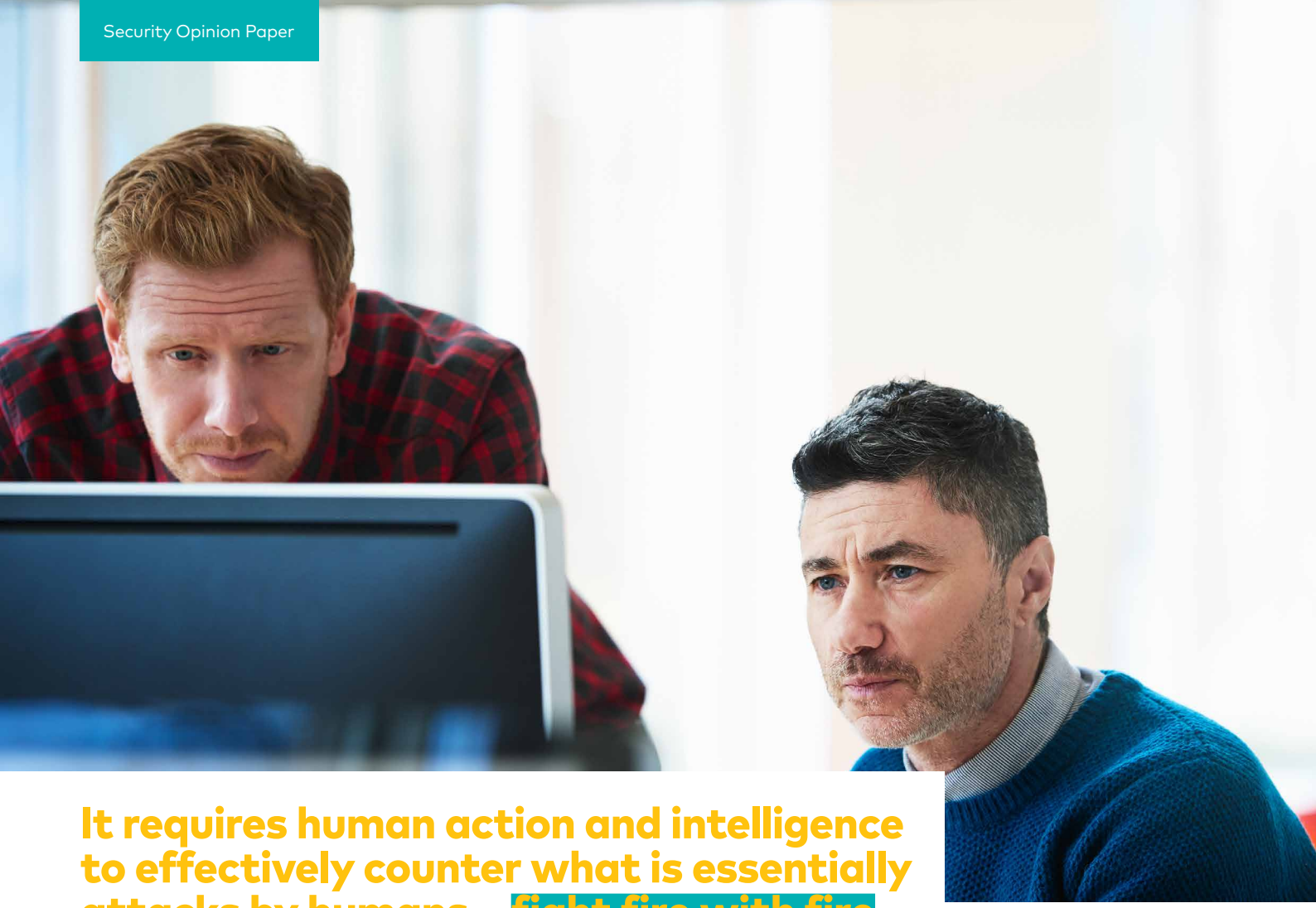
Security Opinion Paper

On guard

Constant vigilance by experts – not just systems – is needed to protect your enterprise from new advanced security threats

Yes

OPTUS



It requires human action and intelligence to effectively counter what is essentially attacks by humans – fight fire with fire

By Andrew Stephanou,
Director of Optus Business' Security Centre of Excellence

The days of relying on technology to protect business networks and data are over. Human ingenuity and skilled capability are now vital in protecting against many of today's new and emerging security threats.

Traditional solutions are still important to detect, block and remove known malware and random attacks, but protecting against unknown and targeted threats requires a combination of the latest technology, security intelligence and analytics, incidence response capability, and specialists with an extremely high level of expertise.

The fact is most organisations don't have – and could never have – the expertise or resources to protect against new advanced threats. This is why many organisations are turning to specialist managed security services providers.

The risks

The consequences of not adequately protecting your organisation are becoming more dire. It's no longer just about securing your networks and devices, or minimising downtime and lost productivity. It's about protecting your customers' personal information, sensitive data and your company's reputation.

The hacking of Sony opened our eyes to threats by showing us that even exposing internal emails can damage an organisation's reputation.[1] It was just one of a long line of corporate breaches that have impacted major corporations such as eBay, Apple, US retailer Target and JP Morgan. More recently we have seen well publicised hacks on Ashley Madison, and the cyber heist on Bangladesh Bank which netted hackers more than $80 million before it was uncovered[2]– not to mention the thousands of breaches that go unreported or even undetected.

Industrial espionage is another danger. Mandiant – the services division of security specialist company FireEye – reports it has definitive evidence that Chinese hackers have stolen secrets from Australian companies.[3]

In the US, health insurance giant Anthem had data on as many as 80 million customers stolen by hackers in a cyberattack investigators have reportedly linked to China[4]. This cyberattack is just one that exposed personal information on millions of people in the United States, triggering calls for companies to beef up their data defences.

The truth is effective enterprise security has always been about people, processes and technology, although many organisations have come to rely heavily on the technology component. It's perhaps an understandable trend as security is a non-productive resource that doesn't increase revenue or reduce costs. But what price would you place on the reputation of your business?

How would your bottom line be affected if you lost your customers' trust?

Then there are the expanding compliance and governance risks, with rules such as Australia's 2014 privacy law reforms[5] that increase the penalties for breaches.

The new threats

Despite continuous advances over many years, traditional security solutions are no longer enough to fight today's more sophisticated threats, though they do still play an important role in an organisation's security posture and layers of defence. A recent FireEye study found in real-world tests of 1,214 security deployments around the globe, that more than 96 percent of systems were breached over a six-month period.[6] That means attacks had broken through or slipped past every point product in these deployments because most traditional point products were built for yesterday's simpler threats. And application vulnerability is not helping – a Trustwave global security report found that 98 percent of applications tested had one or more security vulnerabilities.[7]

The tools required to mount advanced attacks are getting easier to use, while the rewards are greater as both consumers and organisations embrace e-commerce and other online transactions. The shadowy world of hackers has morphed into a booming industry of cybercriminals who

are far more organised, better funded and more effective than ever before. The location and motives of the attackers, year on year, are becoming more diverse.[8]

The variety of threats is also expanding: viruses, worms, spyware, distributed denial of service (DDoS) attacks, hacktivism, Structured Query Language injections (SQLi), ransomware and zero-day attacks – just to name a few. They're all potentially very damaging but perhaps the most insidious is the new breed of advanced persistent threats (APTs). Aimed at infiltrating and melding into organisations normal business activities and remain permanently undetected – thus becoming part of the organisation.

How APTs work

APTs are highly sophisticated, very difficult to identify and have two key characteristics. They are:

1. **highly targeted** – often aimed at one organisation
2. **persistent** – with a series of attacks executed over an extended period of time to gain expert knowledge and understanding of an organisation or industry.

Because APTs typically employ highly targeted malware and intrusion techniques, they're unlikely to be detected by traditional signature-based solutions. Even if they are detected, the perpetrators follow up with additional attacks until they achieve their aim – to infiltrate the organisation.

The ultimate purpose varies from hurting an organisation's reputation by exposing sensitive information to gaining a competitive advantage through industrial espionage. While their goals may differ, the tactics of APT perpetrators are often similar: to subtly but continually probe an organisation with targeted attacks until they gain privileged network access. And then they can blend into the organisation, assign themselves user accounts and quietly collect data.

It doesn't matter if data is located in the cloud or a secure on-premises facility; once the perpetrators have privileged network access, they have data access.

It can be very difficult to detect an APT infiltration. The breach can last for months or even years. A recent Mandiant study revealed that attackers were present on victim networks for a median of 146 days before being discovered[8]. While this has been falling year on year, it is still too long considering the damage an attacker can do in a matter of days after gaining access to an environment.

Fighting advanced threats

The typical modern enterprise has a conventional security arsenal that includes antivirus scanners, firewalls, intrusion prevention systems, sandboxes and endpoint protection solutions. They're battling on an ever-expanding front as the rapid adoption of mobile devices has shifted the perimeter well beyond the traditional corporate network.

However, as we've seen, enterprises face a significant risk of being breached unless they take a smarter, more holistic approach that comprises the right people as well as technology. It requires human action and intelligence to effectively counter what is essentially attacks by humans – fight fire with fire. We recommend organisations' consider:

- **An effective but well-balanced suite of technology solutions.** While conventional security systems are still important, it may be worth conducting a detailed IT assessment to identify potential overspending on solutions that are ineffective against targeted threats. Consider replacing redundant legacy technology with more effective or better-value alternatives.
- **Intelligence and analytics.** Only security specialists have the expertise and resources to keep track of the latest global threats and techniques used by cybercriminals. This intelligence, in combination with analytics, provides security teams with the network visibility they need to quickly identify and act on threats.
- **Incident response capability.** Identifying threats is only the first step. Organisations also need the tools, processes and people to rapidly respond to threats and incursions, and recover from major incidents.
- **Expertise.** At the very least, every organisation should conduct comprehensive risk assessments, but for enterprises that place a high value on security, we suggest hiring specialists, either your own or by working with a managed security services specialist, with the expertise to constantly monitor networks, analyse events and intelligence, identify advanced threats and lead incident response teams.

The need for high visibility

The days of do-it-yourself IT security appear to be numbered. Increasingly, for many organisations, the only feasible way to deploy a comprehensive and effective security solution is to outsource to a specialist managed security service provider (MSSP). Such a service should be completely transparent so that everyone from IT managers to board members understands how their organisation is being protected and always knows the current status of their organisation's security.

MSSPs can bring global security experience, technologies and services covering threat management, vulnerability management, penetration testing and compliance management. This expertise can help protect an organisation's brand and reputation with security services that pre-emptively identify advanced security threats and events before they can cause damage and disruption.

After all, as the Sony hack and other high-profile incidents show, IT security is no longer just an issue for the techies in the back office.

CONTINUE THE CONVERSATION WITH ANDREW
yesopt.us/andrewstephanou

1. '13 revelations from the Sony hack', CNet, 14 December 2014, http://www.cnet.com/au/news/13-revelations-from-the-sony-hack/.
2. Malware Suspected in Bangladesh Bank Heist, 12 March 2016, http://fortune.com/2016/03/12/malware-bangladesh-bank-heist/
3. China ramps up spying on Australian business', Australian Financial Review, 14 October 2014, http://www.afr.com/p/special_reports/opportunityasia/china_ramps_up_spying_on_australian_RAWfIGZ4USnF8RHWsbnA8K.
4. Giant Anthem health data breach could lead to China, 6 February 2015, http://www.businessinsider.com.au/afp-giant-us-health-data-breach-could-lead-to-china-2015-2
5. Office of the Australian Information Commissioner, http://www.oaic.gov.au/privacy/privacy-act/privacy-law-reform.
6. FireEye. "Maginot Revisited: More Real-World Results from Real-World Tests." January 2015, https://www2.fireeye.com/WEB-2015RPTMaginotRevisited.html
7. 2015 Trustwave Global Security Report, https://www2.trustwave.com/rs/815-RFM-693/images/2015_TrustwaveGlobalSecurityReport.pdf
8. M-Trends 2016 – Special Report February 2016 (Madiant Consulting – A FireEye Company), https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf

Give us a call

To discuss how Optus can help you through advanced security solutions; **contact your Optus Account Manager or call the Optus Business hotline on 1800 555 937**

Join the conversation

1800 555 937 optus.com.au/business

@optusbusiness yesopt.us/blog

OPTUS

GMO_N337 0516 KIT