iFHP Cyber Security Report 2019

Executive Summary

The purpose of the iFHP 2019 Cyber Security Survey is to evaluate a range of indicators regarding cyber security in the insurance healthcare sector. These indicators will help iFHP members understand current and future threats and issues that need to address in this market. Overall, 12 iFHP member organisations took part in the survey that was administered via Qualtrics with data collection taking place in June and July 2019.

The survey comprised 38 questions, featuring a range of open and closed questions. The questions were broken down into 7 sections: Organisation, Identify, Protect, Detect, Respond, Recover and Future Threats. A summary of these sections is provided below.

Organisation

The survey was completed by 12 organisations, with the majority of responses being received from Australia. The respondent organisations operate PHI/PMI plans across 12 different countries, covering over 42 million lives in total. The size of the respondent organisations, with respect to the number of employees, varies between 280 and 217,000.

Identify

Respondents report on their maturity measurement approach. Popular frameworks include: NIST Cyber Security Framework, ISO/IEC 270001 Information Security Management and CIS Controls. Details are also given of their reporting approaches. Respondents disclose the way in which security is reported to the board, with the majority including it in IT summary reporting. Various responses are given about the key security metrics shared with the executive team. Finally, the frequency of security governance meetings is disclosed, with the majority happening monthly. Details of how the organisations align security with the risk team is also provided.

Protect

The section reports on the number of dedicated (full-time) security staff and (full-time) security contractors each organisation employs, the majority being the former. Seven organisations also provide detail of the use of office-based, remote and off-shore contractors by percentage split. Figures for operational expenditure on security and capital investment in security are then reported as well as the overall percentage of investment in each threat vector. The threat vector invested in by the greatest number of organisations is Phishing. The key controls used by organisations to protect cloud data are then given, with ‘Identify and access management’ being used by all. The standards and frameworks used by the organisations are also reported as well as the endpoint solutions that are used. The most popular endpoint solutions are Microsoft and Trend Micro. Organisations also report on the endpoint controls implemented as well as the type of SOC/SIEM service they use. The majority use an outsourced service and detect was the most popular level of service.

Detect

Figures for the number of low, medium and high security incidents experienced by organisations are presented. The majority of security incidents were low, with 5 organisations reporting 10+ low incidents and only 5 organisations experienced high security incidents. Further information on the number of security incidents by threat vector is also reported; the most frequent type of incident is phishing whereas devices is the least frequent. Some additional threats are also reported.

Respond

Detail is provided in this section about how incidents are reported at the executive level. Only 1 of the organisations does not report incidents at the executive level. Information on the departments involved in response planning and testing is also provided.

Recover

Respondents report the timeframe to recover impaired capabilities due to experiencing a breach. The time taken to respond to an incident depends on the type of incident; the range being from an immediate response to up to 2 weeks.

Future Threats

A number of perceived threats were reported by respondents such as legacy systems, data breaches, claim fraud and phishing. Respondents also reported the likelihood of a minor or major breach occurring within the next 12 months, the consensus being that a minor breach is likely to occur, but a major breach is unlikely.

Table of Contents

List of Survey Questions 1
List of Figures & Tables 5
Introduction 6
NIST Cybersecurity Framework Functions 6
1. Organisation 8
2. Identify 10
3. Protect 16
4. Detect 24
5. Respond 27
6. Recover 29
7. Future Threats 30
References 32
Appendix A 33

List of Survey Questions

Section	Question	Figure/Table	Page
1. Organisation	1. In which country (or countries) does your organisation operate with PHI/PMI plans?	Figure 2	8
	2. What is the total number of **lives** covered by your organisation? This should be individuals and not the amount of policies (i.e. family policies).	Figure 3 Table 1	8-9
	3. What is the total number of employees in your organisation?	Figure 3 Table 1	8-9

2. Identify	1. In which of the regions below do you have personally identifiable information (PII) or medical data stored?	Figure 4	12
	2. Do you use cloud service providers to store PII or medical data?		10
	3. Describe your maturity measurement approach, including any frameworks, stakeholders, scale, reporting, and how it is perceived.		10-11
	4. How is security reported to the board?	Figure 5	13
	5. What are the key security metrics shared with the executive team?		13
	6. Does your organisation have a dedicated senior security governance committee?		14
	7. How often are security governance meetings held?	Figure 6	14
	8. Is the executive team included in security governance?		14
	9. Is security aligned with the risk team? If yes, please provide some detail.		14
	10. Is security aligned with the legal team? If yes, please provide some detail.		14-15

3. Protect	1. What is the number of dedicated (full-time) security staff in your organisation?	Figure 7	16
	2. What is the number of (full-time) security contractors in your organisation?	Figure 7	16
	3. Please provide the percentage of contractors that are office-based/remote/off-shore.	Figure 8	16
	4. What is the operational expenditure on security in your organisation (in USD)?	Table 2 Figure 9	17
	5. What was the Capital Investment in security for the last two years (in USD)?	Table 2	17
	6. Please provide the percentage of investment in each of the following threat vectors. Allocate percentages out of 100% across each category.	Figure 9 Table 3	18
	7. What key controls are used to protect cloud data?	Figure 10	17, 19
	8. Is your organisation using any of the following standards/frameworks?	Figure 11	20
	9. Is your organisation **certified or compliant** with any of the following?		17
	10. Does your organisation use any of the following endpoint solutions?		21-22
	11. What endpoint controls do you have implemented?	Figure 12	23
	12. Is your SOC/SIEM service insourced or outsourced?	Figure 13 Table 4	24
	13. What level of service does your SOC provide?	Figure 14 Table 4	24
	14. How would you rate the value of your SOC/SIEM service out of 10? (1=poor, 10=very good).	Table 4	24

4. Detect	1. Please specify the number of low, medium and high security incidents in the last year.	Figure 15	25
	2. Please specify the number of security incidents by threat vector.	Figure 16 Figure 17	26
	3. Do you do incident response planning?		25
	4. Do you do incident response testing?		25
5. Respond	1. Are incidents reported at the executive level? If yes, how do you do this?		27
	2. Who is included in your incident response planning and testing?	Figure 18	28
	3. Do you test crisis management in relation to breach of information?		27
6. Recover	1. Do you have cyber insurance?		29
	2. If you have experienced a breach, what is the timeframe to recover the impaired capabilities?		29
7. Future Threats	1. What do you perceive to be the biggest threat for healthcare cyber security?	Table 5	30
	2. How likely is it that in the next 12 months your organisation will experience a minor or major breach?	Figure 19	31

List of Figures & Tables

Figure 1 - NIST Cyber Security Framework 6
Figure 2 - Location of respondent organisations 8
Figure 3 - Size of respondent organisations 9
Figure 4 - Regions where organisations have data stored 12
Figure 5 - Reporting security to the Board 13
Figure 6 - Frequency of security governance meetings 14
Figure 7 - Number of full-time security staff and contractors 16
Figure 8 - Split of contractor workers 16
Figure 9 - Overall percentage of investment in each threat vector 18
Figure 10 - Key controls used to protect cloud data 19
Figure 11 - Standards and frameworks used 20
Figure 12 - Endpoint controls 23
Figure 13 - Type of SOC/SIEM service 24
Figure 14 - Level of service 24
Figure 15 - Number of security incidents 25
Figure 16 - Number of security incidents per threat vector 26
Figure 17 - Estimated total number of security incidents per threat vector 26
Figure 18 - Departments involved in response planning and testing 28
Figure 19 - Likelihood of minor and major breaches 31

Table 1 - Summary of number of lives covered and employees 8
Table 2 - Summary of expenditure 17
Table 3 - Investment in threat vectors 17
Table 4 - Summary of SOC/SIEM services 24
Table 5 - Perceived biggest threats healthcare cyber security 30

Introduction

The purpose of the iFHP 2019 Cyber Security Survey is to evaluate a range of indicators regarding cyber security in the insurance healthcare sector. These indicators will help iFHP members understand current and future threats and issues that we need to address in this market. Overall, 12 iFHP member organisations took part in the survey that was administered via Qualtrics with data collection taking place in June and July.

The survey was comprised of 38 questions These questions were further broken down into 5 sections in line with the NIST Cybersecurity Framework's five functions: Identify, Protect, Detect, Respond and Recover, plus 2 sections on organisation information and future threats. The Framework is displayed in Figure 1 and a description of each of the functions is provided on Page 2. The report is organised in the same format as the survey: beginning with information about the respondent organisations, analyses of the responses to the survey and concluding with recommendations. Where possible, data has been presented visually and text responses summarised. Not all questions were answered completely, and missing data is reported accordingly.

Figure 1 - NIST Cyber Security Framework[1]

NIST Cybersecurity Framework Functions

[1] Source: https://www.nist.gov/cyberframework/framework

1. Identify

The Identify Function assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

2. Protect

The Protect Function outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.

3. Detect

The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events.

4. Respond

The Respond Function includes appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.

5. Recover

The Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

1. Organisation

In total, responses were received from 12 member organisations. Figure 2 displays the locations from where the surveys were taken, of which the majority (7) of responses were received from Australia. The countries in which the organisations operate PHI/PMI plans are Australia, Brazil, Chile, Hong Kong, Mexico, The Netherlands, New Zealand, Poland, Spain, UAE, UK, USA.

Figure 2 - Location of respondent organisations

Figures 3 displays the size of the respondent organisations with regard to number of lives covered (relating to the number of individuals not the amount of policies) and the number of employees, respectively. There is missing data from one organisation for number of lives covered (Organisation 10). Table 1 provides the minimum, maximum, average and total of the number of lives covered and employees.

Table 1 - Summary of number of lives covered and employees

	Minimum	Maximum	Total	Average
Lives covered	20,000	16,500,000	42,560,584	3,546,715
Employees	280	217,000	296,908	24,742

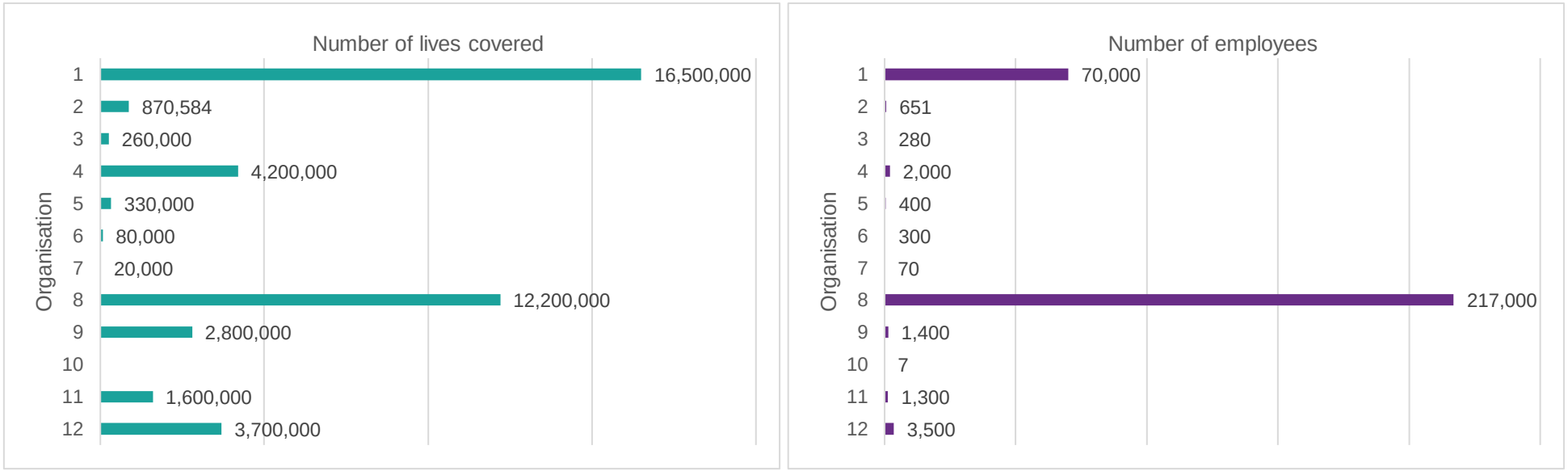


Figure 3 - Size of respondent organisations

2. Identify

The Identify Function assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Eight of the organisations use cloud service providers to store personally identifiable information (PII) and/or medical data. Figure 4 displays the regions where the organisations store PII and/or medical data and provides a total number of organisations in each region.

Respondents were asked to describe their maturity measurement approach, including any frameworks, stakeholders, scale, reporting, and how it is perceived. 9 organisations provided a response; there were a number of frameworks mentioned in the survey responses, of these three were mentioned by multiple organisations[2].

Cyber Security Framework, Version 1.1

This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

ISO/IEC 27001 Information Security Management

ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS). ISO/IEC 27001 specifies a management system that is intended to bring information security under management control and gives specific requirements. Organizations that meet the requirements may be certified by an accredited certification body following successful completion of an audit.

CIS Controls

Centre for Internet Security (CIS) Benchmarks and CIS Controls are consensus-based guides curated by security practitioners focused on performance, not profit. This standard leverages 20 prioritized actions to beat the vast majority of the most common attacks.

Other Frameworks listed:
(iFHP presented) Bupa Top 15 Controls

[2] Logos and descriptions are taken from the respective organisations' websites, sources reported in References.

APRA
OAIC
ASD Essential 8
COBIT

Reporting Approaches:
"Board supported review of maturity using the NIST framework conducted across the whole business by a third party with 2-year remediation and investment plans developed to address the gaps."

"We leverage the framework presented at iFHP from Bupa, this is based on the Top15 controls for cyber security. As a starting point we set a five-year target for each of the 15, and then each year we set an end of year target. Each quarter the 15 controls are assessed by six people across the business against a maturity scale based on CMMI model. This is graphed and presented to the Board for discussion on progress. The simplicity of the reporting is well received. The one area of concern is that this is subjective and dependant on the people's opinions of each controls progress. This year we have aligned the Top15 to the CSC20 and are now moving to a quantifiable measure using the same scale."

"We use a risk-based approach when we want to use any cloud service provider. It is an approach in which different roles have to play a part (IE Audit, legal, Compliance etc.). Also our supervisors are very interested in how we implement the controls before we contract any cloud service."

"Quarterly ISM Forum meeting, to update the senior management, drive the Security strategy and Road map."

"Info Security Framework in place with policies aligned iso27001
No formal maturity assessment completed as yet as Info Sec program just got up and running"

"We internally reviewed ourselves against the NIST Framework to identify major IT gaps (technology, training, policies etc), and have prioritized a set of actions to improve our security posture. We also utilise the ASD Essential 8 for IT configuration best practices, and have Standard Operating Procedures, independent audits and regular GRC tasks to ensure certain standards are met."

"We engage a third party to conduct an enterprise assessment of our capabilities and using the NIST Cybersecurity Framework as a benchmark. This assessment involved capability owners from across the KP enterprise, and results are provided through our governance committees. We plan to repeat these assessments at a defined interval to understand trends."

"We have annual IT Network Assessment conducted and reported to us by our outsourced IT managed service provider."

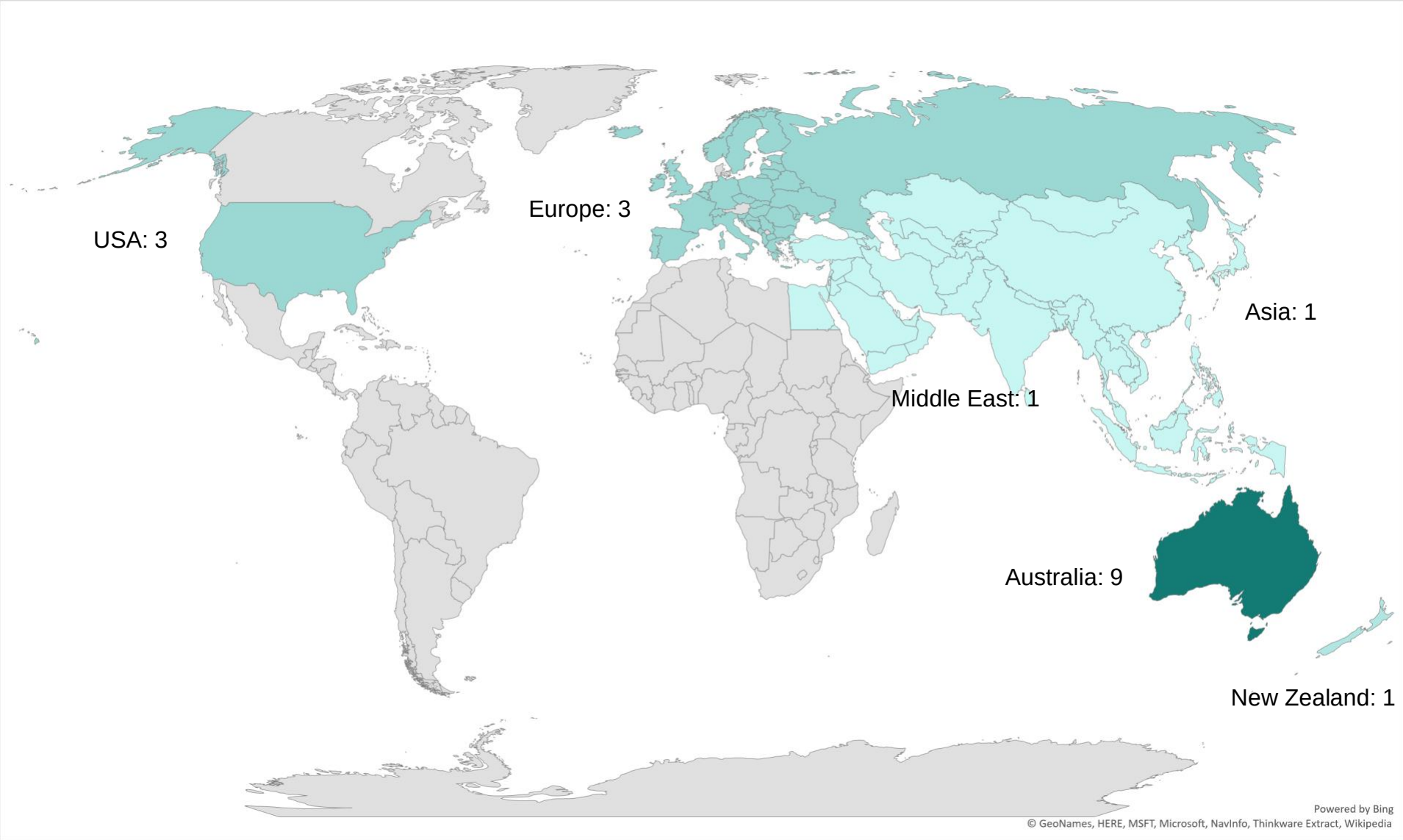


Figure 4 - Regions where organisations have data stored

The way in which security is reported to the Board is shown in Figure 5, with 25% of organisations representing Cyber Security at each meeting. 'Other' was selected by 2 organisations with further detail given by one: *"It is a topic that is reported quarterly. Semi-annually, the Chief Technology Risk Officer delivers a report in person."*

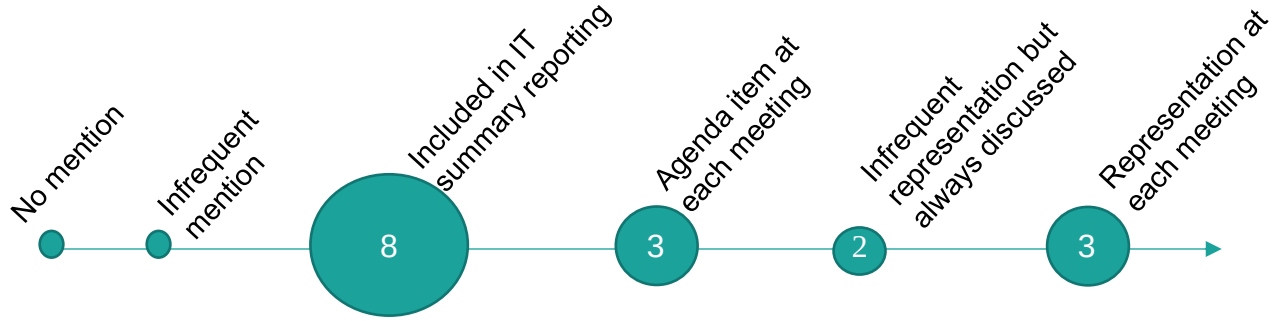


Figure 5 - Reporting security to the Board

Various responses were given when asked about the key security metrics shared with the executive team, these are listed below:

Anti-virus coverage
CPI (critical privacy indicator)
CRI (critical risk indicator)
Environment health
GRC tasks completed
Internal or external audit results
KPI
Maturity
NIST maturity levels across Market Units
Phishing campaign (mentioned by 2 organisations)
Potential security risks
Progress against plan for remediation
Progress on specific projects/tasks related to Cyber sec and DR/BCP
Project delivery
Risk position in terms of cyber appetite
Security incidents (mentioned by 5 organisations)
Severe security risks
SOC2 certification status
Spam filter
Top 15 Control Maturity
Uptime
Virus and SPAM detection rates
Vulnerability management

Eight of the respondents have a **dedicated senior security governance committee** with meetings being held at differing intervals, shown in Figure 6. 3 organisations hold meetings monthly, 1 bi-monthly, 2 quarterly and 1 twice a year. 1 organisation reported that meetings on an operation level are held weekly, every 6 weeks on a tactical level and every quarter on a strategic level. Nine organisations **include the executive team in security governance**.

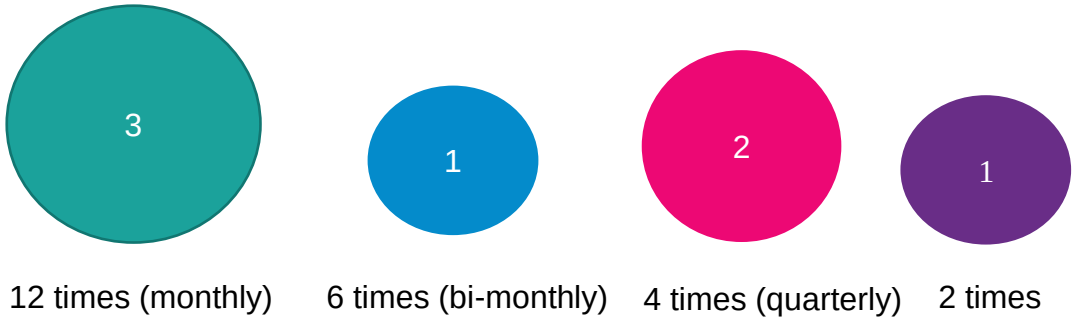


Figure 6 - Frequency of security governance meetings

Ten of the organisations **align security with the risk team**, detail of this was provided by 8 of the respondents; below is a summary of these responses.

"The IT Chief Risk Officer has dual reporting to the Group CIO and Group CRO."

"Security governance is a sub-committee to the Operational Risk Committee; the risk management team attend all meetings. A working group is also established across Security, Risk, and Legal to work on awareness and shared responsibilities e.g. privacy."

"Risk office has representation in the ISM Forum meeting, and all IT risk and exceptions are channelled to the Risk office."

"The Info Sec Committee Reports to Board Risk and 2 Risk staff sit on the Info Sec Committee."

"Risk team determines measurables, business impacts etc that determine actions."

"Security reports into the Technology Risk Office; strategy and risk are aligned through the executive sponsor group."

"Security > DRC > ERC > RMC."

Eight of the organisations **align security with the legal team**, 6 provided detail of this; below is a summary of these responses.

"Legal is included in Security governance meetings, and the working group for awareness and privacy. Engagement across contracting and third-party risk is also a key engagement between these two teams."

"Legal lead on regulatory privacy issues and co-chair the Group Privacy and InfoSec Governance Committee."

“Security and legal are part of the same department.”

“All contracts, SLA, MSA are run through with legal team before engaging third party vendor.”

“Security and legal are aligned through defined reporting channels and processes.”

“Security > Head of Privacy > Sr. Exec LGRA.”

3. Protect

The Protect Function outlines appropriate safeguards to ensure delivery of critical infrastructure services and supports the ability to limit or contain the impact of a potential cybersecurity event. The survey included various questions on measures taken by organisations to protect against cyber threats such as staffing, investment and the implementation of key controls, standards and frameworks.

Figure 7 presents the number of dedicated (full-time) security staff and (full-time) security contractors in each organisation, which were reported as intervals i.e. 0, 1-5, 6-10, 11-20 and 50+.

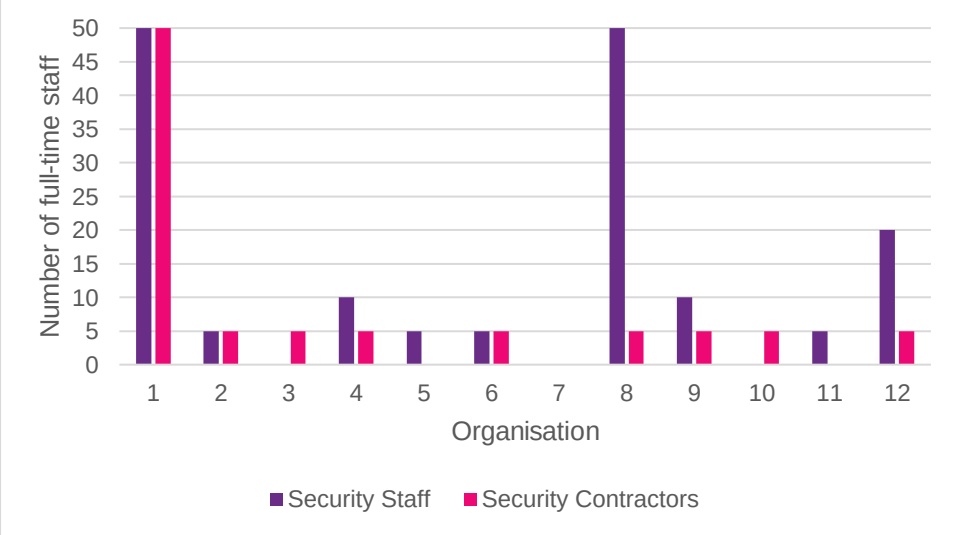


Figure 7 - Number of full-time security staff and contractors

Seven organisations reported the use of office-based, remote and off-shore contractors with the following percentage splits shown in Figure 8.

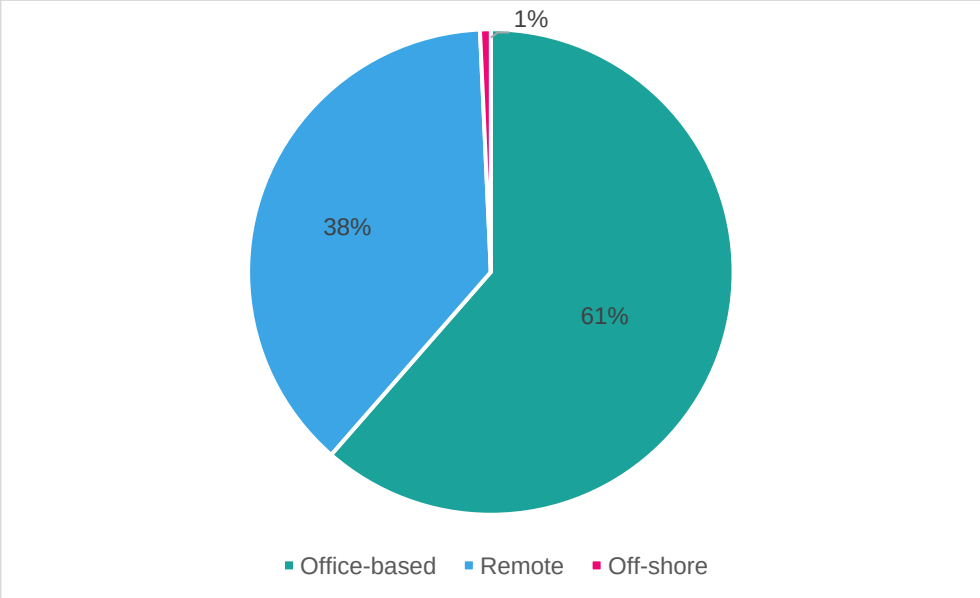


Figure 8 - Split of contractor workers

Three of these organisations reported 100% office-based; 2 reported 100% remote; 1 reported a 50/50 split between office-based and remote; and 1 reported a split of 80%/15%/5% of office-based, remote and off-shore, respectively.

Figures for operational expenditure on security and Capital Investment in security were reported by 7 organisations and are summarised in Table 2.

Table 2 - Summary of expenditure

	Minimum	Maximum	Total	Average
Operational expenditure on security (USD)	$20,000	$120,000,000	$47,905,000	$6,843,571
Capital Investment in security (USD) for the last two years	$0	$150,000,000	$203,260,000	$29,037,143

Figure 9 displays the overall percentage of investment in each of the threat vectors by 10 of the organisations, this data is reported at a disaggregated level in Appendix A. Two organisations reported for 'Other' but did not provide detail. Of the 10 that provided responses, 50% invest in all 8 of the threat vectors. The minimum number of threat vectors invested in by an organisation is 5. The threat vector invested in by the greatest number of organisations is Phishing (10). The threat vector with the highest variance between organisations is vulnerability exploit, where the minimum percentage of overall investment is 0% and the maximum is 50%. Table 3 provides a summary of the data.

Figure 10 presents the key controls used by organisations to protect cloud data, with missing data from 1 organisation. 'Identify and access management' is used by all organisations. None of the organisations use all 12 key controls. The key controls used the least are 'Micro segmentation' and 'Software as code'. Figure 11 displays the standards and frameworks used by the organisations, Fed RAMP, HITRUST, NERC SIP, NZISM are used by none of the organisations. Six of the organisations reported being certified or compliant with the following:

APRA (2)
Australian ISM (3)
COBIT,
CPS 234
GDPR (2)
HIPPA
ISO27001 (3)
MAR
NIST
PCIDSS (2)
Sarbanes-Oxley
SOC 2
SOX

Table 3 - Investment in threat vectors

Threat Vector	Number of organisations investing	Minimum % of overall investment	Maximum % of overall investment	Mode % of overall investment

Insider threat (human error, malicious employee)	9	0%	20%	10% (5)
Denial of service (DDoS, network/application/low and slow)	8	0%	20%	0%, 10% (3)
Privilege escalation (credential harvesting)	8	0%	30%	0%, 10%, 20% (3)
Vulnerability exploit (published vulnerability)	9	0%	50%	20% (3)
Phishing (including vishing, speak phishing, pharming)	10	10%	20%	10% (4)
Malware (drive-by-download)	8	0%	20%	0%, 15% (3)
Devices and things (USB, CD, IoT device, CCTV etc)	8	0%	25%	10% (4)
Third party threats (service provider security exposure)	9	0%	25%	10% (6)

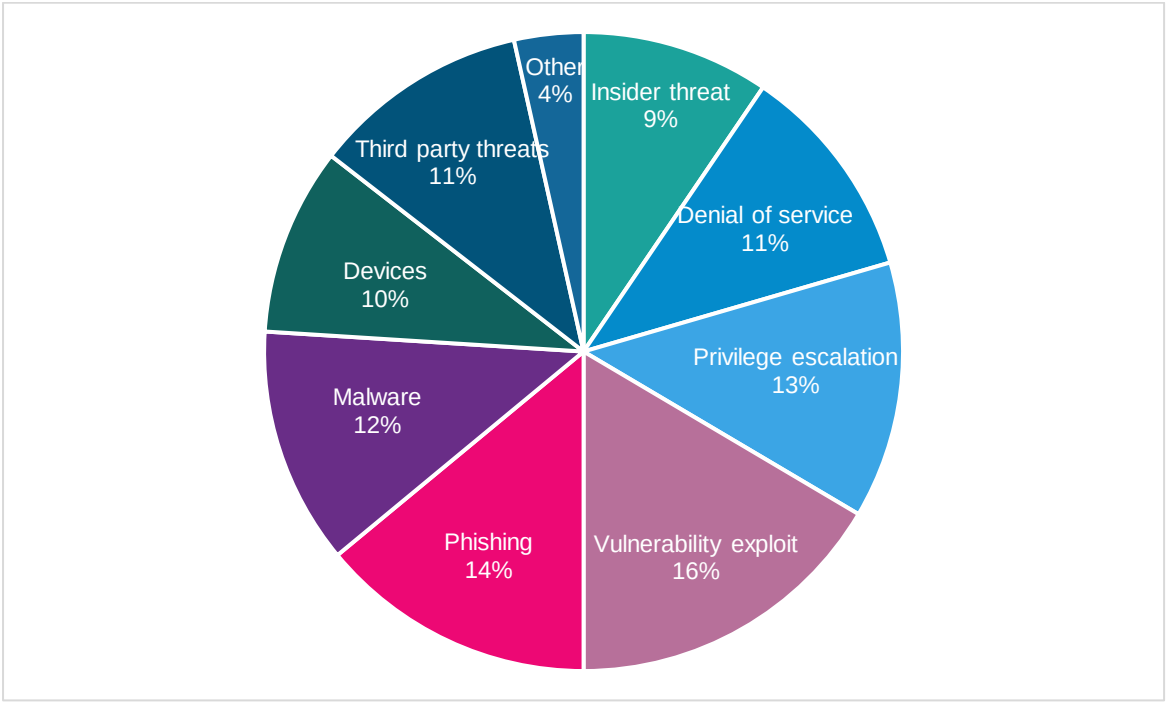


Figure 9 - Overall percentage of investment in each threat vector

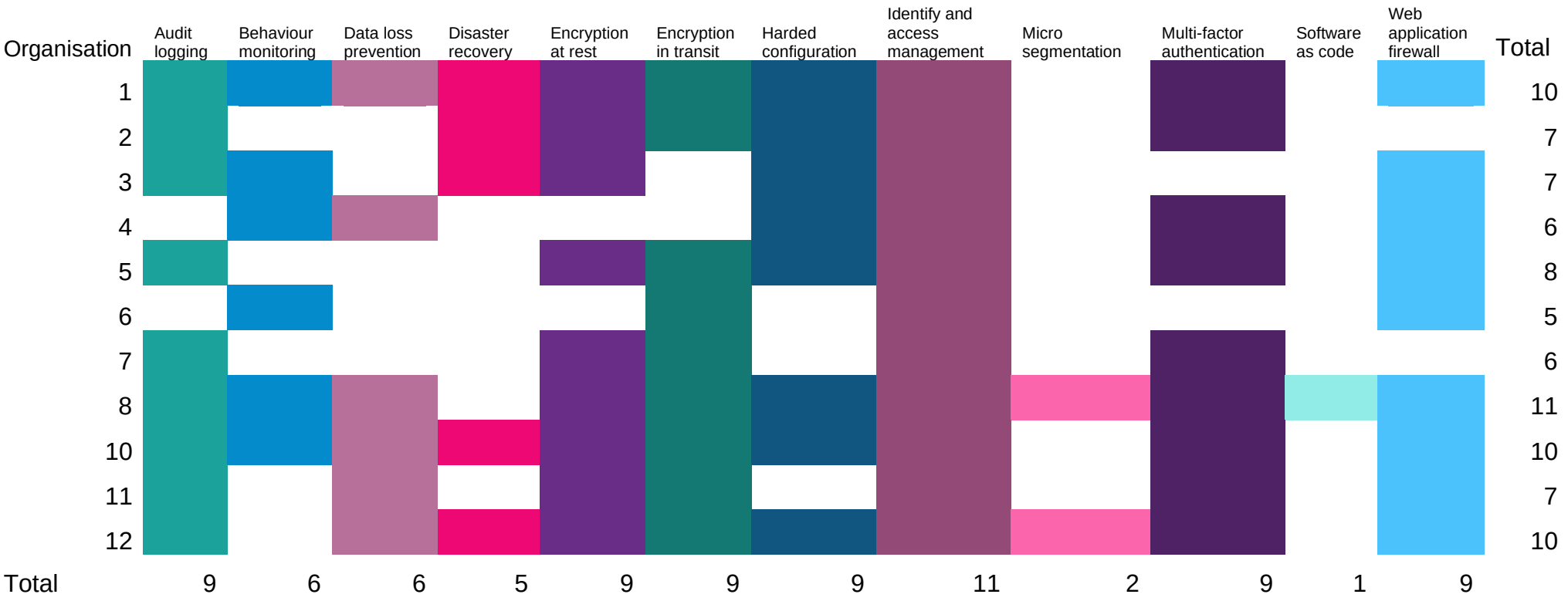


Figure 10 - Key controls used to protect cloud data

Missing data from 1 organisation.

Figure 11 - Standards and frameworks used

.

Eleven organisations provided information on the endpoint solutions that they use: 5 organisations implement 1 solution, 5 organisations implement 3 solutions, 1 organisation implements 4 and 1 organisation implements 2. Microsoft and Trend Micro are the most popular endpoint solutions, implemented by 5 and 4 organisations, respectively. A summary of the reported endpoint solutions is provided below[3]:

AirWatch (1)
VMware AirWatch provides technologies that help IT administrators deploy, secure and manage mobile devices, applications and data, as well as Windows 10 and Apple Mac computers. These products work thanks to a combination of an app installed directly on the endpoint device -- called the AirWatch Agent -- and back-end software that allows IT to set and enforce policies.

Carbon Black (2)
Carbon Black Predictive Security Cloud platform is a cloud-native endpoint protection platform designed to protect against the most advanced threats.

Cylance (1)
The Cylance AI Platform is a cybersecurity suite that protects the complete attack surface with automated threat prevention, detection, and response capabilities.

Force Point (3)
Forcepoint is driven by an understanding of human behaviour and intent. It's built with innovative technology, decades of experience and a clear vision to help solve critical security issues to protect employees, business data and IP. It offers a systems-oriented approach to insider threat detection and analytics, cloud-based user and application protection, next-gen network protection, data security and systems visibility.

McAfee (3)
McAfee products are designed and built to work together. The new McAfee Endpoint Security integrates threat prevention, web control, and a firewall, along with machine learning and advanced threat containment and correction, to stop the spread of malware.

[3] Logos and descriptions are taken from the respective organisations' websites, sources reported in References.

Microsoft (5)

Palo Alto Traps (2)

Palo Alto Networks Traps™ endpoint protection and response stops threats on endpoints and coordinates enforcement with network and cloud security to prevent successful cyberattacks. It is a Cloud-based endpoint security service.

Sophos (1)

Sophos Intercept X employs a comprehensive defence-in-depth approach to endpoint protection rather than simply relying on one primary security technique. Intercept X integrates the industry's top-rated malware detection and exploit protection with built-in endpoint detection and response.

Trend Micro (4)

Trend Micro uses advanced AI learning to stop ransomware. It also protects against malware, online banking and shopping threats and much more. Top rated by industry experts and award-winning, Trend Micro Security delivers 100% protection against web threats.

Webroot (1)

Webroot, a Carbonite company, harnesses the cloud and machine learning to reliably predict and protect against cyberattacks in real time. Webroot secures businesses and consumers worldwide with endpoint and network protection, security awareness training and threat intelligence services.

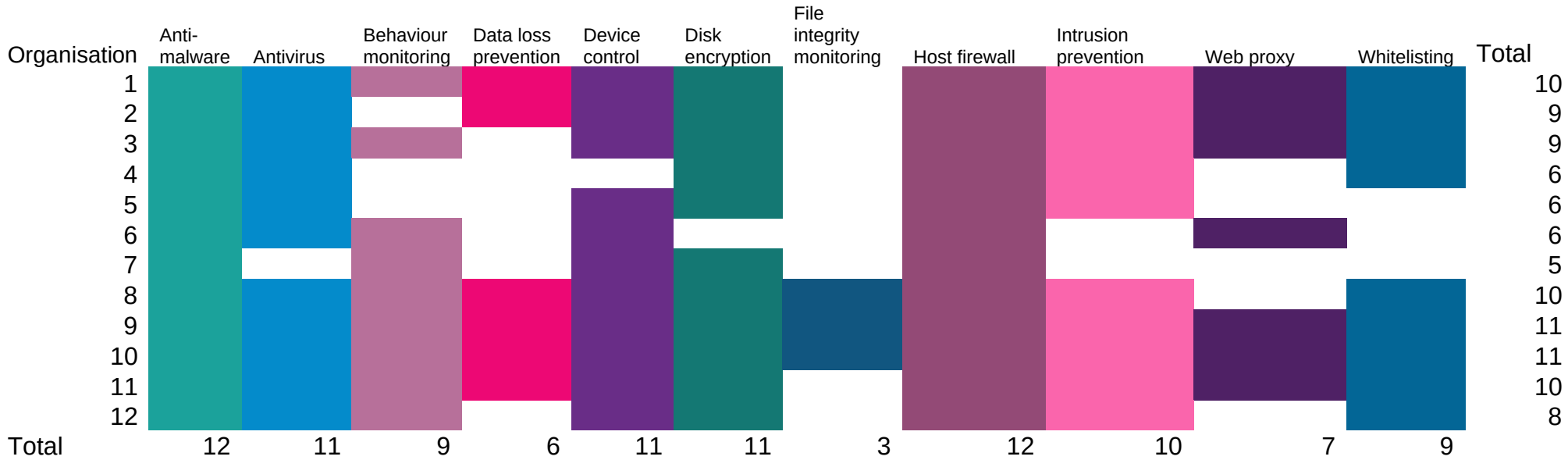


Figure 12 - Endpoint controls

Figure 12 displays the endpoint controls implemented by the organisations. 2 organisations using all endpoint controls.

The survey required respondents to report on the type of SOC/SIEM service they use; detail of this is shown in Figure 13 and Figure 14 with a summary provided in Table 4. The average rating for outsourced services, blended services and insourced services were 6.8, 7.3 and 6.5, respectively.

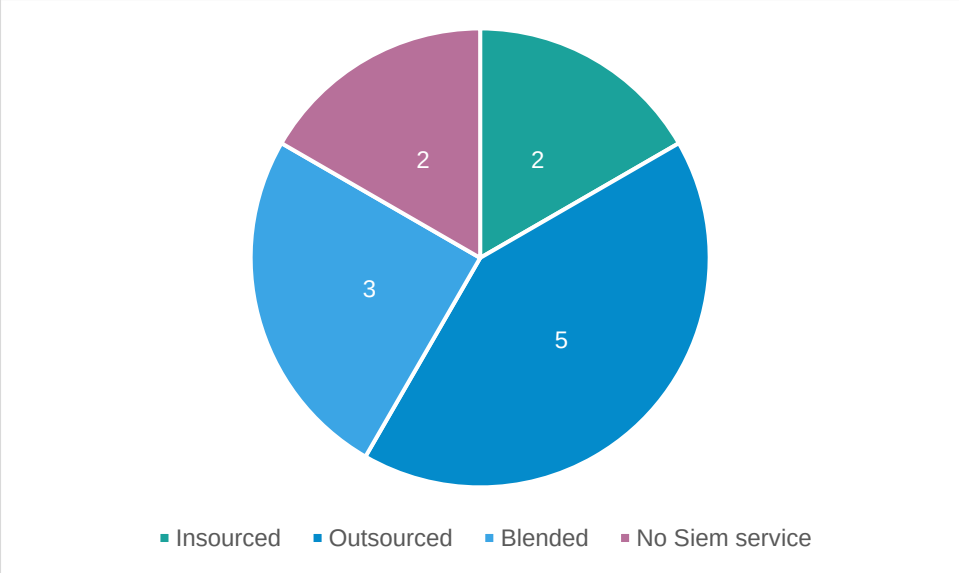


Figure 13 - Type of SOC/SIEM service

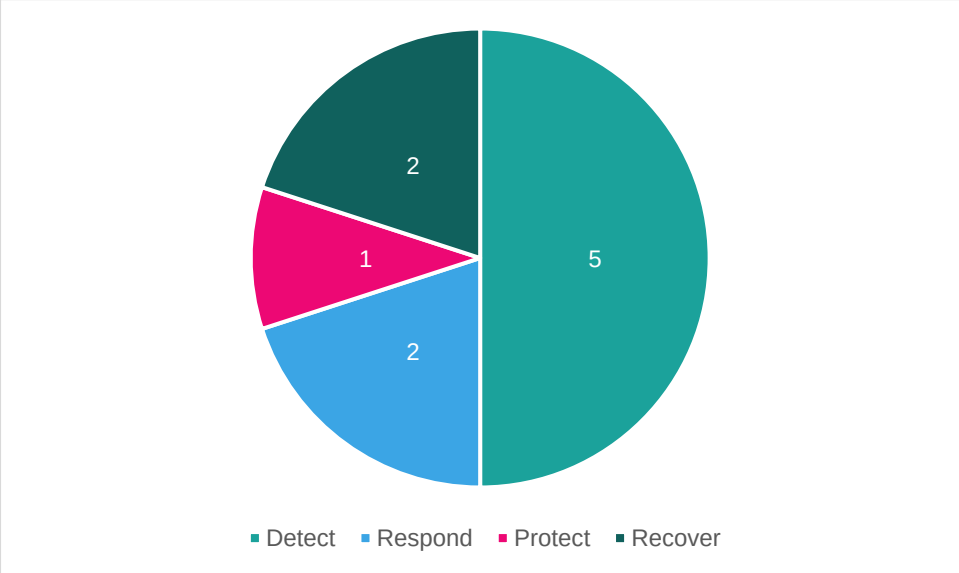


Figure 14 - Level of service

Table 4 - Summary of SOC/SIEM services

Service	Number of organisations	Rating(s)
Blended-detect	2	7, 9
Blended-recover	1	6
Insourced-recover	1	5
Insourced-respond	1	8
Outsourced-detect	3	7, 8, 8
Outsourced-protect	1	10
Outsourced-respond	1	1

4. Detect

Respondents were asked to specify the number of low, medium and high security incidents that had occurred in the last year, which is shown in Figure 15. There is missing data from 1 organisation and one organisation reported to not having experienced any security incidents. The majority of security incidents were low, with 5 organisations reporting 10+ low incidents and only 5 organisations experienced high security incidents.

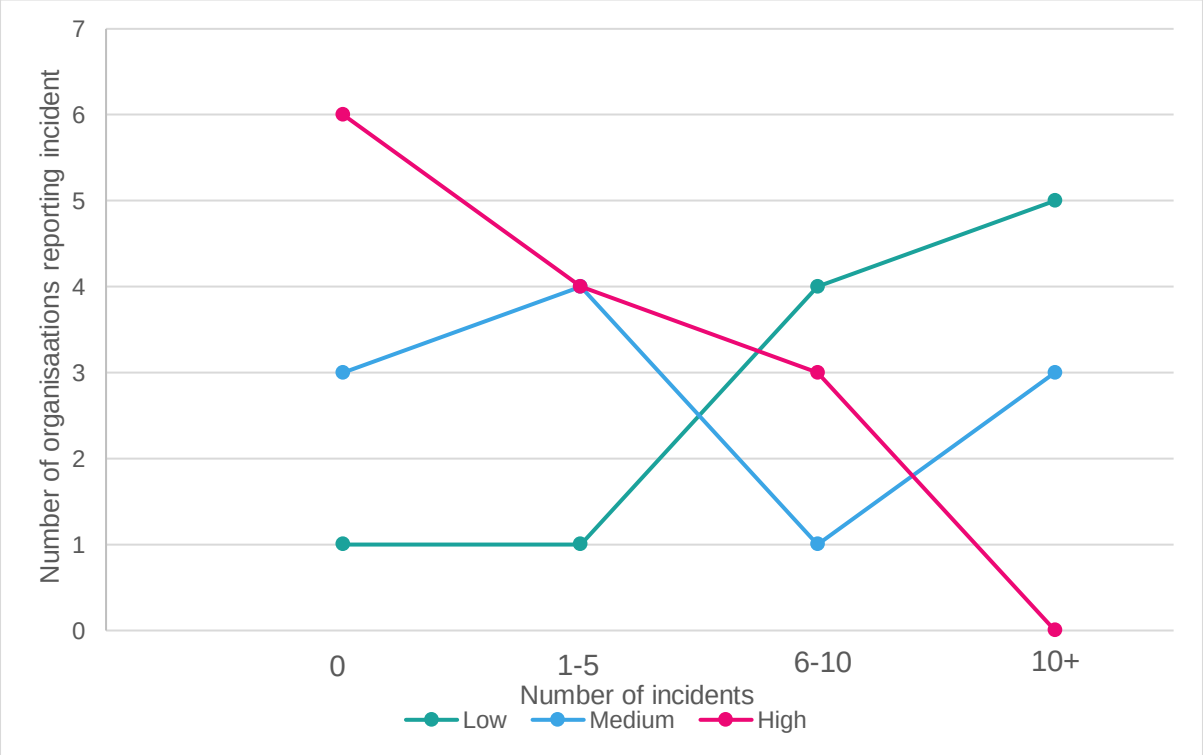


Figure 15 - Number of security incidents

Information regarding the number of security incidents by threat vector is displayed in Figure 16. The most frequent type of incident is phishing whereas devices is the least frequent. Additional threats were reported: backup tapes missing (1-5), imposter domain detection and takedown, and credential dump identification and password (both at 10+).

Figure 17 depicts the total number of security incidents by threat vector. The total has been calculated by taking the midpoint of the intervals multiplied by the frequency. This is, therefore, an estimate (likely to be higher due to reporting of 10+ incidents) but gives an idea of the relative number of incidents.

Part of the purpose of the detect function is to define appropriate activities to identify the occurrence of a cybersecurity event. Such activities are incident response planning and incident response testing. Ten organisations do both activities, 1 organisation does incident response planning, but not incident response testing, and 1 organisation does neither.

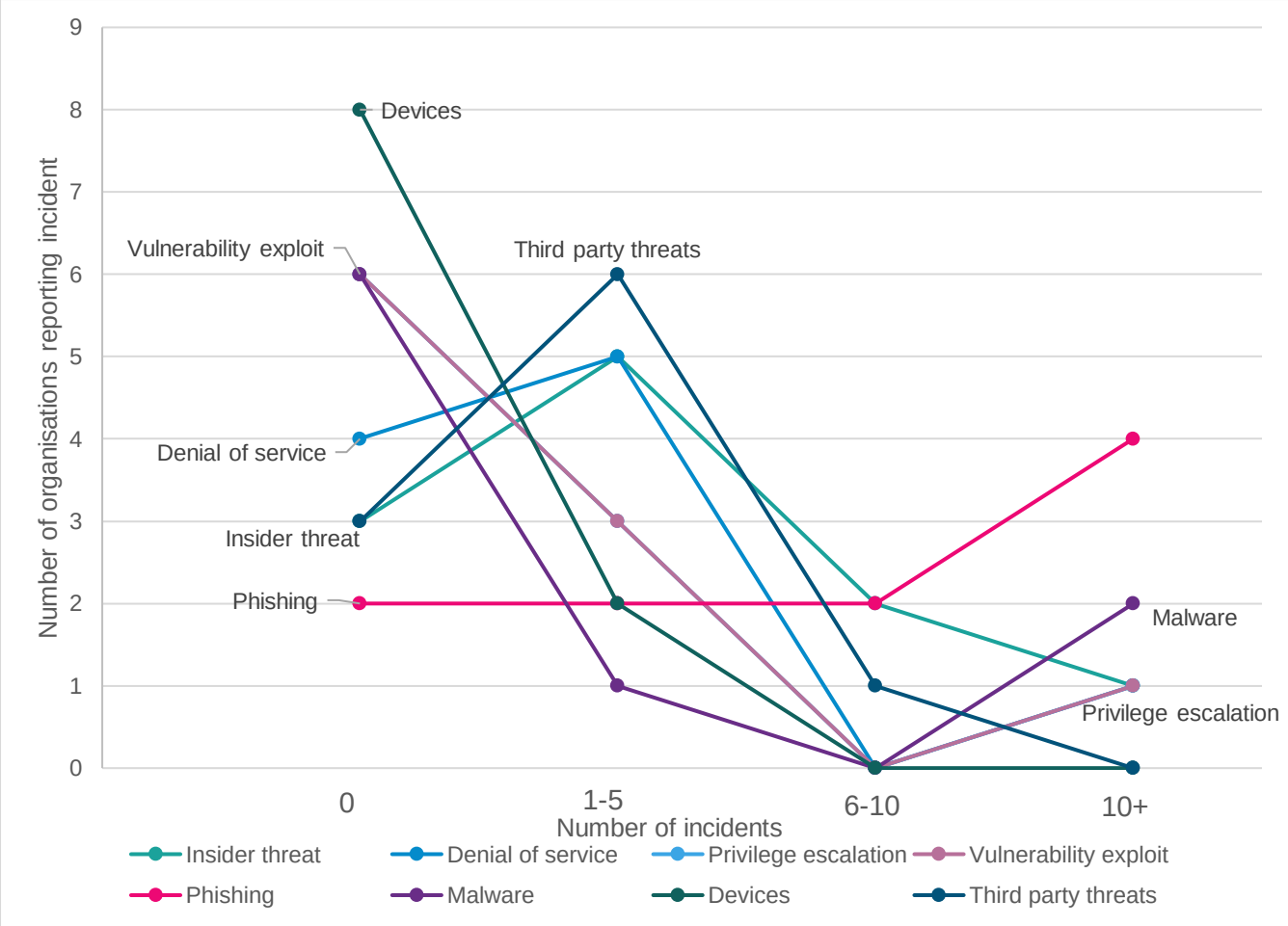


Figure 16 - Number of security incidents per threat vector

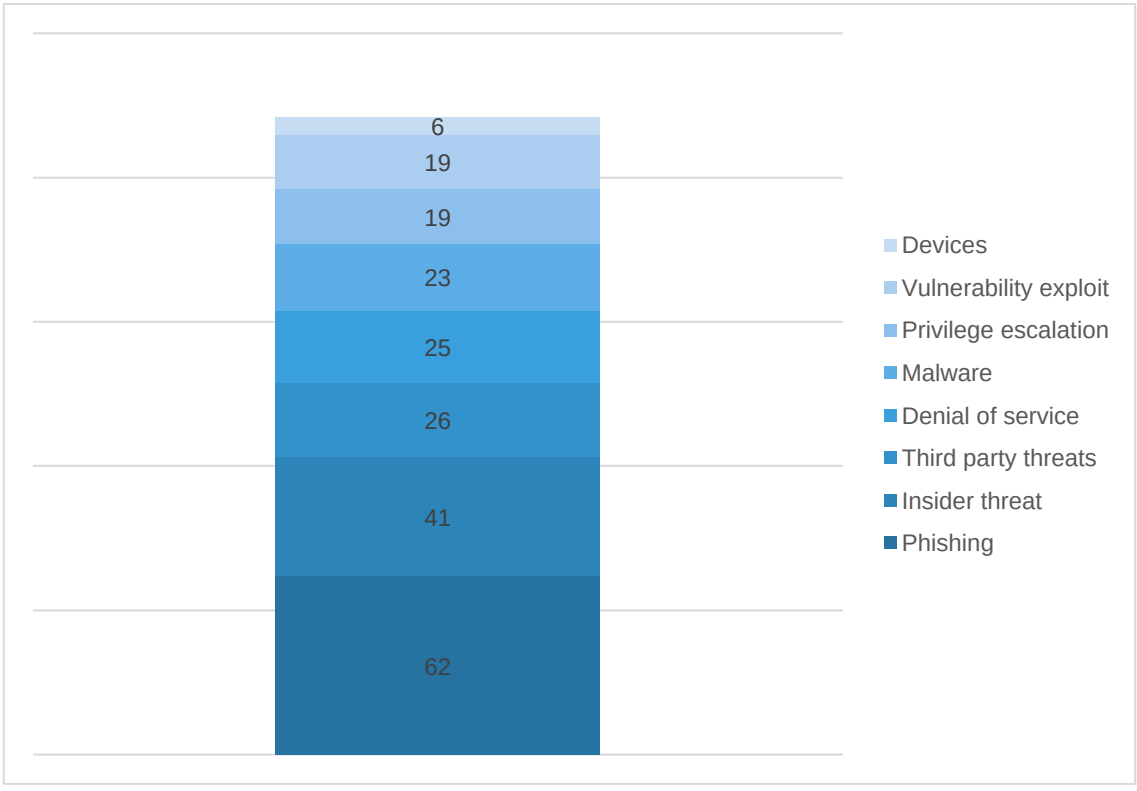


Figure 17 - Estimated total number of security incidents per threat vector

5. Respond

The Respond Function includes appropriate activities to take action regarding a detected cybersecurity incident. Ten of the organisations test crisis management in relation to breach of information. Only 1 of the organisations does not report incidents at the executive level.

With regard to reporting incidents at the executive level respondents reported the following:

“Through the Information Security and Privacy Committee and if required escalated to the Executive Risk Committee.”

“Incidents are reported through the Operational Risk monthly meetings.”

“I have a direct report obligation to the CRO (chief revenue officer).”

“Only Critical or high security incident, incident process is followed, with escalation to crisis management as required.”

“Through Info Sec Reporting - fed up to Exec and Risk committees.”

“All incidents over a certain risk impact level are reported to Exec and Board.”

“They are reported on a monthly basis inside the Technology Risk Office and on a quarterly basis through the CIO dashboard. In addition, individual incidents are reviewed with our executive steering committee - a cross-organizational group of business leaders - and at our executive sponsor group - a group of C-level officers including our CEO - on a monthly basis. Finally, we review incident reporting with the board of directors on at least an annual basis.”

“Team > CISO (chief information security officer) > CIO (chief information officer|) (as required).”

Figure 18 displays those that are included in the incident response planning and testing. Risk managers, IT incident management and security analyst were reported by 10 organisations. Level 2 IT technical, IT support partners and executives were reported by 9 organisations. Level 3 IT technical, IT vendors and internal comms teams were reported by 8 organisations. Level 1 IT services desks and PR and media team were reported by 7 organisations. Finally, IT security consultants and legal were reported the least, by 6 organisations. None of the organisations include all 14 options in incident response planning and testing, however, 2 include 13, and 2 include 11.

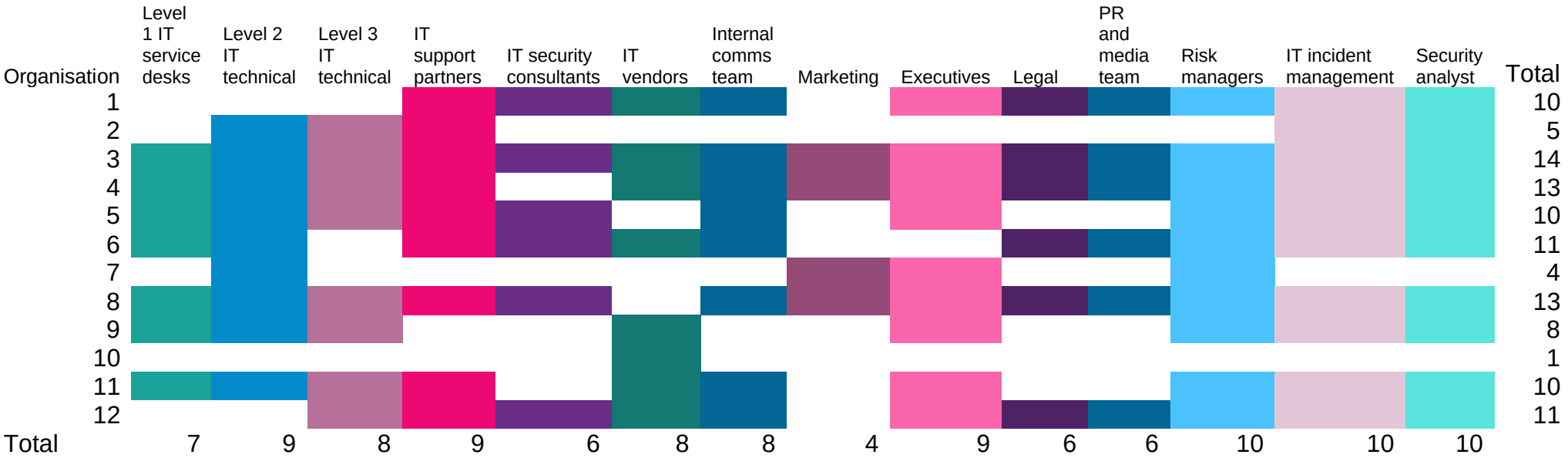


Figure 18 - Departments involved in response planning and testing

6. Recover

The Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. Of the 12 organisations surveyed, 4 are without cyber insurance.

When asked about the timeframe to recover impaired capabilities due to experiencing a breach, only 5 answers were provided, potentially suggesting that the reaming 7 organisations have not experienced a breach.

In general, the time taken to respond to an incident depends on the type of incident; the range being from an immediate response to up to 2 weeks.

For one organisation, a breach takes around three days of effort for the team to trace, respond and close. Another reported that depending on the service impaired it would take 24 hours (e.g. for the core membership app) to 1-2 weeks (e.g. for email). Another is regulated by APRA, and for material affected to be reported no later than 72 hours, and 10 business days if aware of a material IS control weakness which the entity expects to take more time to remediate. Finally, one organisation has a total data protection and business continuity solution to a response is made immediately.

7. Future Threats

The survey required respondents to report on what they perceived to be the biggest threats in healthcare cyber security. The responses are given in Table 5 and have been categorised as internal and external threats.

Table 5 - Perceived biggest threats healthcare cyber security

Internal	External
• Insider threat • Internal staff error in management of information • Legacy systems entering end-of-life support and the ability to secure these systems effectively • Data breach • Compromise or loss of member information due to unmanaged attack surface, privilege management, data security and visibility of the network • Inadvertent disclosure of sensitive data • Insider threat due to misconfiguration and lack of understanding of cloud services • Not managing third party IT providers • Control of access to health information	• Responsible for hosting very personal data and likely to become more of a targeted business • Claim fraud • Supply chain assessment/auditing/management/communication • Credential theft • Phishing • Malware (ransomware) • Configuration error • Data theft • DDOS (Distributed Denial of Service) • Cloud threats with unencrypted data • Sharing of health information

Finally, respondents were asked to report the likelihood of a minor or major breach occurring within the next 12 months, the responses are shown in Figure 19 and there is missing data from 2 organisations. The consensus is that a major breach is unlikely whereas there is more of a likelihood of a minor breach occurring. One organisation noted that it is difficult to detect a breach and once it is detected it is difficult to give a definition (in terms of minor or major).

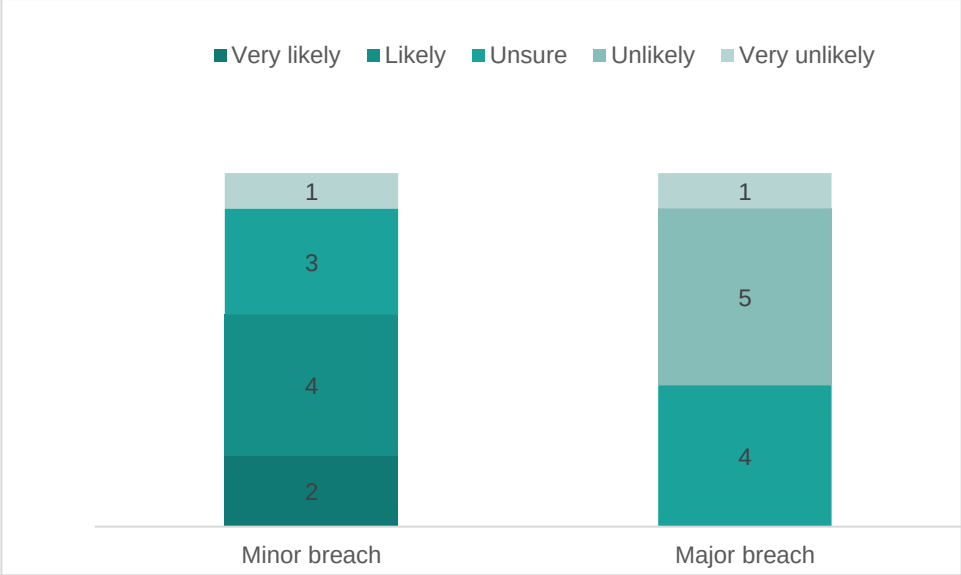


Figure 19 - Likelihood of minor and major breaches

References

Air Watch. 2019. Capabilities. [ONLINE] Available at: https://www.air-watch.com/capabilities/mobile-security. [Accessed 20 September 2019].

Carbon Black. 2019. [ONLINE] Available at: https://www.carbonblack.com. [Accessed 20 September 2019].

CISecurity. 2019. Controls. [ONLINE] Available at: https://www.cisecurity.org/controls/. [Accessed 20 September 2019].

Cylance. 2019. [ONLINE] Available at: https://www.cylance.com/en-us/index.html. [Accessed 20 September 2019].

Force Point. 2019. Cylance. [ONLINE] Available at: https://www.forcepoint.com. [Accessed 20 September 2019].

ISO. 2019. Information Security. [ONLINE] Available at: https://www.iso.org/isoiec-27001-information-security.html. [Accessed 20 September 2019].

McAfee. 2019. Products. [ONLINE] Available at: https://www.mcafee.com/enterprise/en-gb/products.html. [Accessed 20 September 2019].

Microsoft. 2019. [ONLINE] Available at: https://microsoft.com. [Accessed 20 September 2019].

NIST. 2019. Cyber Framework. [ONLINE] Available at: https://www.nist.gov/cyberframework. [Accessed 20 September 2019].

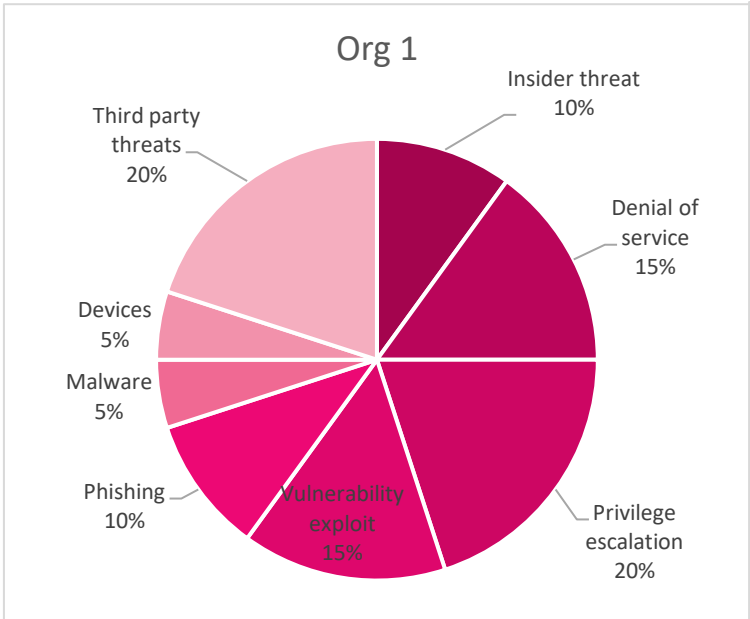
Palo Alto Networks. 2019. Products. [ONLINE] Available at: https://www.paloaltonetworks.com/products/secure-the-endpoint/traps. [Accessed 20 September 2019].

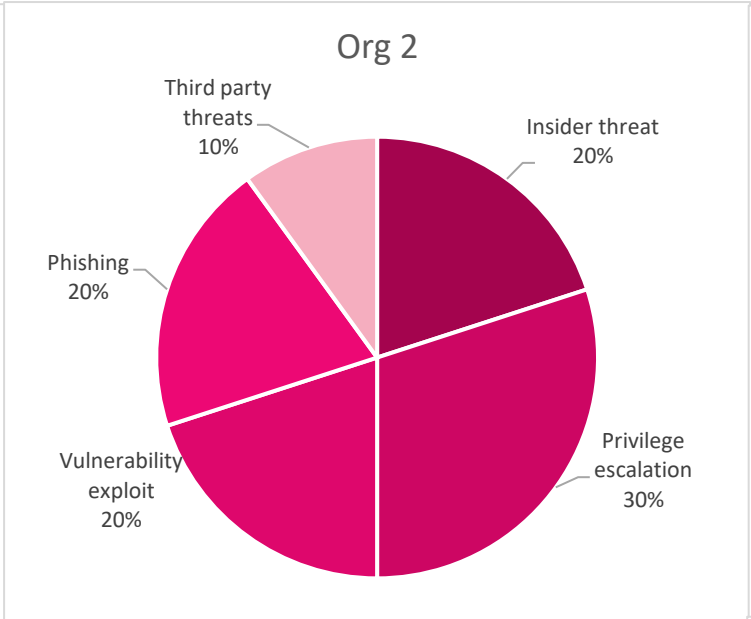
Search Mobile Computing. 2019. VMware-AirWatch. [ONLINE] Available at: https://searchmobilecomputing.techtarget.com/definition/VMware-AirWatch. [Accessed 20 September 2019].

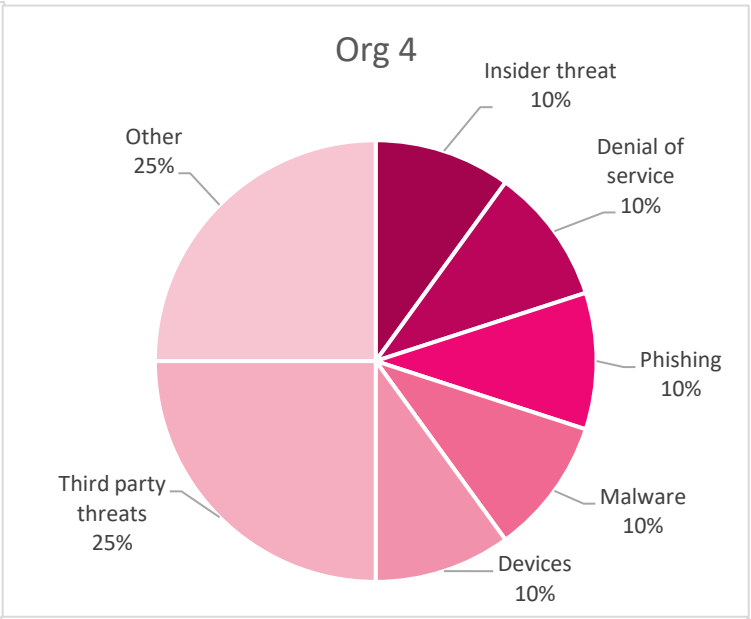
Sophos. 2019. [ONLINE] Available at: https://www.sophos.com/en-us.aspx. [Accessed 20 September 2019].

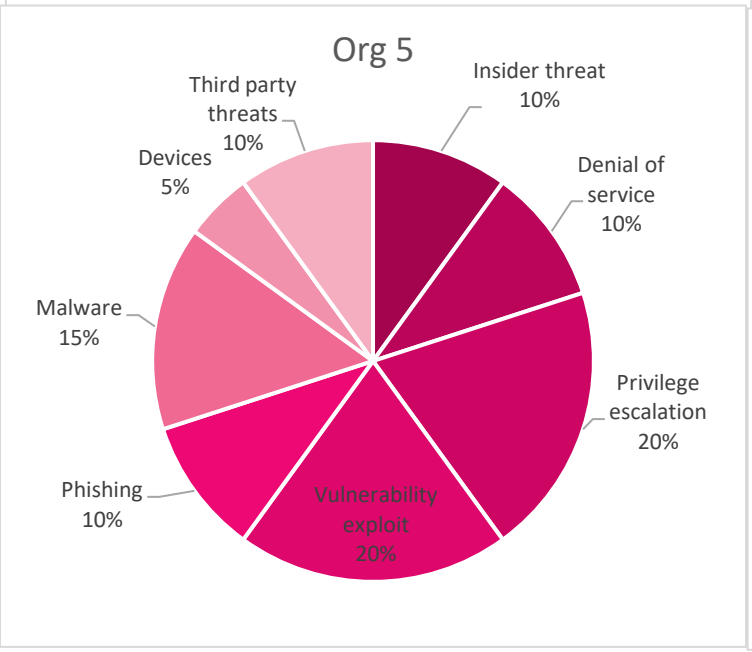
TrendMicro. 2019. [ONLINE] Available at: https://www.trendmicro.com/. [Accessed 20 September 2019].

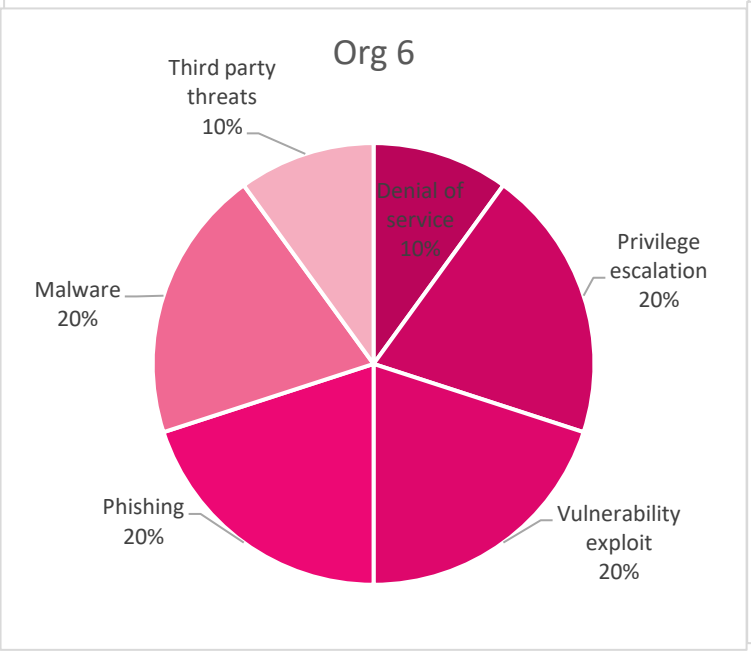
Appendix A – Investment in threat vector per organisation

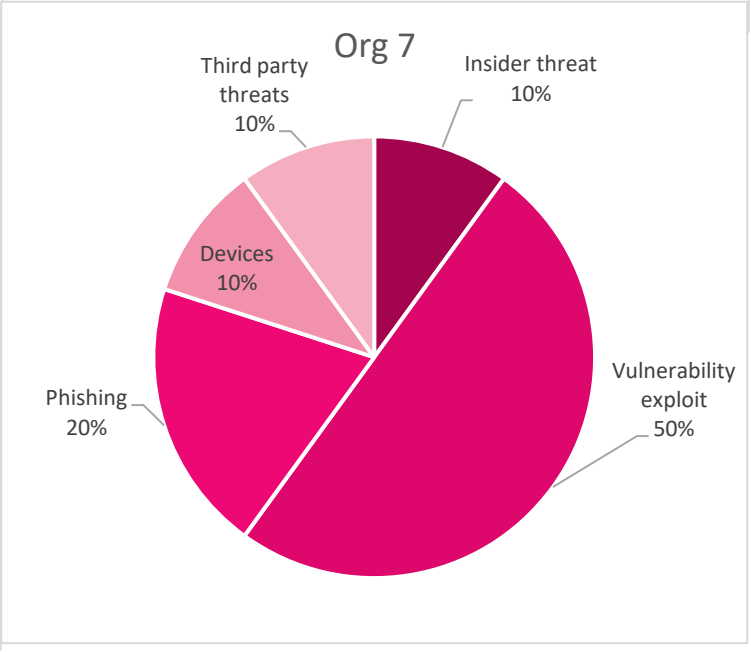


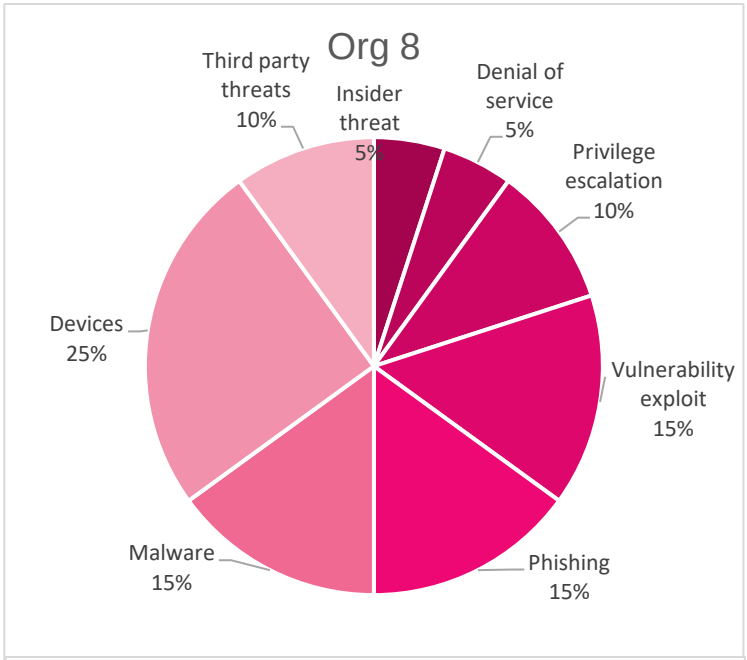


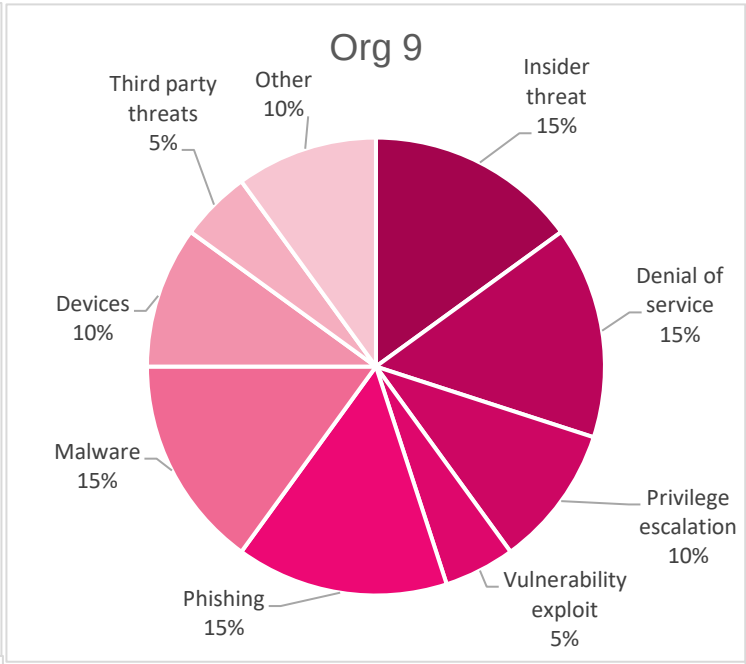


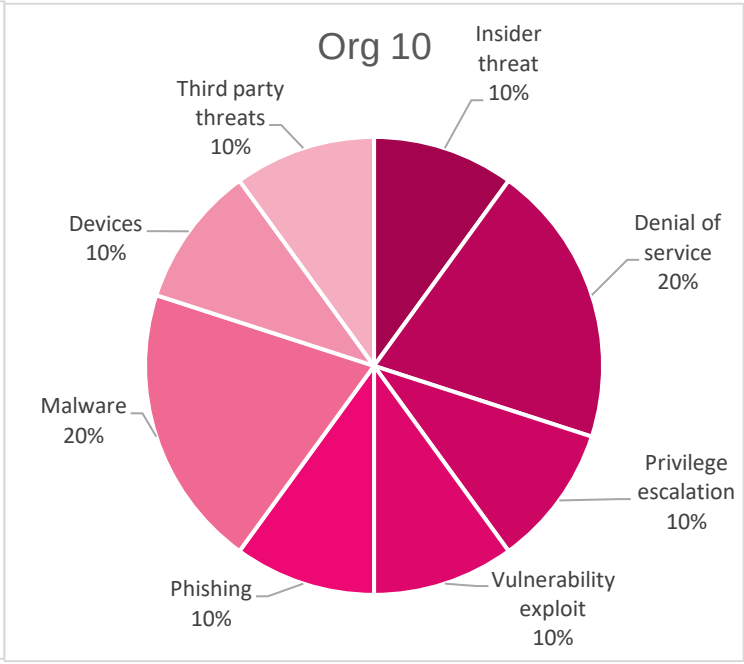


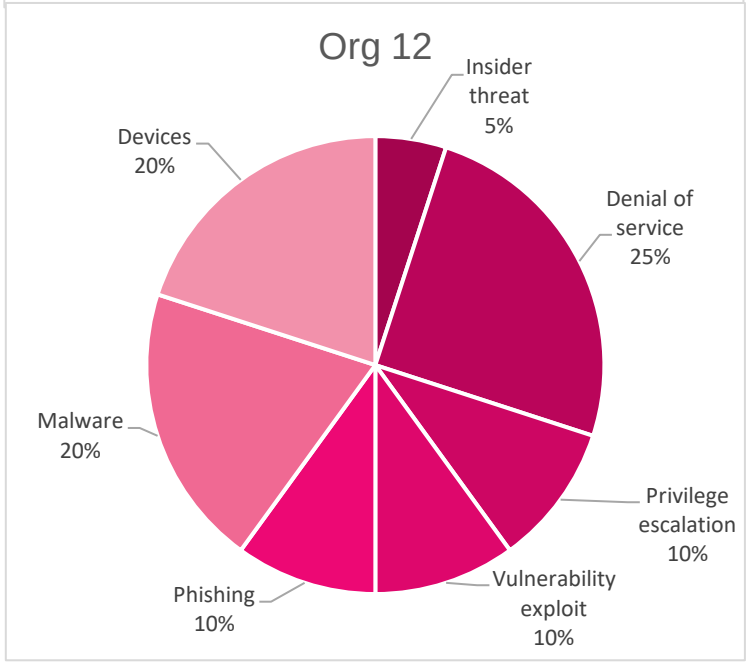





Org 8
Third party threats 10%
Insider threat 5%
Denial of service 5%
Privilege escalation 10%
Vulnerability exploit 15%
Phishing 15%
Malware 15%
Devices 25%


Org 9
Third party threats 5%
Other 10%
Insider threat 15%
Denial of service 15%
Privilege escalation 10%
Vulnerability exploit 5%
Phishing 15%
Malware 15%
Devices 10%


Org 10
Third party threats 10%
Insider threat 10%
Denial of service 20%
Privilege escalation 10%
Vulnerability exploit 10%
Phishing 10%
Malware 20%
Devices 10%


Org 12
Insider threat 5%
Denial of service 25%
Privilege escalation 10%
Vulnerability exploit 10%
Phishing 10%
Malware 20%
Devices 20%