Cybersecurity – Plugging the hole

Through testing, policies and training

October 2023

pwc

CHARTERED GOVERNANCE Hong Kong

Table of contents

Foreword	2
Acknowledgements	4
About the contributing editor and author	5
Executive Summary	6
Part 1 – Plugging the hole	8
Part 2 – Survey Results	20
About HKCGI	38
About PwC	39
Contacts	40

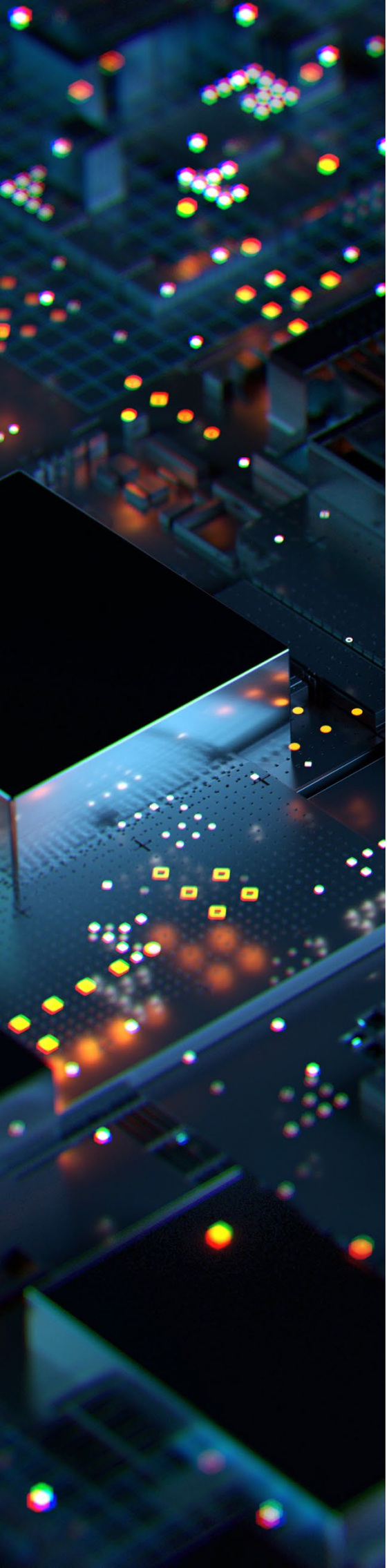
Foreword

In June 2023, PricewaterhouseCoopers Limited (PwC) Hong Kong and The Hong Kong Chartered Governance Institute (HKCGI) surveyed organisations' cybersecurity practices. The premise of the survey is that directors should be concerned with cybersecurity because breach poses serious dangers to their companies, including monetary loss, reputational harm, legal repercussions, and operational disruptions as part of risk management. There were over 1,400 responses to the survey, and an analysis shows that there are governance gaps from the cybersecurity perspective.

While there is no one-size fit all in manging cyber risks, directors and governance professionals should prioritise the following imperatives to strengthen their organisation's cybersecurity and navigate the dynamic digital ecosystem.

1. **Prioritise cybersecurity testing:** Regularly conduct comprehensive testing, which must be by qualified and accredited individuals and organisations, including red teaming exercise, penetration testing, vulnerability assessments, and social engineering simulations, to stop possible cyber threats from taking advantage of vulnerabilities, identify weak points and take proactive measures to fix them.

2. **Establish security policies and procedures:** To reduce potential vulnerabilities, develop and maintain current security policies, include security in the software development lifecycle, and promote secure coding practices.



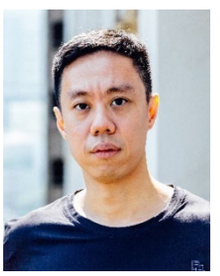
3. **Implement identity and access management (IAM) policies:** To manage access to sensitive data and systems, granting authorisation only to authorised employees.

4. **Monitor third-party cybersecurity risks:** To reduce risks related to external dependencies, assess and evaluate the cybersecurity measures of third-party vendors and partners, and implement effective third-party risk management procedures to protect the organisation's digital ecosystem.

5. **Invest in cybersecurity awareness training:** To promote a security-conscious culture, offer regular cybersecurity awareness training for stakeholders and employees. Inform them of the most recent online dangers and safe practices for protecting digital assets and data.

By following these imperatives, organisations may proactively secure important assets and reputations while reducing cyber threats in today's quickly evolving digital ecosystem.

Ernest Lee FCG HKFCG(PE)
President
The Hong Kong Chartered Governance Institute



Kok Tin Gan
Partner, Cybersecurity and Privacy
PwC Hong Kong

Acknowledgements

This research is supervised by the Institute's Technical Consultation Panel (TCP) with Mrs April Chan FCG HKFCG as Chairman. Mr Mohan Datwani FCG HKFCG(PE) Institute Deputy Chief Executive serves as secretary to the TCP and author of this research report. Mr KT Gan, Cybersecurity and Privacy Partner at PwC Hong Kong is contributing editor. The Institute expresses gratitude to Mr Ernest Lee FCG HKFCG(PE) Institute President and Ms Ellie Pang FCG HKFCG(PE) Institute Chief Executive for their contributions to the project. The Institute is also grateful to TCP members and Mr KT Gan.

About the contributing editor and author

Author

Mohan Datwani FCG HKFCG(PE)
Solicitor
LLB, LLM, MBA(Iowa)(with Distinction)
Deputy Chief Executive
The Hong Kong Chartered Governance Institute

Mohan Datwani is currently the Deputy Chief Executive of The Hong Kong Chartered Governance Institute (HKCGI), to represent Chartered Secretaries and Chartered Governance Professionals in Hong Kong and China.

In addition to his day-to-day managerial duties at HKCGI, Mr Datwani, a thought leader, develops practical advice and research to advance good governance. Additionally, as a member of the global governance profession, he collaborates with the Chartered Governance Institute, where HKCGI originates, on research projects and contributes to global thought leadership initiatives. To offer viewpoints on law, governance, and management in the public sector, Mr Datwani also served on many government boards. He was honoured as a Director of the Year (2018) by The Hong Kong Institute of Directors for his efforts with the Equal Opportunities Commission.

Contributor

Kok Tin Gan
Partner, PwC Hong Kong

Kok Tin is a Partner in PwC Hong Kong's Cybersecurity & Privacy practice with over 17 years of experience. Kok Tin is also the founder of PwC's Dark Lab, Hack A Day and Ethical Hack Bot. Kok Tin is currently the Vice Chairman of itSMF Hong Kong Chapter and the member of security committee of Fintech Association of Hong Kong.

Kok Tin's key areas of expertise and experience include Cybersecurity strategy, framework, IT security framework (ISO27001, NIST, Multi Level Protection), application security (OWASP, OWASP Mobile) and data security (e.g., PCI DSS), secure development life cycle, DevSecOps, Cloud security, IT risk, security / technology architecture and white hat hacking.

Kok Tin has co-authored a number of cybersecurity and technology risk related guidelines for the Regulators in the Asia Pacific Region.

Kok Tin has led ~300 small to large size of security assessment / transformation engagements and has worked across different continents including, Asia, America, Europe and Africa.

Kok Tin is a TED talk speaker and he also founded a dot.com company during his early days of his career.

Executive Summary

There were over 1,400 persons who responded to the survey (details set out under Part 2). The pertinent findings include:

- **Board participation in cybersecurity governance:** A sizable number of organisations reported only 'Little involvement' (32.63%) or 'Moderate level' (33.92%) of board participation in cybersecurity governance. This raises the possibility of a governance gap that boards may not be fully involved in monitoring cybersecurity measures.

- **How often should cybersecurity strategies be reviewed?** Around 36% of businesses said their boards evaluate their cybersecurity strategy 'Regularly' (at least annually). However, a sizable percentage of companies either have 'No review' (12.75%) or 'Infrequent review' (25.58%), which may point to a problem with regularly assessing and revising cybersecurity strategy.

- **Cybersecurity gaps:** Although more than 60% of businesses rank cybersecurity as a 'Moderate' (38.94%) or 'Top' (21.44%) priority, a sizeable portion (39.62%) either see it as 'Not a priority' (12.62%) or 'Little priority' (27.00%). This reveals a governance gap in recognising cybersecurity as a significant commercial risk.

- **Cybersecurity committees:** Only 21.51% of businesses claimed a specific cybersecurity committee with defined responsibilities and lines of authority. Most organisations either don't have one (72.45%) or have another committee with that responsibility (6.04%), which suggests a potential governance gap in establishing specialised oversight for cybersecurity.

- **Knowledge of online threats:** While some businesses have a 'Comprehensive understanding' (32.62%) or a 'General understanding' (49.17%) of the particular cyber threats they face, a sizable portion (18.21%) either do not know (10.11%) or is unsure (8.10%) about the cyber hazards they face. This suggests that there is a governance gap in terms of possible risk awareness and knowledge.

- **Cybersecurity team's confidence:** While 63.51% of organisations say they are 'Very confident' (15.24%) or 'Somewhat confident' (48.27%) in their cybersecurity teams, there is still a sizable portion (36.49%) that is either 'Not very confident' (22.99%), 'Not confident at all' (5.47%), or 'Not sure' (8.03%). This might point to a governance flaw in providing cybersecurity knowledge and assistance.

- **Education and training:** Most directors (56.74%) receive 'Occasional' training on cybersecurity awareness, although a sizeable portion (27.24%) receive 'None.' This indicates the lack of consistent and thorough cybersecurity training for directors.

- **Testing and assessment frequency:** Organisations differ greatly in how frequently they do penetration tests, vulnerability scans, social engineering tests, and other cybersecurity testing and assessments. Some people engage in these activities regularly, whereas others do so infrequently or on an as-needed basis (details set out under Part 2). This suggests that putting into practice standardised and systematic testing practices may have governance deficiencies.

- **Cyber insurance protection:** Despite 20.04% of businesses having cyber insurance, a sizable portion (47.89%) are 'Not sure' regarding its availability or scope. This indicates a governance flaw in assessing and obtaining the proper cyber insurance to reduce potential financial damages.

- **Compromises in cybersecurity:** 52.59% of organisations are unsure about whether there were cybersecurity compromises, which affected approximately 18.09%. The existence of prior occurrences and uncertainty highlights ineffective governance in identifying and remediating cybersecurity breaches.

The survey results point to governance flaws in organisations' cybersecurity practices, including a lack of board involvement, infrequent plan reviews, and different degrees of awareness and training. These holes must be filled to improve overall cybersecurity and safeguard organisations from cyber threats.

Imperatives to improve cybersecurity

While there is no one-size fit in managing manging cyber risks, directors and governance professionals may improve their organisation's cybersecurity, proactively minimise cyber risks, and protect crucial assets and reputations in today's rapidly changing digital ecosystem by concentrating on the following five imperatives.

1. **Prioritise cybersecurity testing:** Regularly conduct comprehensive testing, which must be by qualified and accredited individuals and organisations, including red teaming exercise, penetration testing, vulnerability assessments, and social engineering simulations, to stop possible cyber threats from taking advantage of vulnerabilities, identify weak points and take proactive measures to fix them.

2. **Establish security policies and procedures:** To reduce potential vulnerabilities, develop and maintain current security policies, include security in the software development lifecycle, and promote secure coding practices.

3. **Implement identity and access management (IAM) policies:** To manage access to sensitive data and systems, granting authorisation only to authorised employees.

4. **Monitor third-party cybersecurity risks:** To reduce risks related to external dependencies, assess and evaluate the cybersecurity measures of third-party vendors and partners, and implement effective third-party risk management procedures to protect the organisation's digital ecosystem.

5. **Invest in cybersecurity awareness training:** To promote a security-conscious culture, offer regular cybersecurity awareness training for stakeholders and employees. Inform them of the most recent online dangers and safe practices for protecting digital assets and data.

Part 1

Plugging the hole

1.1 Overview

Cybersecurity aims to prevent malicious activities that could jeopardise computer systems' confidentiality, integrity, and availability from entering computer networks, devices, and digital data. Identifying and counteracting cyber threats, including viruses, malware, hacking, phishing, and social engineering and maintaining the resilience and continuity of digital activities require using various technologies, processes, and best practices. To prevent financial loss, reputational damage, legal consequences, and operational disruptions, directors must take into account at least some or all of the security procedures listed below:

- Incorporate security into the software development lifecycle, from design to testing to deployment, to ensure that applications are secure by default.
- Develop and enforce strong identity and access management policies and procedures to ensure that only authorised users can access sensitive data and systems and adhere to the principle of least privilege (an information security concept which maintains that a user or entity should only have access to the specific data, resources and applications needed to complete a required task).
- Implement regular red teaming exercise, vulnerability assessments and penetration testing to identify and remediate security vulnerabilities in your organisation's systems and applications.
- Use security information and event management (SIEM) tools to monitor and detect potential cybersecurity incidents in real-time.
- Regularly review and update your organisation's security policies and procedures to ensure they are up-to-date and effective.
- Use secure coding practices and conduct code reviews to minimise the risk of vulnerabilities in applications and systems.
- Implement a data backup and recovery plan to ensure that critical data can be restored during a cybersecurity incident.

- Establish a cybersecurity incident response plan that outlines roles and responsibilities, escalation procedures, and communication protocols in the event of a security incident.

- Use strong encryption algorithms and key management practices to protect sensitive data in transit and at rest.

- Conduct regular cybersecurity awareness training for employees to educate them on the latest cybersecurity threats and best practices.

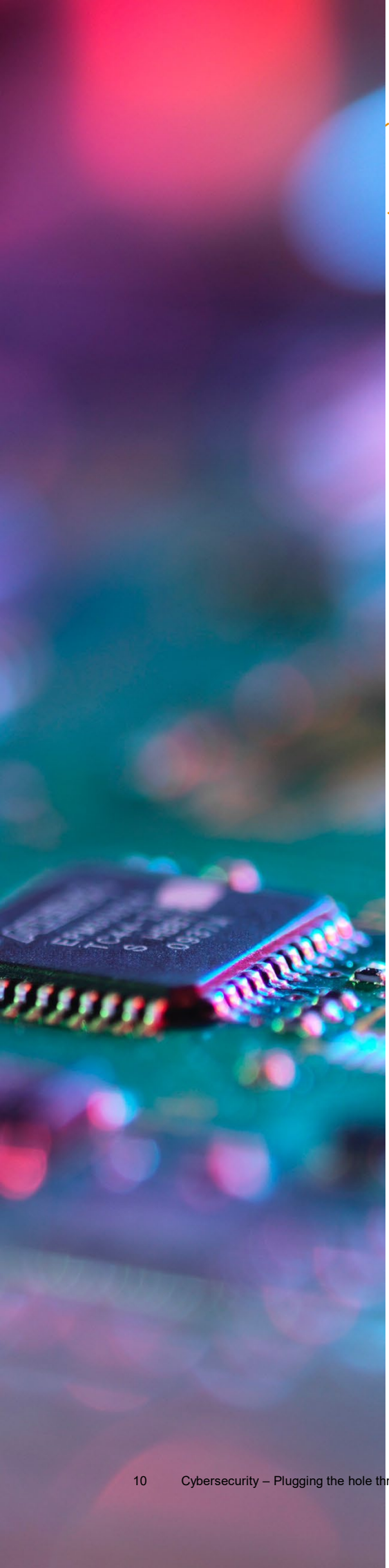
- Ensure that your organisation complies with applicable regulatory requirements and standards, such as Personal Data (Privacy) Ordinance (PDPO), General Data Protection Regulation (GDPR), The China Personal Information Protection Law (PIPL) and Payment Card Industry Data Security Standard (PCI-DSS), as appropriate.

- Monitor and assess third-party vendors and partners to ensure they adhere to the organisation's cybersecurity standards.

- Implement a continuous improvement process to evaluate and enhance the organisation's cybersecurity architecture and framework based on evolving threats and risks.

- Leverage cyber threat intelligence throughout the abovementioned procedures to identify relevant threats and allocate resources in a risk-based prioritisation approach to effectively manage cybersecurity risks.

Governance professionals, as trusted advisers to the board, should help raise awareness of cybersecurity issues as set out under this report and inform directors of the tools available to manage cyber risks efficiently.



1.2 Risk assessment

Determining the possibility and potential effects of cyber threats and vulnerabilities on an organisation's assets, operations, and reputation should form part of risk assessment. Directors must be aware of the tools to manage cyber risks appropriately. Among the most important tools for mitigating cyber risks are:

- **Cybersecurity frameworks:** Organised collections of standards, recommendations, and best practices created by business groups, regulatory bodies, and other groups to assist businesses in managing their cyber risks.

- **Security controls**: Measures include firewalls, endpoints detection and response, encryption, access controls, monitoring, incident response, business continuity, and disaster recovery planning. Security controls are also applied to prevent, identify, and respond to cyber threats and vulnerabilities.

- **Cybersecurity awareness:** Employee and stakeholder education and ongoing training in cybersecurity to increase knowledge of cyber threats and the best practices for safeguarding digital assets and data.

- **Cybersecurity insurance:** Data breaches, network outages, and cyber extortion are just a few examples of the financial damages and legal obligations covered by speciality insurance policies known as cybersecurity insurance.

Directors can more effectively assess the cyber risks of their organisation, create effective cybersecurity strategies, and oversee the implementation and monitoring of cybersecurity measures to safeguard their organisation's digital assets and reputation by understanding these and other cybersecurity tools.

1.3 Role of governance professionals

Governance professionals who serve as trusted advisers to the chairman and board of their respective organisations can help directors understand that tools are available to manage cyber risks efficiently. Some of the most important tools to assist their firms in controlling cyber threats are listed below:

- **Cybersecurity frameworks:** For managing cyber risks based on industry standards and best practices, such as ISO/IEC 27001 and Center for Internet Security (CIS) Controls, which offer a prioritised list of security measures businesses can be used to stop, find, and address cyber threats and vulnerabilities. For more technical frameworks, directors may request their team to align with the MITRE ATT&CK Framework, a globally recognised framework used to describe and categorise the tactics, techniques, and procedures (TTPs) used by sophisticated adversaries during a cyber-attack. These form the basis for effective cyber threat operations, including how to perform targeted security monitoring and incident response against the latest TTPs.

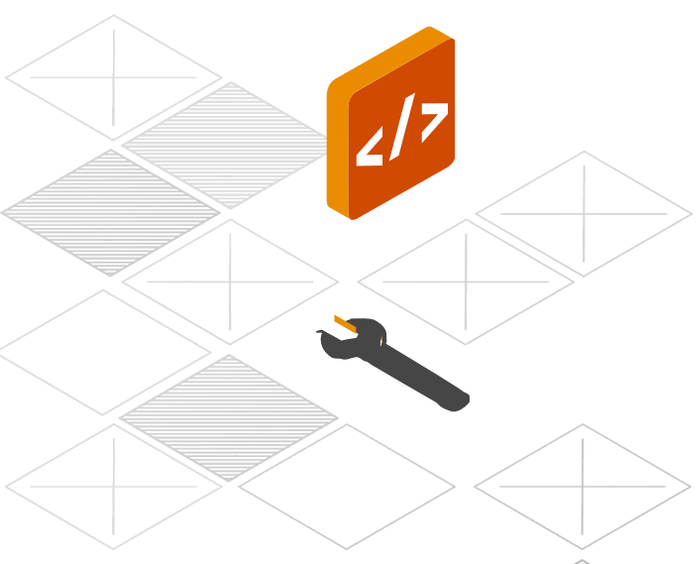
- **Risk assessment methodologies:** Examples include the FAIR (Factor Analysis of Information Risk) and OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) frameworks, which assist organisations in identifying and ranking their cyber risks using quantitative and qualitative data.

- **Incident response plans:** For responding to cyber incidents, including who to call, how to control and contain the problem, how to resume regular operations, and how to prevent similar incidents from recurring.

- **Cybersecurity training programs:** These programs inform staff members and other interested parties on the dangers of cyber threats, the best practices for safeguarding digital assets, and how to handle cyber event

- **Third-party risk management** refers to the rules and practices used to control the cybersecurity risks posed by partners, suppliers, and third-party vendors.

- **Cybersecurity audits and assessments:** These assess the efficacy of a company's cybersecurity procedures, pinpoint areas for development, and make suggestions for correction.



1.4 Cybersecurity experts

Governance professionals would not be able to perform an accurate cyber risk assessment, and specialised cybersecurity experts would be required to carry out particular tests for cybersecurity, including penetration testing. The following are some of the approaches that experts might use as part of a risk assessment:

- **Penetration testing:** Also referred to as ethical hacking, is the process of simulating a cyberattack on the systems, networks, or applications of an organisation to find weaknesses and vulnerabilities that a malicious actor could exploit.
- **Vulnerability scanning** entails employing automated technologies to search an organisation's networks and systems for weaknesses that online criminals could use.
- **Social engineering:** This entails sending phoney emails or messages to company employees to see if they are susceptible to social engineering assaults like phishing.
- **Web application testing** entails checking a company's web applications for security flaws that online criminals might use, like Structured Query Language (SQL) injection or cross-site scripting.
- **Wireless network testing** involves examining a company's wireless network for holes and flaws that hackers could exploit, such as shoddy encryption or unprotected access points.
- **Threat modelling:** A process used to improve security by identifying potential threats and vulnerabilities in a system. It involves identifying and enumerating potential threats, such as structural vulnerabilities or the absence of appropriate safeguards, and prioritising countermeasures to address them.
- **Red teaming:** A technique for identifying vulnerabilities in an organisation's overall cybersecurity posture by simulating a full-scale cyber-attack against its systems, networks, and personnel.

Organisations can better their cybersecurity posture through these technologies by identifying and addressing system, network, and application vulnerabilities and weaknesses. It is crucial to remember that cybersecurity experts should only utilise these technologies with the knowledge and experience to do so safely and successfully.

Organisations should consider individually accredited and also company-accredited qualifications when shortlisting cybersecurity professionals for practical assessments. Accreditation bodies such as CREST International, Offensive Security (OffSec), and SANS Institute offer practical assessments of the individual and organisation's technical skills, quality management systems, and adherence to ethical practices and provide assurance over their ability to conduct these sensitive exercises in a controlled and safe manner, in turn minimising the risk of disrupting business operations and jeopardising the organisation's critical systems and sensitive data.

The following is a non-exhaustive list of certifications that may indicate a cyber professional's capability to conduct these technical assessments. Other alternatives may require similar technical competency to pass, though these are more commonly observed options recognised globally by industry practitioners. Meanwhile, we also supplement the accreditation list for security monitoring, incident response, and threat intelligence, as these would typically be required to understand the observations and recommendations from the assessments and, in turn, facilitate the design and implementation of appropriate safeguards to mitigate the risks associated with the attacks performed by the assessors.

Domain	Accreditation Body	Individual Accreditation Name
Offensive Security (e.g., Penetration Testing, Red Teaming, etc.)	CREST International	• CREST Certified Simulated Attack Manager (CCSAM) • CREST Certified Simulated Attack Specialist (CCSAS) • CREST Certified Infrastructure Tester (CCT Infra and CCT Web App) • CREST Registered Penetration Tester (CRT)
	Offensive Security	• Offensive Security Experienced Penetration Tester (OSEP) • Offensive Security Wireless Professional (OSWP) • Offensive Security Certified Professional (OSCP) • Offensive Security Web Expert (OSWE) • Offensive Security Web Assessor (OSWA)
	SANS Institute	• GIAC Penetration Tester (GPEN) • GIAC Exploit Research and Advanced Penetration Tester (GXPN) • GIAC Web Application Penetration Tester (GWAPT)
Security Operations	Offensive Security	• Offensive Security Defense Analyst (OSDA)
	SANS Institute	• GIAC Security Operations (GSOC) • GIAC Certified Incident Handler (GCIH)
Incident Response	CREST International	• CREST Registered Intrusion Analyst (CRIA) • CREST Certified Network Intrusion Analyst (CCNIA) • CREST Certified Host Intrusion Analyst (CCHIA) • CREST Certified Incident Management (CCIM)
	SANS Institute	• GIAC Certified Forensic Examiner (GCFE) • GIAC Certified Forensic Analyst (GCFA)
Threat Intelligence	CREST International	• CREST Certified Threat Intelligence Manager (CCTIM) • CREST Registered Threat Intelligence Analyst (CRTIA)
	SANS Institute	• GIAC Cyber Threat Intelligence (GCTI) • GIAC Open Source Intelligence (GOSI)

1.5 Cybersecurity best practice examples

Singapore government and ethical hacking

The Singaporean government ran "Exercise Cyber Star," a sizable cybersecurity exercise in 2019 to test the cybersecurity defences of several government organisations. This exercise includes ethical hacking and red teaming.

The government hired a group of ethical hackers to assess the security of a federal agency's digital infrastructure, including its networks, systems, and apps. To mimic a cyberattack, the ethical hackers employed a variety of tools and tactics, looking for any holes or vulnerabilities they could exploit.

The agency's systems had several vulnerabilities discovered by ethical hackers, including unpatched software, weak passwords, and improperly configured access controls. Additionally, they acquired unlawful access to private data, including employee records and secret documents.

The government agency used the exercise results to strengthen its cybersecurity defences s by fixing vulnerabilities, enhancing password restrictions, and putting more stringent access controls in place.

Ethical hacking activities help firms strengthen their overall cybersecurity posture by allowing them to find and fix system vulnerabilities before they are used maliciously.

Singapore Government and New Vulnerabilities Reward Programme

The Singapore government launched a bug bounty programme using crowdsourcing vulnerability discovery programmes that offer a blend of continuous reporting and seasonal in-depth testing capabilities that taps the larger community, in addition to routine penetration testing conducted by the government. This new vulnerabilities reward programme offers rewards ranging from US$250 to US$5,000 to white hat hackers, depending on the severity of the vulnerabilities discovered. A special bounty of up to US$150,000 will be awarded for discovering vulnerabilities that could cause exceptional impact on selected systems and data.

This signals the Singapore Government's commitment to secure critical systems and sensitive personal data.

US Department of Defense cyber audit

The US Department of Defense (DoD) conducted its first full-scope cyber audit in 2020. This audit includes a thorough cybersecurity review of the DoD's networks, systems, and applications.

A team of auditors from the DoD's Office of the Inspector General and other outside audit firms conducted the cybersecurity audit, using a risk-based methodology to evaluate the efficacy of the DoD's cybersecurity controls and procedures.

The auditors noted some areas where the DoD's cybersecurity controls needed strengthening, including tightening user access controls, fortifying vulnerability management procedures, and increasing incident response protocols.

Based on the audit's findings, the DoD implemented several corrective measures to address the highlighted inadequacies, including enhancing security awareness training, network security controls, and incident response capabilities.

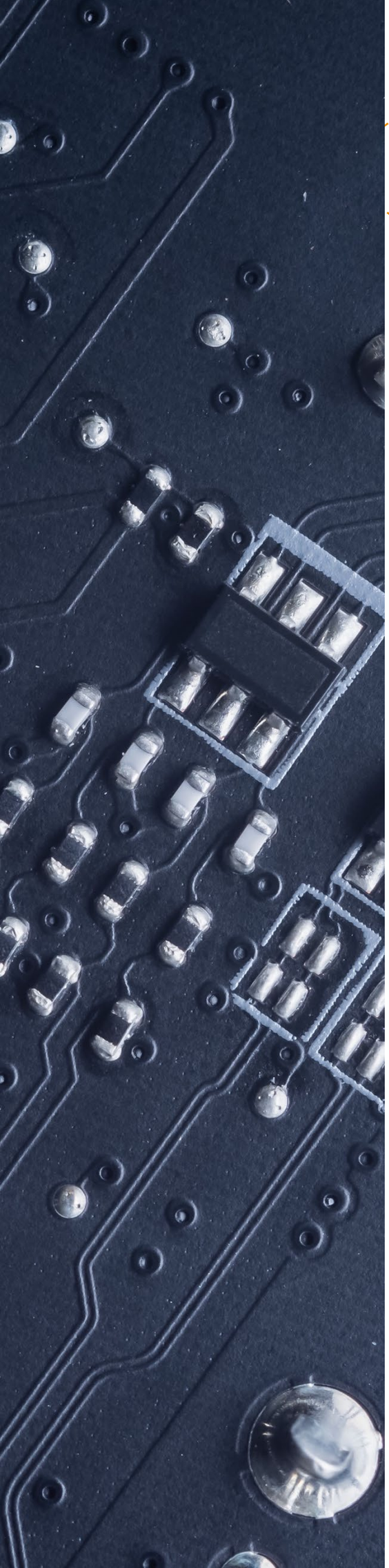
The DoD showed its stakeholders and the general public that it takes cybersecurity seriously and is dedicated to safeguarding its digital assets from cyber threats by completing its cybersecurity audit and putting the recommended remedial steps into practice.

1.6 Risk exposures

Cybersecurity testing is crucial. However, many businesses have not sufficiently tested their cybersecurity weaknesses with potential risk exposures. This is partially due to the complexity and expense of cybersecurity testing, and many companies might not have the requisite resources or experience to carry out regular testing. Additionally, some companies might be underestimating the value of cybersecurity testing or the possible ramifications a cyberattack could have on their day-to-day operations, brand, and financial stability.

However, it is becoming more crucial for businesses to conduct routine cybersecurity testing to discover and fix vulnerabilities before they can be used by criminal actors, given the frequency and sophistication of cyberattacks. This is particularly true for businesses that deal with sensitive information or offer essential services, such as financial institutions, healthcare facilities, and governmental organisations.

Certain sectors, such as financial services, will mandate regular cybersecurity testing as part of the regulatory requirements. Companies can incorporate creativity into their cybersecurity testing programmes, such as having a bug bounty program to incentivise cybersecurity professionals or white hat hackers.



1.7 System vulnerabilities

Companies that require assistance with cybersecurity testing may find that specialised cybersecurity firms are an excellent resource because they can offer the knowledge, experience, and equipment needed to conduct successful testing and find potential threats and vulnerabilities, such as exposures to:

- **Ransomware:** Malware that encrypts a victim's data and demands payment in exchange for the decryption key.
- **Denial-of-service (DoS) attacks:** Attacks that overwhelm a target system or network with traffic so that it is unavailable to legitimate users.
- **Phishing:** An attack that uses phoney emails or websites to deceive victims into divulging private information like passwords or credit card numbers.
- **Man-in-the-middle (MitM) attack** allows the attacker to overhear, alter, or inject data into a conversation between two parties by intercepting their connection.
- **Advanced persistent threat (APT):** A prolonged, focused attack using cutting-edge methods to infiltrate a target system or network, such as social engineering, zero-day exploits, and lateral movement.
- **Malware:** Software that aims to harm, interfere with, or access a computer system or network without authorisation.
- **Insider threat:** A danger posed by personnel, subcontractors, or other vetted insiders who have access to confidential information or systems and might abuse that access.
- **Supply chain attack:** An attempt to access a target organisation's systems or data via targeting a third-party vendor or supplier.

These are just a few instances of the various kinds of cyber risks that businesses may encounter. Organisations must deploy effective cybersecurity measures and keep abreast of the most recent threats and vulnerabilities to protect their systems and data.

1.8 The repercussions

Different outcomes are possible depending on the type and extent of the breach. Some possible repercussions include:

- **Financial losses:** The firm or people whose information has been compromised may suffer financial losses due to a cyber breach. This may result from financial theft, dishonest commercial dealings, or lost business opportunities.
- **Reputational damage:** Damage to a company's reputation from a cyberattack could result in a decline in customer confidence and trust. This may make it challenging to draw in new clients or keep hold of current ones.
- **Legal repercussions:** A cyber breach may have legal implications for the organisation or people who committed the violation, which can involve penalties, lawsuits, or even criminal prosecutions.
- **Data loss:** A cyber breach may cause data loss, which can be disastrous for a business or person. This can include private information, intellectual property, or delicate commercial information.
- **Service interruptions:** Cyberbreach may result in lost productivity or downtime. This may hinder the business's ability to run efficiently and cost money.

A paid ransomware example:

The attack on the US-based Colonial Pipeline in May 2021 resulted in a sizeable payment.

Gasoline and other petroleum products are delivered to the eastern and southern parts of the United States via the Colonial Pipeline, a significant fuel pipeline. The business was the subject of a ransomware attack by the DarkSide gang in May 2021.

Due to Colonial Pipeline's forced shutdown of operations due to the attack, there were fuel shortages and price increases across much of the US. Colonial Pipeline paid the assailants a $4.4 million ransom in response to the episode to retake control of its systems.

The ransom payment has generated debate because it encourages other ransomware operations. Colonial Pipeline clarified that it paid to resume operations and lessen customer impact promptly.

The Colonial Pipeline attack is only one of the well-publicised ransomware attacks that have recently targeted businesses worldwide. These attacks underscore organisations' need to adopt efficient cybersecurity measures to avoid and mitigate such attacks because they may have significant financial and operational repercussions.

1.9 In conclusion

Directors and governance professionals should consider the imperatives to (1) prioritise cybersecurity testing; (2) establish security policies and procedures; (3) implement Identity and Access Management (IAM) policies; (4) monitor third-party cybersecurity risks; and (5) invest in cybersecurity awareness training.

Specifically, there should be awareness of the significance of policies and procedures in ensuring that a business has a solid basis for cybersecurity. It is also true that testing systems for vulnerabilities are a crucial component of successful cybersecurity and one that is occasionally disregarded or not given enough attention.

Before cyber attackers take advantage of system weaknesses, businesses can find and fix them with effective cybersecurity testing. This encompasses technical and behavioural weaknesses, such as careless password management and vulnerability to phishing attempts.

Cybersecurity testing can be conducted using various tools and methods, such as red teaming exercise, vulnerability scanning, penetration testing, and social engineering testing. With the aid of these technologies, businesses may find areas of vulnerability in their systems and take action to fix them before attackers can take advantage of them.

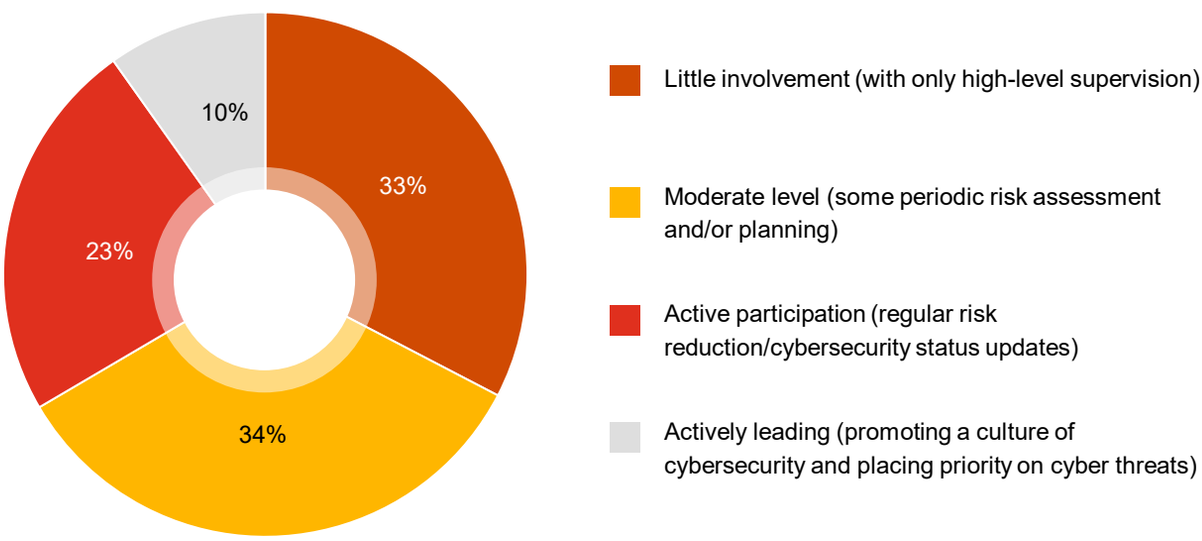
According to an applied governance approach, organisations should prioritise cybersecurity testing as part of their cybersecurity strategy. This could entail investing in cybersecurity tools and technology, collaborating with outside experts to conduct testing as appropriate, and ensuring testing outcomes are considered when making continuous cybersecurity enhancements. Organisations can significantly minimise their risk of cyberattacks and better safeguard their systems and data by adopting a proactive approach to cybersecurity testing.

Part 2

Survey Results

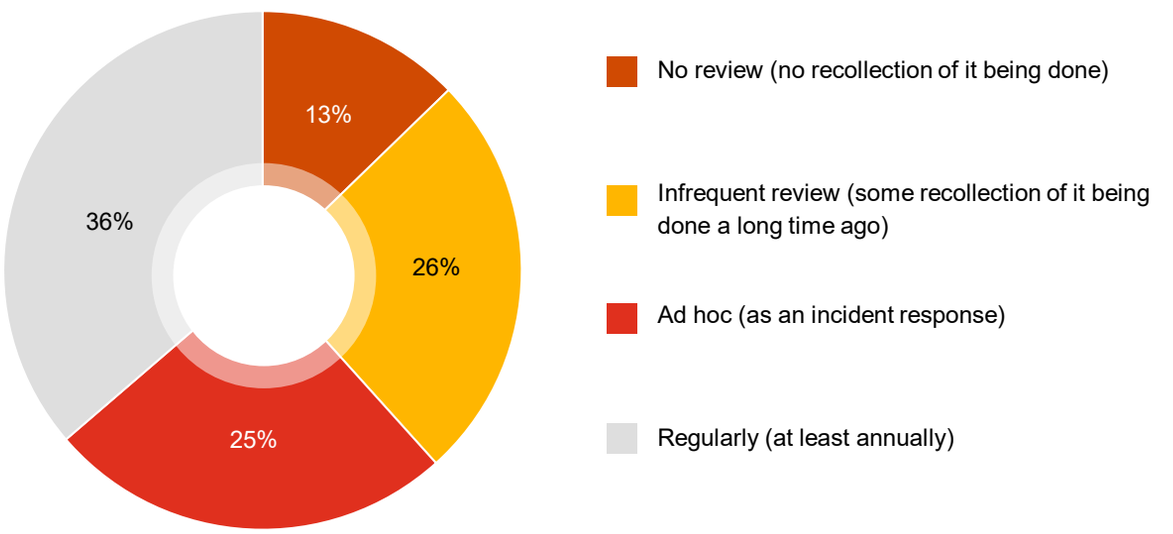
2.1 Questions

1 **What role does your board of directors play in your organisation's cybersecurity governance?**



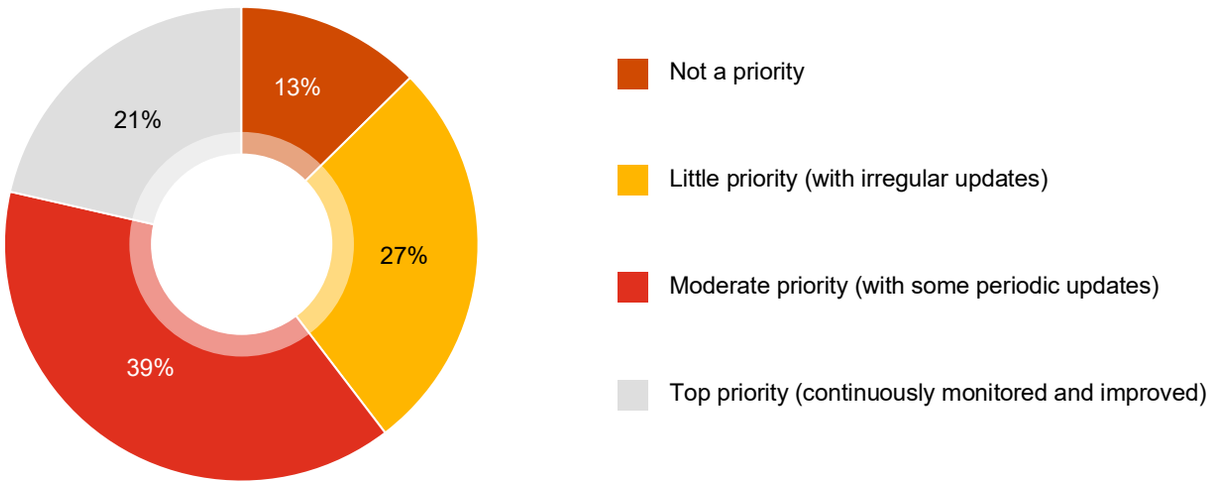
ANSWER CHOICES	RESPONSES	
Little involvement (with only high-level supervision)	32.63%	481
Moderate level (some periodic risk assessment and/or planning)	33.92%	500
Active participation (regular risk reduction/cybersecurity status updates)	23.61%	348
Actively leading (promoting a culture of cybersecurity and placing priority on cyber threats)	9.84%	145
TOTAL		**1,474**

2 How frequently does your board of directors examine your organisation's cybersecurity strategy?



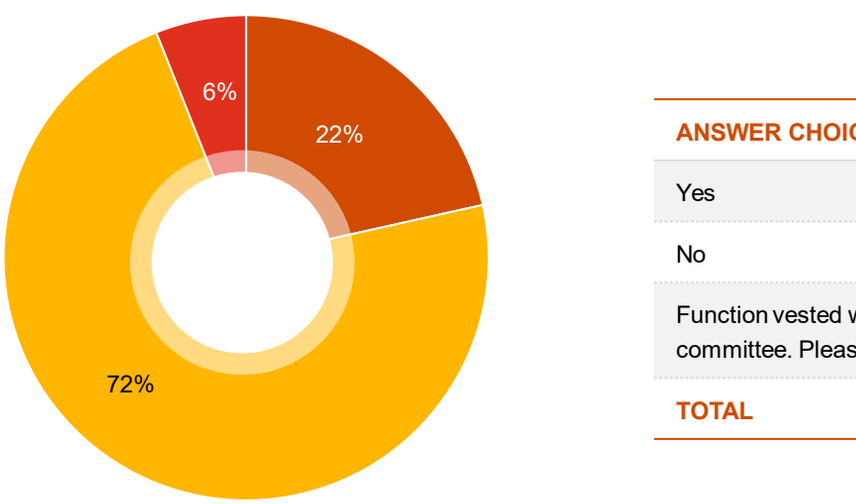
ANSWER CHOICES	RESPONSES	
No review (no recollection of it being done)	12.75%	188
Infrequent review (some recollection of it being done a long time ago)	25.58%	377
Ad hoc (as an incident response)	25.37%	374
Regularly (at least annually)	36.30%	535
TOTAL		1,474

3 How high a priority does your board of directors place on cybersecurity as a significant business risk?



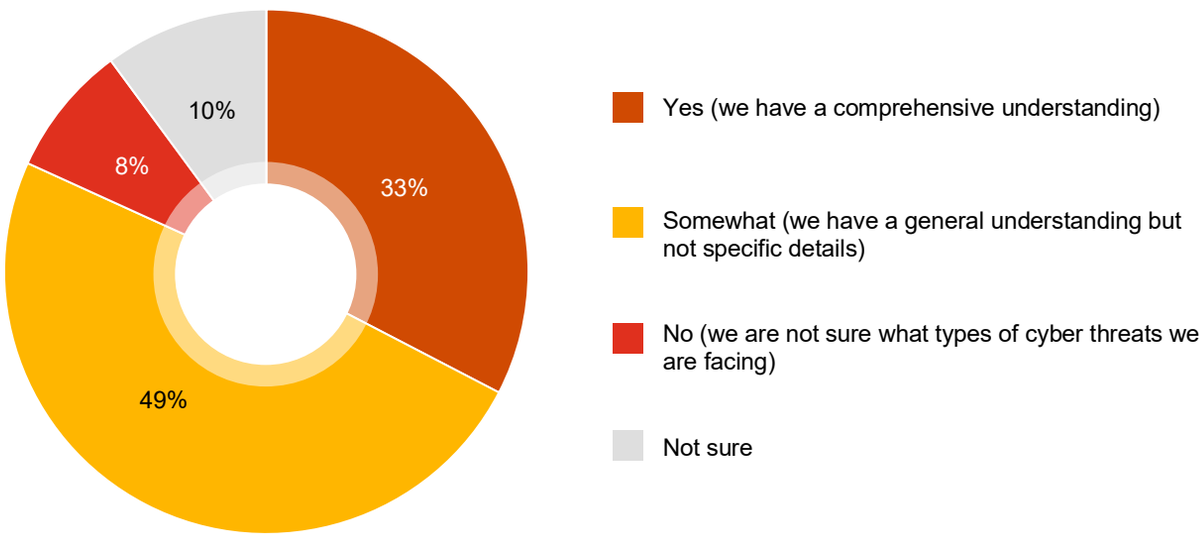
ANSWER CHOICES	RESPONSES	
Not a priority	12.62%	186
Little priority (with irregular updates)	27.00%	398
Moderate priority (with some periodic updates)	38.94%	574
Top priority (continuously monitored and improved)	21.44%	316
TOTAL		**1,474**

4 Has your board established a cybersecurity committee with clear roles and lines of authority?



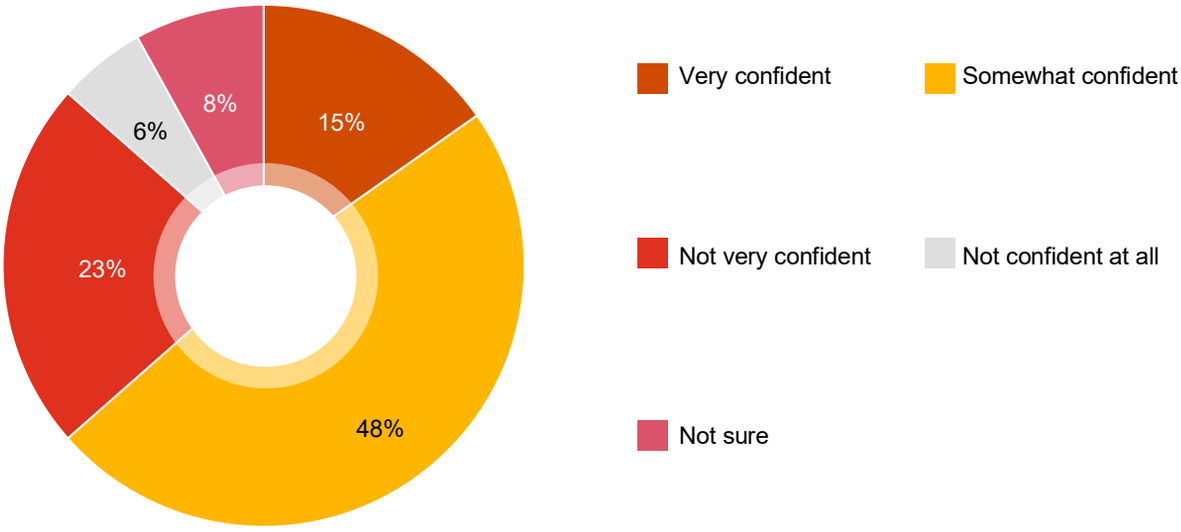
ANSWER CHOICES	RESPONSES	
Yes	21.51%	317
No	72.45%	1,068
Function vested with another committee. Please specify:	6.04%	89
TOTAL		**1,474**

5 Does your organisation clearly understand the specific types of cyber threats it faces?



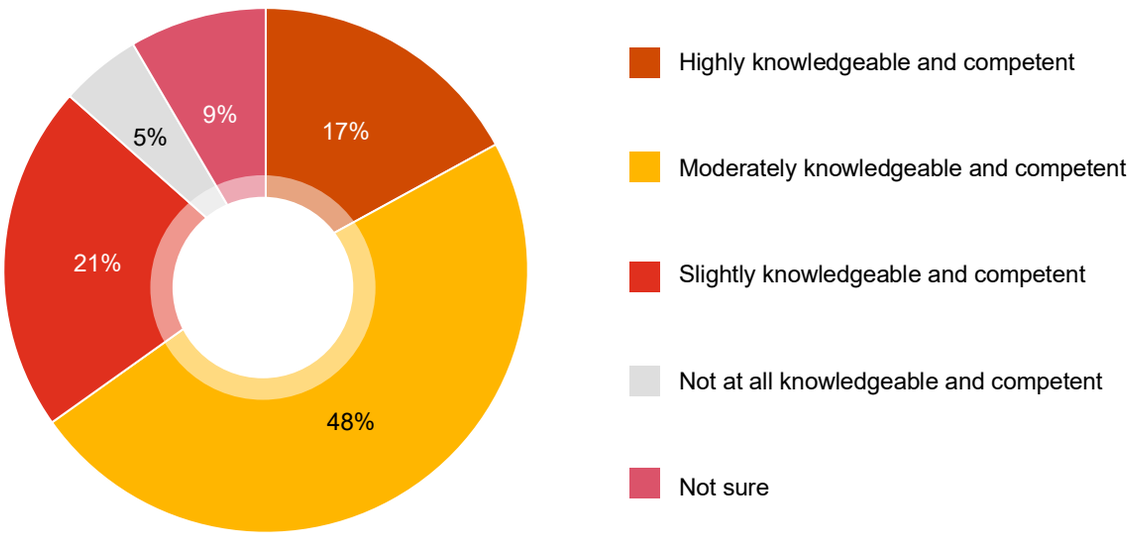
ANSWER CHOICES	RESPONSES	
Yes (we have a comprehensive understanding)	32.62%	471
Somewhat (we have a general understanding but not specific details)	49.17%	710
No (we are not sure what types of cyber threats we are facing)	8.10%	117
Not sure	10.11%	146
TOTAL		1,444

6 What confidence do you have in the team currently in charge of your organisation's cybersecurity strategy?



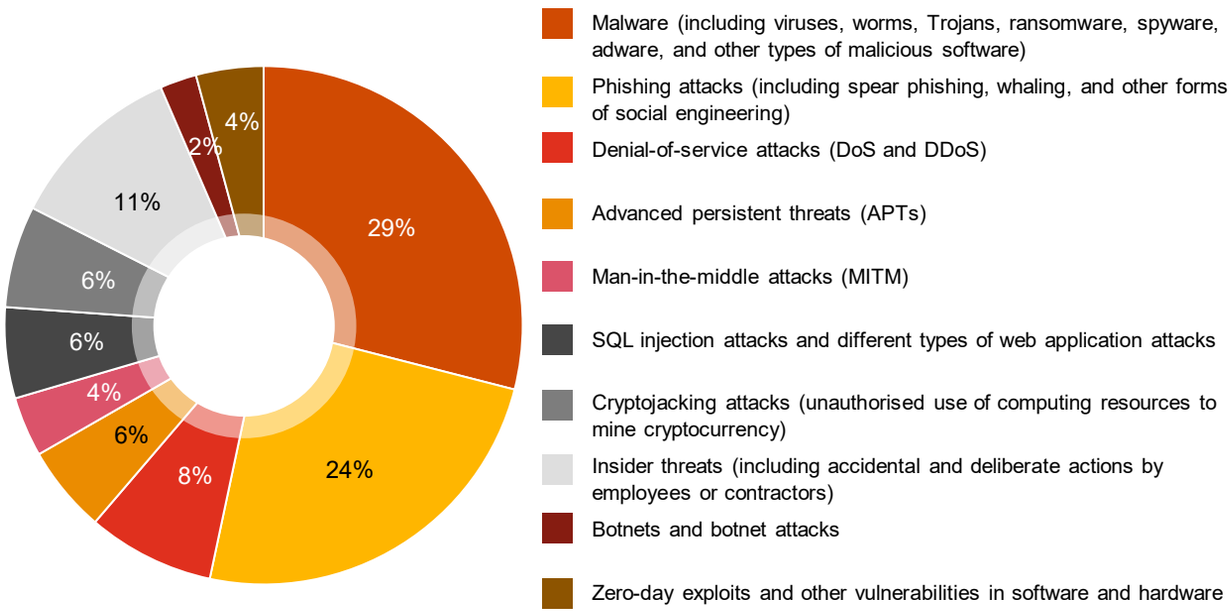
ANSWER CHOICES	RESPONSES	
Very confident	15.24%	220
Somewhat confident	48.27%	697
Not very confident	22.99%	332
Not confident at all	5.47%	79
Not sure	8.03%	116
TOTAL		1,444

7 **How would you rate the knowledge and competency of implementation by your organisation's cybersecurity team?**



ANSWER CHOICES	RESPONSES	
Highly knowledgeable and competent	17.03%	246
Moderately knowledgeable and competent	48.13%	695
Slightly knowledgeable and competent	21.40%	309
Not at all knowledgeable and competent	4.99%	72
Not sure	8.45%	122
TOTAL		**1,444**

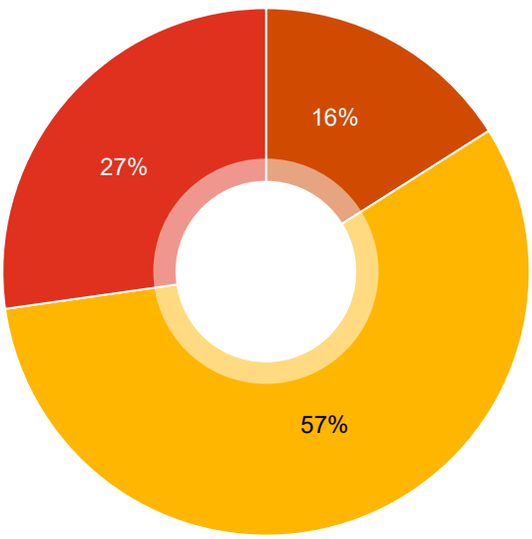
8 Please also choose from the list of cyber threats that your organisation has faced and/or is facing (select one or more):



ANSWER CHOICES	RESPONSES	
Malware (including viruses, worms, Trojans, ransomware, spyware, adware, and other types of malicious software)	69.14%	986
Phishing attacks (including spear phishing, whaling, and other forms of social engineering)	58.06%	828
Denial-of-service attacks (DoS and DDoS)	18.93%	270
Advanced persistent threats (APTs)	12.97%	185
Man-in-the-middle attacks (MITM)	8.91%	127
SQL injection attacks and different types of web application attacks	13.53%	193
Cryptojacking attacks (unauthorised use of computing resources to mine cryptocurrency)	15.15%	216
Insider threats (including accidental and deliberate actions by employees or contractors)	26.30%	375
Botnets and botnet attacks	5.47%	78
Zero-day exploits and other vulnerabilities in software and hardware	10.03%	143
TOTAL		**1,426**

Note: On average there were 2.38 incidences of cyber threat, faced and/or is facing by each respondent.

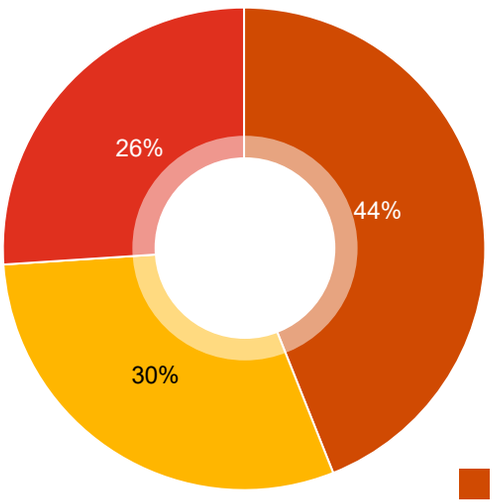
9 **To what extent are directors trained in cybersecurity awareness? (About cyber dangers and how to guard against them)**



- Widespread (directors have regular training and are highly aware of cybersecurity risks and how to mitigate them)
- Occasional (directors receive periodic training but may not be highly aware of cybersecurity risks)
- None (directors receive no cybersecurity training or education)

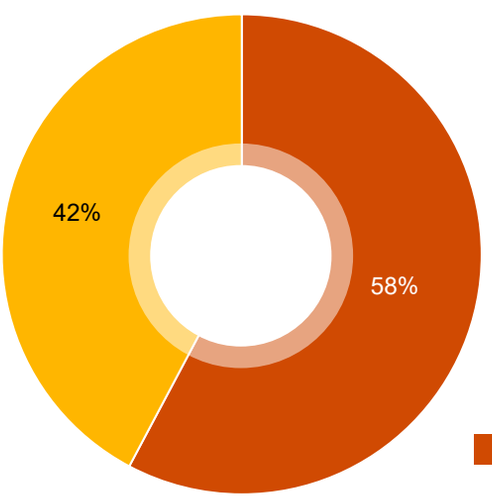
ANSWER CHOICES	RESPONSES	
Widespread (directors have regular training and are highly aware of cybersecurity risks and how to mitigate them)	16.02%	227
Occasional (directors receive periodic training but may not be highly aware of cybersecurity risks)	56.74%	804
None (directors receive no cybersecurity training or education)	27.24%	386
TOTAL		**1,417**

10 **Has your organisation helped your business units put together cybersecurity training programs for staff members and/or pertinent stakeholders (who may be able to access your system or supply of cyber services)?**



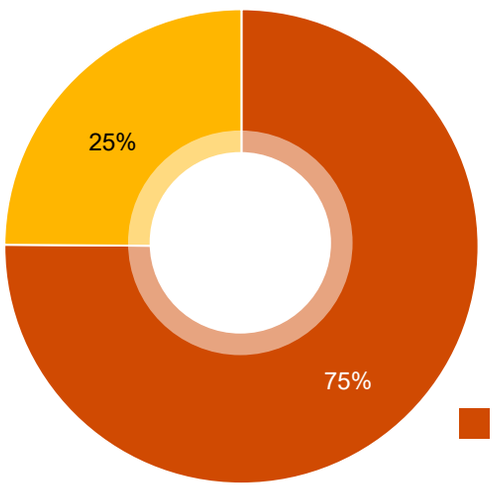
ANSWER CHOICES	RESPONSES	
Yes	43.96%	623
No	29.99%	425
Not sure	26.14%	369
TOTAL		1,417

11 **Has your business established a cybersecurity framework? (A cybersecurity framework is a collection of guidelines for controlling and lowering cyber risks within an organisation)**



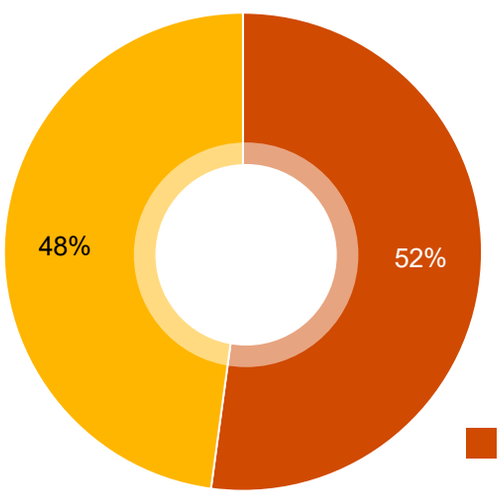
ANSWER CHOICES	RESPONSES	
Yes	57.77%	810
No	42.23%	592
TOTAL		1,402

12 **Does your business have security measures in place to reduce online risks? Security controls are procedures or precautions that lessen or mitigate the dangers of online threats.**



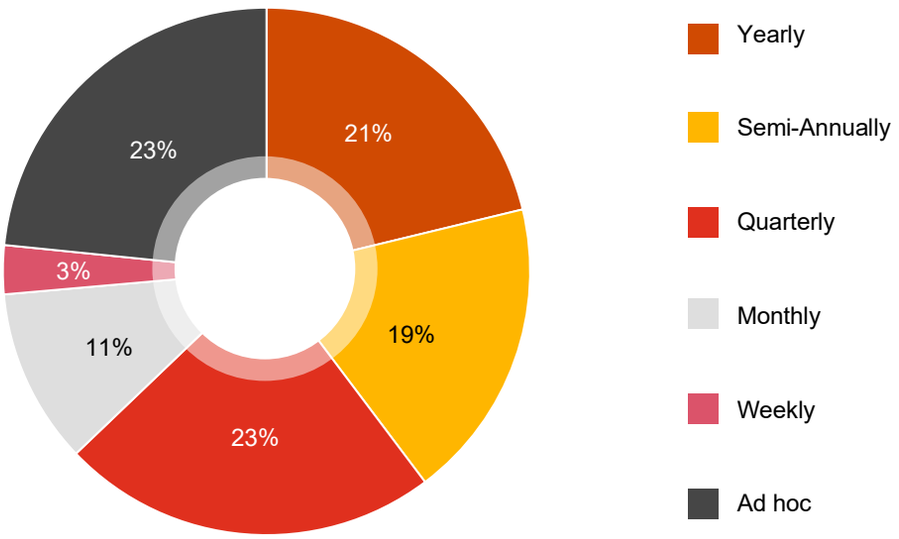
ANSWER CHOICES	RESPONSES	
Yes	75.11%	1,053
No	24.89%	349
TOTAL		1,402

13 **Has your business performed penetration tests? (Penetration testing, commonly called "pen testing", examines an organisation's computer networks and systems for flaws that an intruder could exploit. Consider ethical hacking.)**



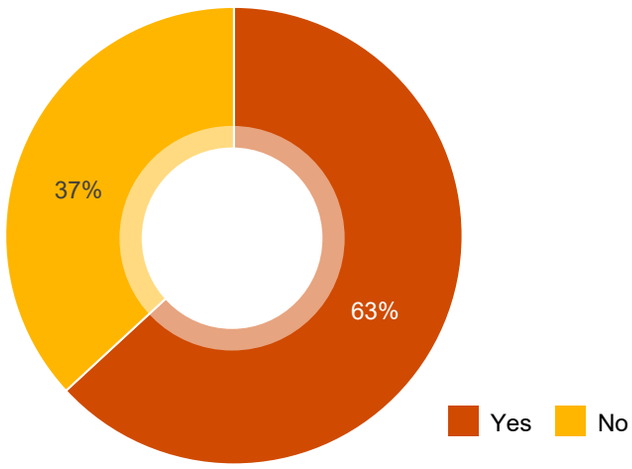
ANSWER CHOICES	RESPONSES	
Yes	52.14%	731
No	47.86%	671
TOTAL		1,402

14 What is the frequency of testing?



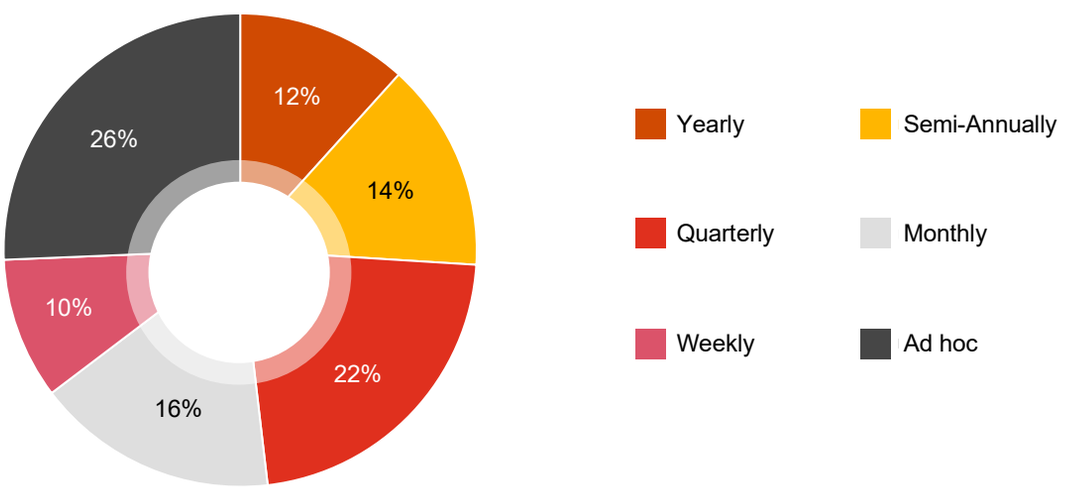
ANSWER CHOICES	RESPONSES	
Yearly	21.23%	156
Semi-Annually	18.50%	136
Quarterly	23.13%	170
Monthly	10.75%	79
Weekly	2.99%	22
Ad hoc	23.40%	172
TOTAL		**735**

15 **Has your business scanned for cyber vulnerabilities? (Identifying security holes and vulnerabilities in an organisation's computer systems and networks is a process known as vulnerability scanning.)**



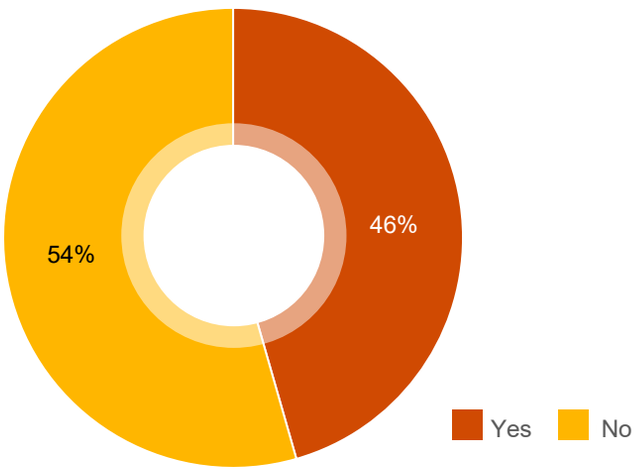
ANSWER CHOICES	RESPONSES	
Yes	63.14%	884
No	36.86%	516
TOTAL		1,400

16 **What is the frequency of scanning?**



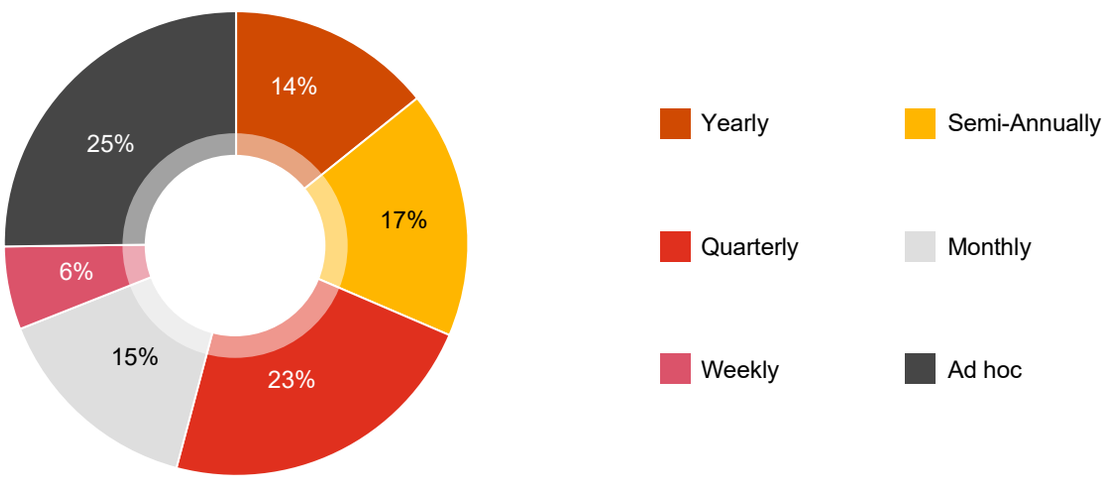
ANSWER CHOICES	RESPONSES	
Yearly	11.70%	104
Semi-Annually	14.29%	127
Quarterly	22.15%	197
Monthly	16.54%	147
Weekly	9.67%	86
Ad hoc	25.65%	228
TOTAL		889

17 **Has your business tested for social engineering? (Testing employees' vulnerability to cyberattacks that use social engineering techniques like phishing, pretexting, and baiting is known as social engineering testing.)**



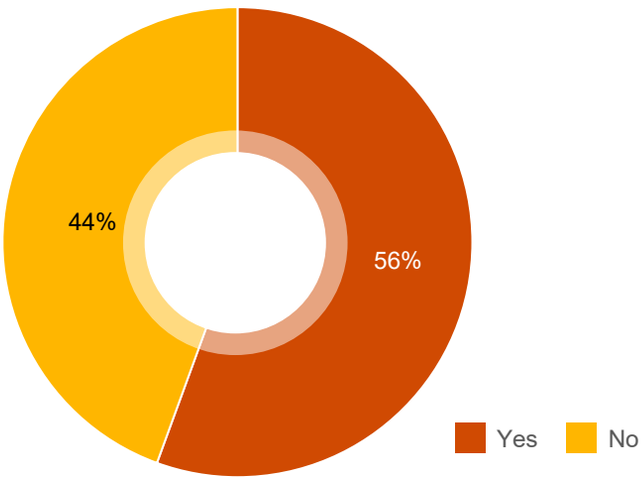
ANSWER CHOICES	RESPONSES	
Yes	45.56%	636
No	54.44%	760
TOTAL		1,396

18 **What is the frequency of testing?**



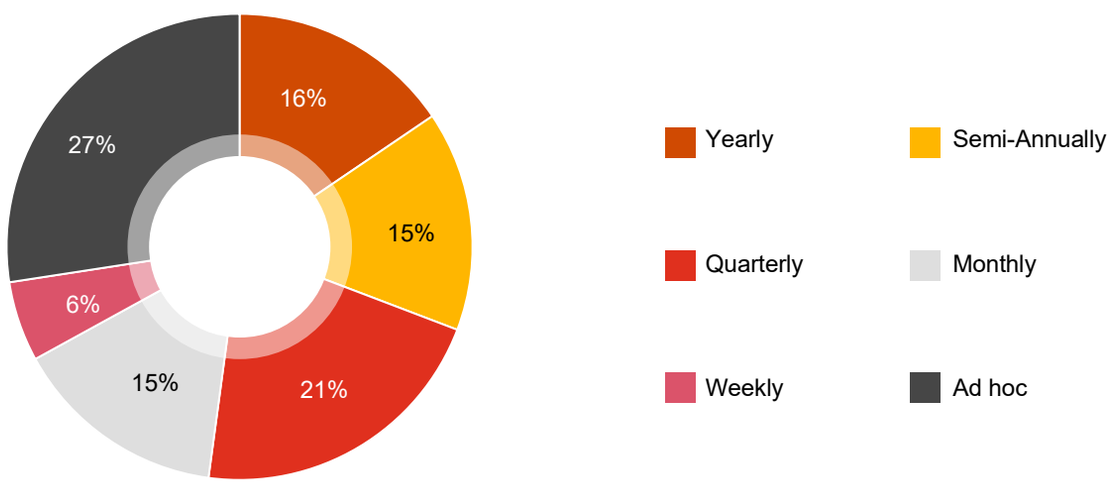
ANSWER CHOICES	RESPONSES	
Yearly	14.24%	91
Semi-Annually	17.21%	110
Quarterly	22.69%	145
Monthly	14.87%	95
Weekly	5.79%	37
Ad hoc	25.20%	161
TOTAL		639

19 **Has your business tested web applications? (Evaluating an organisation's web apps to find security flaws is known as web application testing.)**



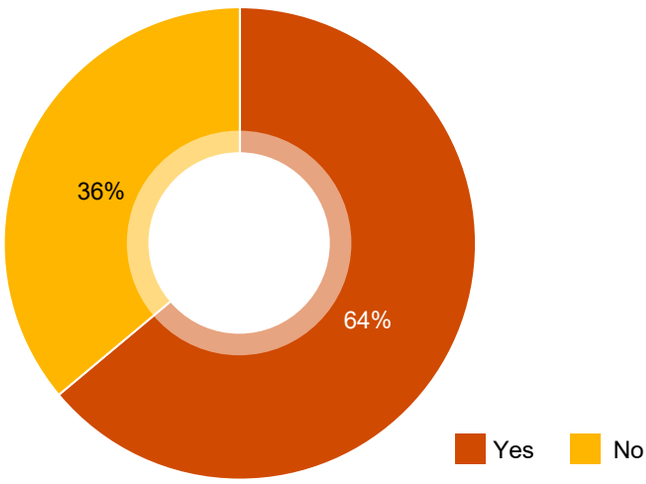
ANSWER CHOICES	RESPONSES	
Yes	55.57%	773
No	44.43%	618
TOTAL		1,391

20 **What is the frequency of testing?**



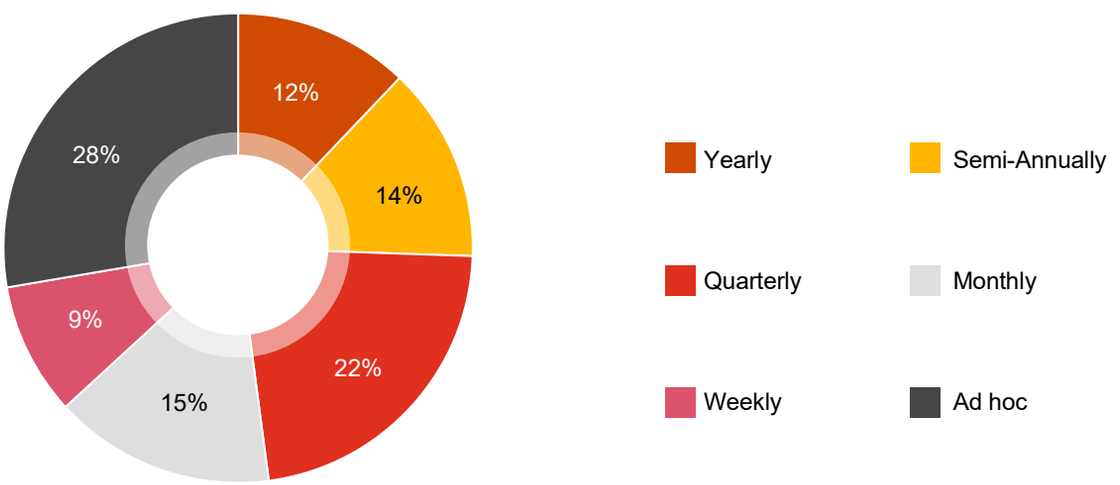
ANSWER CHOICES	RESPONSES	
Yearly	15.52%	120
Semi-Annually	15.26%	118
Quarterly	21.35%	165
Monthly	14.88%	115
Weekly	5.56%	43
Ad hoc	27.43%	212
TOTAL		773

21 **Has your business tested wireless networks? (The process of trying an organisation's wireless networks to find security flaws is known as wireless network testing.)**



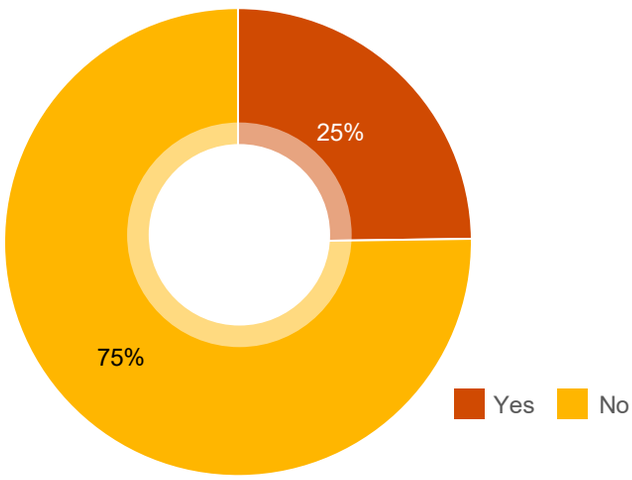
ANSWER CHOICES	RESPONSES	
Yes	63.92%	886
No	36.08%	500
TOTAL		1,386

22 **What is the frequency of testing?**



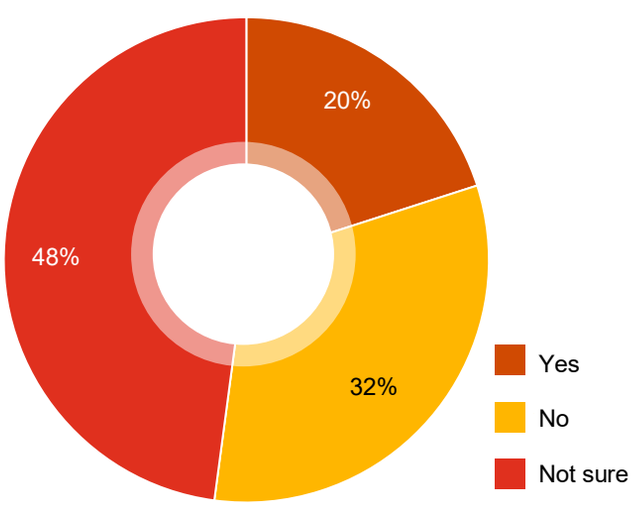
ANSWER CHOICES	RESPONSES	
Yearly	12.09%	107
Semi-Annually	13.45%	119
Quarterly	22.38%	198
Monthly	15.25%	135
Weekly	9.15%	81
Ad hoc	27.68%	245
TOTAL		885

23 **Has your business used red teams? (Red teaming is a form of cybersecurity testing that simulates an attack on the network by an expert and determined foe.)**



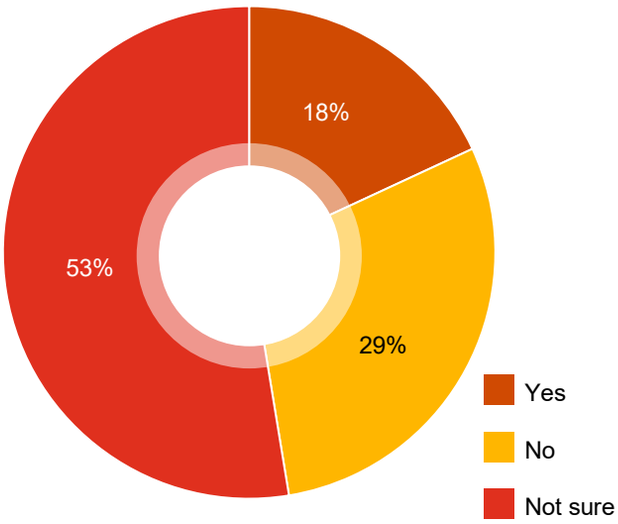
ANSWER CHOICES	RESPONSES	
Yes	24.78%	340
No	75.22%	1,032
TOTAL		1,372

24 **Does your business have cyber insurance? (To reduce the economic effects of cyber events.)**



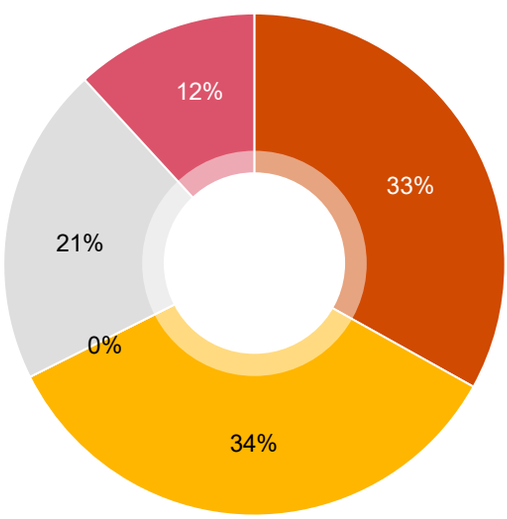
ANSWER CHOICES	RESPONSES	
Yes	20.04%	275
No	32.07%	440
Not sure	47.89%	657
TOTAL		1,372

25 Has there ever been a cybersecurity compromise at your company?



ANSWER CHOICES	RESPONSES	
Yes	18.09%	248
No	29.32%	402
Not sure	52.59%	721
TOTAL		1,371

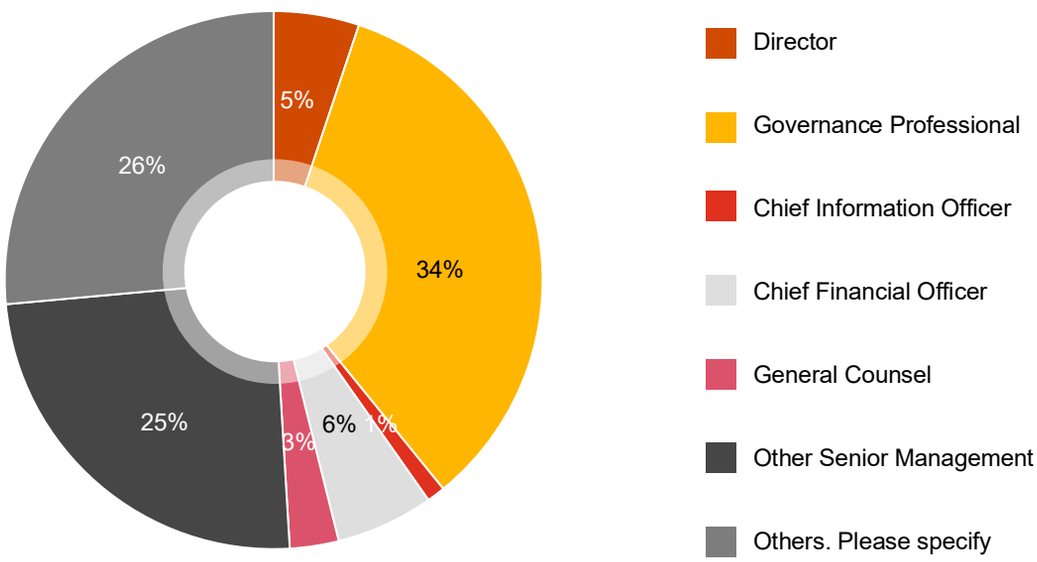
26 What were the repercussions of a cybersecurity breach at your company? (select one or more):



ANSWER CHOICES	RESPONSES	
Loss of money (the breach resulted in financial losses)	56.22%	140
Damage to reputation (the breach resulted in reputational damage)	58.63%	146
Both (the breach resulted in both financial losses and reputational damage)	0.00%	0
Possible breach of government rules and regulations	34.94%	87
No adverse effects (the breach had no significant negative impact)	20.08%	50
TOTAL		249

Note: On average there were 1.70 adverse repercussions by the company of each respondent.

27 **Please kindly indicate if you are:**



ANSWER CHOICES	RESPONSES	
Director	5.14%	70
Governance Professional	33.99%	463
Chief Information Officer	1.10%	15
Chief Financial Officer	5.87%	80
General Counsel	2.95%	40
Other Senior Management	24.52%	334
Others.	26.43%	360
TOTAL		**1,362**

About HKCGI

(Incorporated in Hong Kong with limited liability by guarantee)

The Hong Kong Chartered Governance Institute (HKCGI), formerly known as The Hong Kong Institute of Chartered Secretaries (HKICS), is the only qualifying institution in Hong Kong and Mainland China for the internationally recognised Chartered Secretary and Chartered Governance Professional qualifications.

With over 70 years of history and as the Hong Kong/China Division of The Chartered Governance Institute (CGI), the Institute's reach and professional recognition extends to all of CGI's nine divisions, with about 40,000 members and students worldwide. HKCGI is one the fastest growing divisions of CGI, with a current membership of over 7,000, 300 graduates and 2,600 students with significant representations within listed companies and other cross-industry governance functions.

Believing that better governance leads to a better future, HKCGI's mission is to promote good governance in an increasingly complex world and to advance leadership in the effective governance and efficient administration of commerce, industry and public affairs. As recognised thought leaders in our field, the Institute educates and advocates for the highest standards in governance and promotes an expansive approach that considers all stakeholders' interests.

Better Governance. Better Future.

For more information, please visit www.hkcgi.org.hk.

About PwC

PwC — Globally

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with nearly 328,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

PwC — Mainland China, Hong Kong SAR and Macau SAR

PwC in Mainland China, Hong Kong SAR and Macau SAR work together on a collaborative basis, subject to local applicable laws. Collectively, we have over 800 partners and more than 20,000 people in total.

We provide organisations with the professional service they need, wherever they may be located. Our highly qualified, experienced professionals listen to different points of view to help organisations solve their business issues and identify and maximise the opportunities they seek. Our industry specialisation allows us to help co-create solutions with our clients for their sector of interest.

We are located in these cities: Beijing, Shanghai, Hong Kong, Shenyang, Tianjin, Dalian, Jinan, Qingdao, Zhengzhou, Xi'an, Nanjing, Hefei, Suzhou, Wuxi, Wuhan, Chengdu, Hangzhou, Ningbo, Chongqing, Changsha, Kunming, Xiamen, Guangzhou, Shenzhen, Macau, Haikou, Zhuhai and Guiyang.

For more information, please visit: www. https://www.pwchk.com.

Contact Us

Ellie Pang FCG HKFCG(PE)
Chief Executive
The Hong Kong Chartered Governance Institute
+852 2830 6029
ellie.pang@hkcgi.org.hk

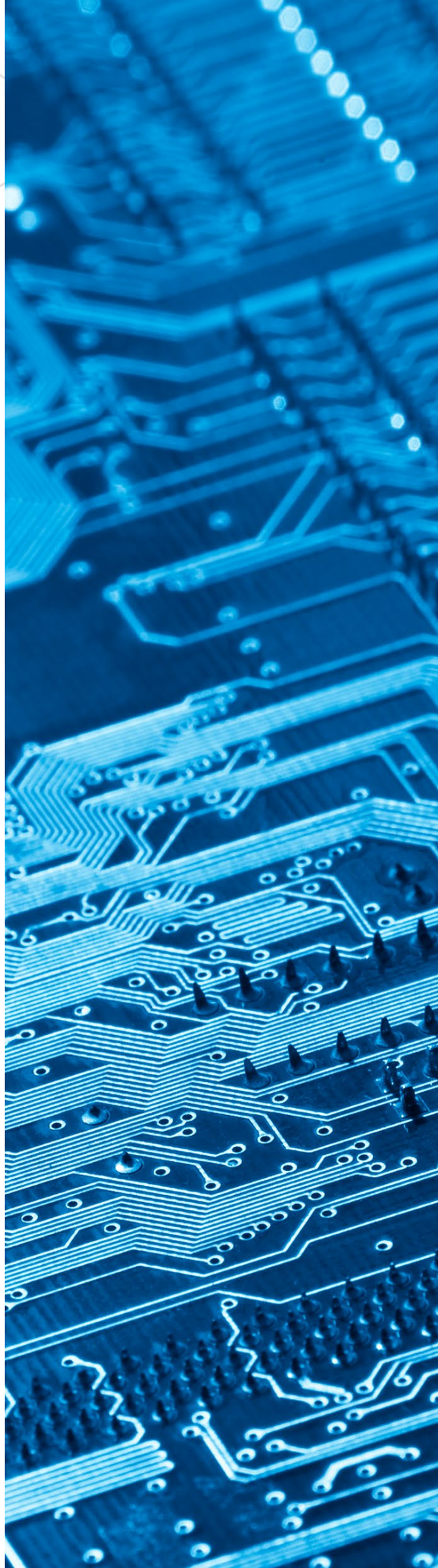
Mohan Datwani FCG HKFCG(PE)
Deputy Chief Executive
The Hong Kong Chartered Governance Institute
+852 2830 6012
mohan.datwani@hkcgi.org.hk

Joyce Li
Senior Manager, Marketing and Communications
The Hong Kong Chartered Governance Institute
+852 2881 6177
joyce.li@hkcgi.org.hk

Kenneth Wong
PwC Mainland China and Hong Kong
Cybersecurity and Privacy Leader
+852 2289 2719
kenneth.ks.wong@hk.pwc.com

Kok Tin Gan
Partner, Cybersecurity and Privacy
PwC Hong Kong
+852 2289 1935
kok.t.gan@hk.pwc.com

Jason Lee
Senior Manager, Cybersecurity and Privacy
PwC Hong Kong
+852 2289 2084
jason.ka.lee@hk.pwc.com



Disclaimer and copyright

The information contained in this Report is of a general nature only. It is not meant to be comprehensive and does not constitute the rendering of legal, tax or other professional advice or service. Before taking any action, please ensure that you obtain advice from your professional advisers.

All contents of the Report are provided “as is” with no representation or warranty, express or implied, including warranties of accuracy, completeness, timeliness, fitness for a particular purpose, appropriateness to your situation. To the extent permitted by law, HKCGI, PwC Hong Kong, their respective partners, employees and relevant agents shall be liable to you or any third party for any loss, damage or expenses arising out of use of this Report, even if advised of the possibility of such damages.

The materials contained in this Report were assembled on 1 August 2023 and were based on information available at that time. HKCGI or PwC Hong Kong is not responsible for updating the information contained in this Report after its publication.