Increasingly, organisations will want to protect IoT-type devices where, again, it may not be practical or possible to install a software agent. Think about a custom medical device, or network-attached machine tool, or even facilities technologies like heating, ventilation and air conditioning (HVAC) controllers, or even an Internet-aware television. Vulnerable? Potentially yes. Innovative? Potentially yes. Desirable? Well, it would be nice to find out, rather than hear a flat 'No, we can't allow that on the network' from the security team.

"The more we help IT organisations to focus on their business and developing innovation for their businesses instead of trying to fight cybercrime or cyberthreats, the better," says Ziften's Roark. Indeed, the default answer to the 'May I connect this thing to the network?' should become 'yes' – because organisations can now deploy technology that will manage that risk.

Wedge's Weiner explains: "If you can get really confident that you're going to block the vast majority of threats, then suddenly you're free to start using the Internet of Things more pervasively and enable BYOD policies where people are bringing technology from home. Even within the enterprise, when an IT group wants to try something – and even if new and even artificial intelligence-based endpoint protection might not be available for that device – we can still feel comfortable bringing it in if we have a reliable level of network security."

Forget 'Lock it down! Button it up tight!'. Let's open up and allow innovation, productivity and competitiveness to flourish in a safe, controlled environment.

About the author

Alan Zeichick is president and principal analyst at Camden Associates, a bespoke analyst firm in Phoenix, Arizona that focuses on enterprise IT. His background includes consulting to the IT industry, as well as creating and hosting many conferences and trade shows since the 1980s. As an editor and publisher, Zeichick served as editor-in-chief of LAN Magazine *and was the founding editor of* Network Magazine, *which later merged with CMP's* Network Computing. *He also founded BZ Media's* SD Times, *a publication for software development managers. Today, Zeichick is a regular contributor to* Network World *and other online publications.*

Artificial intelligence – the next frontier in IT security?

Rohit Talwar and April Koury, Fast Future

Security has always been an arms race between attacker and defender. He starts a war with a stick, you get a spear; he counters with a musket, you upgrade to a cannon; he develops a tank, you split the atom. While the consequences of organisational cyber-security breaches may not be as earth-shatteringly dramatic today, the arms race of centuries ago continues into the digital sphere of today.

The next challenge for companies with an eye towards the future should be to recognise that artificial intelligence (AI) is already entering the scene – with tools such as PatternEx focused on spotting cyber-attacks and Feedzai for fraud detection across the e-commerce value chain. The technology is developing so rapidly that it is too early to say whether the impact will be revolutionary or just the next evolution.

Artificial intelligence

Some AI evangelists argue that this new technological force could render all others seemingly irrelevant, given the scale of change, risk and opportunity it could bring about in IT security. This new dark art offering seemingly magical technological wizardry does indeed have the potential to change our world and – depending on who you choose to believe – either make life a little better, lead to total societal transformation or end humanity itself.

Artificial intelligence has the potential to disrupt all industry sectors – it is a field of computer science focused on creating intelligent software tools that replicate critical human mental faculties. The range of applications includes speech recognition, language translation, visual perception, learning, reasoning, inference, strategising, planning, decision-making and intuition.

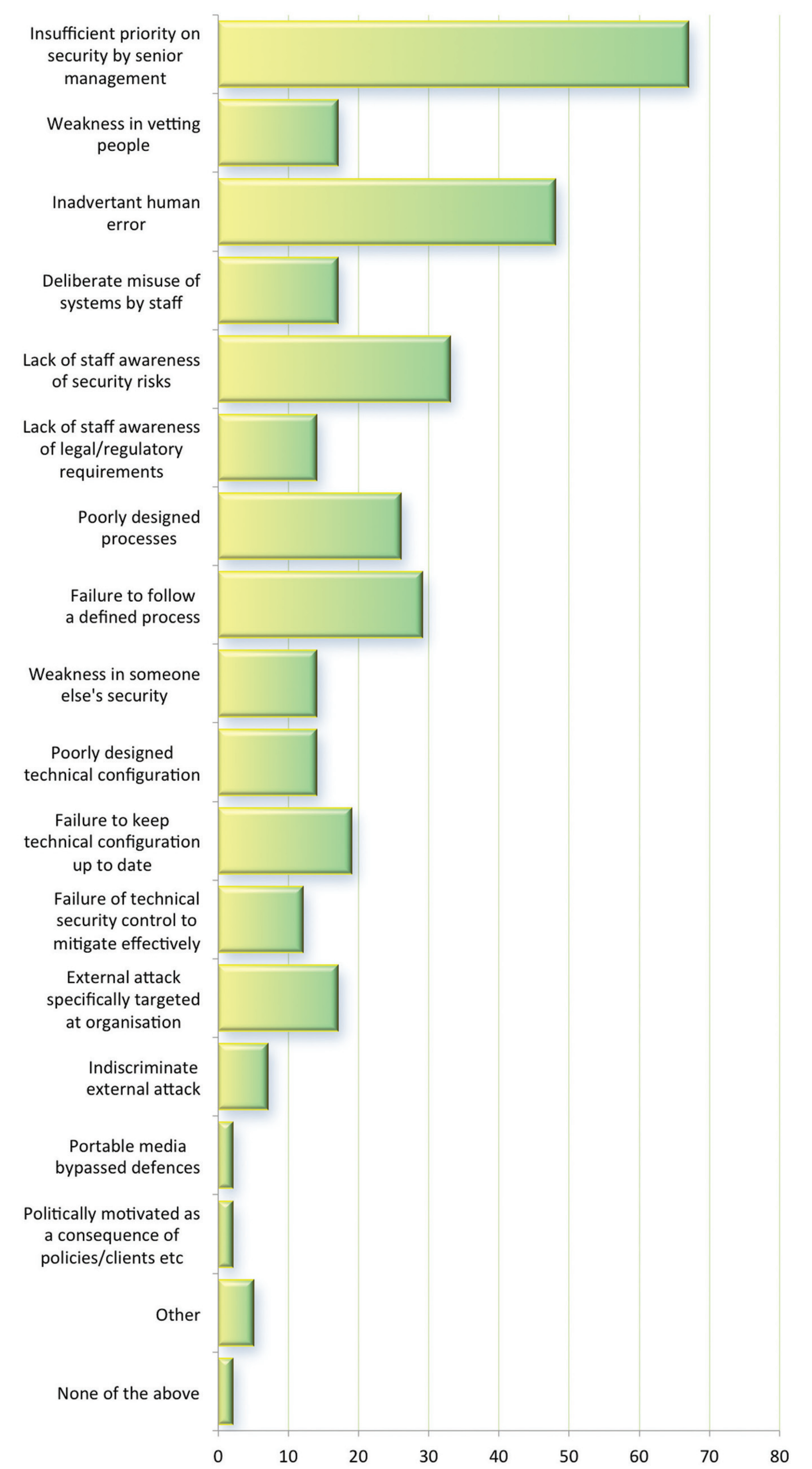
As a result of a new generation of disruptive technologies and AI we are entering a fourth industrial revolution. The three previous revolutions gave us steam-based mechanisation, electrification and mass production, then electronics, information technology and automation. This new fourth era, with its smart machines, is fuelled by exponential improvement and the convergence of multiple scientific and technological fields such as big data, AI, the Internet of Things (IoT), super-computing hardware, hyperconnectivity, cloud computing, digital currencies, blockchain distributed ledger systems and mobile computing. The medium to long-term outcomes of these converging exponential technologies for individuals, society, business, government and IT security are far from clear.

The pace of AI development is accelerating and is astounding even those in the sector. In March 2016, Google DeepMind's AlphaGo system beat the world Go champion, demonstrating the speed of development taking place in machine learning – a core AI technology. The board game Go has over 560 million possible moves – you cannot teach the system all the rules and permutations. Instead, AlphaGo was equipped with a machine learning algorithm that enabled it to deduce the rules and possible moves from observing thousands of games. This same technology can now be used in IT security in applications ranging from external threat detection and prevention to spotting the precursors of potentially illegal behaviour among employees.

Current state of security

In 2015 in the US, the Identity Theft Resource Centre noted that almost 180 million personal records were exposed to data breaches and a PwC survey report highlighted that 79% of responding US organisations had experienced at least one security incident.[1,2] Industry research indicates that while hackers exploit vulnerabilities within minutes of their becoming known, companies take roughly 146 days to fix critical vulnerabilities. With the average cost of a data breach estimated at $4m, there is growing concern over how companies can keep up with the constant onslaught of ever stealthier, faster and malicious attacks today and in the future.

As it stands, many firms focus more on reacting to security breaches than on preventing them and the current approach to network security is often aimed more at standards compliance than at detecting new and evolving threats. The result is an unwinnable game of whack-a-mole that could overwhelm companies in the future unless they are willing to adopt and adapt the mindset, technology and techniques used by the hackers. And there is very little doubt that hackers are – or soon will be – developing AI tools to increase the frequency, scale, breadth and sophistication of their attacks.



Factors that led to security incidents. Source: PwC 2015 Information Security Breaches Survey.

Organisations in this digital age create infinite amounts of data, both internally through their own processes and externally via customers, suppliers and partners. No one human is capable of analysing all that data to monitor for potential security breaches – our systems have simply become too widespread, data-laden and unwieldy. However, when combined with big data management tools, AI is becoming ever more effective at crunching vast amounts of data and picking out patterns and anomalies. In fact, with most AI systems, the more information they are fed, the smarter they become.