Cyber security in the Middle East

In this e-guide

In this e-guide:

As organisations increase their reliance on IT through rapid digital transformations, the threat of cyber attack grows.

It is not just western countries such as the US and the UK that are being targeted by hackers, as the rapidly developed and wealthy nations of the Middle East become targets of both politically and financially driven attacks.

For example, the Saudi Arabia state media confirmed that attacks on several Saudi Arabia government agencies, involving the use of a new variant of Shamoon known as StoneDrill, which destroys everything on the infected computer, happened over a two-week period late last year. Read more about it in this e-guide.

There is a lot at stake in the Middle East. For example, banks in the region are moving to digital services and the threat of disruption caused by hackers is increasing as a result. The Middle East is increasingly seeing the use of IT to support the

In this e-guide

everyday lives of its citizens, with autonomous vehicles and passenger-carrying drones, which you can read more about in this issue, being introduced. These could become targets of cyber criminals and terrorists intent on causing maximum damage. The adoption of internet of things technology is another trend that is potentially opening doors for those with malicious intent. Read in this issue how to keep those doors locked.

In this e-guide, discover how cyber security expertise can help businesses in the Middle East navigate digital transformations and keep cyber criminals at bay.

Karl Flinders, Emea editor

In partnership with GISEC and IoTx

In this e-guide

New wiper malware hits Middle East and Europe

Warwick Ashford, security editor

Like Shamoon and its variants, the newly-discovered StoneDrill wiper malware destroys everything on the infected computer, according to Kaspersky Lab's Global Research and Analysis Team.

StoneDrill also features advanced anti-detection techniques and espionage tools in its arsenal.

In addition to a target in the Middle East, a StoneDrill target has also been discovered in Europe, where wipers used in the Middle East have not previously been spotted in the wild.

In 2012, Shamoon was identified as the latest in a line of attacks that targeted infrastructure that included Stuxnet, which was designed to hit nuclear infrastructure in Iran, and Duqu, Flame and Gauss, which sought to infiltrate networks to steal data.

"From Stuxnet to Shamoon 2 there is a distinct evolution to more advanced malware being targeted at industrial controls systems, according to Azeem

In this e-guide

Aleem, director of advanced cyber defence practice for Europe, Middle East and Africa (Emea) at RSA.

In 2012, Shamoon took down around 35,000 computers at oil and gas company Saudi Aramco, putting 10% of the world's oil supply at potential risk.

However, the malware was not seen again until late 2016, when a heavily updated version of the malware was identified and dubbed Shamoon 2.0.

While exploring these attacks, Kaspersky Lab researchers discovered StoneDrill, which, although similar in style to Shamoon 2.0, has unique characteristics and is more sophisticated.
Although researchers believe StoneDrill was created separately from Shamoon, it shares enough characteristics to have been picked up by tools developed to detect Shamoon.

The researchers said that while it is still not known how StoneDrill is propagated, once installed, it injects itself into the memory process of the user's preferred browser.

During this process, they said, it uses two sophisticated "anti-emulation" evasion techniques and then starts destroying (wiping) the computer's disc files.

The researchers also found a StoneDrill backdoor, which appears to have been developed by the same code writers and used for espionage purposes. They discovered four command and control panels which were used by attackers to run espionage operations with the help of the StoneDrill backdoor against an unknown number of targets.

To protect organisations from such attacks, Kaspersky Lab advises:

- Conduct a security assessment of the control network to identify and remove any security loopholes.
- Review supplier security policies to ensure none have direct access to the control network.
- Request external intelligence that helps organisations predict attacks on industrial infrastructure.
- Train employees, paying special attention to operational and engineering staff.
- Provide protection inside and outside the perimeter, including detection and response.
- Evaluate advanced methods of protection such as specialised network monitoring.

Although similar in style to Shamoon, StoneDrill also appears to have connections to several other wipers and espionage operations observed previously, said researchers.

They observed code similarities to the NewsBeef APT, also known as Charming Kitten – another malicious campaign which has been active in the last few years.

"We were intrigued by the similarities and comparisons between these three malicious operations," said Mohamad Amin Hasbini, senior security researcher of the global research and analysis team at Kaspersky Lab.

The most likely scenario, he said, is that StoneDrill and Shamoon were developed by two different and unconnected groups with similar objectives.

Next article

In this e-guide

Middle East organisations urged to prioritise cyber defence

Edward Banda, guest contributor

In the wake of a series of cyber-attacks that targeted Saudi Arabia government agencies and private firms, security experts have warned Middle East organisations to strengthen and prioritise their defences.

Middle East organisations, both public and private, are finding themselves at the forefront of the cyber security battle.

Some of the biggest cyber security attacks of 2016 were on several Saudi Arabia government agencies, which were targeted in a series of attacks over a two-week period, erasing data and wreaking havoc in the computer banks of the agency running the country's airports and hitting five additional targets. The Saudi state media confirmed the attacks happened over a two-week period, in November 2016, but no further details were provided.

Experts said the attacks involved the use of a new variant of Shamoon (Shamoon 2), a malware tool that made headlines five years ago for erasing the hard disks of more than 30,000 computers belonging to petroleum giant Saudi Aramco.

In this e-guide

In January 2016, Saudi Arabia's telecoms regulator, the Communication and Information Technology Commission (CITC) warned organisations in the oil-rich kingdom to be on the alert for the virus, as the labour ministry said it had been attacked and a chemicals firm reported a network disruption.

Ahmed Baig, founder and CEO of the CISO Council, a non-profit industry body with approximately 4,000 members in the Middle East, said organisations in the region need to ensure cyber security is taken seriously at board and executive management level.

He said it should be addressed as a business risk and not merely as a technology problem as it threatens every aspect of an organisation, including business continuity and, most importantly, reputation.

"The recent wave of regional and global attacks have had consequences like never before," he said. "The attacks have targeted critical infrastructure, central banks and popular internet websites with data breaches resulting in the compromise of billions of records."

Organisations in the region need to proactively invest more in security by implementing the right controls and hire competent people or external security service providers. "As no one is immune to the cyber-attacks, organisations in the region should start assessing their security posture and address the weaknesses," said Baig.

In this e-guide

He pointed out that cyber security maturity is lacking in most regional organisations in the Middle East, and more needs to be done considering the sophisticated and persistent attacks used by cybercriminals.

"Regional organisations are investing and working with external partners to implement security solutions and practices that are considered important," he said. "However, it's clearly not enough as the evolving threat landscape and advanced attacks such as Shamoon, Stuxnet and others have given an edge to hackers as they were able to gain access due to lack of holistic and inconsistent security practices."

Organisations can't afford one wrong move

Baig said what's troubling with most attacks in the region is that adversaries have to be right just once to succeed in an attack, whereas the victim organisations have to be right always to protect their organisation.

Mohammad Amin Hasbini, senior security researcher at Kaspersky Lab Middle East, Turkey and Africa, agreed with Baig on the lack of security maturity in the region. He said the recent attacks highlight a lack of readiness and maturity of the organisations and employees.

"Keeping in mind that reaching the required levels of maturity is extremely difficult to achieve, IT security shouldn't be treated as a technology issue but a pertinent business imperative," he said. "It is not only about the

configuration and protection of systems and data, it's also about making sure that not a single employee makes a basic mistake."

He added that recent cyber security attacks targeting organisations in the Middle East have showed that some of the most serious security vulnerabilities remain the most simple ones, such as phishing, poor passwords and unsupported software.

Middle East remains a cyber-attack target

Nicolai Solling, chief technology officer at Dubai-based systems integrator Help AG, said the recent cyber-attacks that rocked Saudi Arabia highlight that the Middle East is still a target.

Solling said what is unique about Shamoon and Shamoon 2 is that these types of malware are not created for financial gain, but to destroy or render a computer system unusable.

Christopher Green, regional director, Middle East, Africa and Turkey, at Malwarebytes, warned that an attacker will always have the advantage because he or she only needs to find one flaw in an organisation's security, whereas the latter must defend against a large number of potential weaknesses, not limited to software but also including the "human factor".

The job of any organisation is to evaluate risk and prioritise areas where most efforts are needed in order to make the attacker's job considerably

harder. "Many of these kinds of attacks seem to be politically related, and attackers are continuously trying to breach their targets, even if it takes years to achieve that goal," said Green.

He emphasised that the lack of visible compromise does not mean that threat actors aren't trying or haven't already succeeded while lying low until they get further instructions.

Governments must have a good backup policy

He added that, like any other organisation, governments in the Middle East must ensure that they have a good backup policy in place and that they encrypt their data any time that's possible. "Patching software vulnerabilities is important but not enough," he said. "The kind of attackers wreaking havoc now are usually well funded and able to use zero-day exploits where no patch is available yet."

He said signature-less protection that instead relies on behaviour attributes is well suited to counter such threats.

Looking to the future, Baig warned of the impact of future cyber attacks on physical systems that are part of smart and intelligence cities that are being implemented to gain the economic advantage and sustainability. "cyber security attacks such infrastructure could endanger human life."

In this e-guide

Airborne cars to transform Dubai's public transportation

Edward Banda, guest contributor

As Dubai continues its smart city transformation journey, the Roads and Transport Authority (RTA), has revealed plans to unveil passenger-flying cars are in the final stages, with the initiative expected to launch in July 2017. According to the RTA, the strategy to make airborne passenger drones available to the public in summer is part of a broader vision to transform Dubai into a global driverless mobility leader by 2030.

Speaking at the World Government Summit 2017, Mattar Al Tayer, director general and chairman of the board of the RTA, said: "Autonomous mobility has become a fait accompli, and is continuously evolving. This technology has been tested in several places, including Dubai, Singapore and the US.

Unlike other cities and countries, where driverless mobility has been a private sector-led initiative, Dubai is leading the transition to driverless mobility in the city and plans to take a leading position worldwide in the next 13 years.

"The RTA has successfully trialled the autonomous aerial vehicle [AAV], a single-seat flying car in Dubai, and we are making every effort to launch in July this year," said Al Tayer.

The AAV will have a range of 40-50km and a flying time of around 30 minutes. The vehicle will be able to carry a load of 100kg, and fly on autopilot while being monitored by a central command centre.

He said the RTA was testing autonomous vehicles as part of Dubai's goal to have autonomous vehicles account for 25% of all journeys in Dubai by 2030.

The AAV measures 3.9m in length, 4.02m in width and 1.60m in height. In addition, it weighs about 250kg – up to 360kg with a passenger. The maximum cruising height is 3,000ft and the battery charging time is 1 to 2 hours. The AAV is designed to operate under all climatic conditions apart from thunderstorms.

The RTA added that the vehicle has been developed in collaboration with Chinese manufacturer Ehang.

Industry pundits say the global realisation of automated flight signifies a major turning point, not only for the transportation industry, but also for a swathe of other fields, such as shipping, medical care and retail.
The Cloud Security Alliance (CSA), an organisation advocating secure cloud together with Securing Smart Cities, a non-profit global initiative focused on

identifying cyber security problems for smart cities, recently released the *Establishing a safe and secure municipal drone programme* report. In the report, the two organisations pointed out that drones are increasingly playing a crucial role in smart city transformation.

"Whether you are a fan of them or not, it is becoming increasingly evident that drones will play an important and even critical role in the smart city environment," said Brian Russell, co-author of the report and chair of CSA's IoT [internet of things] Working Group. "Cities around the country are working to implement large-scale drone programmes to support various functions, ranging from medical, transportation and agricultural to emergency management and infrastructure protection."

Russell emphasised that it is important for the drone systems to be safe, stable, resilient and sustainable.

Global and local challenges for flying cars

Al Tayer said there are global and local challenges facing autonomous mobility progression, including infrastructure, laws and legislations, safety and public acceptance of driverless vehicles and technological requirements, and efficiency of sensors and cameras in various circumstances – including electronic piracy protection procedures.

"The RTA has gained experience with the Dubai driverless Metro train system," said Al Tayer.

He said that at the start of the Metro train service, the RTA had to deploy a person to pose as a driver for a period of about six months just to reassure passengers and encourage them to use the service.

Besides the global challenges, there are other hurdles facing Dubai, including harsh weather conditions (high temperatures and humidity) and their impact on driverless transportation technological systems. Another factor is the multinational and multicultural makeup of Dubai, a tourism and business hub. "This may increase people's reluctance to embrace modern technology," he said.

To cope with the challenges, the RTA has prepared the Dubai Smart Autonomous Mobility Strategy, which, compared to other global plans, is characterised by the leading role the Government of Dubai is playing in helping the city transition to driverless mobility. "Dubai's vision is to integrate technology systems of all mass-transit modes, such as trains, buses, marine transit modes and taxis," said Al Tayer.

Pre-set destinations for passengers

According to the RTA, a passenger in the AAV will be able to select from a number of pre-set destinations displayed on a map on a touchscreen in the cockpit. The drone will then fly to the selected destination.

The AAV is a quadcopter vehicle, with four pairs of propellers, which Al Tayer said would mean in the event of one propeller failing, the drone would still be able to complete the flight smoothly.

Huazhi Hu, CEO at EHang, said: "It's been a lifetime goal of mine to make flight faster, easier and more convenient. The Ehang 184 AAV will provide a viable solution to the many challenges the transportation industry faces in Dubai and elsewhere around the world in a safe and energy-efficient way."

With the collaboration with the RTA, Ehang will make a global impact across dozens of industries beyond personal travel. "The commercial adoption of drones by cities including Dubai implies that thousands of programmable connected mobile devices will not only operate in the streets, but also above and below them."

"Drones in the sky, drones in the sea and drones on land, but are we ready?" asked Mohamad Amin Hasbini, senior security researcher, Kaspersky Lab and Securing Smart Cities board member.

Hasbini said that from a security perspective, it's crucial the drones are secured to prevent potential disasters should one of several systems or the software used to control them become compromised or manipulated.

"That's why we are trying to raise issues around security to the public early, ensuring safety guidelines and regulatory frameworks can be in place and strengthened."

Flying cars already being tested

At the World Government Summit, Al Tayer showed a video of the AAV being tested at SkyDive Dubai's desert campus and a Dubai seafront hotel. "This is not only a model," he said. "We have actually experimented with this vehicle flying in Dubai's skies."

Al Tayer said the Dubai Civil Aviation Authority (DCAA) was a partner during the trials, and the organisation defined the safety criteria required, issued the permits for the trials and inspected the autonomous vehicles. "Etisalat contributed to the success of the test run of the AAVs in its capacity as a network provider," he said.

Al Tayer said Etisalat also provided the support needed to ensure the continued communication between the AAV and the control centre through machine-to-machine (M2M) and long-term evolution (LTE) technologies.

The AAV is fitted with numerous basic systems all in operation at the same time, though independently. In case of any system malfunction, the standby system would be capable of controlling and safely steering the AAV to the programmed landing point," Al Tayer said.

Next article

In this e-guide

How information security professionals can help business understand cyber risk

Warwick Ashford, security editor

The UK government's latest National Cyber Security Strategy requires businesses to have a detailed understanding of the risks to their information systems and raise standards to mitigate them.

The challenge comes as businesses are becoming increasingly reliant on digital and online systems, making it all the more difficult to achieve a good understanding of cyber risks across the whole company.

In the digital era, new points of entry are opening up for most business from email to cloud environments, from mobility to applications, from the payment gateway to the datacentre and many more.

Information security professionals have a key role in digital transformation processes to ensure the business understands the risk, implements the necessary mitigations and accepts the residual risk.

But engaging with business leaders and boardrooms on cyber security can sometimes be as challenging as understanding the threat landscape in the first place, according to information security professionals.

Osterman Research shows that only 37% of IT security professionals believe risk is reduced as a result of conversations with their boards.

Many feel overlooked, ignored and underappreciated when trying to get a budget to address security holes, says Tim Holman, chief executive at 2-sec security consultancy.

"The challenge we face isn't the business failing to grasp cyber risk, it's addressing the communications gap between technical staff and business owners," he says.

Cyber insurance a grudge purchase for business owners

Business owners also do not like spending money on anything that does not make them money, says Holman, adding that even cyber insurance is a grudge purchase.

"I'm never fond of paying a high premium, but I accept it if there's a niggling feeling that I could lose my livelihood and house if I fail to get the right insurance cover," he says. "And mitigating cyber risk is exactly the same. If companies don't do it, they could go out of business."

But businesses tend to be overconfident in existing defences and often doubt they could be seriously affected by a cyber attack, leaving infosec pros with the challenge of persuading them there is a real need to mitigate security risks.

Holman cautions against demanding cash after something has happened to plug a hole. "It's about taking a proactive stance, dealing with cyber security before something happens, and being prepared to tell security suppliers where to stick their hardware if it doesn't fit into your security programme.

"I've never seen a business turn down a carefully prepared cyber security risk mitigation programme that fits the business. Fortunately, creating one is remarkably simple. Define scope. Carry out a security audit on said scope. Conduct a gap analysis, work out three costed options with pros and cons to address each gap, and present to the business," he says.

If that does not work, Holman suggests a short, sharp exercise that demonstrates to the business exactly what could go wrong in their cyber world.

"Simulate a phishing email, put a malware test file on your CEO's laptop, take your CFO's laptop away for an hour and simulate critical hardware theft. Then leave a suspicious package in the mail room or simulate a web server hack to raise awareness over time, which will ultimately loosen the purse strings and get support for implementing change."

Raising cyber security awareness

Cyber security is everybody's responsibility, says Maxine Holt, principal analyst at the Information Security Forum (ISF). "Start by raising awareness

across the organisation because people are an organisation's biggest asset and also potentially its biggest risk. How these people take decisions and behave in key moments is essential to strengthening resilience."

Holt advises capturing the attention of the business with a "sell not tell" message. "Promote a cyber-secure culture by using business language; individuals switch off if they don't understand what is being said."

A business relationship manager role can be used to great effect, providing a bridge between the information security function and the rest of the business. This helps explain what needs to be done to support cyber security.

According to UK government, only around 20% of businesses provided cyber security training for their employees in 2016. "If individuals are unaware of how to behave in key moments, they are likely to make poor security decisions," she says. "Develop an awareness programme and prioritise it based on the risk profiles of employees. Secure behaviours can be reinforced with regular training and communications."

Holt believes organisations should focus on rewarding good security behaviour and having strategies in place to address behaviour requiring improvement. "Leading organisations recognise that a network of trained information security champions from within the business can play a vital role

in introducing and embedding positive information security behaviours," she says.

Holt also suggests using various standards to prioritise cyber security requirements and explain these priorities to the business, such as the ISO/IEC 27002 code of practice for information security controls and the ISF's *Standard of good practice for information security*.

Business as usual

Adrian Davis, managing director for Europe at (ISC)², advocates a more "business as usual" approach. "As businesses become more digital by nature, cyber security has to become a part of everyday operations. This means seeing cyber security as another operational risk, such as physical damage or theft, rather than confined to the IT department. This approach has seldom been taken but is desperately needed.

"Businesses have to become more responsible for their own cyber security, and to achieve the government's aims, we must move away from the misguided approach of reducing cyber security to a technology problem. Cyber security must be recognised as a fundamental component of business, a critical responsibility that business leaders must not ignore," he says.

In this e-guide

Davis believes infosec pros can help in communicating information risk as a business risk by looking at treating it as something more than a technical issue and assessing it in the context of customer service, PR and business reputation.

"These risks must be communicated in a way that clearly explains the potential harm to the business should a malicious or accidental incident occur. The risk treatments that can be put in place given the resources – and the residual risk to the business – must be clearly stated and updated as the business changes," he says.

Davis believes there needs to be a dialogue between business leaders, IT and information security around information risk.
"Business leaders should regularly and actively challenge IT and information security leaders on information risk and its business impacts, and not just accept that technology can solve the problem. This is a two-way street: as much as information security leaders can push this dialogue, business leaders must give the time to listen, comprehend and discuss," he says.

According to Davis, organisations should also examine how to include information security requirements from idea through to design, development, engineering, testing and production of any product or service built, produced or bought by the business.

"This "security by design" approach is cheaper and more effective than adding security as an afterthought once the product is in market and problems arise," he says.

An important element of the "business as usual" approach is for information security professionals to ensure it is easy for people in an organisation to follow good security practices, says Alex Ayers, co-founder and consulting director at Turnkey Consulting.

Different industries have different concerns

In addition, he says information security professionals need to recognise that security is one of the many things businesses are concerned about, and understand that different industries have different concerns. They must accept that "good-enough" security is an acceptable state, and understand that financially quantifying risk, while difficult to achieve, allows budget holders to make better funding decisions and are less likely to see security as a poor investment.

"As security professionals, it is very important that we communicate in ways that resonate with our audience," says Ayers. "We may be comfortable talking about data exfiltration to a CISO, but that same terminology may leave a CFO or COO confused. We have to understand the risk in the context of the business to make our advice relevant and pragmatic to implement. By doing this, we are demonstrating value as trusted advisors."

In this e-guide

The threats to digital business are only going to get more complex. "As an industry, we need ensure we can attract and retain individuals who fulfil the broad spectrum of roles that the industry has to offer," he says. "We need to recognise and reward business engagement skills in the same way we do technical skills, and provide clear paths for progression that do not involve leaving the industry."

While digitally enabled businesses certainly have an increased attack surface, the key principles of cyber security best practice will always remain the same, says Ramsés Gallego, past international vice-president of the Isaca board of directors and strategist and evangelist in the office of the CTO at Symantec.

"Whatever the type of business, it's fundamental that there is a plan in place that takes into account all of the emerging technologies we're seeing, from cloud to increased mobility, big data and the internet of things (IoT).

"It is also critical that organisations, no matter the size or industry, comprehend where data that is instrumental for the day-to-day activities of a company lives and, in consequence, how it should be protected."

Beyond the technical processes and procedures, Gallego says security professionals should also be familiar with the latest legislation and regulations that companies have to abide by, with a clear understanding of the various governance frameworks.

Tailoring the security message for business

Key to tailoring the security message for the business is recognising that businesses understand profit and loss, and the need and cost of marketing and sales, says Peter Wenham, committee member of the BCS Security Forum strategic panel and director of information assurance consultancy Trusted Management.

Just as a company cannot survive without marketing and sales, many will – in the worst-case scenario – fall victim to an information security breach and fail without good information security.

The message that should be given to the business, says Wenham, is simply this: "If you don't do X, Y will happen, and that will cost the business £Z.

"X is an information security control such as ensuring the IT estate is security patched with the latest patches, or that all people in a company are given regular training and education in being security-aware citizens who know what to do when things start to go wrong.

"Y is of course a security breach, which could be someone hacking into a company's IT estate and taking copies of data. But it is more likely to be someone opening a malware-infected email attachment or clicking on a link in an email that takes their browser to a website that is a source of malware, which increasingly these days could be ransomware.

"£Z is the cost to the business of recovering from the breach. It's the cost to the business that needs to be articulated, and in a way, that is understandable. Simply saying it will take two days to recover from a breach isn't sufficient," he says. "You also need to identify the potential cost to the business and of lost productivity across the whole company, the anticipated loss in sales, and the typical cost of using external specialist help."

Wenham says a funding request should be written with the recommendations immediately following the management summary, and structured along the lines X, Y and Z.

"If there is a range of options available, prioritising the options along the lines of 'must have', 'need to have' and 'nice to have' will help the business reach appropriate decisions," he says. "Detailed risk reviews and analysis, work identification and costs to implement, and the potential costs to the business if various work is not done should be included as supporting appendices."

Next article

In this e-guide

Multi-layer approach to IoT security needed

Aaron Tan, senior editor, APAC

The internet of things (IoT) may have spurred innovation and unlocked revenue opportunities for many organisations, but the security of the technology remains a key concern among senior business leaders.

According to the *Internet of things business index 2017* report by the Economist Intelligence Unit (EIU), 26% of 825 respondents globally cited security and privacy as one of the top obstacles to IoT deployments.

The high cost of investing in IoT infrastructure – cited by 29% of respondents – remains the top bugbear.

The EIU said in its report that security concerns are likely to have been "exacerbated by several cyber attacks in the US in late October 2016 that caused major issues for users of internet services, including Twitter and Spotify".

The two popular internet services were victims of distributed denial of service (DDoS) attacks on Dyn, the DNS service provider that they and other internet companies rely on to resolve their domain names to IP addresses.

In this e-guide

The source of the attacks was traced to networks of compromised IoT devices, such as baby monitors, thrusting IoT security into the spotlight.

Responding to concerns over IoT security at a Seagate IoT event in Singapore, Hugh Ujhazy, IDC Asia-Pacific's associate vice-president of IoT and telecoms, highlighted the need to put in place multiple layers of security to ensure a level of trust in IoT systems.

"We're reintroducing concepts of physical security at the end-points – you could use accelerometers, so if the devices have been moved from where they are supposed to be, you know something is wrong," said Ujhazy.

Ujhazy said organisations can also encrypt data at-rest and in-transit, as well as constantly profile the connection between an IoT device and its gateway to pick up any anomalies, such as the volume of data transmitted.

"A connected water bottle shouldn't be giving me 25MB of data – it should only give me 200 bytes," he said.

Tobias Puehse, vice-president of innovation management, digital payments and labs at Mastercard Asia-Pacific, noted that tokenisation services, which create tokens to enable specific uses and transactions, can also play a part in bolstering IoT security.

"Tokenisation is already used in payment services such as Apple Pay, Samsung Pay and Android Pay," he said, adding that tokens, along with

tokenisation standards, will help to secure IoT devices, which have a higher chance of being compromised as compared with networks.

Kwong Dim-Lee, executive director at the Institute for Infocomm Research, an organisation under Singapore's Agency for Science, Technology and Research (A*Star), said a multi-layer approach to IoT security is here to stay until quantum technology, which can provide higher levels of security than what is available today, becomes more widespread.
Ujhazy noted that the while IoT security remains an ongoing discussion in the industry, one thing is clear – that is, "the old moat and castle wall defence is not going to work".

Quocirca analyst and director Bob Tarzey recently wrote in Computer Weekly about the need to orchestrate between different IT security tools to fend off sophisticated threats.

"Such orchestration enables the enforcement of unified network security policy addressing both traditional and IoT devices. Security information and event management and/or operational intelligence tools have a role to play here," he wrote.

With the rise in the number of IoT devices, technology research firm Gartner expects more than 25% of cyber attacks on enterprises will involve IoT by 2020. That said, IoT will account for less than 10% of IT security budgets.

Specifically in Southeast Asia, organisations are generally not prioritising IoT security due to internal security cultures and the prevalence of ad-hoc security systems.

"Security suppliers will be challenged to provide usable IoT security features because of the limited assigned budgets for IoT and the decentralised approach to early IoT implementations in organisations," Gartner said.

Next article

In this e-guide

Getting more CW+ exclusive content

As a CW+ member, you have access to TechTarget's entire portfolio of 120+ websites. CW+ access directs you to previously unavailable "platinum members-only resources" that are guaranteed to save you the time and effort of having to track such premium content down on your own, ultimately helping you to solve your toughest IT challenges more effectively – and faster – than ever before.

Take full advantage of your membership by visiting www.computerweekly.com/eproducts

Images; Fotalia