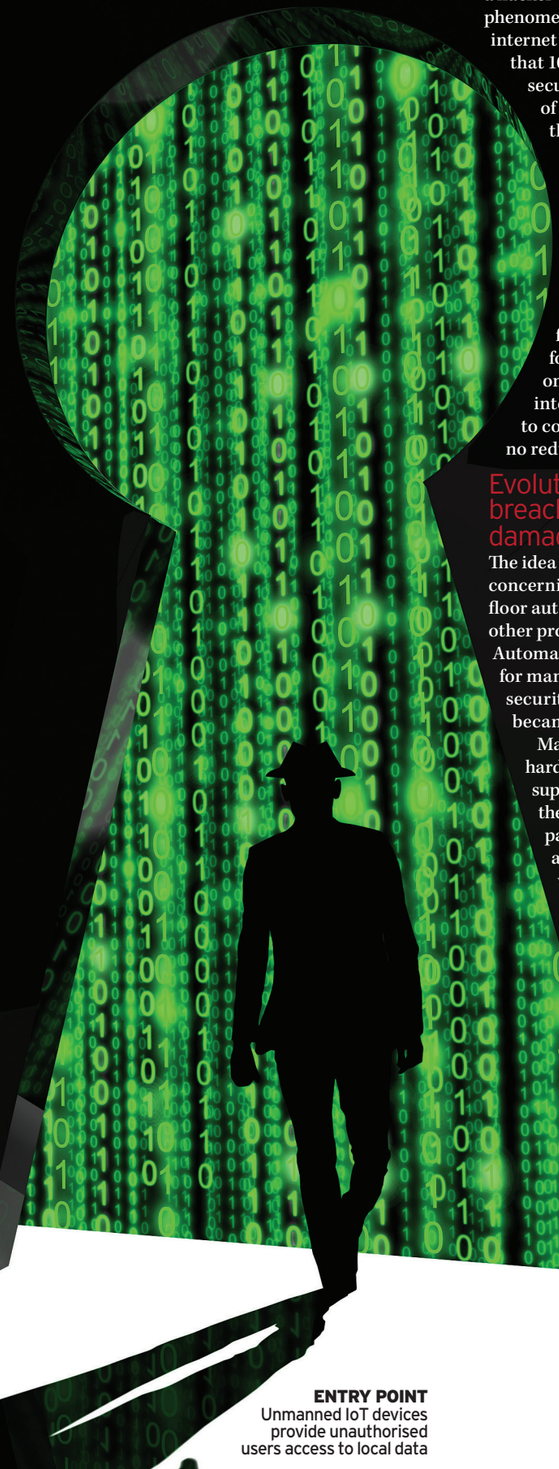
Risks of interconnectivity – the bad news

As is often the case, the benefits of the IoT are accompanied by an equal amount of risk. Each of the billions of devices connected to the internet now and in the future, whether it is a wearable, a thermostat, a home appliance or a smart car, is similar to a traditional computer in several ways.

First, since they are 'connected' they present an entry point to a network or at least one other device. Just as a lost or stolen laptop or mobile phone can provide an unauthorised user access to local data or remote resources on the same network, so too, can a connected, unmanned device on the IoT. And while data theft is certainly a key concern, even more frightening is the thought of the potential damage that can be done when an unauthorised user is able to manipulate the exchange of information between the connected device and its controller and thus send bogus instructions to the device, causing it to do harm. A related threat is a distributed denial-of-service attack in which a hacker controls not just a single IoT device but hundreds or thousands of them. By having each of those devices attempt to connect to a target website simultaneously, the hacker can take down that company's servers or customer-facing web applications and/or demand ransom in order to stop the attack.

Perhaps of greater concern than the threat scenarios themselves, though, is the fact that these connected devices, like traditional computers, often come to the marketplace with insufficient built-in security. Because time to market is so critical to companies competing in this space, product development cycles may be shortened with quality assurance and information security steps curtailed. The result is a product that enters the marketplace with vulnerabilities, i.e. weaknesses in the design or the configuration of a product that a hacker can exploit. Highlighting this phenomenon, a 2014 Hewlett Packard internet of things research study found that 10 commonly used IoT home security devices each had an average of 25 vulnerabilities on board when they were sold.

Since vulnerabilities are not being addressed in development and are usually only discovered once a product is in use, they can't always be easily remediated. The 'patching' process that we use to keep our desktops, laptops, tablets and phones updated and free of vulnerabilities may not work for many devices now connected on the IoT, or may require user intervention which could lead to confusion, errors and ultimately no reduction in vulnerabilities.



ENTRY POINT
Unmanned IoT devices provide unauthorised users access to local data

Evolution of cyber breaches – property damage and bodily injury

The idea of 'vulnerable' systems is very concerning when we consider bringing shop floor automation, SCADA controls and other process-related systems into the IoT. Automated processes have been around for many years but were not a significant security concern until these systems became connected to the internet.

Many of these systems were built using hardware and software that are no longer supported by the vendors who produced them originally. This means that patches are no longer being developed and distributed to remediate vulnerabilities that are constantly being discovered. Without such support, these systems become rife with exploitable vulnerabilities, a dangerous scenario considering that these systems manage critical electric grids, water treatment plants and chemical facilities. The fear is that a destructive attack on systems like these could cause widespread physical harm to both organisations and individuals.

The threat has already been realised. Stuxnet was a Trojan inserted into Iran's uranium enrichment facilities in 2007 that caused centrifuges to spin out of control and break down. In late 2014, massive damage was caused to a German steel mill after hackers forced a blast furnace to malfunction. More recently, hackers with ties to Syria infiltrated a water utility's control system in an undisclosed US location and changed the levels of chemicals used to treat tap water.

Business attitudes to cyber needs

Cyberattacks have become a fact of life and businesses today are often left with difficult risk-management decisions related to cybersecurity and how best to handle the risks they face – deciding whether they should retain the residual risk of a cybersecurity breach or transfer it through the purchase of insurance.

Historically, there was a high degree of reliance on IT to simply manage the security and privacy exposures, but more high-profile breaches have gotten the attention of C-suite executives and boards of directors.

C-suites now see the importance of increased communication and bringing all key stakeholders to the table, including risk management, general counsel and supply chain teams. While there is increased awareness of the threats, businesses are still struggling to understand the risks associated with cybersecurity issues: the full scope of their exposures and how best to protect themselves and their customers.

Risk mitigation solution – a mindset of resilience

For years, the threat of being hacked was either ignored or was addressed simply with firewalls and antivirus software. As cyberattacks and data breaches became more prominent, organisations responded with more investment in preventive technologies – security products designed to keep malware and the bad guys out of networks altogether.

But it eventually became apparent that prevention may not provide complete security and perhaps the IoT brings this into even sharper focus based on the threat scenarios and the financial, physical, legal and reputational damage that a cyberattack can bring to bear. While investment in prevention is still necessary and worthwhile, state-of-the-art information security is becoming more and more about detection and resilience. »

Cyberattacks have become a fact of life and businesses today are often left with difficult risk management decisions related to cybersecurity and how best to handle the risks they face

Organisations are accepting that at some point they will be hacked, but they are building out their detective controls so that indicators of compromise are discovered quickly and are isolated, disabled and removed before they can do major harm. Here are some key steps to creating and maintaining a philosophy of resilience:

- **Adopt a cybersecurity framework, such as the NIST Cybersecurity Framework** Created in 2014 by the National Institute of Standards and Technology, the NIST CSF is a valuable tool, not just for the information security department, but also for cross-functional teams charged with defining and prioritising the information necessary to build security into an organisation. There are five key activities outlined by the framework for a good security programme: **identify** the data and processes that need to be protected and conduct thorough risk assessments on those processes and data, as well as the hardware, software and network devices that are involved; **protect** those assets through the implementation of technical, physical and administrative controls; **detect** threats within the network by close and continuous monitoring of controls; **respond** to threats with a documented and tested Incident Response Plan; and finally, **recover** any lost information or assets.

The NIST framework was designed to protect critical infrastructure, such as banking and energy systems, but the standards have been adopted by everyone from retail chains to the Italian government. Nearly a third of US firms are already using the framework, according to 'Best Practices in Implementing the NIST Cybersecurity Framework' a 2016 analysis by technology research firm Gartner.

- **Elevate the cyber and IoT issues to the C-suite** Information security can no longer be considered an 'IT thing.' The impact of a cyberattack, particularly on the IoT, can be devastating or even terminal to an organisation. C-suites and boards must be kept aware of these risks so that they can provide the support and resources needed to provided security and resilience
- **Educate everyone on the importance of data security** Humans are indeed the weakest link in the security chain. A security awareness and training program is the lowest cost security measure with arguably the highest return on investment
- **Extend beyond the four walls of the company** Engage with an insurance carrier or a broker's risk management team in an ongoing, comprehensive review of all business partner relationships, including how those vendors/partners approach their own exposures and controls and how the vendors suppliers' approaches fits into their overall resilience plan
- **For developers of IoT products – bake security into the development process** For security to work well, it must be considered in the very earliest stages of product development and reassessed and retested as part of all subsequent stages. Security, if it is to be effective, must be baked in, not bolted on

ROBOT DEVICES Billions of devices are now connected through IoT applications

Conclusion

The future of IoT is exciting because of the improved convenience, productivity and profit it offers both the producers and users of connected devices.

As more devices become connected, risks amplify and many companies are frankly unprepared. Still, the tools needed to make the IoT more secure already exist – companies and institutions have to recognise the threat and prioritise the solutions. It isn't going to require any new concepts or any new technologies, but rather a commitment to the fundamentals of a proven cybersecurity framework, such as the NIST CSF.

Businesses must encourage a culture of awareness from the boardroom to the mailroom; identify all possible risks and have a risk management framework from which to work. Those that do can prove most resilient and quickly get back to meeting the expectations of their customers and their shareholders.