Enterprise-grade networks: the answer to IoT security challenges

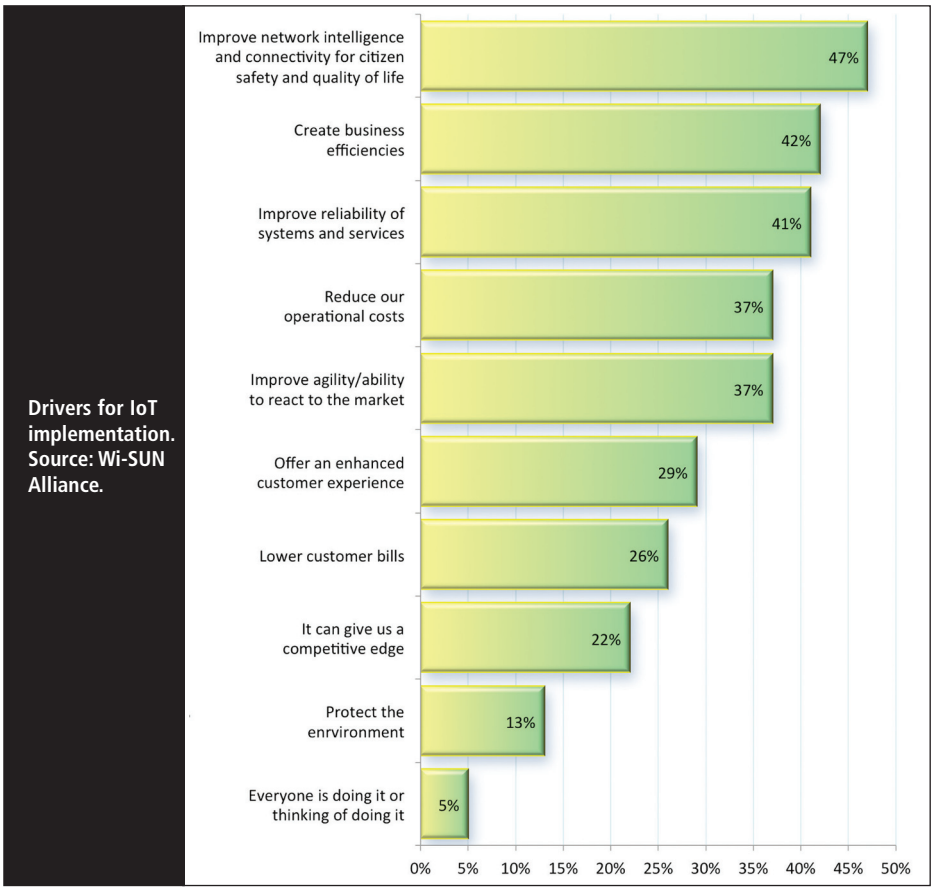
Phil Beecher

Phil Beecher, Wi-SUN Alliance

The Internet of Things (IoT) is quietly transforming the way utilities, industrial firms and smart city stakeholders operate. Some sectors are certainly accelerating faster than others to an IoT-driven future. But one thing is true across the board: cyber-security remains the primary barrier to the success of projects, both in terms of technical challenges and getting all-important board-level buy-in. Enterprise-grade networks should therefore be a priority for organisations wanting to improve the quality of life of citizens, drive business efficiencies, lower costs and increase the reliability of systems and services.

The IoT utilities sector alone is estimated to be worth $11.7bn by 2020.[1] In the smart cities space, it is predicted to reach $147bn by 2020, while in industrial IoT (IIoT) the figure is even higher – $195bn by 2022.[2,3] The Wi-SUN Alliance recently polled hundreds of IT executives around the world working in these markets and found that nearly all had begun IoT projects or were planning to do so.[4] Some of the most popular use cases included security and surveillance implementations (76%), water and gas metering (72%), electric vehicle charging (64%), street lighting (57%) and smart parking (56%).

Yet, while newer, smarter networks offer a range of benefits to drive competitive advantage, the proliferation of billions of new endpoints exposes organisations to a step change in the volume and range of cyberthreats. Security was by far the biggest concern of respondents in the IIoT, smart city and utilities sectors and it was cited by 59% of those working on IoT projects. Proven security with multi-layer protection and continuous monitoring was described as 'absolutely crucial' by half of smart city organisations and 44% of smart utility IT bosses.

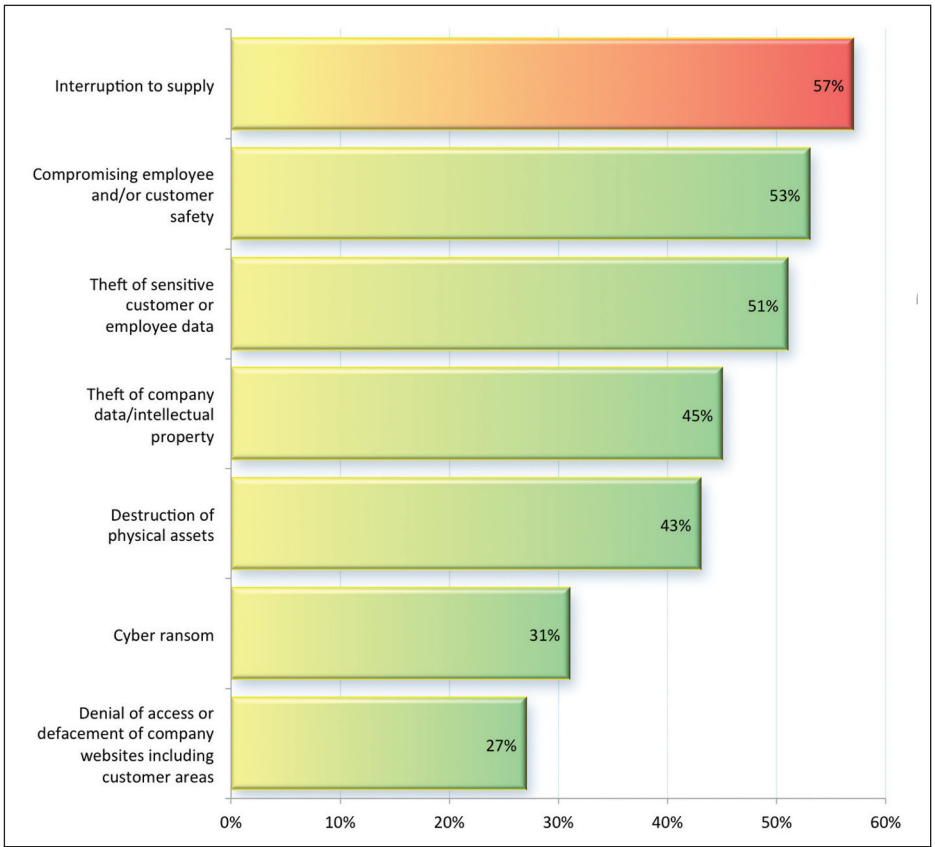


Drivers for IoT implementation. Source: Wi-SUN Alliance.

The threat landscape

This preoccupation with security is perhaps not surprising given the stories populating our news feeds today. We are bombarded by reports of state-sponsored attacks on critical national infrastructure (CNI) networks. Most notable are the alleged nation-state assaults on Ukrainian energy firms in December 2015 and 2016, which resulted in power outages for hundreds of thousands of customers.[5,6] That is not to mention the persistent threat from other nation states that reportedly have been observed conducting reconnaissance work on the US power grid.[7]

Certainly in the case of the Ukraine power outages we are talking about sophisticated and highly targeted multi-stage attacks. But ransomware worms, such as WannaCry and NotPetya, showed us last year that widespread chaos can be wrought against critical infrastructure providers by exploiting known vulnerabilities yet to be patched by firms. Global shipper Maersk ($300m in losses), logistics giant FedEx ($300m) and health company Reckitt Benckiser (£100m) all suffered major costs as a result.



Major concerns among electricity utility firms relating to cyber-security attacks. Source: Accenture.

An Accenture report polling 100 executives from utilities companies in 20 different countries revealed that 63% believe they will face supply interruption resulting from cyber-attacks on electricity grids in the next five years.[8] Tellingly, less than half (48%) felt well prepared for such challenges. Yet the threats to smart grids and IoT networks in these sectors do not just revolve around possible life-threatening service disruption. Hackers can also target under-protected IoT endpoints with a view to stealing sensitive data and intellectual property from other parts of the corporate network.

"Hackers can target under-protected IoT endpoints with a view to stealing sensitive data and intellectual property from other parts of the corporate network"

As IoT drives an explosion in large and complex networks of connected endpoints, it will provide new opportunities for state-sponsored operatives and financially motivated cyber-criminals alike.

The security challenge

These challenges are reflected in the attitudes of IT professionals, according to the survey. The good news is they recognise the need for improved IT security – 74% highlighted it as their organisation's biggest priority. Interestingly, even more respondents in the US (83%) and UK (79%), ranked it as a priority. They also ranked security as a number one challenge in greater numbers - 65% of US IT bosses and 64% of their UK counterparts.

Of some concern will be the fact that little more than a third (38%) claimed that their organisation features protecting IoT devices from cyberthreats in their overall IoT strategy, while just over half (51%) said that considering how to secure data collected by these devices is part of their strategy. Being generous, you could argue that these figures are so low because such tasks are being considered by a separate function in the organisation, but they remain concerning.

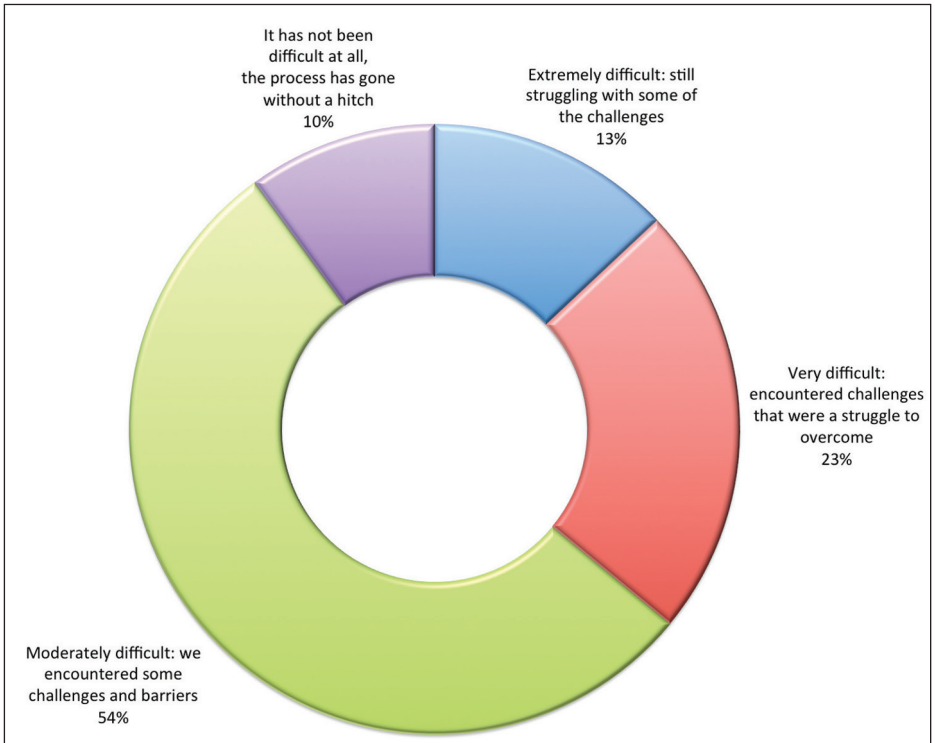
This is especially true in the context of strict new EU privacy laws that landed in May. The General Data Protection Regulation (GDPR) gives regulators the power to levy fines of up to €20m or 4% of global annual turnover for non-compliance. While it is not suggested that any firms will be targeted with these, at least not to begin with, the large sums being talked about certainly raise the stakes. Yet only 43% of IT leaders claimed they are including data protection compliance in their IoT strategy. This could be an expensive mistake. Organisations must address these challenges by implementing enterprise-grade secure networks for IoT implementations. But what features should be considered?

Security in context

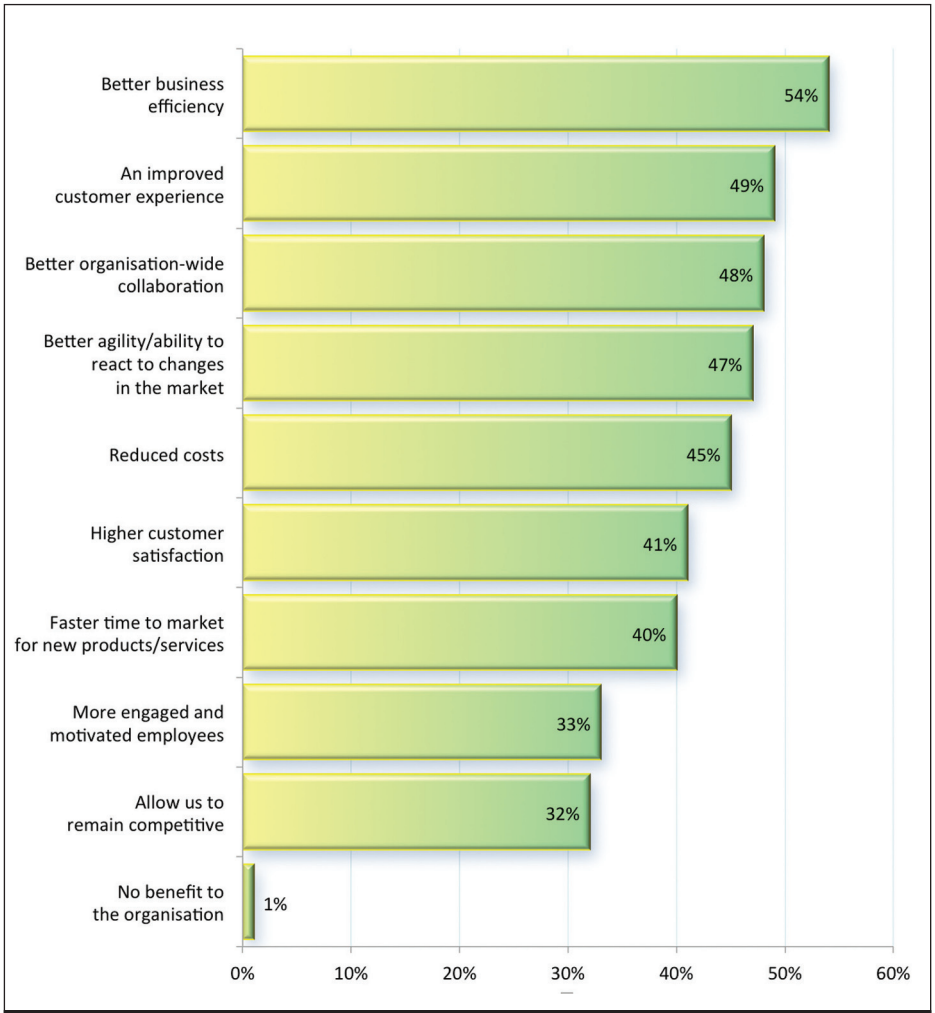
Network topology was judged to be the most important criterion for selecting new IoT technology by the majority of respondents (58%). The majority also claimed to favour a combination of star- and mesh-based networks. However, mesh networks offer a number of improvements that cannot be matched by star networks – such as greater resilience to signal jamming and denial of service (DoS) attacks, which makes them a better choice for critical national infrastructure providers.

Mesh networks are also built around the model of IoT devices communicating with one another as well as the network base station. This allows for multiple, redundant connection paths, drastically reducing single points of failure and connectivity black spots and improving reliability and performance with scale, as possible communication paths multiply. In addition, devices on mesh networks usually transmit short distances, allowing for higher data rates, meaning lower latency but with low energy consumption, providing long battery life.

Open standards are another key feature to look for in secure IoT networks, removing the risk of vendor lock-in and giving organisations peace of mind by following industry best practices. In fact, more than half of IT decision-makers claimed standardisation was a key requirement for IoT projects. Over two-fifths (45%) said that smart city IoT solutions should be built using industry-wide open standards and a similar number (43%) said the same for utilities projects.



Challenges when implementing an IoT strategy. Source: Wi-SUN Alliance.



Benefits realised as a result of an IoT implementation. Source: Wi-SUN Alliance.

One such standard to look for is the IEEE 802.1AR specification for Device Identity.[9] This supports cryptographically binding a secure device identifier (DevID) to a device and enabling authentication of that device. By doing this, network administrators can establish trust and support policies for transmission and reception of data and control protocols to and from the device.

Enterprise-grade networks

In fact, certificate-based authentication and trust is key to establishing enterprise-quality security on IoT networks. However, the devil is in the detail. With industry standards and interoperability as their watchwords, organisations should look to establish an authentication chain of trust using public key infrastructure with x.509 certificates as well as cryptographic key exchange and rotation.

This is all about establishing trust and blocking any attempts to compromise and update firmware residing on the IoT endpoint. Also important are role-based access controls to mitigate the insider threat and ensure that if accounts are compromised, risk exposure is minimised.

Finally, firms should not underestimate the importance of over-the-air (OTA) update capabilities. By ensuring that devices are upgradable over-the-air, they can stay protected at all times and can be rendered unable to connect if the firmware has been replaced by an unauthorised third party.

The threat landscape moves at an unforgiving pace and none of us can predict what tactics attackers may be looking to use in the future. That makes it vital to have the ability to quickly and easily update endpoints from a centrally managed location.

Establishing and maintaining this kind of cyber best practice can go a long way to improving the resilience of a network, both now and in the future. It is particularly important given the growing volume of new vulnerabilities discovered on an almost monthly basis and the relatively long expected lifespan of IoT networks in industrial, utility and smart city implementations. Interoperable standards are

also your friend here, providing backwards compatibility for older systems and also a baseline with which to move forward.

C-suite buy-in

A third of IT decision-makers said that securing funding is still a major barrier to IoT adoption, with a similar number citing a lack of leadership buy-in. It is more than likely that cyber-security concerns have a role to play here, perhaps leading many senior executives to favour other less-risky projects instead.

It is vital, therefore, to have a clear strategy in place from the start to mitigate any expected security risks involved in a project – and it is just as important to communicate them in a way that the C-suite understands.

Research claims that smart grid cyber-security spend alone will reach $3.2bn by 2026.[10] The key is in knowing where to spend it.

About the author

Phil Beecher is president of the Wi-SUN Alliance (www.wi-sun.org), an industry organisation that promotes standards-based interoperable wireless communications products for smart cities and other Internet of Things (IoT) applications, and implements a rigorous testing and certification programme. Since 1997, Beecher has played a key role in the development of communications standards, including Bluetooth, wifi, IETF, IEEE and cellular and the specification of test plans for a number of smart utilities network standards, including Advanced Metering Infrastructure (AMI) and home energy management systems. He was chairman of IEEE 802.15 TG4g (a wireless standard for smart utility networks), chairman of IEEE802.15 TG4u and TG4v (defining RF spectrum for IoT networks globally), vice chairman of IEEE 802.15 TG4m (TV Whitespace), vice chairman of the WiFi Alliance Smart Grid Task Group, chairman of OpenSG Edge Conformity Task Group, contributing editor to IEEE802.15.4-2006 and has held positions in the US Smart Grid Interoperability Panel (SGIP) Test and Certification Committee, Telecom Industry Association and Bluetooth SIG. He is a graduate of the University of Sussex with a degree in electronic engineering and holds patents in communications and networking technology.

References

1. 'Internet of Things (IoT) in the utility market is big business'. Engerati, 22 Apr 2016. Accessed Jul 2018. www.engerati.com/article/Internet-things-iot-utility-market-big-business.
2. 'Internet of Things (IoT) in smart cities market by solutions (remote monitoring, data management) platform (application & device management) application (building automation, energy management, transportation) – global forecast to 2020'. Markets and Markets, Feb 2016. Accessed Jul 2018. www.marketsandmarkets.com/Market-Reports/iot-smart-cities-market-215714954.html.
3. 'Industrial IoT market by device & technology (sensors, RFID, industrial robotics, DCS, condition monitoring, smart meters, AHS, camera system, networking technologies), software (PLM systems, MES, SCADA), vertical, and geography – global forecast to 2022'. Markets and Markets, Jun 2018. Accessed Jul 2018. www.marketsandmarkets.com/Market-Reports/industrial-Internet-of-things-market-129733727.html.
4. 'The Rise of the Internet of Things'. Wi-SUN Alliance, 4 Dec 2017. Accessed Jul 2018. www.wi-sun.org/index.php/vb-iot-rpt/file.
5. Zetter, Kim. 'Inside the cunning, unprecedented hack of Ukraine's power grid'. Wired, 3 Mar 2016. Accessed Jul 2018. www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.
6. 'Ukraine power cut was cyber-attack'. BBC News, 11 Jan 2017. Accessed Jul 2018. www.bbc.co.uk/news/technology-38573074.
7. Mitchell, Andrea; Dilanian, Ken. 'Experts: North Korea Targeted US Electric Power Companies'. NBC News, 11 Oct 2017. Accessed Jul 2018. www.nbcnews.com/news/north-korea/experts-north-korea-targeted-u-s-electric-power-companies-n808996.
8. 'Outsmarting grid security threats'. Accenture. Accessed Jul 2018. www.accenture.com/us-en/insight-utilities-outsmart-grid-cyber-security-threats.
9. 'ANSI/IEEE 802.1AR-2009 – IEEE Standard for Local and metropolitan area networks – Secure Device Identity'. IEEE Standards Association, 2010. Accessed Jul 2018. https://standards.ieee.org/findstds/standard/802.1AR-2009.html.
10. 'Global smart grid cyber-security spending is expected to near $3.2 billion in 2026'. Navigant Research. Accessed Jul 2018. www.navigantresearch.com/newsroom/global-smart-grid-cyber-security-spending-is-expected-to-near-3-2-billion-in-2026.

Why is patch management necessary?

Colin Dennis, OGL

Colin Dennis

If you're a UK business that relies on any form of technology, then patch management should be at the top of your 'to do' list. More and more companies rely on a form of software and/or IT infrastructure to streamline their processes, maximise return on investment and store valuable data.

However, as technology evolves, so does its arch nemesis – cybercrime. As fast as