Kamino Cyber Security Survey 2017

About this survey

This survey was conducted in October 2017 to gauge the financial services industry's sentiment when it comes to cyber security. These survey results are intended to be used for comparison against peers in the industry, as well as to open conversations and bring awareness to how advisers, brokers and accountants can better protect ourselves and our clients from the ever-increasing cyber threats.

A total of 69 completed the survey. The survey reached out to a very wide audience all over Australia, from metropolitan areas to country towns.

Introduction

Digital transformation has brought many benefits and efficiencies for advisers, accountants and superannuation funds, but technology also comes with new risks and threats that are often not thoroughly understood. Whilst some have grasped the idea of information security risk, few truly understand it in its entirety due to the complexity and ever-changing landscape of technology.

Key findings

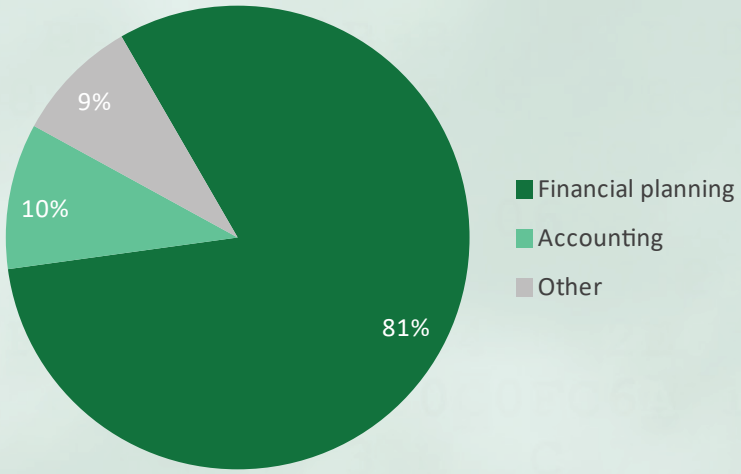
Our survey results suggest that overall there is a good awareness of cyber security, however:

- There appears to be over-confidence especially with business owners when it comes to dealing with cyber threats. Many believe that they are well protected against threats, relying only on their own expertise or general computer technicians.
- Most are not aware of their responsibilities with the incoming mandatory data breach notification laws. Ignorance of cyber security risks could be become a very costly for those who are affected (all accountants, and any business that deals with a TFN or with a turnover over $3M).
- The most common cyber incidents are caused by malware or phishing emails, indicating that there is a lack of basic security hygiene in the industry, and some very basic blind spots around user education.
- Some critical controls that can help in preventing cyber incidents or minimising the damage when cyber incidents occur are missing across the board.

Survey results

The majority of respondents were within financial advice, though respondents did include both individuals from the accounting and superannuation industries also. While many financial planners do not hold credit card data or make financial transactions. they do hold a lot of private, personal identifiable information for their customers.

Figure 1. Which industry do you work in?



Most respondents were also from small businesses and drilling down further – results of the survey revealed that most respondents were the owners of these businesses.

Figure 2. How large is your organisation?

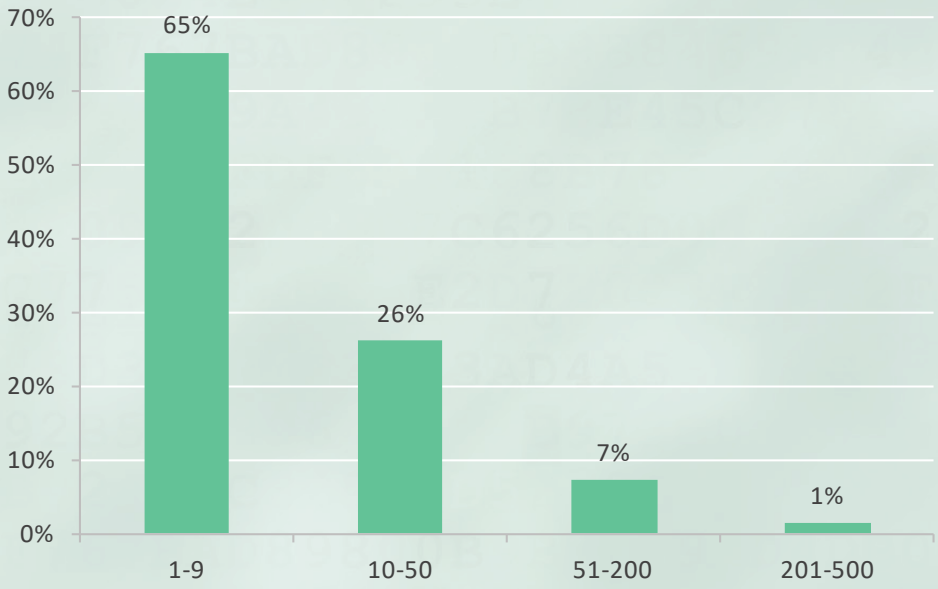
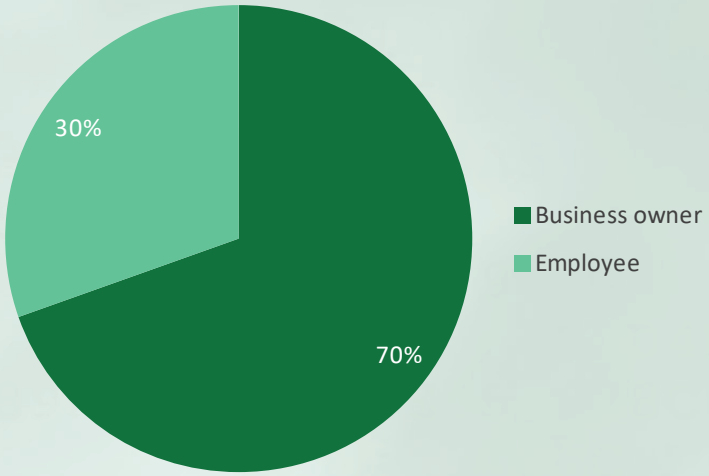
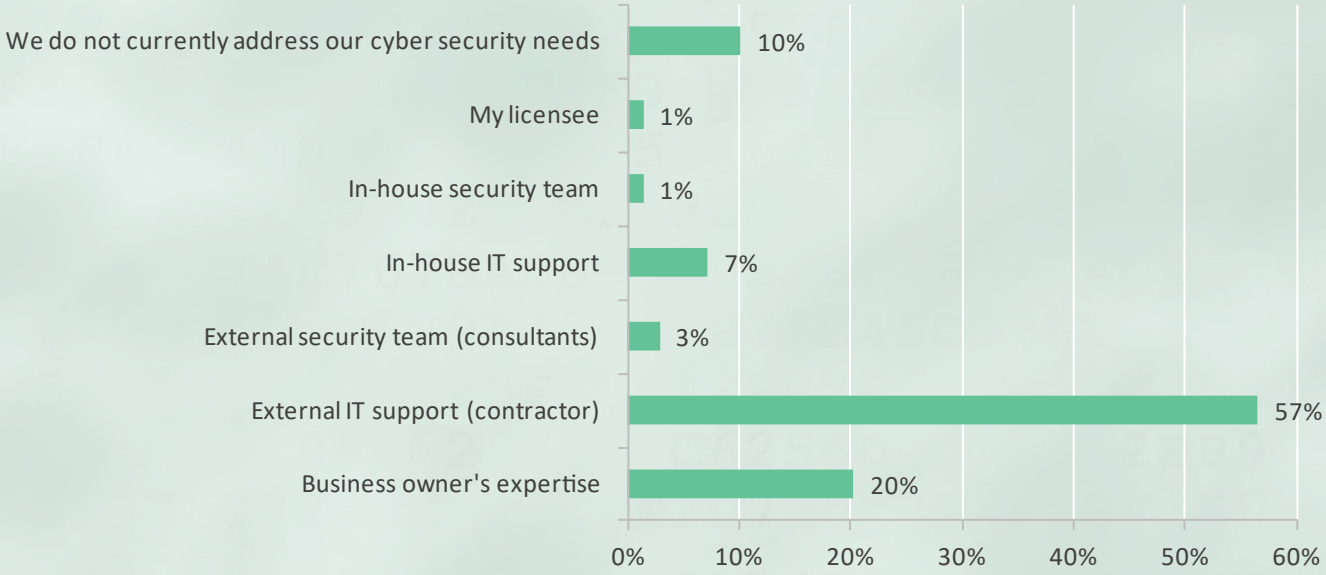


Figure 3. Are you a business owner or employee?



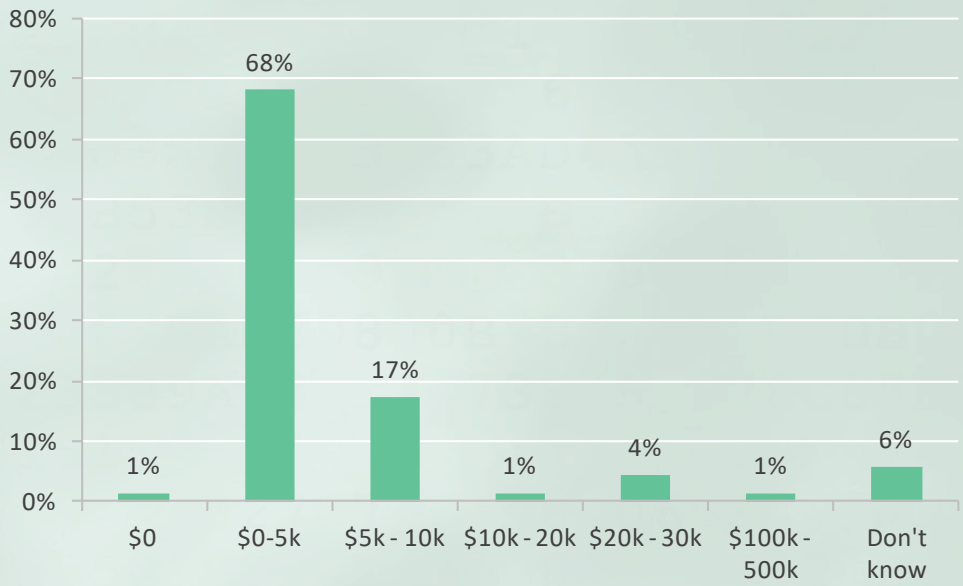
Of these organisations, 57% respondents said that they employ an external IT contractor to help meet their information security demand. Only 4% of the organisations said they would consult with a security specialist. Alarmingly 20% rely on their own knowledge and 10% **do not even address information security at all**.

Figure 4. How do you currently address your security needs?



This is somewhat reflected in their budget for information security, with 69% spending under $5K on information security per year. While $5K can make a lot of difference to a small office, many are spending close to nothing. Compared to the potential monetary loss due to a cyber breach incident which can easily go into the tens of thousands of dollars, it shows that many business owners have yet to grasp the risk and the value of investment in information security.

Figure 5. How much per annum do you invest in information security?



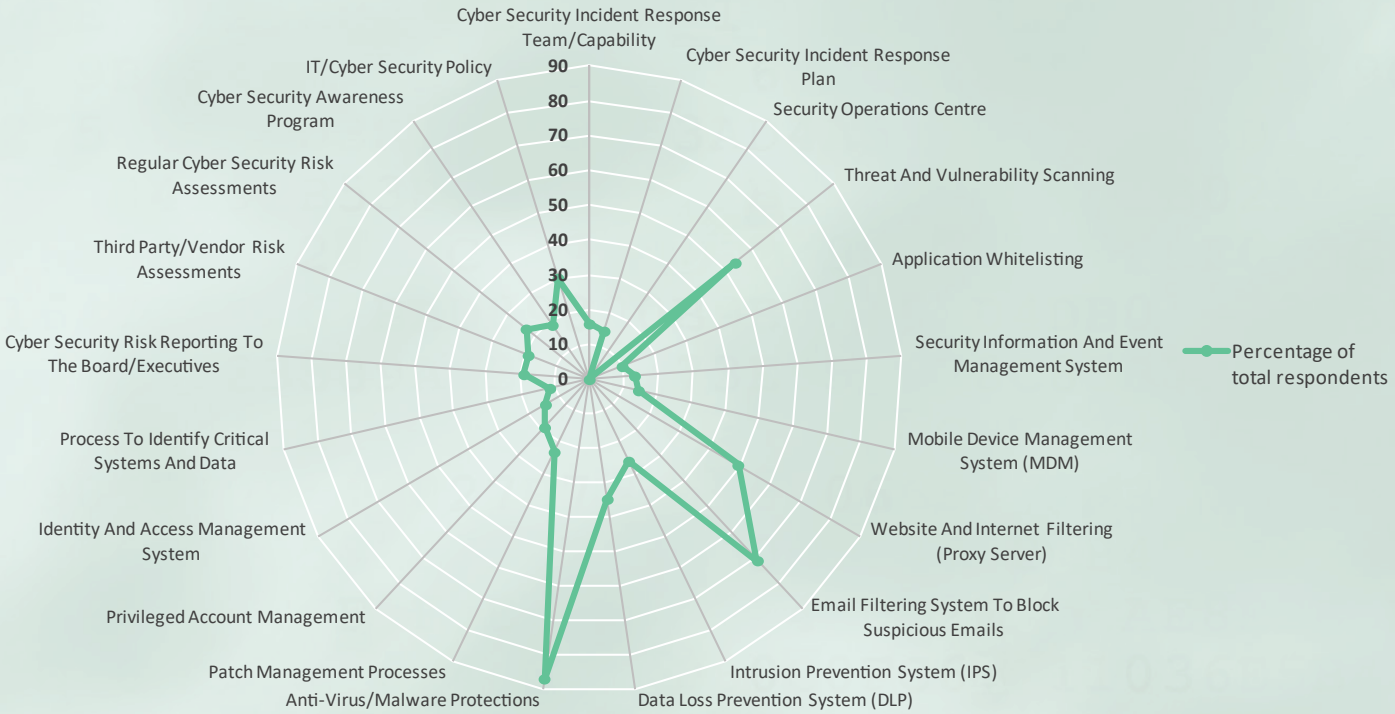
A proper information security program requires an upfront investment to establish a baseline, and from there on, ongoing maintenance to remediate existing and new risks.

Without a proper program in place, many businesses are not utilising the full value of their investment and would most certainly have blind spots in their security controls, leaving them vulnerable to cyber breaches.

When asked which security controls have been implemented or are currently being implemented within these, **the vast majority of respondents said that they have anti-malware and email filtering software installed**. Some also have intrusion prevention and website filtering capabilities. These are common feature in Unified Threat Management security devices designed for small and medium businesses.

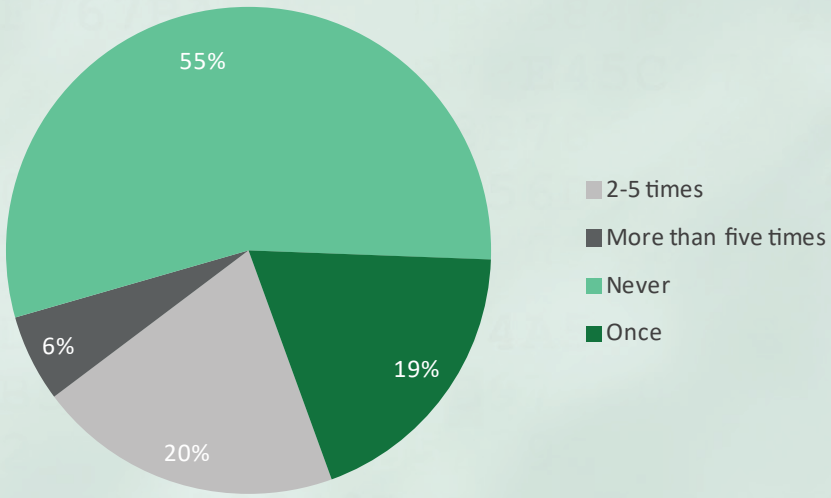
However, some very basic but important security controls are missing. These include incident response plans (14%), security awareness programs (18%), patching (23%) and privileged account management (18%). These are well-known blind spots and with so many financial services businesses without them, it's no wonder they are the weakest links when it comes to cyber security.

Figure 6. What security controls have you implemented or are implementing?



The occurrence of cyber security incidents is directly related to how well security awareness is in the business, and how well the security controls are implemented. Of the respondents, 45% experienced at least one cyber incident last year. **26% have experienced multiple cyber incidents**.

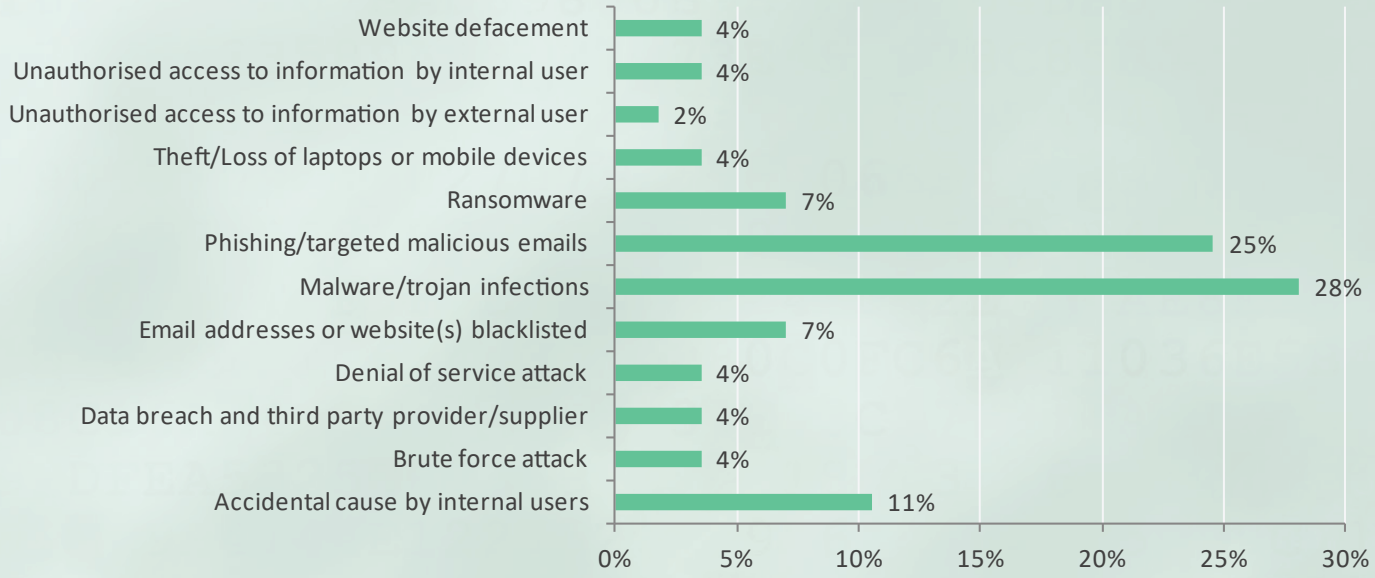
Figure 7. How many cyber incidents have you experienced in the last 12 months?



Out of all the incidents, **malware infections and phishing emails were revealed to be the largest threat to survey respondents**. This is an indication that financial advisers, accountants and superfunds may be missing some basic security hygiene despite having anti-malware and email filtering software installed.

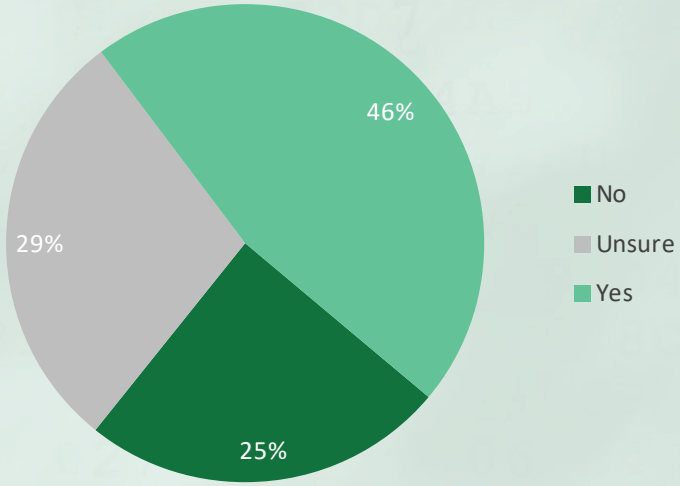
Ransomware is remarkably lower than expected. It's also particularly worth noting that 'accidental cause by staff' is one of the major causes of incidents.

Figure 8. Type of cyber incidents experienced last 12 months



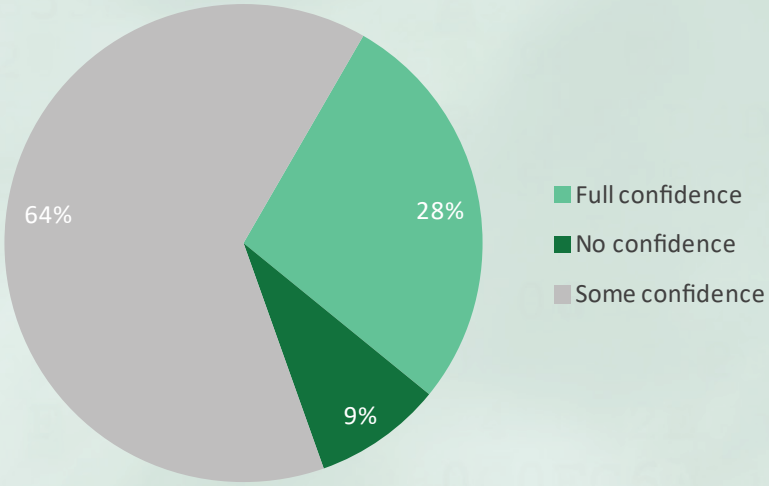
Without an expert to provide a subjective and independent view of the state of security, the frequency of cyber security incidents directly affects how the businesses feel about their own security posture. Just **over half of respondents believe they are not prepared to deal with a potential cyber-attack**. This means there is still almost half of businesses which feel they are comfortable with where they are when it comes to cyber security.

Figure 9. Do you feel your business is doing enough to adequately protect its systems from cyber threats?



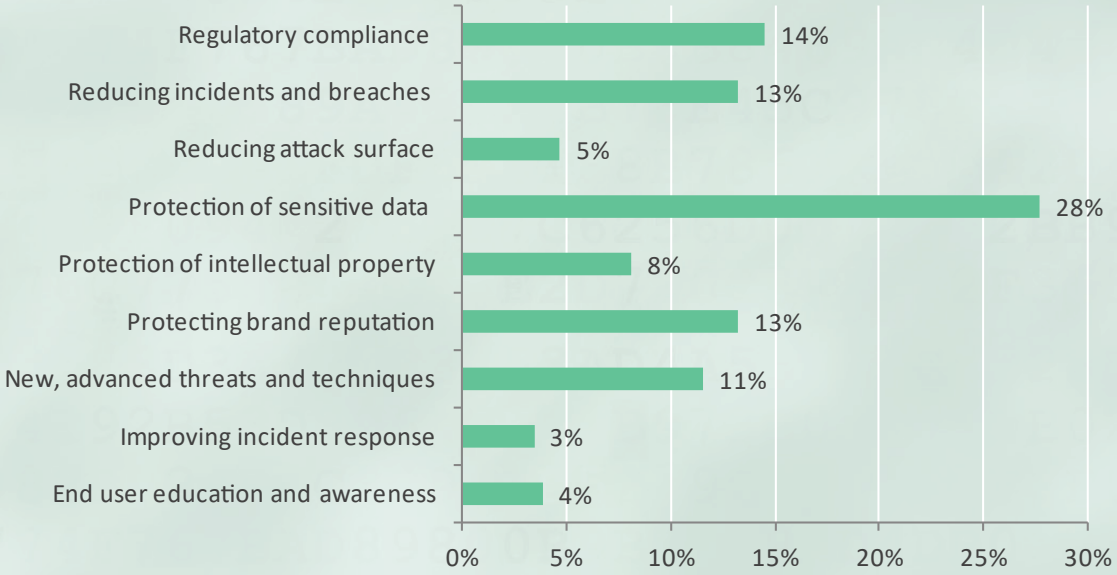
In contrast, when asked a similar question about their peers and/or workers, most respondents only have some degree of confidence that their colleagues or employees have enough user education and awareness to withstand attacks. This is worth noting because 'human error' is one of the biggest weaknesses in enterprise security defense.

Figure 10. How much confidence do you have in your staff's security hygiene?



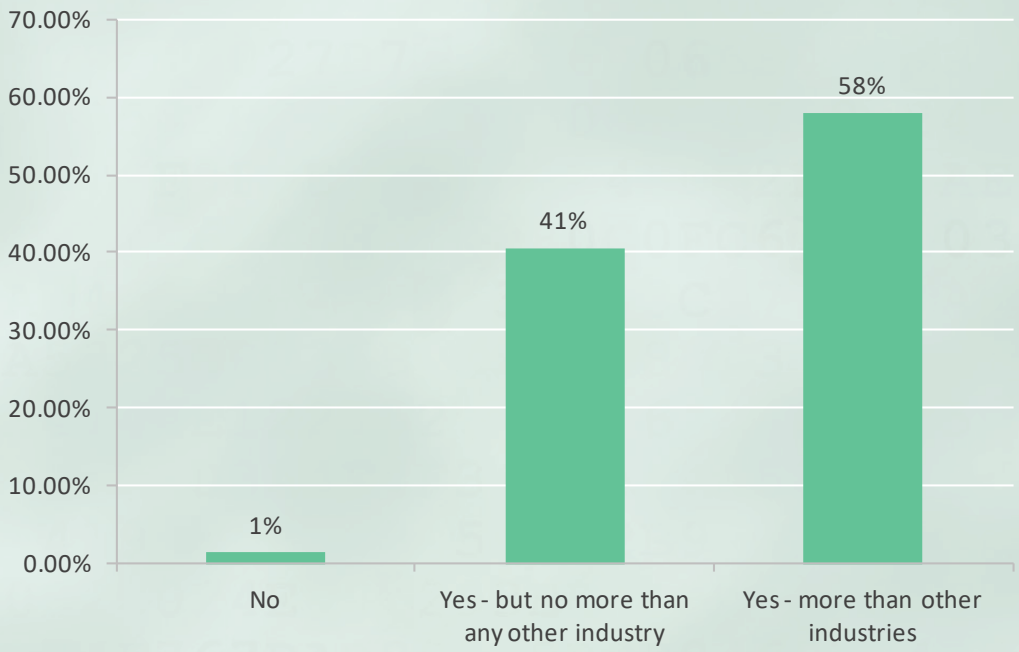
Most respondents appeared to have a very good understanding of what is at stake in the face of a cyber incident. Customer information is utmost important, and they understand that their brand must be protected from being tarnished by cyber incidents, which could lead to direct revenue loss.

Figure 11. What drives your investment in security?



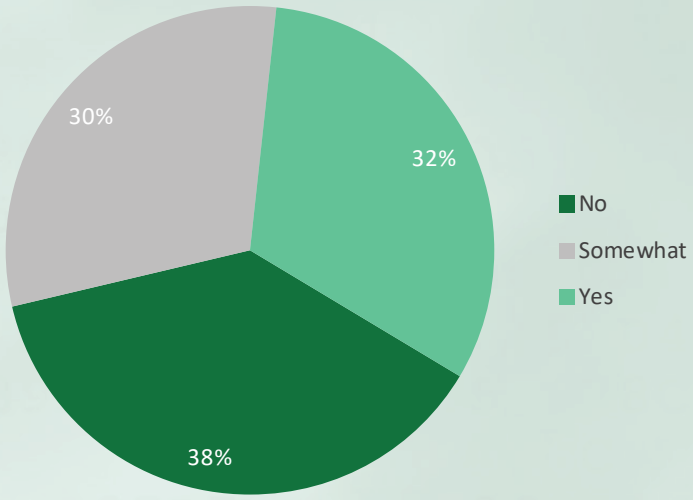
In terms of awareness of the industry's security implications and importance, many respondents did not seem overly concerned. Interestingly however, when compared against similar overseas surveys, financial services as an industry that spends far more than other industries in information security. Major financial institutions in Australia also invest heavily in defending themselves against cyber criminals. This leads to the conclusion that perhaps, there is a blind spot within the financial advice and accounting communities - that they do not perceive information security to be as high a priority as the wider financial services community. Unfortunately, this in turn makes them easy targets for cyber criminals for financial gains.

Figure 12. Do you think your industry should be worried about security given the client data you have?



At the time of survey, many respondents were not familiar with the new mandatory data breach notification laws effective in February 2018. This law will have a big impact on the businesses affected. This lack of awareness of the new laws could in turn translate to an overall lack of preparedness for the changes now in effect, which is alarming considering the ramifications on the businesses affected if a cyber breach incident takes place.

Figure 13. Are you aware of the upcoming mandatory data breach notification law?



Feeling concerned?

Kamino Cyber Security was founded in 2017 to provide advisers and accountants with peace of mind when it comes to cyber security. In a digital world where a cyber security breach can destroy a business overnight, we want to ensure that small to medium businesses still have the means to protect their data and systems.

Kamino provides a range of cyber security packages for the advice, accounting and superannuation sectors. If you are feeling concerned about the cyber vulnerability of your business, we'd like to help in any way we can. Please feel free to either call the Kamino hotline on **1300 882 938** or shoot us through an enquiry at info@kamino.com.au and we can get the ball rolling on protecting your business.