CROWDSTRIKE

itnews
FOR AUSTRALIAN BUSINESS

Business leaders assume endpoint security is in place – but IT leaders know it isn't

Executives uncertain about cybersecurity exposure, over-optimistic about technology adoption

Australian business leaders know much less about their companies' cybersecurity protections than they think they do, according to new CrowdStrike-iTnews research that found more than 50 percent of businesses cannot definitively say whether they have been breached or not.

Respondents to the iTnews Security Breach Report sponsored by CrowdStrike, conducted in late 2016 amongst 168 IT and business decision-makers at Australian businesses and government organisations with 250 or more employees, were generally optimistic about their level of cybersecurity protection. For example,69.8 percent of the respondents were confident that their organisation could identify and contain a cyber attack, while just 11.2 percent admitted they were not confident of doing so.

Although their confidence was high, many respondents were poorly informed about their company's actual cybersecurity experiences. Many couldn't say with certainty whether their company had actually had to deal with a breach during 2015 and 2016: some 30 percent said they didn't think they had been breached, while just 20.4 percent were totally confident that they had not been breached. In other words, 4 out of 5 respondents either had been breached, or couldn't say definitively that they had not.

Business leaders were much less certain about their cybersecurity vulnerabilities than IT staff, with 11.4 percent of business leaders and just 3.7 percent of IT leaders admitting they didn't know whether they had been breached. IT staff were also more likely to state definitively that they had not been breached (30.4 percent) than business leaders (22.7 percent) – suggesting that they had access to tools providing better visibility of cybersecurity activities than the business leaders.

Similar disparities were evident in comparing sentiments about malware-free intrusions such as insider compromise: just 56.8 percent of business leaders said their organisations were concerned about malware-free intrusions, far less than the 68.2 percent of IT leaders who said the same. And while 31.8 percent of business leaders admitted they didn't know whether their organisations were concerned about such compromise, only 17.8 percent of IT staff didn't know.

The figures suggest that the often-recognised gap between business and IT perceptions remains strong within Australian companies. IT leaders were generally more able than business leaders to say, with confidence, whether they had or had not been compromised by external attacks and whether they should be concerned about specific types of attacks. Business leaders were less confident and more likely to say that they didn't know what had happened.

Such a wide gap in perception and understanding highlights the need for IT executives to better engage and educate business leaders about deficiencies in current methods of IT security practice, according to CrowdStrike vice president of technology strategy Mike Sentonas, who said the results also highlighted the ongoing challenges in communicating technology-related messages to business leaders.

"Everybody is using some kind of security product across the network but many organisations don't realise that their existing investments in security products just aren't up to the task until it is too late," Sentonas said. "Statistics show that data breaches in 2016 resulted in over 4 billion files exposed. Clearly something is not right, and the answer is not throwing more money at what is not working."

The lack of understanding around cybersecurity issues poses challenges for efforts to tighten the security and control of an expanding range of endpoint devices

The lack of understanding around cybersecurity issues – particularly within businesses that spent much of 2016 trying to fend off an ever-increasing wave of attacks – poses challenges for efforts to tighten the security and control of an expanding range of endpoint devices that increasingly includes not just traditional desktops and mobile devices, but Internet of Things (IoT) sensors and other networked devices.

Even as businesses work to tighten their network protection, hackers are continuing to ravage those that remain unprotected: recently, for example, hackers managed to steal http://www.itnews.com.au/news/hackers-steal-42m-from-russian-central-bank-443388 from a compromised Russian bank as well as $US81m ($A111m) from Bangladesh's central bank. Such attacks have become so persistent that payments clearinghouse SWIFT was last year forced to warn http://www.itnews.com.au/news/swift-confirms-new-cyber-thefts-hacking-tactics-444504 of "persistent, adaptive and sophisticated" attacks that had stolen customer funds in around a fifth of instances.

The explosion of attacks with real-world business consequences has kicked industry into action, with many business organisations joining forces with IT groups to drive secure coding techniques deep into the organisation. Macquarie Group, for one, has pushed hard to embrace Secure DevOps (SecDevOps) capabilities http://www.itnews.com.au/news/macquarie-group-to-adopt-secdevops-442817 that link security with operational and development processes. Similarly, Telstra recently created an internal development group http://www.itnews.com.au/news/telstras-new-infosec-cops-will-police-all-dev-code-442302 dedicated to securing all internally developed software. These pioneers are likely to be followed by more and more of their peers as the need for end-to-end security becomes a recognised business imperative.

FROM PERIMETER TO ENDPOINT

Early detection and mitigation of breaches is critical if companies are to have any hope of managing their cybersecurity exposure. In recognition of the potential business consequences of cybersecurity breaches, many companies are bolstering their next-generation antivirus and endpoint detection and response (EDR) capabilities.

Some 31.5 percent of respondents to the CrowdStrike-iTnews survey said they were planning projects to implement EDR technology, which increasingly draws on cloud-based security platforms to provide consistent, policy-based management of devices and the cybersecurity threats they face.

As with other technologies, there was a yawning gap in understanding around the state of EDR projects: while just 23.7 percent of IT executives didn't know whether an EDR project was underway, nearly twice as many business respondents – 45.5 percent – didn't know.

Although similar proportions of business and IT leaders could say definitively that their company was undergoing an EDR project, there was also a sizeable gap between the 43.7 percent of IT leaders who could definitively say they were not pursuing an EDR project – and the 25 percent of business leaders who could do the same.

The consequences of this finding are clear, says Sentonas – and worrying. "Business leaders assume that endpoint security is in place," he explains, "but IT leaders know that it isn't. The attacks keep coming, and so do the differences in perception that stop

business and IT from working more effectively together to stop them."

Respondents – many of whom had previously suffered cybersecurity attacks that had caused company downtime – cited a range of reasons for their increased investment. Many noted that traditional antivirus solutions were no match for modern threats and that contemporary solutions were better positioned to protect critical internal infrastructure.

One respondent pointed out the value of EDR solutions in protecting the company's clients, while others highlighted the vulnerabilities created by Wi-Fi and non-employee connectivity. EDR was noted for its ability to provide a consistent security footprint, while another respondent flagged the need for early detection to reduce the chance of infecting customer networks.

"The landscape never stops changing and vigilance is necessary," one IT manager noted.

"We want to make sure we have the right security across all devices, as well as the network," another said.

One property-related business flagged the importance of EDR tools in meeting security and compliance requirements across both office based and remote customer-site based staff. And another respondent said EDR would provide "that extra edge in protecting sensitive data".

Getting that edge is particularly important given the movement of the cyberattack focus outside of the organisational perimeter. "The traditional corporate boundary becomes irrelevant as attackers operate outside its boundaries," Sentonas says, noting the changing profile created by increasing adoption of cloud and mobile solutions.

"That means that endpoint security becomes critical, because users are working from wherever they are and they don't have the traditional armoury that's going to help them. In many cases, the endpoint is where the battle will be won or lost."

IT IS IN THE POST-MALWARE ERA – BUT IS THE BUSINESS?

Survey responses confirmed that Australian business and IT leaders all see a range of cybersecurity threats as posing immediate risks for the business.

Ransomware was the most frequently-cited security fear (named by 61.1 percent percent of respondents) but phishing attacks (54.3 percent), social engineering (43.2 percent), insider threats (43.8 percent), and DDoS attacks (28.4 percent) were also widely cited. Some 48.8 percent also voiced strong concern about malware.

Yet despite fears about conventional malware attacks, many organisations are also waking up to the additional risks posed by non-malware attacks – in which exploits use access credentials to infiltrate corporate resources using otherwise legitimate channels.

Non-malware attacks pose particular problems for many existing cybersecurity tools, which generally focus on malware and similar attacks but fail to consider the whole of the endpoint interaction – and how to protect it.

"If attackers come in a way that existing tools aren't used to, they can't deal with it," Sentonas says. "It doesn't matter whether you buy your latest and greatest firewall or sandbox; if someone has purchased a bunch of email addresses and passwords online and logs into your network, how would you be able to detect someone compromising your network using those – as compared to the legitimate user?"

"The traditional corporate boundary becomes irrelevant as attackers operate outside its boundaries," Sentonas says

Despite the massive damage they may cause, just 20.4 percent of respondents to the CrowdStrike-iTnews survey ranked non-malware intrusions among their biggest fears. Yet fully 68.5 percent said non-malware attacks were a concern – suggesting that while their dangers are appreciated, non-malware attacks have yet to build the brand awareness that ransomware, Trojans and other attacks already enjoy.

Interestingly, comparing business and IT attitudes towards non-malware attacks once again expose gaps in perception. IT staff were not only more concerned about non-malware attacks than business people (68.2 percent vs 56.8 percent) but they were far less likely to say they didn't know whether non-malware attacks were a concern (17.8 percent vs 31.8 percent).

The fact that more than 31 percent of business respondents didn't even know whether non-malware attacks were a concern, reflects the ongoing challenges organisations face in raising awareness of the risks

posed by outsider abuse of legitimate endpoints and access credentials.

It appears that many business leaders simply don't understand that there are many worse threats than malware – something of which other respondents were well aware. "It is a genuine concern in this industry," one government IT analyst noted.

Others called such attacks "subtle", warned that they "often open the doors for other malware", noted that they are "simple to perform and difficult to detect", and flagged the risk of loss of proprietary and confidential data to outside data mining efforts.

BAD INTELLIGENCE ON THREAT INTELLIGENCE. Effectively dealing with non-malware attacks requires a different approach to threat detection, which includes threat-intelligence systems that work on concert with tight endpoint security controls. Yet the same business-IT gap emerged when respondents were questioned about their organisations' use of threat intelligence tools.

Indeed, while 54.6 percent of business leaders said their organisation was definitely using threat intelligence, just 45 percent of IT leaders agreed. And while 25 percent of business leaders said they didn't know if their business was using threat intelligence, only 14.8 percent of IT leaders were unsure.

Instead, IT leaders were more than twice as likely than business leaders (39.3 percent vs 18.2 percent) to say definitively that their business was not using threat intelligence. This is likely because those IT leaders would be working at the coalface of threat intelligence efforts, so are in a better position to attest to its status.

These results both suggest that IT leaders may be well apprised of the maturity of threat intelligence efforts within the business, but that they may not have effectively communicated this to business leaders – who seem ready to assume, incorrectly, that their IT organisations are more prepared to deal with current threats than they actually are.

Such persistent attitudes threaten the integrity of corporate networks but they may also have other, more insidious effects. They may, for example, have direct implications on IT managers' ability to secure funding for such efforts – since business leaders may erroneously believe threat intelligence initiatives are already in place.

If IT leaders don't get better at communicating the true state of their security maturity to business leaders, those same IT leaders are likely to be in the firing line when something goes wrong.

"As much as the security industry likes to talk about this being a boardroom issue, the reality is that we're not there yet," says Sentonas. "The data from this CrowdStrike-iTnews survey backs up the contention that business and IT leaders need to think about the way they're connecting the two."

The implications of the survey results are clear: IT leaders must be aggressive in their pursuit of security improvements during 2017, working to close the perception gap with business leaders to ensure that their mutual interests aren't compromised by ever sneakier and more-effective cybercriminal attacks.

About CROWDSTRIKE

CrowdStrike is the leader in next-generation endpoint protection, threat intelligence and response services. CrowdStrike's core technology, the Falcon platform, stops breaches by preventing and responding to all types of attacks – both malware and malware-free.
CrowdStrike has revolutionized endpoint protection by combining three crucial elements: next-generation AV, endpoint detection and response (EDR), and a 24/7 managed hunting service — all powered by intelligence and uniquely delivered via the cloud in a single integrated solution. Falcon uses the patented CrowdStrike Threat Graph™ to analyze and correlate billions of events in real time, providing complete protection and five-second visibility across all endpoints.

Many of the world's largest organizations already put their trust in CrowdStrike, including three of the 10 largest global companies by revenue, five of the 10 largest financial institutions, three of the top 10 health care providers, and three of the top 10 energy companies. CrowdStrike Falcon is currently deployed in more than 170 countries.

We Stop Breaches. Learn more: **www.crowdstrike.com**

CROWDSTRIKE

CrowdStrike Australia Pty Ltd
Level 18, 141 Walker Street
North Sydney, NSW 2060
(+61) 1300 245 584
apac.sales@crowdstrike.com

About iTnews

This report was produced by the team at iTnews, Australia's most awarded technology publication for Australian business. In an age when the right information at the right time can make or break a deal, Australia's technology leaders rely on iTnews for their daily fix of accurate, up-to-the-minute news, analysis and research.

Information and communications technology is the engine room of the modern business. Business leaders tell us they rely on iTnews to inform their strategy, make business cases for technology investments, set policies and chart their careers. Collectively, the team at iTnews has won a swag of awards which include Technology Title of the Year, Best News Title, Best Editor, Best Business Journalist, Best News Journalist and Best Technical Journalist.

The iTnews team also curates technology conferences and judges the annual Benchmark Awards for excellence in ICT project delivery.

itnews FOR AUSTRALIAN BUSINESS

www.itnews.com.au