Eric Eifert, Paul Lawson and **Robert Statica** outline the key trends driving developments over the next couple of years.

CYBER SECURITY FUTURE TRENDS

The exponential growth of ICT integration with all aspects of our economies, governance and personal lives means that cyber security is likely to remain crucial to the resilience of the global economy in the next decade. Expect to see the number of successful attacks rising in the years ahead, and for their speed, sophistication and real-world impact to increase. Consumers will have to get smart about protecting an expanding range of smart everyday appliances, while cyber security experts will need to use their creativity to get ahead of the threat curve.

Over the past few years we have witnessed a paradigm shift in cyber crime: attacks have migrated from attacks for fame to attacks for gain and are moving towards attacks for pain. Increasingly, industrial control systems are linked to the wider internet, while this has increased efficiency, enabled the collection and analysis of performance data and allowed remote maintenance; it has also left systems vulnerable to malicious interference. Control system targeted attacks were once only within the capabilities of sophisticated intelligence services; famously Stuxnet, generally thought to be the product of nation state cyber co-operation, targeted computers that controlled centrifuges in their nuclear enrichment programme, subtly altering their rotation speeds to hamper the process. However as more and more control systems become linked with the wider internet we could see the rise of cyber mercenaries offering hacking-as-a-service (HAAS) to the highest bidder and the use of cyber attacks against critical computer infrastructures in target countries in support of terrorism, hacktivism, espionage, cyber crime and cyber war.

Attacks on critical infrastructure including gas and oil distribution systems, power grid, financial markets, air traffic controllers' networks, nuclear power plants and satellites represent a clear and present danger to the most advanced economies and countries in the world, potentially destabilising a recovering global economy. For example, in Ukraine 80,000 customers were left without electricity in mid-winter after a focused cyber-attack disabled a portion of the power grid. The nations of the Gulf Cooperation Council (GCC) face the reverse of Ukraine's environmental challenge; large populations live in desert environments that could in pre-industrial times support only a fraction of the number of people. An attack on oil installations or desalination facilities could pose not just a threat to the economy, but also a threat to the lives of millions of people.

Two factors are likely to see a growing number of companies taking advantage of cloud-based technology; the lacklustre performance of the global economy will continue to force organisations to tighten their budgets, at the same time as improvements in bandwidth allow companies to outsource core functions, such as email, to the cloud. Ultimately internal IT departments will feel the pressure to justify their privileged in-house position against competition from cheaper and often more skilled external service providers. An escalating

©Getty Images

number of organisations will take advantage of cloud-based services, which offer fast and scalable solutions for processing and data storage.

In the medium term this trend will also be exacerbated by the failure of Moore's law; the assumption that the processing power of computers will double every two years as smaller transistors are packed into computers. As this law reaches its physical limits, increased processing power will be contained not in the device itself, be that a smartphone or a PC, but in the cloud and the server farms that support it.

This consolidation of processing power creates a very attractive target for hackers who will endeavour to gain access to cloud services used by governments and enterprise, potentially holding their data for ransom. Ransomware attacks, often combined with shrewd social engineering, will likely skyrocket.

The hyper-connectivity associated with the Internet of Things (IoT) is increasing functionality, manageability and convenience for the consumer. In the next decade we are likely to see many private homes in advanced economies linking everything from air conditioning, water systems, and coffee machines to the web, allowing citizens to control their house temperature prior to returning home, or have coffee brewing in the morning before rising. One theory is that central processing power for the household may be housed in the refrigerator; the one item in the house that is always plugged into the electricity grid, sufficiently spacious to hide the odd circuit board and cold enough to prevent overheating of the computing equipment.

Computer hackers test their hacking skills at the final rounds of the SECCON Security Contest

However, unlike older hardware, many IoT devices have minimum or no security and yet are embedded in the home, collecting a wealth of the owners' personal identifiable information (PII). This is particularly true of home security systems, which, if compromised could be used against their owners leading to identify theft, exploitation or extortion.

Most, although not all, users have become used to installing and updating anti-virus software on their PC or laptop. They are soon going to have to adjust to a world where they will need to update similar patches on their fridge.

As the speed, frequency and complexity of malware attacks increases, passive defence is no longer sufficient. Security Operation Centres (SOCs), centralised hubs where experts are able to monitor the security status of multiple organisations, are moving from a reactive defensive posture to a more proactive protection posture. This proactive posture will leverage machine learning capabilities and security orchestration to facilitate automated remediation and mitigation to prevent security incidents from escalating.

SOCs will no longer just focus on traditional detection and response services, but will become active participants in vulnerability management identifying and mitigating vulnerabilities before they can be exploited. This is essential as the speed of modern malware attacks means that once a compromise has been detected, the damage has often already been done. SOCs will start to build cyber hunt teams, often comprising former 'black hat' hackers who have turned from poacher to game keeper, who will proactively search for indicators of compromise. SOCs will likely expand their range of services, leveraging their 24/7/365 operational environment, to provide further round-the-clock capabilities including: insider threat monitoring, data loss prevention, vulnerability management, continuous monitoring, and governance, risk, and compliance.

Big Data is here to stay and so are the accompanying analytics; both play their part in analysing highly sophisticated cyber attacks. Predictive analytics has been around for a while

©Getty Images

A man using a smartphone with an app that uses biometric authentication for secure online payments

solving complex marketing and other business-related problems. Analytics have already been used to identify conventional crime hotspots, allowing officers to divert patrols to target both areas and times of day when crimes are most likely to occur, based on analysis of historic patterns. Big data will be enriched by diverse cyber threat intelligence obtained through commercial providers, government sources, research and academic institutes, and industry sharing programs. 2016 will see greater use of predictive models in the field of cyber security; these will help predict when an attack might occur using known attack vectors, establish the origin of the attack and identify its key aims.

Not all cyber security problems going forward will be high tech; the demand for skilled cyber security professionals will increase, but finding these skill sets in the marketplace will be difficult. Too few graduates worldwide are specialising in the harder STEM (Science, Technology, Engineering and Mathematics) disciplines that provide the foundation for the cyber economy. This is particularly true in the GCC, where the public sector still provides a powerful lure to gifted graduates. There is a high demand for top talent that understand security architectures, technologies, Security and Information Event Management (SIEM) systems and correlation, forensics, event management and now, with analytics in the mix, pattern analysis across large, diverse datasets. This is a troubling situation; companies will need to put serious efforts into training, development and retention incentives if they want to keep ahead of the curve. In particular they will need to make real efforts to distinguish themselves from the competition, and not just in the obvious area of remuneration; millennials are increasingly interested in the opportunity to make a real and lasting impact on their sector, not simply a secure pay cheque and the promise of a pension. As well as attracting talent, companies will need to invest in developing the skills of their staff; cyber academies and cyber labs allow professionals to acquire the experience of handling real-world threats, but in a controlled environment where the impact of errors is limited to embarrassment.

All of the aforementioned challenges, are aspects of a single development; the increasing integration of the cyber world with everyday life. If your fridge contains more processing power than to seventies supercomputer, we can no longer view cyber security as simply a niche activity of interest only to intelligence services and the IT departments of multi-nationals. Over the next decade, cyber security is going to become everyone's problem, and unlike traditional security functions provided by the state, maintaining cyber safety has to be devolved to the level of the individual. There are simply too many servers connected to the web to entrust cyber security solely to state enforcement bodies. This is not a counsel for despair, but a call to raise awareness and educate the population about their responsibilities in keeping themselves safe from attack. It's going to be a challenging time ahead, but with the right planning, commitment to innovation and sensible practices, nations and companies can mitigate, if not completely prevent, cyber security attacks.

Cyber security is not a project. It is a science, an art and a lifestyle. But it has a starting point. Companies and governments must get to that starting point before it is too late. Only those who adapt fast to the ever-changing threats of cyber security will be able to save their data and operations from becoming cyber prey.

Eric Eifert is the senior vice president of managed security services at DarkMatter, **Paul Lawson** is the vice president of infrastructure and system integration and **Robert Statica** is the senior vice president of technology and research.