PANEL OF EXPERTS

With the help of our Panel of Experts, *Counter Terror Business* looks at the growth of the Internet of Things (IoT) and the potential benefits and pitfalls of connected devices

IoT – SECURITY RISK OR BRAVE NEW WORLD?

GABE CHOMIC, PRESIDENT, ISSA UK

Gabe is a technologist at heart who has been tinkering with things from an early age.

He has served as president of a national cyber security association, bootstrapped a cryptocurrency crowdfunding platform from wireframe to profitability, built security programs, analysed security processes across 14 countries and performed in-depth security engineering in heavy industry. His current passions involve the economic drivers behind insecurity and the cascading effects of small business failure.

SIMON DAYKIN, CHIEF TECHNOLOGY OFFICER, LEIDOS

Simon Daykin is chief technology officer for Leidos UK's Civil, Defence and Health business units, providing strategic business technology leadership for UK customers.

Motivated by the benefits technology can bring, Simon is passionate about supporting digital transformations through strategy, design and delivery to solve some of the most challenging problems in today's world. Before joining Leidos, Simon served as chief architect of NATS and CTO of Logicalis.

PAUL PARKER, SOLAR WINDS

Paul Parker brings over 22 years of IT infrastructure experience, having worked with multiple miltary, intelligence, civilian and commercial organisations.

Paul has received multiple military and civilian awards for service, support and innovation, having served as vice president of engineering for the federal division of Inflobox, an IT automation and security firm, as well as holding positions at CS2, Ward Solutions, Eagle Alliance and Dynamics Research Corporation.

Much is made of the incredible transformation potential of the Internet of Things (IoT), but in many ways it's simply an extension of the original network. Gartner suggests that there will be 20.4 billion connected devices by 2020. Connected devices are now everywhere, from home appliances and cars in the domestic setting, to industrial controls, body worn sensors and security systems for business - even in the defence sector. It's not just the smart thermostats and light bulbs you might use at home: field operatives are using increasingly intelligent wearable devices to monitor activity like drawing a weapon, and body cameras are one of the most talked about changes in civilian defence. However, just as BYOD left many organisations with new vulnerabilities, so do the sensors and remote devices that make up the IoT.

Gabe Chomic outlines a 'cynical and plausible' scenario to outline the idea of framing IoT as a technology that multiplies the potential of human achievement or fallacy. Consider walking down the road to your local station, pulling the alarm and watching the chaos as the alarm blares and the staff try to validate it before they have to evacuate.

Tomorrow, the same person could pull the same stunt, but the systems could identify the location the smart switch was pulled, pull the location from the CMDB, access the local CCTV and give the control room a good view. The trained operators present could handle the situation appropriately. More likely, the moment that alarm is tripped, alerts go out to all neighbouring alarms in the Community Metro Network (CMN). Approximately

half of those alarms are miscalibrated, including some internal ones in the station, and the ensuing cascade failure state escalates. Unfortunately the CMN is only lightly staffed nowadays. The station is evacuated, authorities of various calibre called in and the alarm system operator given a firm talking to. Nothing more can be done as this type of failure is not covered under standard contractual terms.

Good design, security-focused or not, should be able to prevent something like the above from happening. But it should also be able to prevent it from happening today. Today, security failure is rife - as the latest breach headline will testify.

A BIT OF BOTH?

As Gabe Chomic points out when we posed the *Security Risk or Brave New World* question to ISSA UK, you cannot pigeonhole a class of technology into the mental frame of security, no matter how polarising the question. With the IoT as much the result of the evolution of technology as information security itself, the two must be viewed in balance - 'IoT is both a security risk and a pathway to a brave new world'.

Lets look first at the tangible benefits - potential innovation, alternate technological applications, the very concept of cross-trust machine-to-machine negotiations. We can now gather vast volumes of rich new data in real time, improving our ability to make informed decisions and even immediately react through direct control of connected devices. In fact, as Simon Daykin suggests, we are now at a point where open source operating systems, IP networking ▶


leidos
Security by Design.
Always on.
FOR MORE INFORMATION
VISIT LEIDOS.COM/UK

EXPERT FINAL THOUGHTS

GABE CHOMIC, ISSA UK

"IoT is a security risk - we cannot secure the things we do now. Enabling us to do things faster and more efficiently will enable us to fail at scale.

"IoT is also a pathway to a Brave New World. One of technological enablement and potential dystopian abuse. IoT, like many technological improvements before it, is not something that can be stopped, just adjusted for. IoT is a tool after all. We determine how it is used and how well we use it. But based on our track record, I would plan for it's abuse as well as it's use."

SIMON DAYKIN, LEIDOS

"IoT is a natural evolution of our technology enabled and connected world, and whilst it can and will bring new security risks, these can be mitigated. We must recognise the importance of Secure-By-Design processes as we develop, integrate and test these technologies. We need to ensure we evaluate the new risks the technology can bring, embed proportional controls in the technology, and continuously reassess and respond to risks as they mature."

PAUL PARKER, SOLAR WINDS

"Is IoT a security risk or a brave new world? Well, it's a little bit of each and a lot of neither. Certainly, there are more IoT devices around, especially as they become smaller and less resource-dependent. With the many benefits and innovations that these devices bring on the horizon, it's just as important as ever, if not more so, to make sure they are secured and managed effectively as part of the whole defence sector IT infrastructure.

"Mitigating any security threat of IoT requires visibility into the network and devices running on it. Sophisticated monitoring and threat detection systems are necessary to find and remove problems as quickly as possible. When this is taken into consideration, the use of IoT devices becomes both achievable and beneficial for the defence sector."

◀ hardware and the computing processing capacity is so ubiquitous, stable and low cost it can easily be technically integrated into virtually any system with minimal impact on price.

On the flip side, whilst the hardware and software cost is insignificant, the critical factor, often stressed by companies such as Leidos, is recognising the investment required in securing the system and the application. Modern IoT technology is often based on the same highly capable and secure underlying software as our mission critical systems; however, the pace of implementation, the time-to-market pressure and the less rigorous engineering processes often mean security is not considered properly and the secure capabilities are not included.

Paul Parker agrees, highlighting that, just as BYOD left many organisations with new vulnerabilities, so do the sensors and remote devices that make up the IoT. Virus protection and network monitoring are critical and Parker says that defence organisations should look at whitelisting or blacklisting devices in line with what they're required to do.

Realistically, the risk from an IoT device is quite limited. If a hacker has control of the Ministry of Defence thermostat, they might be able to make the office environment quite uncomfortable, but they won't necessarily be able to access server files. The most significant risk comes from IoT devices being used as botnets - and this can also be mitigated. But how can this be done?

IOT DEVICES

SolarWinds pinpoints three steps for IT professionals in the defence sector to consider: consider automation; understand security information and event management processes; and monitor devices and access points. Administrators need to make sure they are using monitoring solutions to complement their automated network. Security information and event management allows users to keep an eye on real-time data and provide insight into forensic data.

Only devices with adequate security should be added to the network, and administrators should monitor for any unauthorised devices that are connecting. In addition, administrators should establish a baseline for what 'normal' IoT device usage looks like, and then check when devices aren't behaving in accordance with this, such as using more bandwidth than usual or generating unexpected traffic.

We have already seen examples of this through poorly implemented IoT devices making CTV, including baby monitor live video, available to anyone in the world, or exposing control of industrial process equipment to the internet by mistake. Daykin says that embedded and proportionate cyber security cannot be an afterthought, it needs to be considered and implemented as a foundation of technology, however mundane the use case appears to be.

SECURE-BY-DESIGN

Leidos advise that, when developing, selecting or testing IoT equipment, consider the system as a whole and the relevant threats, identifying potential vulnerabilities and risks that require control for successful low risk deployment. In the same way as virtually any technology platform, the tools are there to implement security controls and implement a secure solution, it simply needs the investment of time and effort in a structured risk identification and management approach.

> YOU CANNOT PIGEONHOLE A CLASS OF TECHNOLOGY INTO THE MENTAL FRAME OF SECURITY, NO MATTER HOW POLARISING THE QUESTION

Additionally, through this risk review process it is important to consider the unique factors IoT brings, such as the new information they are producing and making available (and who that may be valuable too), but also the nature of control over the physical world these devices may have. Understanding the control you have is critical to managing risks. Whilst accessing remote CCTV images or live data can expose new information sets, the control plane is often the more impactful area. Being able to remotely control home appliances, cars, buildings or industrial processes can have a more tangible impact on the real world, either individually or if co-ordinated to shared resources such as electrical grids or transport systems. This does not mean it cannot be secured, simply that the security controls need to be proportionate. It is critical to respond to the unique nature of these threats and continually reassess and respond to the risks as they mature.

IoT brings commercial automation within reach of a far wider audience than as possible before. What happens next isn't inherently the fault of the IoT, nor any one device within it. Chomic stresses that it is our ability to apply rigour to our developments that matters. ■