mimecast

WHITE PAPER

Australian companies leaving themselves exposed on security and compliance: survey

Half of firms won't be ready for data breach legislation and most are struggling to train staff to improve security practices.

Security managers already know first hand about the wide gulf between data-security best practices and employees' everyday behaviour. Yet a new survey confirms that most are doing very little to fix the situation: although IT managers report that 95 percent of security breaches happen because a manager has done the wrong thing, just 40 percent of companies report actively training staff to improve their cybersecurity practices.

Tony Duckmanton knows how hard effective staff cybersecurity training can be. As information services manager at industrial-supplies giant Coventry Group, he has been on the front line in the fight to improve the company's cybersecurity profile – which took a hit this year after a "pretty substantial" ransomware attack drove a period of review and security upgrades.

Staff training across the company's 70 branches was "fairly inconsistent and recognised as a big problem" in the past, Duckmanton says, and the mix of training videos, compliance tips and similar training only went so far in encouraging staff to be careful.

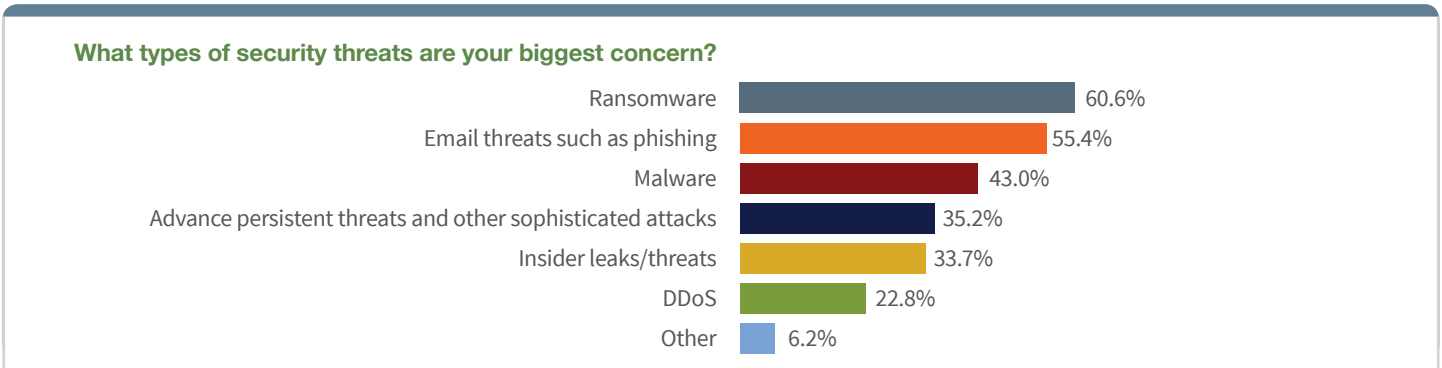
"These days it's difficult to see what is legitimate and what is not," he explains. "You can never push out enough training to staff, to be honest. Analysis of our incoming emails has subsequently shown that we are a highly-targeted organisation – so we need to be on our toes even more than usual."

Duckmanton's experience is typical of that conveyed by the 193 Australian IT decision-makers that participated in the Mimecast survey of iTnews readers. The survey revealed some surprising weaknesses in security practice, and found that nearly half of Australian companies aren't sure they will be ready to comply with new Notifiable Data Breach (NDB) legislation when it comes into effect in February 2018.

Reflecting the surge of recent serious ransomware outbreaks (WannaCry and NotPetya were headliners but far from the only major strains to cause damage) ransomware was the top security concern – cited by 60.6 percent of respondents. Talk to any group of security or IT managers and most will have a ransomware infection story to share.

Yet email threats such as phishing weren't far behind, named as a key concern by 55.4 percent of respondents. Malware was also named by 43 percent – although these three responses reflect several ways of saying the same thing, since malware and ransomware are usually distributed through scattershot or targeted phishing campaigns.

Interestingly, distributed denial of service (DDoS) attacks were a relatively low concern – named by just 22.8 percent of respondents – even though recently surging DDoS attacks have had significant impact. The sabotage of Australia's 2016 online Census was the highest-profile local example of this, but security-industry studies regularly show that DDoS attacks have become the new normal for organisations working to maintain business continuity.



Compliance concerns

The wide distribution of responses around NDB compliance suggests there are busy times ahead for Australia's Office of the Australian Information Commissioner (OAIC), which will be policing the legislation and is likely to be flooded with new breach reports as well as investigating unreported breaches that surface in other ways.

Just 17.6 percent of respondents said they were ready for the NDB legislation and confident that they can comply already, while 38.3 percent said they were confident they would be able to comply by the 23 February 2018 deadline.

This left 18.1 percent who admitted that "it'll be touch and go", 7.8 percent who were not confident of their compliance, and 18.1 percent who said they didn't know much about the legislation – which leaves no chance they will be able to get compliant within the first two months of the new year.

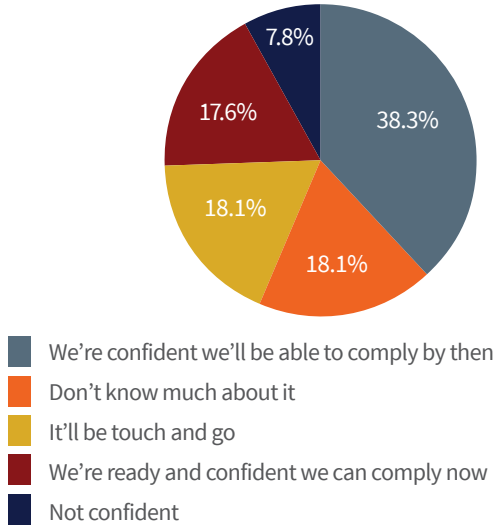
Companies failing to meet reporting obligations face significant fines from the Australian government, but the long-term damage can be even more significant as many customers will quickly abandon service providers that don't protect their personal data.

"Unless you have a program of work in place by now, you're going to struggle to get yourself compliant in time," warns Alison O'Hare, Technical Director consultant at Mimecast. "Everyone talks about the fines, which can be substantial – but it's what customers could do that should have most companies more worried than anything that's going to come from the government."

Respondents were prioritising investments in technology-based security, with tools such as data loss prevention (23.3 percent), machine learning (23.3 percent), end point protection (18.1 percent), ID management and access control (18.1 percent), and managed security service (17.6 percent) all on the priority list.

By contrast, fewer respondents were investing in solutions designed to improve overall resilience and recovery of data after an attack. Just 59.1 percent said they had disaster recovery measures in place while backup – which has been identified as potentially the only way to recover after many ransomware attacks – was in place at 80.8 percent of businesses.

How prepared is your organisation for the mandatory data breach notification laws when they are due to take effect?



Backup's prevalence may have contributed to its being named as an investment priority by just 8.3 percent of respondents – lower even than email archiving and e-discovery (13.5 percent) and disaster recovery (17.1 percent) – but with data distribution changing rapidly in the era of mobile and cloud platforms, even companies with established backup tools should be reviewing and updating them accordingly.

The relatively low priority of information-management solutions suggests either that companies are overconfident in their compliance status, or that they still lack understanding of what infrastructure elements are required to meet their compliance obligations.

Most are prioritising investment in technological solutions for detecting and dealing with security issues, rather than reviewing and reinforcing their policies for data protection and reinstatement. This could leave company data exposed once hackers work around their front-line protections.

Avoiding such breaches has been a continuous motivator for Jeremy Bree, CIO at building firm Henley Properties Group, who has been working through the implications of the NDB scheme as well as supporting his security work with continual education of the company's more than 600 staff.

Meeting breach-reporting requirements requires companies take "reasonable steps" to protect their data and much of Bree's work has revolved around defining the extent of the company's data, then defining what happens if it gets into the public domain.

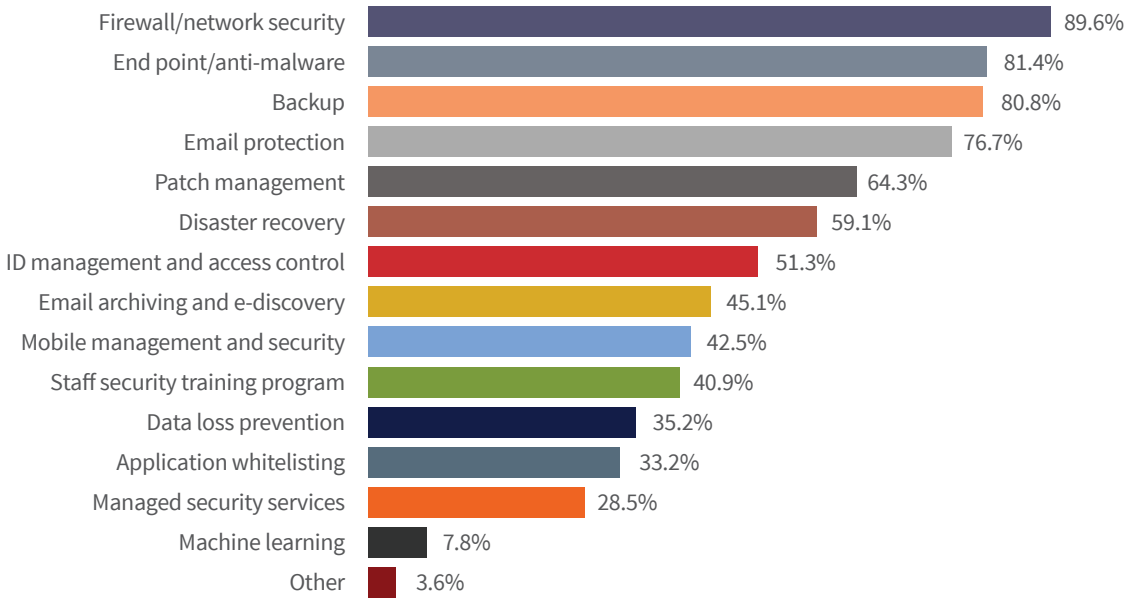
"The more data you collect, and the more impactful it is, the more emphasis you need to put into the security around it as well," he says. Many companies may only collect basic name and contact details but can easily forget that such data can be matched with data from other sources to help criminals profile potential targets for email phishing or other cybercrime.

Such threats have kept staff cybersecurity education at the top of Bree's priority list, with high-profile incidents like the WannaCry outbreak or recent Uber hack providing opportunities to remind staff of what's at stake from poor security habits.

"Not everyone has gone to university and studied digital security, but they're still expected to operate in this digital world," he says. "They may not understand that some seemingly innocuous task that they're doing, can have much bigger ramifications. So the educational piece is extremely important for both our users, to protect customers, and to protect themselves in the real world too."

"People in the office are inevitably already talking about these breaches," he continues, "so we are able to put a little education piece behind that. We can say 'don't blame us for being overprotective, because this is what we've just protected you from.'"

What security measures does your organisation currently have in place?



Targeting the Essential Eight

The survey identified a number of areas where Australian companies have fallen behind when it comes to data protection security compliance. In particular, many organisations still lack capabilities in the core areas advised by the Australian Signals Directorate's Top 4 and Essential Eight guidelines – which are widely accepted as best-practice information-security controls.

Patch management, for example, was only in place at 64.3 percent of companies while application whitelisting was being used by just 33.2 percent. Just 51.3 percent of respondents said they were using identity management and access control solutions – crucial for adoption of next-generation cloud architectures, and fundamental to Essential Eight recommendations to restrict administrative privileges.

By contrast, most organisations' current security protections are heavily skewed towards perimeter protections such as firewalls (used by 90 percent of respondents), endpoint and anti-malware protection (81.3 percent), and email protection (76.7 percent).

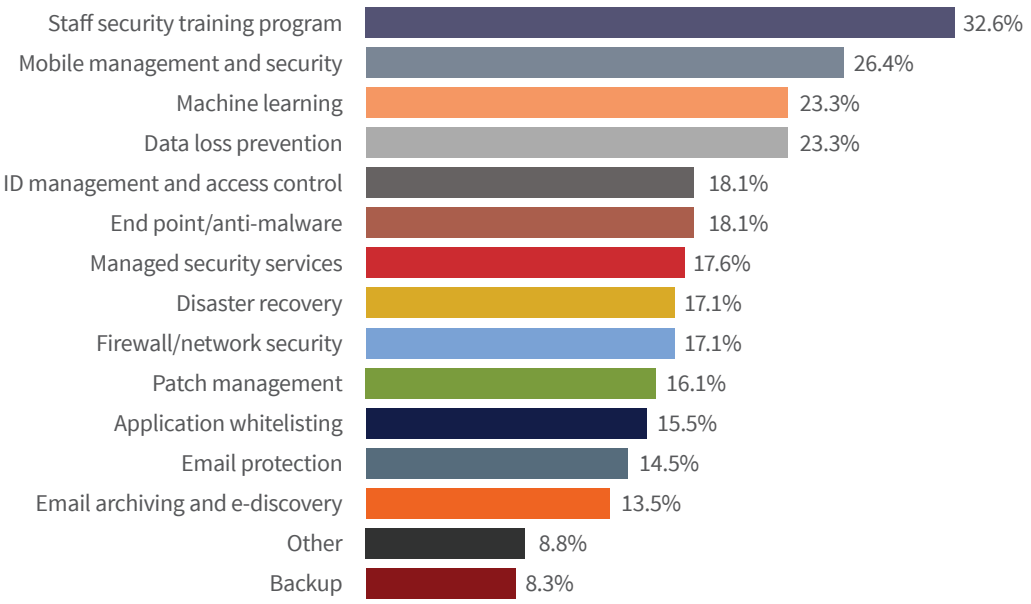
Many respondents seemed aware that they were focusing too much on infrastructure protection and not enough on data protection: asked what was the single most important thing they could do to improve the company's security posture, many cited a need for better application whitelisting, up-to-date systems, better security architectures, and building robust incident response strategies.

Mobile technologies were a particular soft spot: many users recognised that they needed to improve mobile management, which was installed at just 42.5 percent of companies but was the highest technological priority, cited by 26.4 percent more.

These results suggest that many companies are only now realising the full impact of the introduction of mobile technologies – and are racing to control it with new systems that can plug the many security gaps that poor mobile management introduces.

"One of the first things companies need to do is to figure out where their data lives," says O'Hare. "People are using apps for potentially very sensitive corporate data flowing through their devices, so it's surprising that mobile management hasn't moved further along given the potential for information to be stored on mobile devices."

What security measures is your organisation considering or planning to introduce (or refresh)?



The human challenge

While the survey identified a variety of technological soft spots that compromise Australian organisations' data protection, by far the most consistent message from respondents was that their staff security education is broken – and that they are struggling to fix it.

Just 40.9 percent of respondents said they currently had a staff security training program in place, with 32.6 percent saying they were considering or planning to introduce such training.

Asked to name the single most important thing they could do to improve security, more than half of respondents named staff education – but 42 percent said that staff education was their single biggest challenge when it comes to data security.

Freeform answers conveyed an overriding sense of frustration that messages about information security still aren't getting through to staff. Educating staff about security threats would "help them to protect themselves from themselves," one respondent wrote, while another noted that users are "the first and last line of defence."

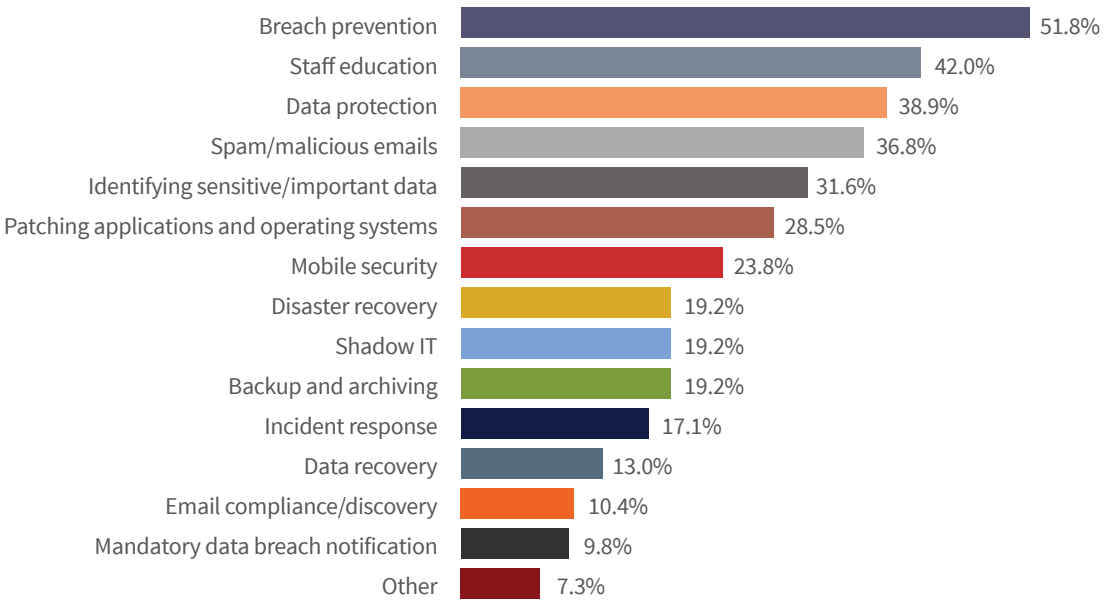
"Ninety percent of the times we have had a security breach has been through staff clicking on an email," one respondent noted, while another said staff are "the most obvious (and generally successful) attack vector.

"Complacency seems to be the one defining factor that lets us down each time," said yet another IT manager, while another noted that "most security threat comes from 'within' our organisation, ie from disgruntled employees."

A number of respondents highlighted specific groups of users that had proven particularly problematic: "staff turnover and independent contractors using corporate facilities make this an ongoing challenge," one IT manager noted.

Another reflected on the challenge of embedding security into the working culture of the organisation: the biggest challenge, he said, is "developing a rational security culture whilst not impeding on work styles."

What are your biggest challenges when it comes to data security?



Training priorities

Given these sentiments, it was understandable that staff security training was the most commonly-cited priority amongst respondents – 32.6 percent of whom said they were considering or planning to introduce a staff security training program.

Yet the details of such programs vary widely between organisations, with some relying on physical staff training sessions and others using technological controls such as URL filters – which intercept clicks on malicious email links. This approach provides detailed reporting on which users are most likely to click on malicious emails, and lets security administrators steer users through a range of educational interventions as soon as they take an action that potentially compromises security.

"You can't run a one-day security workshop and expect people to do the right thing from then on," O'Hare says.

"You need to post smaller reminders, that happen regularly, so that education becomes a social norm within the company. Every time someone clicks on a malicious link, that's an education opportunity."

Security education needed to be driven from across the organisation, with security staff often delivering too-technical training that disengages users and fails to convey the potential business impact of a security breach.

"Security people, by their nature, might not be the best people to write the communications that will win over the people on the front desk," O'Hare explains.

"That education piece needs to be done by people who understand messaging and education – but often the challenge comes because IT teams can see the requirement, but the culture and herd security awareness have to be driven from the top."

About the survey

This survey was conducted in October 2017 by iTnews on behalf of Mimecast, and attracted 193 respondents: 39.9% were CIOs, IT managers or equivalent, another 25.4% were IT professionals or workers, and the balance were business owners, executives or in other lines of business; 34.7% worked in large organisations (1000+) and the rest were fairly evenly spread across small and mid-sized businesses. The key sectors represented were the IT industry, education, financial services, healthcare, government and telecommunications.