Security in Depth

State of Cyber Security in Australia 2018

Contents

Executive Summary

41% of all Australian companies have no Cyber Security Governance

- **14% of Australian companies are confident in the security practices of the companies they work with**
- **17% of companies are prepared for a Data Breach**
- **47% of Australian companies have never conducted Cyber Security Awareness Training**
- **24% of Companies believe their organisations are secure**
- **41% of Australian organisations have no Cyber Security Governance program**
- **70% of Australian companies have not increased their Cyber Security Budgets**

It took four days into 2018 before we learnt about Spectre and Meltdown. Cyber Security Specialists around the world went into panic, advising us that almost every PC was vulnerable. It was an interesting start to the year. Since then, organisations have been continuously affected by various Cyber Attacks. From phishing to ransomware, brute force attacks to attacks via third party suppliers, the issue has become - not if an attack will happen, rather when an attack will happen and how we can manage it.

Since the mandatory data breach notification laws came into effect in February 2018, the Office of the Australian Information Commissioner (OAIC) has received 305 separate data breach notifications. This means that over 2.5 million Australians have had their personal information become public. Recently, organisations such as Telstra, Australia Post and The Red Cross were affected by the PageUp data breach, resulting in millions of Australians who had applied for jobs with these organisations having their personal information shared publicly. These companies are not alone. Our research indicates that almost 72% of all Australian companies are targeted on a weekly basis.

According to research, it is concerning that 75% of these data breaches are not failures of technology, but individuals making simple mistakes. The cost of these mistakes to Australian businesses exceeds $10 million (which we believe is a conservative figure). Data breaches are costly.

As Cyber Incidents evolve and we better understand the challenges, change begins to happen and governments begin to act. The Federal Government has committed over $250 million in Cyber Security to make our online environment safer and has supported Cyber Awareness campaigns and governance throughout Australia. Further, technology that detects, identifies and responds to Cyber Incidents continues to develop here and globally. Whilst government and technology moves in the right direction, Australian companies have failed to keep up.

Based on the number of companies that have failed to implement what we believe to be Cyber Basics, it is our view that Australian organisations are now more vulnerable to a Cyber Incident than ever before. As most security experts will attest, technology is critical, but only provides part of the solution. Larger ICT teams and specialised security personnel are also part of the solution, but not the panacea. We are all interconnected and we are all in this together. To win this battle, we need buy in from the entire organisation, not just a few.

We are moving forward in the right direction. The journey ahead may be long and the current statistics may be challenging, but we believe it is a journey worth taking.

Michael Connory
CEO, Security in Depth

Our Method

The purpose of this study is to highlight the dependencies between the attitudes of Australian Corporate boards, Senior C-Level executives and ICT departments towards the challenge of Cyber Security. With this purpose, the study was conducted through both qualitative and quantitative research, which we believed allowed gaining the most relevant results about the relations between the Cyber Security challenges and corporate performance.

Research Approach

The respondents to this study represented 722 organisations across Australia with a minimum of fifty staff. Respondents included Board members, CEOs, Managing Directors, CIOs, CISOs and IT Managers. The organisations were selected without regard to their existing Cyber Security practices or technologies.

Questionnaire

The method of the questionnaire enables the research to be more quantitative because it requires the collation of standardised information from a specific number of people. The method also enables the data to be both qualitative and quantitative, which is the most appropriate way to research the connection between Cyber Security technologies, processes and organisational performance. We sent the questionnaire to 9,728 executives without regard to their age, gender or performance. The questionnaire asked questions that revealed the respondents' information on position, experience, performance and use of technology as well as information about Security Governance. We received 722 responses with 427 providing detailed answers to both the qualitative and quantitative questions. The data we obtained allowed us to build cause and effect relationships based on the answers. Accordingly, our research takes into account the organisational structure, people, technology, processes and Cyber Experience in our results.

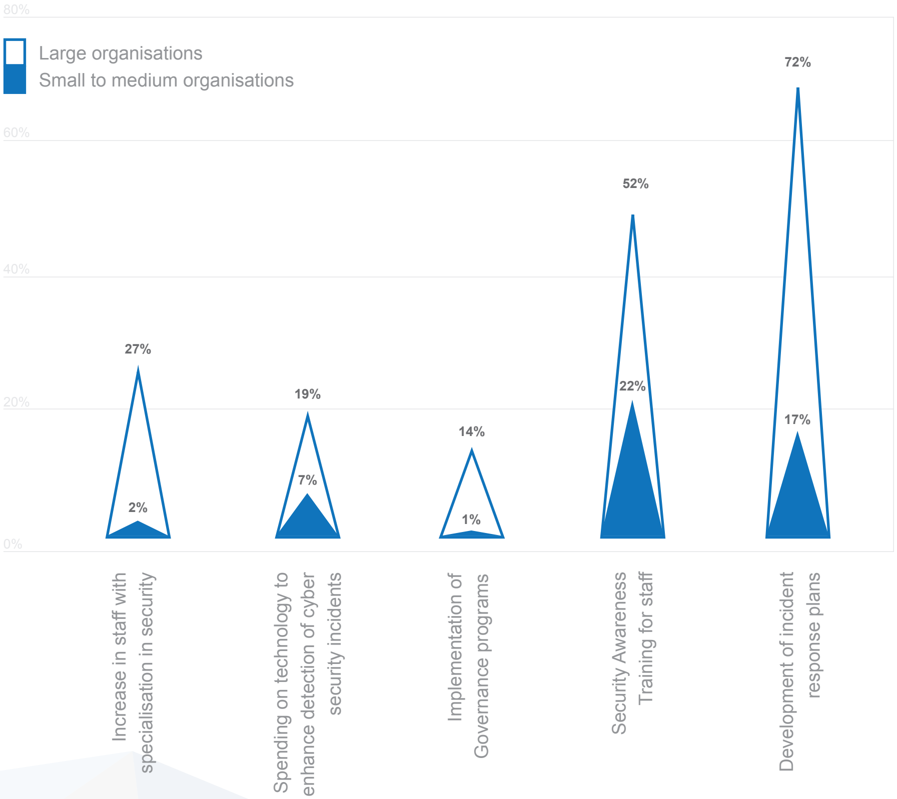
Statistical Data Analysis and the Documentary Analysis

The method enables obtaining additional data from documents and studies that already exist. This fills any informational gaps that may not be revealed by the responses to the questionnaire. The research uses documents to describe the background of Cyber Challenges across Australia as well as to complement the results with reliable scientific findings. Further, the documentary analysis enables obtaining various statistical data, which adds more credibility to the research. Examples of this come from the *OAIC Notifiable Data Breaches Quarterly Statistics Report 1 April - 30 June 2018 and the Ponemon Cost of Data Breach Study 2017*.

The evolution of security guidelines and governance

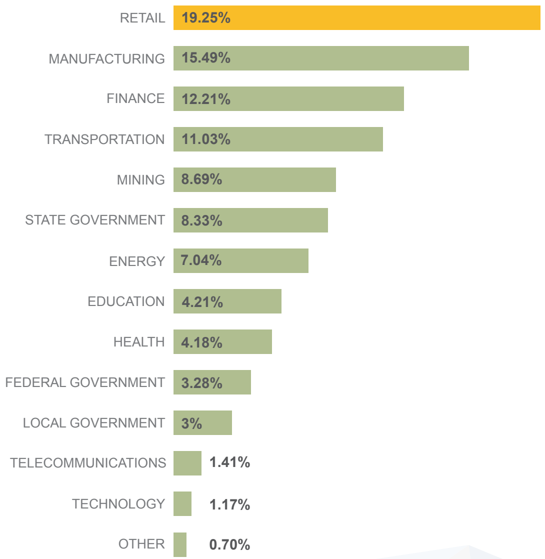
What was evident when we reviewed the responses from all organisations was: **Large Government, corporate and multinational organisations** (with staff in excess of 2,000 people and revenue in excess of 500m) **had made the most significant changes to their Cyber Security posture in different areas as compared to small and medium organisations** (with staff number of 1,999 or less). Our results found that large organisations focus more on the development of staff, awareness, incorporating incident response plans to manage risk associated with greater than 4 types of Cyber Incidents while small and medium organisations tend to focus more on managing existing technology more effectivly, and with an increased awareness provided better training to support cyber basics with existing staff.

We believe these key findings demonstrate the vast majority of Australian organisations have not taken Cyber Security seriously. With over 18,000 business not having any procedures and processes in place to either support staff from identifying potential Cyber Security attacks or more importantly have the ability to respond effectively to a Cyber incident.



Which industry is your organisation in?

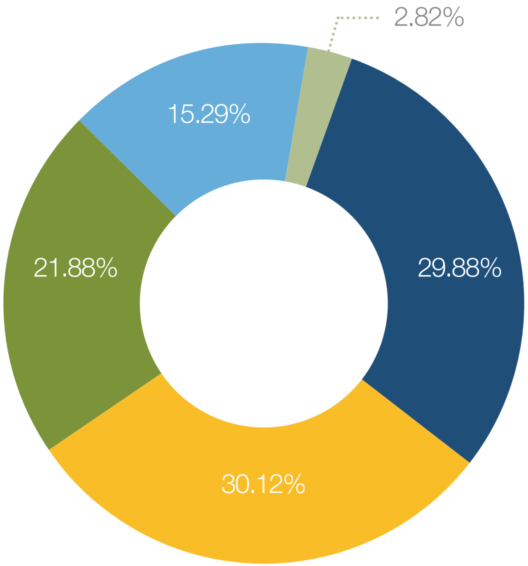
Total number of organisations surveyed is* ***722*



Of the 722 organisations that responded to our survey, the breakdown of organisations across Australia that responded is represented here. The majority of organisations responding come from both retail and manufacturing environments.

It is important to note that of the 139 retail organisations responding, all retail organisations had both a corporate web site as well as an online store, 122 had loyalty programs that allowed customers to log in to a portal to review and access loyalty rewards as well as update personal information.

How many people does your IT department employ?

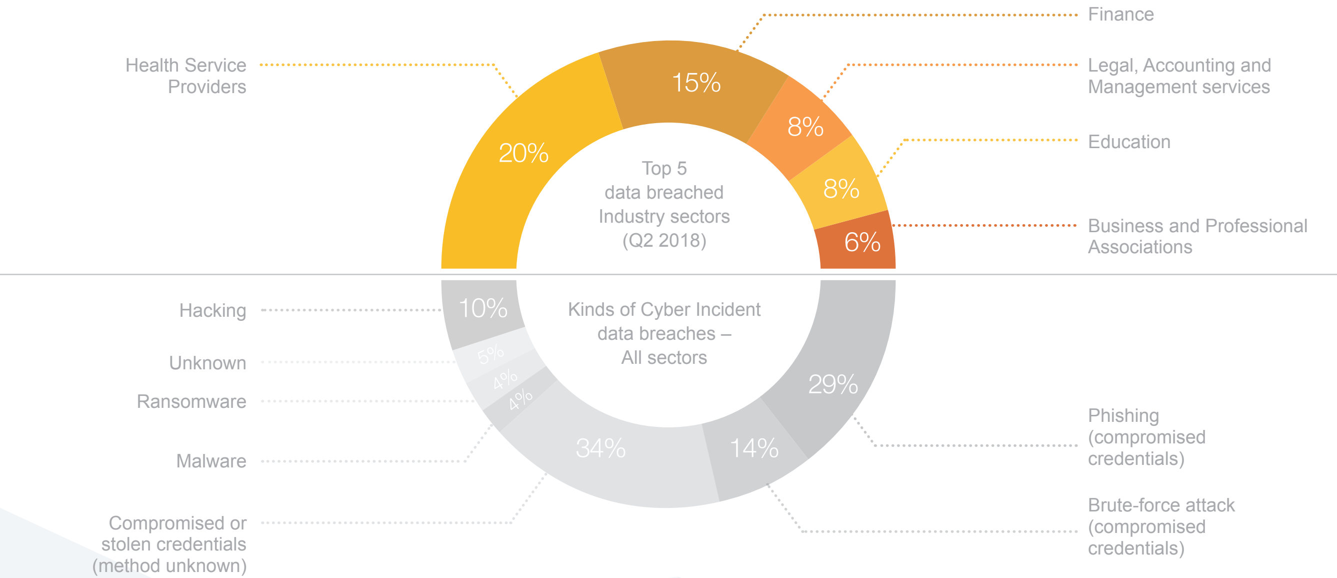


Of the 722 organisations that responded to this question, our researchers noted that **30% of organisations that did share detailed staff numbers, have less than 7 IT staff supporting their corporate infrastructure**. When we reviewed these numbers in more detail and against organisation size and maturity across Australia, we believe that over 10.000 Australian companies have an average of 2.8 dedicated IT staff.

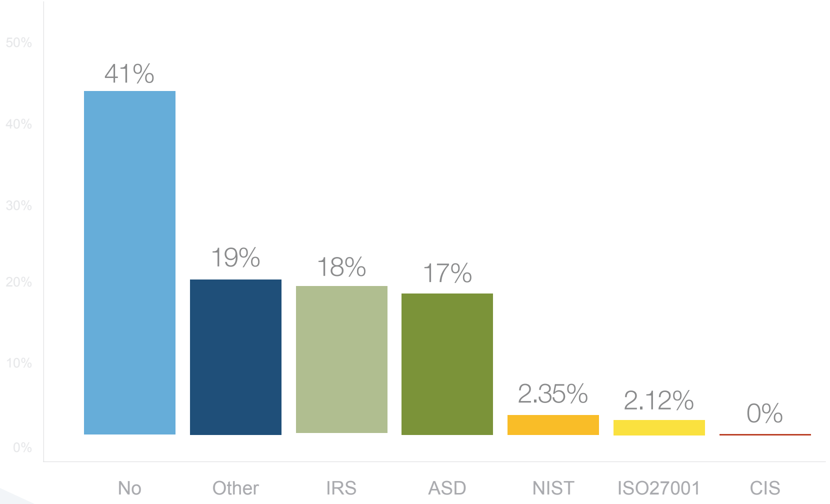
Of these organisations less than 120 small to medium organisations have an individual on staff, who have over 2 years of ICT security experience.

Top 5 industry sectors that reported data breaches in 2nd Quarter 2018

**OAIC Notifiable Data Breaches Quarterly Statistics Report 1 April – 30 June 2018*



Does your organisation adhere to ICT security frameworks?

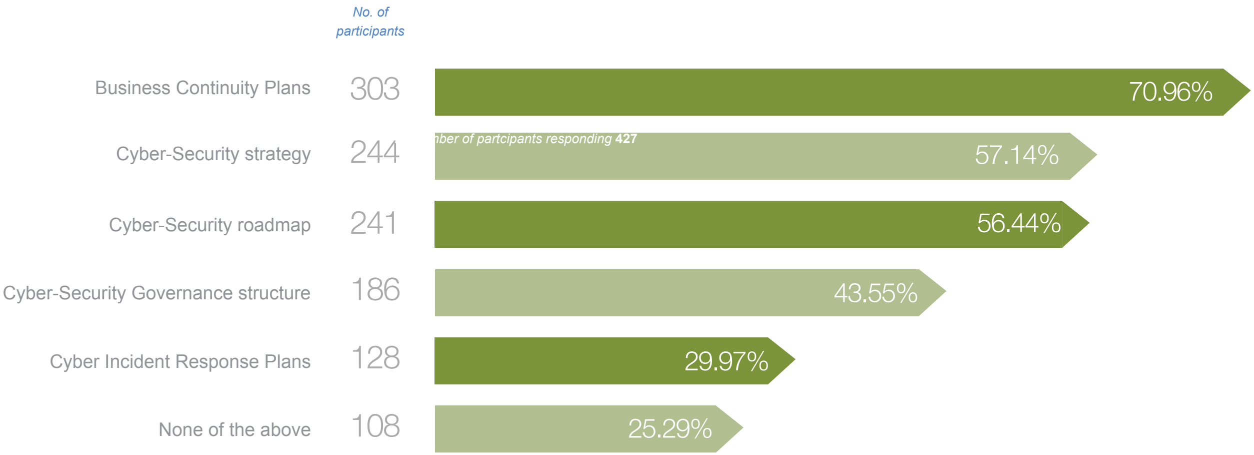


41% of organisations surveyed indicated they did not understand what an ICT security framework was

Out of the 722 organisations that responded to our research project, only 427 answered this question. 295 organisations did not know what a ICT security framework was.

Which of the following policies / procedures has your organisation documented and approved?

The number of partcipants responding **427, multiple responses allowed:*



How would you describe your organisation's cyber security maturity level?

The number of partcipants responding* ***427*

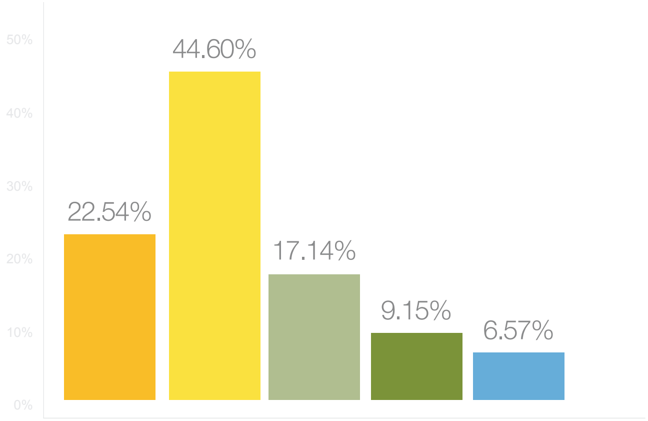
● **Optimised**: focus is on continuous improvement and innovation.

● **Repeatable**: some processes are repeated, perhaps with reliable results, poor discipline process, agreed benchmarks.

● **Basic**: undocumented, dynamic change, ad hoc, uncontrolled and reactive, individual heroics

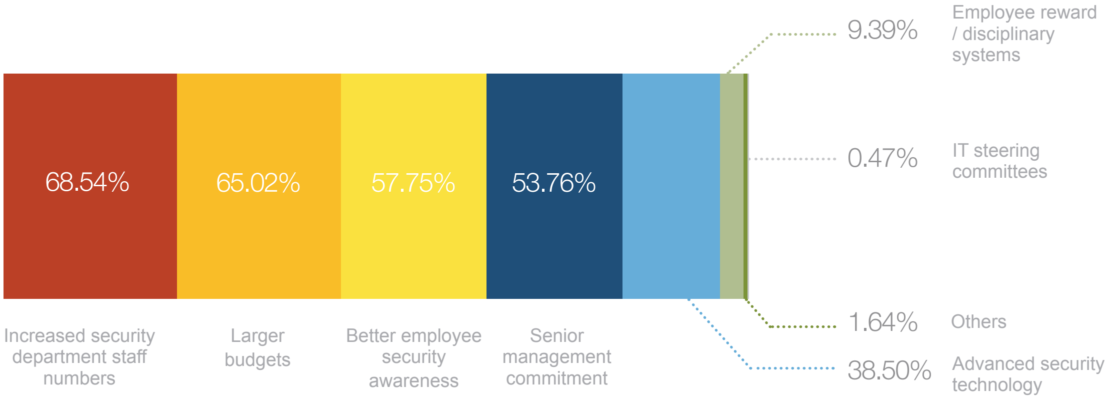
● **Fixed**: a set of defined and documented standard processes, some degree of improvement over time

● **Managed**: benchmarking process, effective management control, adaptation without losing quality.



What do you think will help improve your organisation's security levels?

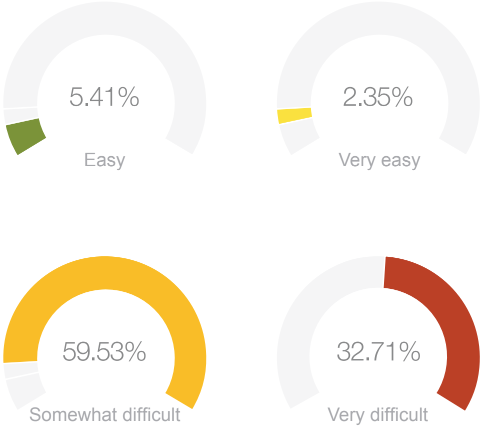
The number of partcipants responding* ***411**, multiple responses allowed:*



Over 53% of ICT management believe that better staff training and senior management commitment is more important than utilising and procuring advanced security technology

How difficult is it, in your opinion, to convince management to invest in security solutions?

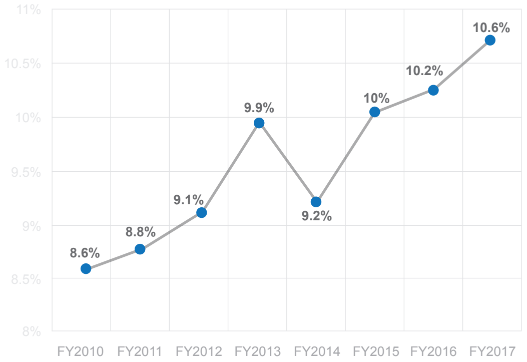
The number of partcipants responding* **411



The section was specifically targeted and answered by the ICT team, and demonstrated the gap in commuinication between ICT staff and either CEO, CFO and board level. With 92.24% of ICT managers struggling to obtain greater investment for Cyber Security.

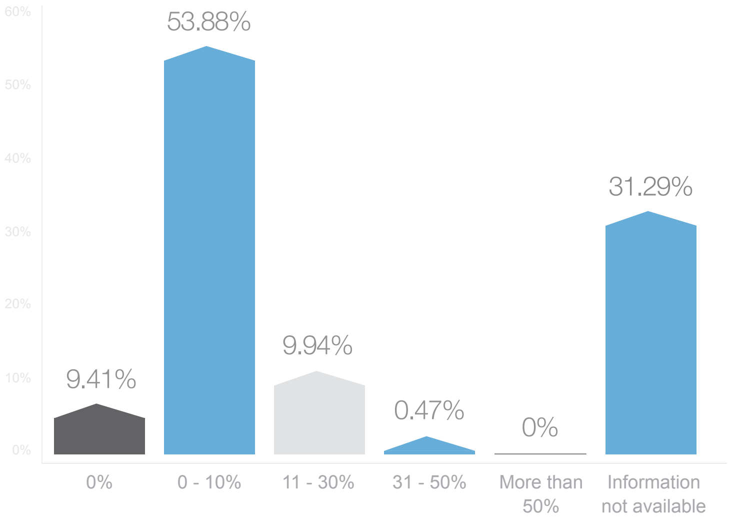
What percentage of your IT-budget was spent on security in the last 12 months?

Percentage of total IT budgets spent on IT security from FY2010 to FY2017



As of January 2018, according to respondents, enterprises currently spend an average of 10.6 percent of their overall IT budgets on IT security.

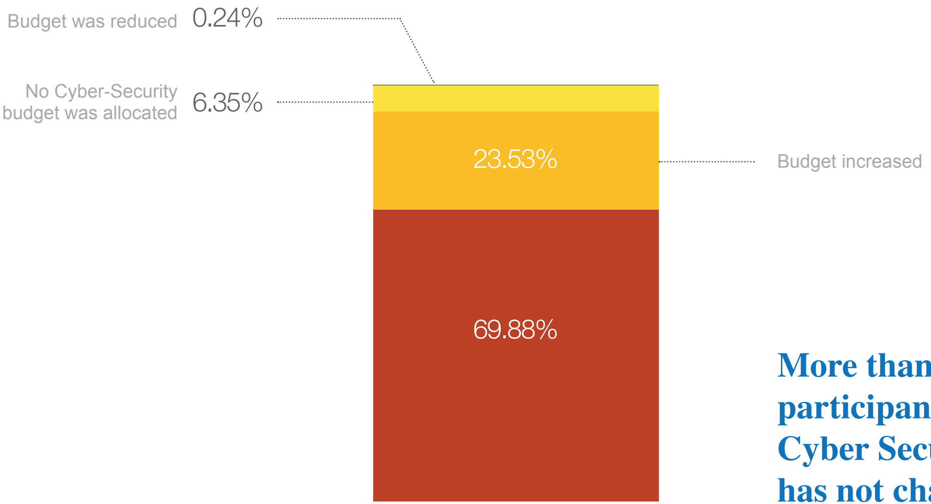
Source: https://www.statista.com/statistics/536764/worldwide-it-security-budgets-as-share-of-it-budgets/



2018 Security in Depth Cyber Research survey

Can you describe year-to-year spending in terms of your Cyber-Security budget?

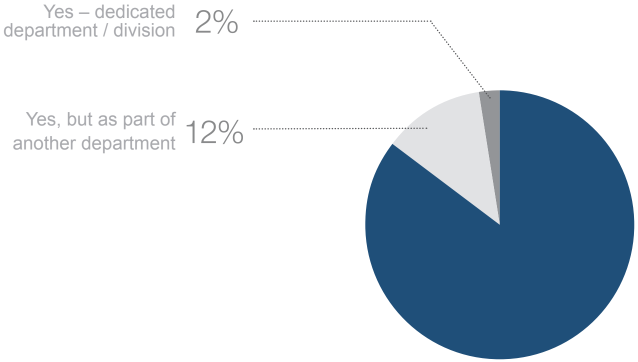
The number of organisations responding* **722



More than half of the participants say their Cyber Security budget has not changed

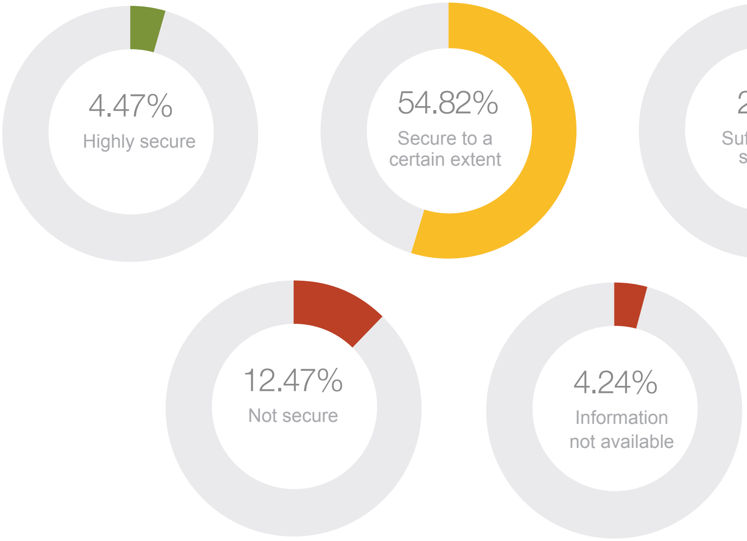
Does your organisation have a dedicated department responsible for information / network security?

The number of organisations responding* **722



85% of all companies surveyed said their organisation don't have dedicated security staff

How secure do you believe your network is?

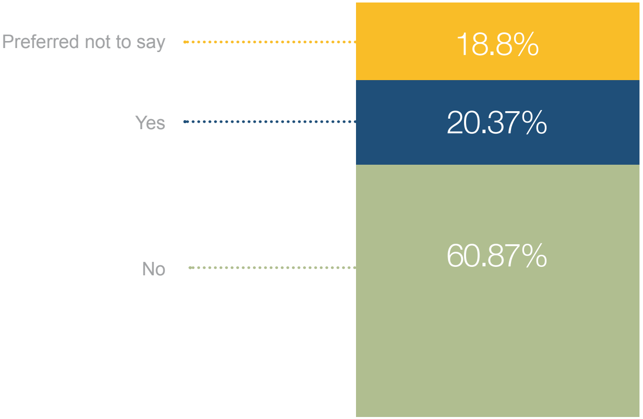


Over 16%
believe that their organisations insfrastructure is not secure

Off the 722 organisations interviewed we spoke to 411 ICT leaders – CIOs, CISOs and IT Managers.

Have you experienced a cyber security event in the last 12 months?

The number of organisations responding* **722



We defined a Cyber security event as the following:

Cyber security event was defined as a successful cyber incident such as phishing, malware, ransomware, brute-force attack, compromised or stolen credentials and hacking by other means, as well as social engineering or impersonation and actions taken by a rogue employee or insider threat. Theft of paperwork and / or storage devices was a significant source of malicious or criminal attacks.

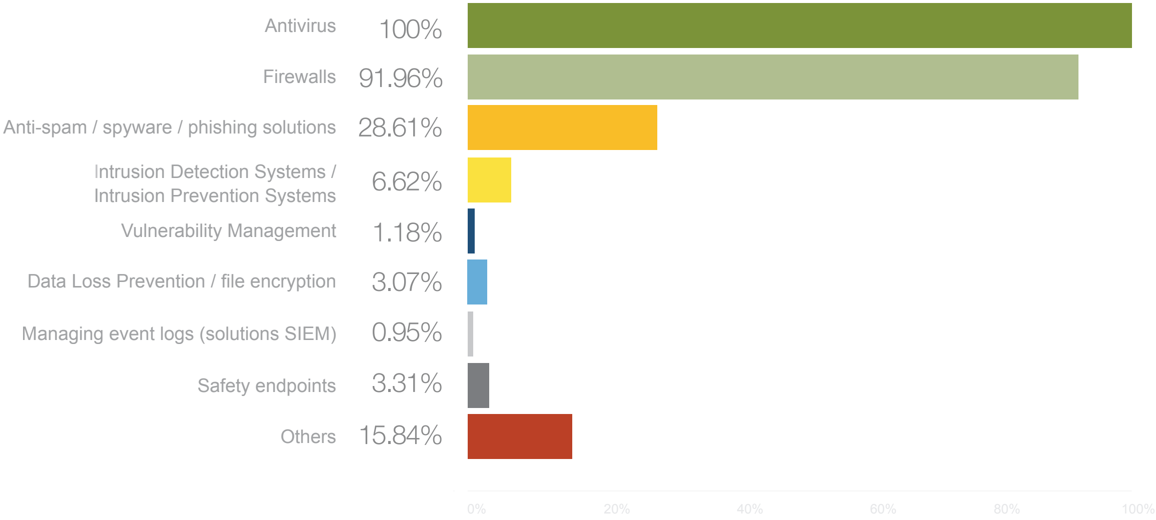
What do you consider to be your greatest security risk?

The number of parcticipants responding **722, multiple responses allowed:*

80%	●	Insider attacks
78.35%	●	Phishing, Malware, Ransomware
77.41%	●	E-mail viruses
68.54%	●	Brute-force attack, compromised or stolen credentials and hacking by other means
60%	●	Uncontrolled portable devices
59.06%	●	Incorrect configuration
53.41%	●	Internet downloads
2.12%	●	Others

Which security measures has your organisation implemented?

The number of partcipants responding **722, multiple responses allowed:*



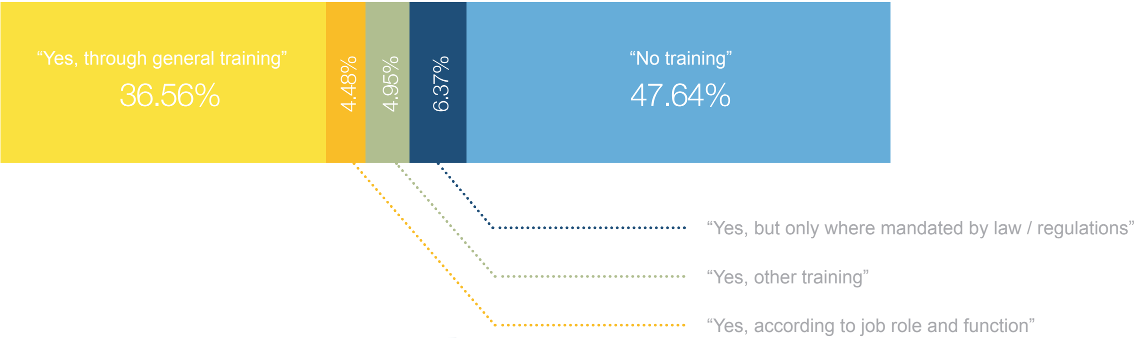
Does your organisation provide employee training to raise Cyber-Security awareness?

The number of organisations responding* **722

With over 75% of reported Australian data breaches directly related to human error as reported by the OAIC for the April-June period is 2018 is it a surprise that over 15,000 Australian organisations provide no training on Cyber awareness.

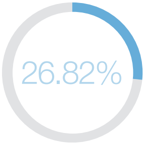
During 2018 we have witnessed an exponential growth in data breaches involving personally identifieable information. The OAIC have for 2018, in their mandatory data breach reporting statistics, communicated that over 300 Australian organisations have had a data breach this year.

With over 75% of these data breaches caused due to human error or phishing attacks we are concerned that only 37% of Australian organisations are providing staff with Cyber Awareness Training.



Has penetration testing ever been performed in your organisation?

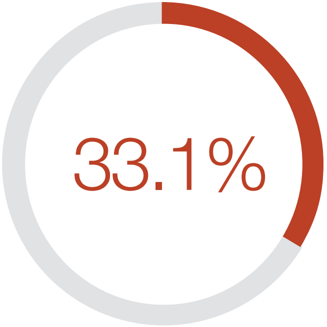
The number of parcticipants responding **427, multiple responses allowed:*



Conducted by either internal or external staff on Network services

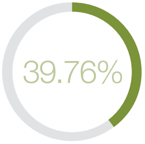
A Pen Test examines any weaknesses in the IT infrastructure of a corporation by trying to discover and exploit them, in a safe manner. These vulnerabilities can be found in the software itself at these particular points of entry:

- Backdoors in the Operating System;
- Unintentional flaws in the design of the software code;
- Improper software configuration management implementation;
- Using the actual software application in a way it was not intended to be used.



No testing has been completed at all

**The section was specifically targeted and answered by the ICT team*



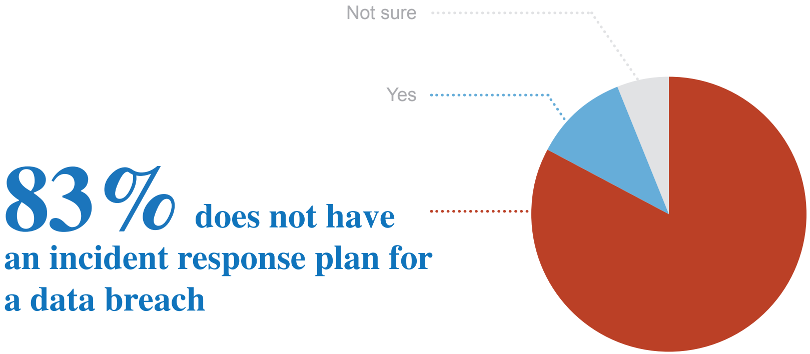
This covers Penetration testing for web applications and utilises either Black, White or Gray box

To uncover the vulnerabilities which can be found in type or kind of Web Application, there are three types of Pen Testing which can be used, which are as follows:

- Black Box Testing; in this type of Pen Test, there is no information given to the tester about the internal workings of the particular Web Application, nor about its source code or software architecture.
- White Box Testing; The tester has full knowledge and access to both the source code and software architecture of the Web Application.
- Gray Box Testing; penetration tester only has a partial knowledge of the internal workings of the Web Applications. This is often restricted to just getting access to the software code and system architecture diagrams.

Do you currently have an incident response plan for a data breach?

The number of organisations responding* **722



According to the OAIC:

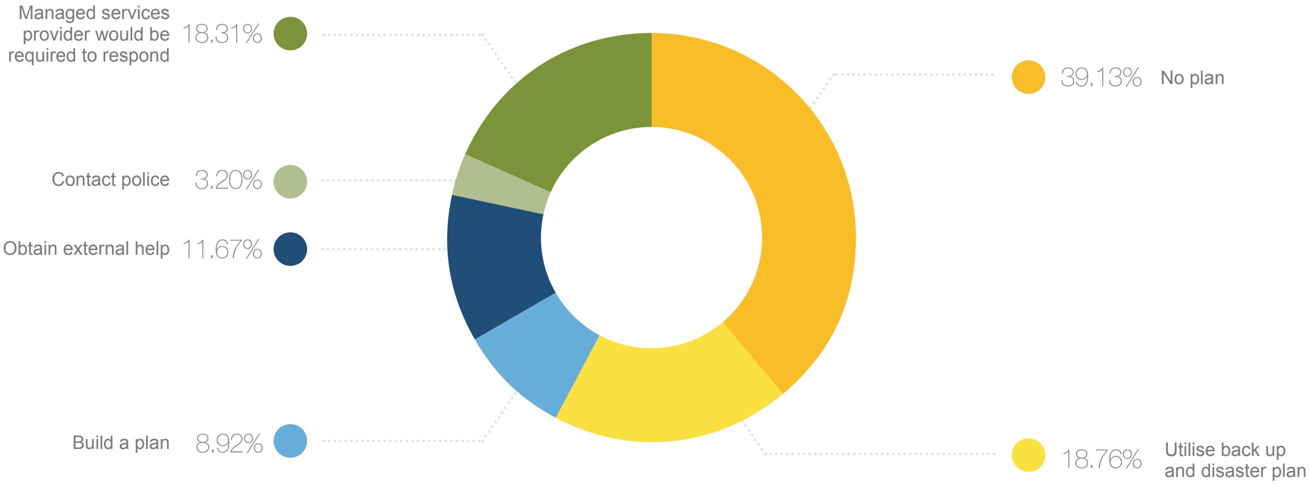
All entities should have a data breach response plan. Your actions in the first 24 hours after discovering a data breach are often crucial to the success of your response. A quick response can substantially decrease the impact on the affected individuals.

High profile data breaches, both in Australia and overseas, highlight the significant disruption caused by a breach of personal information. Research suggests that the cost to an organisation for a data breach can be significant. Implementing a data breach response plan can assist in mitigating these costs.

Having a data breach response plan is part of establishing robust and effective privacy procedures. And having clear roles and responsibilities is part of good privacy governance.

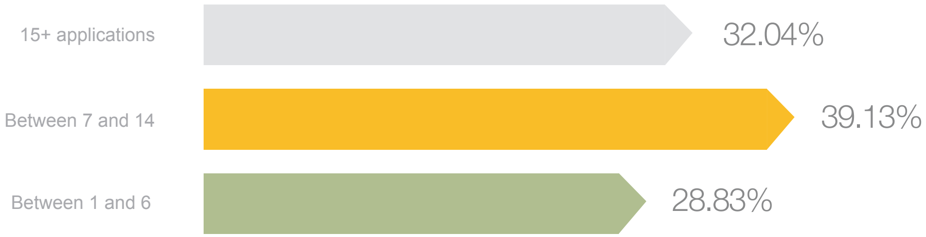
How do you plan to respond to a data breach?

The number of organisations responding* **722



How many applications do you have that either integrate or are supplied by third party providers?

The number of organisations responding* ***722*



Major Data Breaches - Third party suppliers

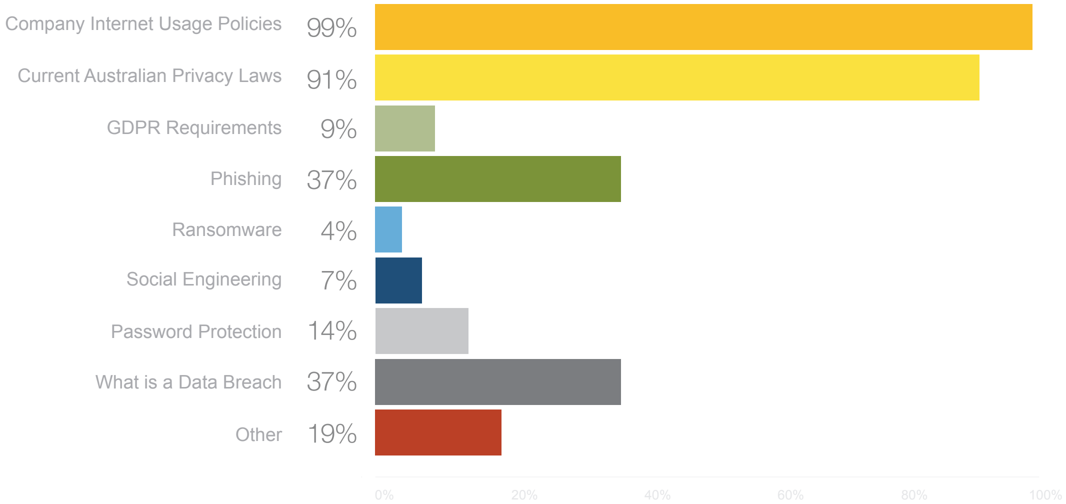
Third party suppliers can be an attractive way for cyber criminals to gain access to data and networks that would otherwise be beyond their reach. And while key operations and processes can be outsourced, your business risks cannot.

According to Gartner, **"By 2022, cyber-security ratings will become as important as credit ratings when assessing the risk of business relationships."**

The report continues, "Over the next six years, these [cyber-security rating] services will become a mandatory precondition for a growing number of business relationships and part of the standard of due care for providers and procurers of services. These cyber-security scores will impact the degree to which other companies engage in high-value business with the organization."

How confident are you in the Cyber-Security practices of your third parties with reviewed security practices?

The number of partcipants responding **427, multiple responses allowed:*

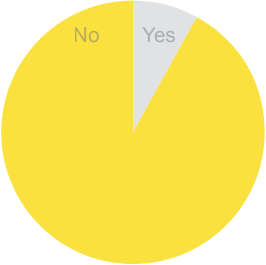


Have you conducted security reviews of third-party providers? Will you be conducting third-party provider security checks within the next 12 months?

The number of organisations responding* ***422*

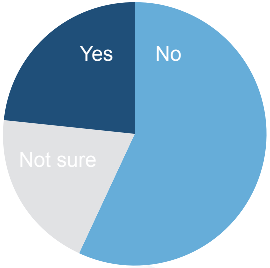
91.99%

have not conducted security reviews of thrid party providers



56.75%

will not be conducting third party provider security checks in the next 12 months



Many of the high profile data breaches we learn about come directly from integration with third party suppliers. This could be your HR system, Payroll, Online Booking system etc. We ask ourselves why do so many organisations fail to assess their third party supplier IT security risks and put appropriate controls in place to ensure the ongoing security and availability of their business critical information?

We believe organisations must ensure comprehensive security reviews of third party suppliers and partners are carried out, not doing so significantly increases risk of a major cyber incident.

How does your organisation ensure an adequate and appropriate level of Cyber-Security over third parties? If you have conducted a third party review, wow does your organisation ensure an adequate and appropriate level of Cyber-Security?

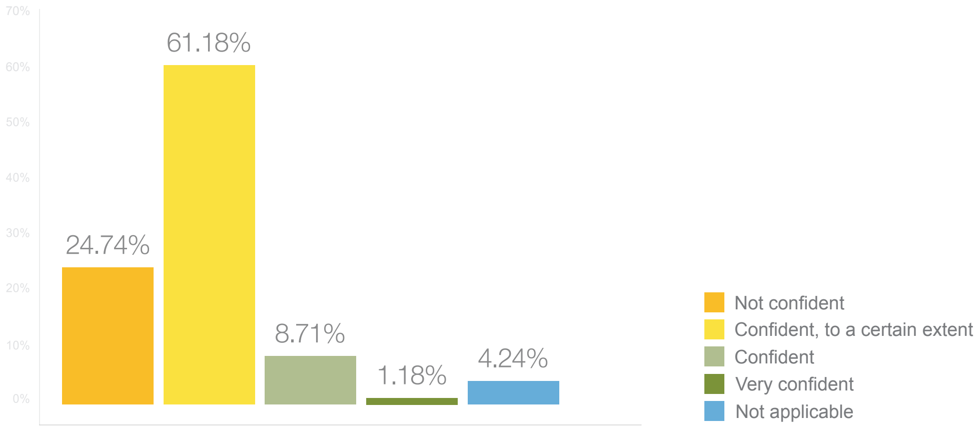
The number of partcipants responding **422, multiple responses allowed:*

84.94%	●	Signs confidentiality and/or non-disclosure agreements
74.82%	●	Addresses Cyber-Security issues in a contract
68.47%	●	Identifies risks related to third parties as part of information risk assessments
66.82%	●	Imposes corporate security policy and controls on third parties

16.71%	●	Where permitted, performs background verification checks on selected high-risk
8.24%	●	Controls third-party access to systems and data
5.18%	●	Performs random spot checks of third-party sites
12.94%	●	Requires independent attestation (e.g. ISAE3402, ISO27001:2005 certification)
2.59%	●	Regularly monitors and reviews third-party services
1.18%	●	Others
5.41%	●	Not applicable

How confident are you in the Cyber-Security practices of your third parties?

The number of organisations responding* **722



> Cybersecurity risks are also growing, both in their prevalence and in their disruptive potential. **Attacks against businesses have almost doubled in five years**, and incidents that would once have been considered extraordinary are becoming more and more commonplace. **The financial impact of cybersecurity breaches is rising, and some of the largest costs in 2017 related to ransonware attacks**, which accounted for 64% of all malicious emails. Notable examples included the WannaCry attack - which affected 230,000 computers across 150 countries - and NotPetya, with estimated damages of around $1.2 billion.

THE GLOBAL RISKS REPORT 2018
WORLD ECONOMIC FORUM

Security in Depth

Phone: +61 3 8678 1818
Email: research@securityindepth.com.au