



MOBIUS
GROUP



CYBER SECURITY SURVEY REPORT

November 2023



TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
THE PARTICIPANTS	4
KEY FINDINGS	6
INCIDENTS AND ROOT CAUSES	9
INFORMATION ASSETS	11
GOVERNANCE AND DRIVERS	13
IMPROVEMENT INITIATIVES	15
STAFF AND SKILLS	16
ADDRESSING THE CYBER CHALLENGES	17
MEET THE MOBIUS GROUP EXPERTS	19
CONTACT US	22

EXECUTIVE SUMMARY

This is the third edition of the Mobius Group Cyber Security Survey, and this year, the results echo the shifting cyber landscape that our world is going through. Our 2022 survey was conducted just after our clients had completed securing remote access to systems and scrambling to secure the need to work from home. This survey highlights that cyber security maturity improved, with gains in securing infrastructure, remote access, improved protection against Ransomware, and being better prepared to respond to an incident. And although there has been a decrease in the number of successful attacks, it also highlights that attacks are becoming increasingly sophisticated and lead to far-reaching impacts, with major data breaches leading to reputational damage, a breakdown in trust and increased regulatory implications.

The 2023 survey highlights that cyber security initiatives must adapt to businesses formalising their plans for future expansion and a post-pandemic digital boom. Organisations are putting those plans into action by accelerating their digital journeys, completing their cloud migration, implementing digital platforms, and starting to leverage big data and modern technologies.

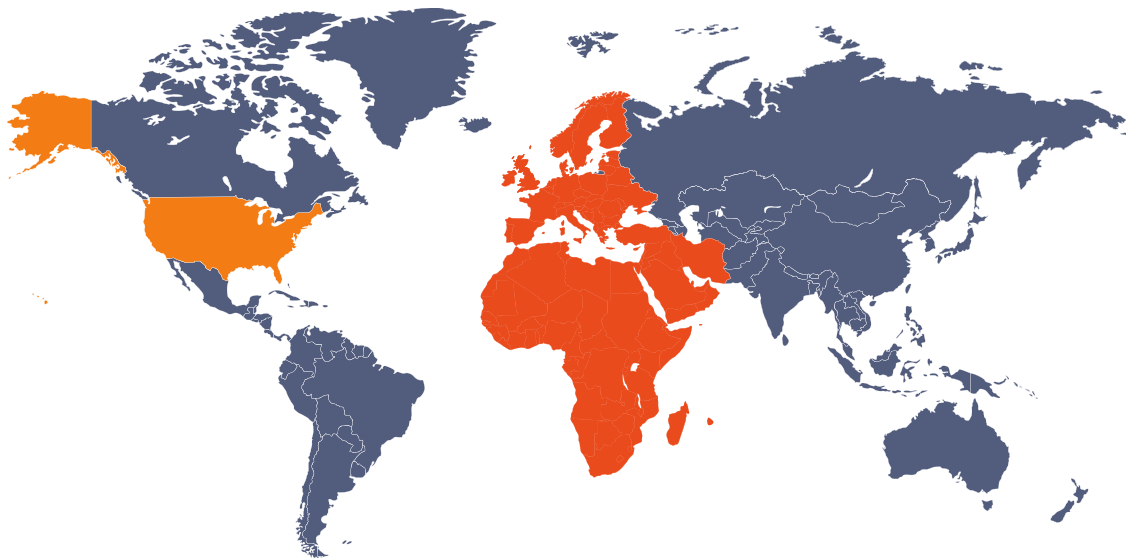
The survey results also highlight that, as part of this journey, organisations seek to understand their new risk landscape and the need to be more proactive in preventing major incidents. Social engineering and security awareness are still a challenge and need fresh ideas to instil good habits amongst users. Identity and Access Management, Data Security, and web interface security are increasingly in focus, with identity and data volumes growing exponentially as digital services are required for organisations to remain competitive. The increase in partners also requires that Third Party Risk Management capability and capacity be improved.

Cyber security management and operations teams must develop new skills to understand and manage threats to the digital landscape, and to contribute to the organisation's requirement to secure digital trust.



THE PARTICIPANTS

Most respondents were from organisations within the regions we serve, namely Africa, Mauritius, the United Kingdom, Europe, and the Middle East, as well as some respondents from North America.



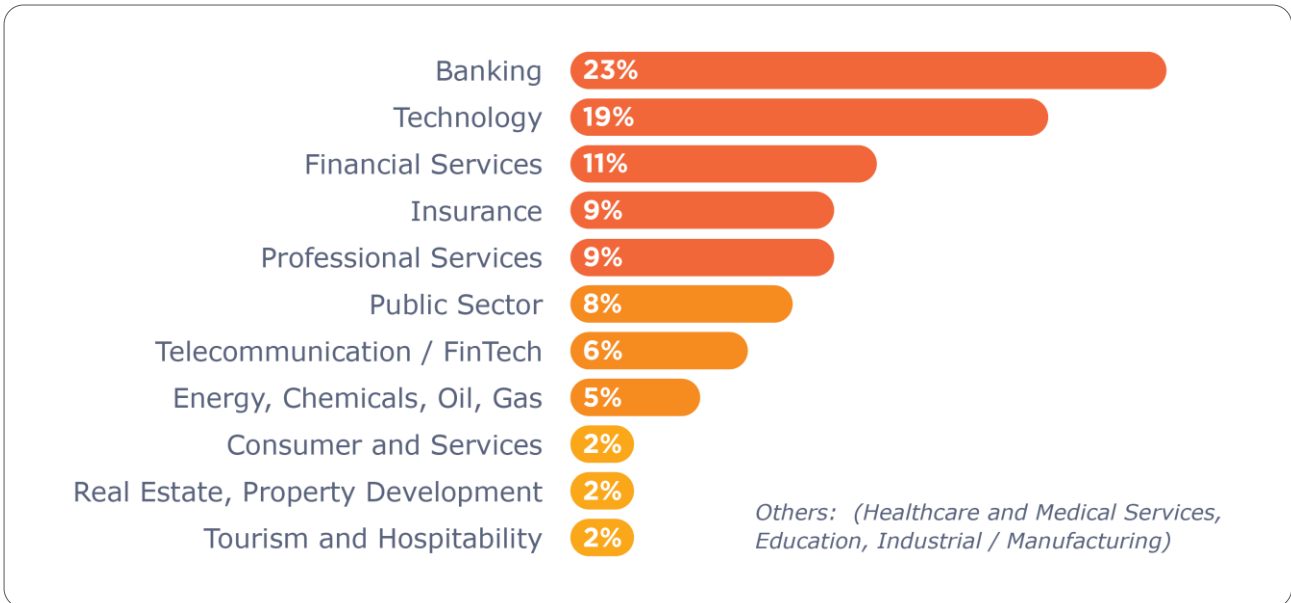
In keeping with our survey objectives of being able to compare year-on-year changes, we once again asked these organisations about the following:

- Cyber trends and challenges
- Levels of cyber security maturity
- Incidents and major threats
- Initiatives to reduce cyber-related risks

We also added a few new questions in line with the rapid advancements in the technical and threat landscapes, as well as the evolving regulatory and compliance requirements.



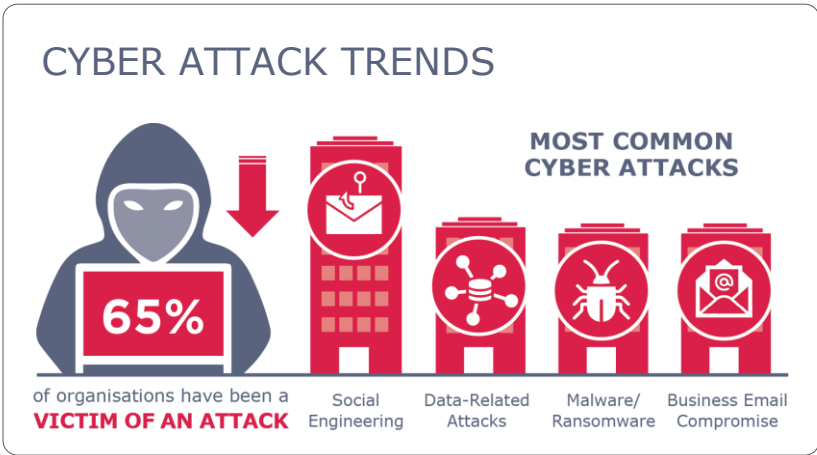
Respondents to our survey were predominantly our clients that span a broad demographic of industries and included clients that are global market leaders with tens of thousands of employees, to medium-sized enterprises with fewer than a hundred employees.



The individual roles of the respondents included the following:

- C-Level Executives
- GRC Management
- IT and Information Security Management
- Various specialist roles across GRC
- Cyber security Operations Management

KEY FINDINGS



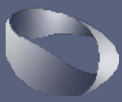
Fewer organisations experienced a breach in the last 12 months (down from 72%). Attack types experienced have not changed, except that Business Email Compromise has become very prevalent and is now on the list of top attacks.



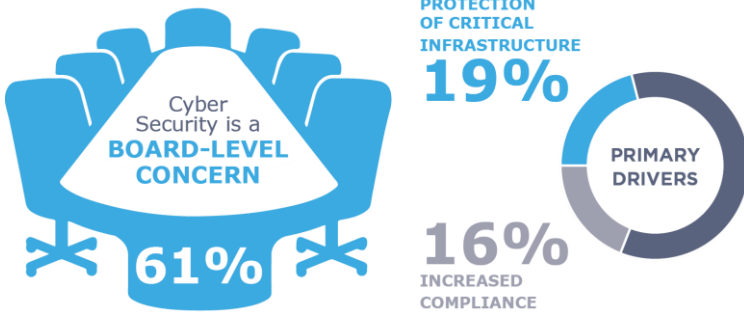
With an increase over our last survey, 65% attributed the lack of security awareness as the primary root cause of breaches. Top weaknesses include:

- third parties with inadequate controls (still top of the list)
- inadequate Identity and Access Management
- inadequate monitoring of cyber threats

Untested incident response processes fell off the list as most have performed simulations in the last 12 months.



STRATEGIC ALIGNMENT



Cyber security remains a board-level standing agenda item for most organisations.

Primary drivers include:

- protection of infrastructure
- increased compliance requirements
- reduced damage to reputation, business disruptions, and increased pressure from clients and third parties

CYBER SECURITY GOVERNANCE, RISK AND COMPLIANCE



Most organisations are adopting a combination of frameworks and standards that include a mix of ISO 27001, NIST CSF, COBIT, SANS CIS and industry-specific standards.

36% of organisations rate their cyber security maturity as defined and managed, a decline from 44% last year.

CYBER SECURITY SKILLS



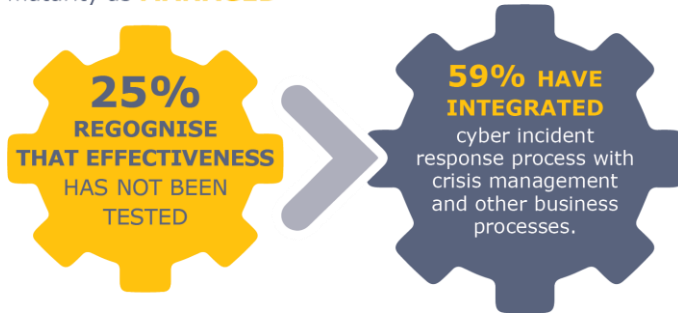
49% of cyber management indicated that they are understaffed, which is better than last year's 60%.

Skills in demand:

- Security Testing – Penetration Testing, Web and API Testing
- Threat Management – Threat Intelligence, Threat Hunting, and Threat Remediation
- Information Asset Management – due to massive increases in data volumes and increased risks of data breaches

INCIDENT RESPONSE READINESS

Most organisations rate their **INCIDENT RESPONSE** maturity as **MANAGED**



Organisations continue to improve their incident response processes, plans and playbooks.

- 25% are shifting their focus to effectiveness testing of the processes
- 59% indicated that cyber incident response was not yet fully integrated with other processes

Most organisations have **NOT DEVELOPED A THREAT PROFILE** specific to their organisation.



Most organisations have still not developed a threat profile specific to their organisation. The areas that management believes require the most cyber security remediation have shifted from Cloud to:

- Third-party access
- Active Directory
- Application Programming Interfaces
- Legacy Systems

PROGRAMMES AND INITIATIVES



Cybersecurity management areas that require the most improvement

- Proactive threat management practices and cyber operations
- Improved understanding of current posture
- Awareness and training

50% of organisations have a defined cyber security programme, although budgets remain very tight.

Cyber initiatives that organisations believe will most positively impact their cyber posture:

- Proactive threat management practices and cyber operations
- Improved understanding of current posture
- Awareness and training

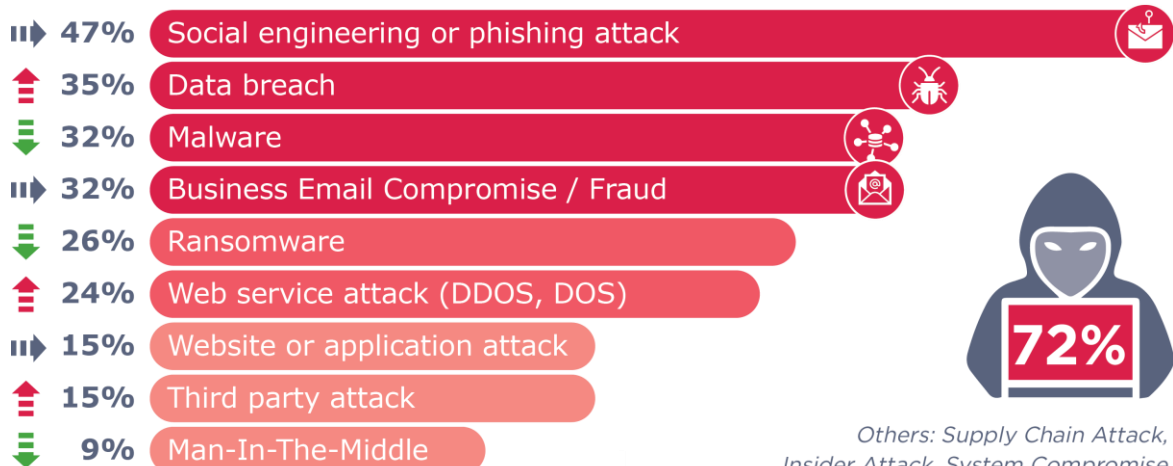
INCIDENTS AND ROOT CAUSES

65% of the respondents indicated that they had experienced some form of cyber breach over the last 12 months, and this is an improvement over the 72% of the previous 12 months. However, most organisations have also indicated higher levels of impact as incidents have resulted in serious data breaches and disruptions to business.

Social engineering remains the number one attack type and there is also an increase in web service attacks and attacks via third parties. Organisations have had to focus on **ransomware** and **malware** in the previous 12 months and the efforts have resulted in a general decrease in these malicious code types of attacks.

Web Applications and APIs remain high, and this can be attributed to the high-level exposure of these attack surfaces. Business Email Compromises are also still very prevalent, and this is due to the attack being relatively easy to execute without much technical expertise.

CYBER SECURITY INCIDENTS (last 12 months)



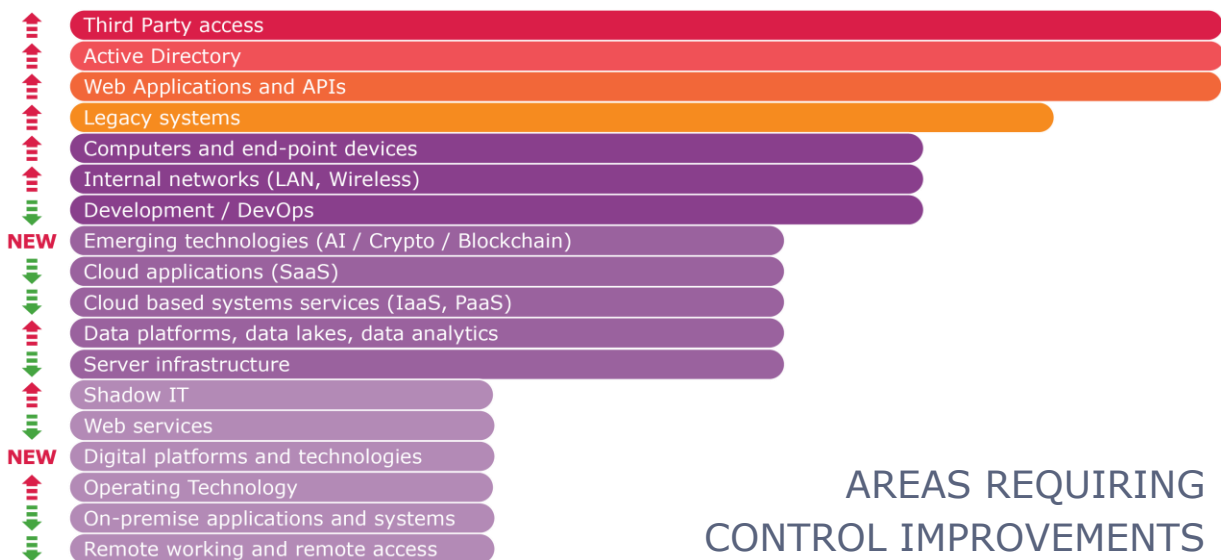


The primary root causes remain **awareness** and **third parties** with inadequate controls. The rest of the root causes have changed significantly over the last 12 months. During and post-COVID saw most organisations focusing on improving technical controls to support remote working, including secure remote access and cloud-based application security, and these initiatives have resulted in a decline in these areas as root causes. Respondents have cited failures in management controls, including Identity and Access management, and Third-Party risk practices, as high-ranking root causes.

ROOT CAUSES OF BREACHES



Two new entrants in the technology areas that cyber management identified as requiring control improvements are not surprisingly Emerging Technologies such as AI and Digital Platforms for large data, as these technology areas ARE becoming more widely adopted and mainstream.



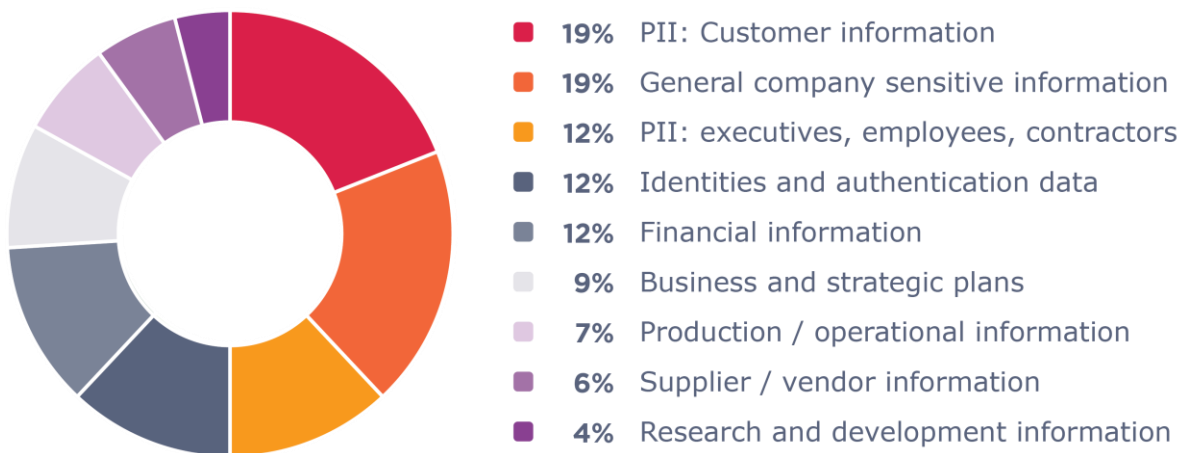
AREAS REQUIRING CONTROL IMPROVEMENTS

INFORMATION ASSETS

New for this year’s survey is information about our client’s information and data. We asked the respondents to rank the information assets they deemed to be the most valuable, either from a company-value or a risk perspective.

Personally Identifiable Customer Information is ranked the highest, above general company-sensitive data. Personally Identifiable information of employees and workforce ranked third highest, and this can be attributed not only to privacy legislation, but also to the fact that this information can be used for a variety of attack methods.

MOST VALUABLE INFORMATION ASSETS

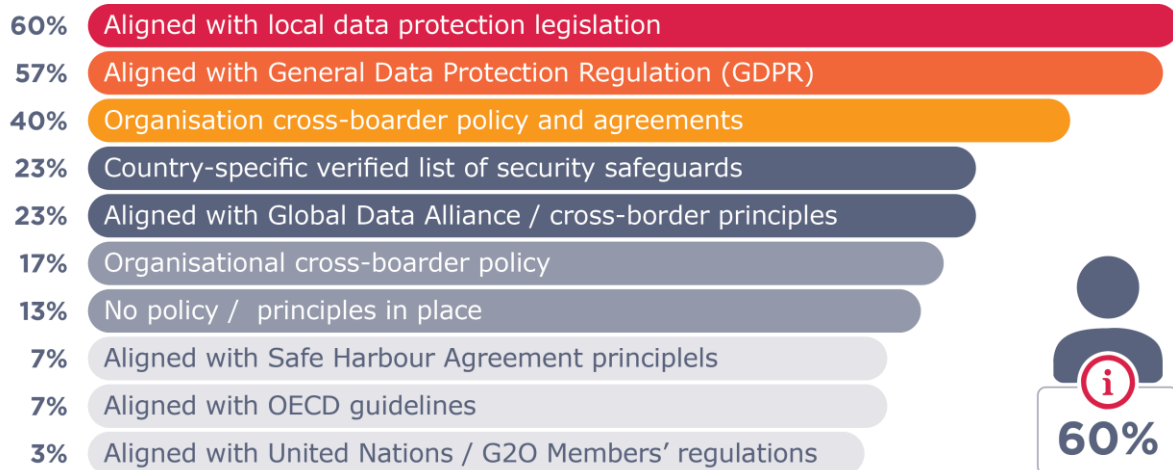




GOVERNING AND MANAGING PERSONALLY IDENTIFIABLE INFORMATION

Since Personally Identifiable Information was ranked as the most valuable, we asked the respondents what they based their PII data processing principles and policies on. Most organisations have aligned firstly to local legislation and then to the General Data Protection Regulations.

PRINCIPLES AND POLICIES USED TO GOVERN AND MANAGE PII DATA PROCESSING



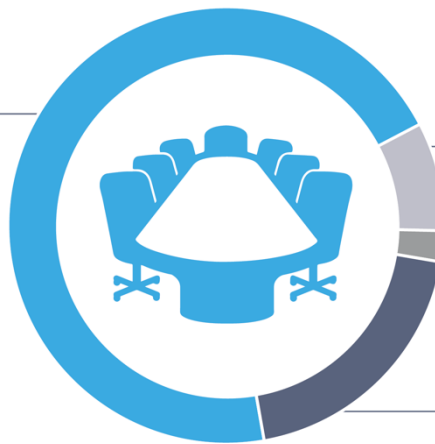
GOVERNANCE AND DRIVERS

Most organisations confirmed that cyber security is still a concern at the highest levels, with cyber as a standing board meeting agenda item. Once again, this highlights that cyber risk is amongst the top risks globally and that organisations are significantly concerned with the potential impacts of cyber-attacks or breaches.

CYBER SECURITY – A BOARD LEVEL CONCERN

61%

Standing Board agenda item



7%

Unsure

2%

No

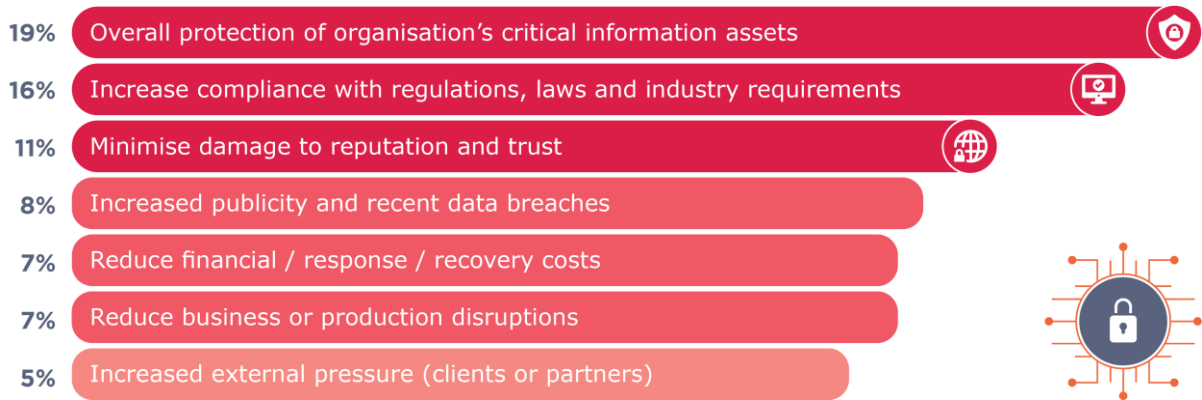
17%

Adhoc Board agenda item



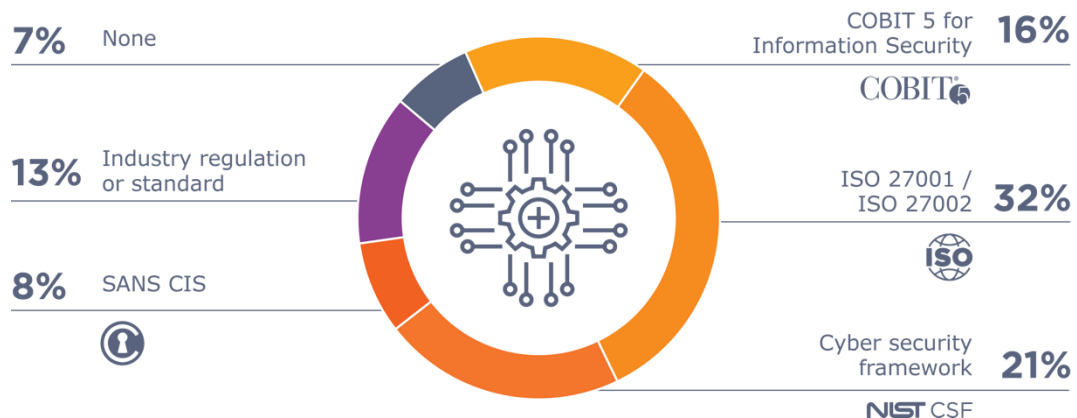
The organisational drivers of cyber security have not changed since last year. The general protection of the organisation’s critical information assets remains the primary driver, with increased compliance and the potential of reputational damage rounding out the top three. What has changed this year is that key initiatives and skills gaps centre around information asset management demonstrate that organisations’ cyber strategies are closer aligned to the primary drivers.

ORGANISATIONAL DRIVERS OF CYBER SECURITY



To manage cyber security risks, most organisations have adopted a combination of cyber risk management frameworks and standards. ISO 27001, NIST CSF and COBIT are still the most relied-upon control frameworks, with SANS CIS and industry-specific standards the most utilised for technology security. From previous years, we see an increase in the use of ISO from 27% last year to 32% this year, and NIST has also increased from 17% to 21%.

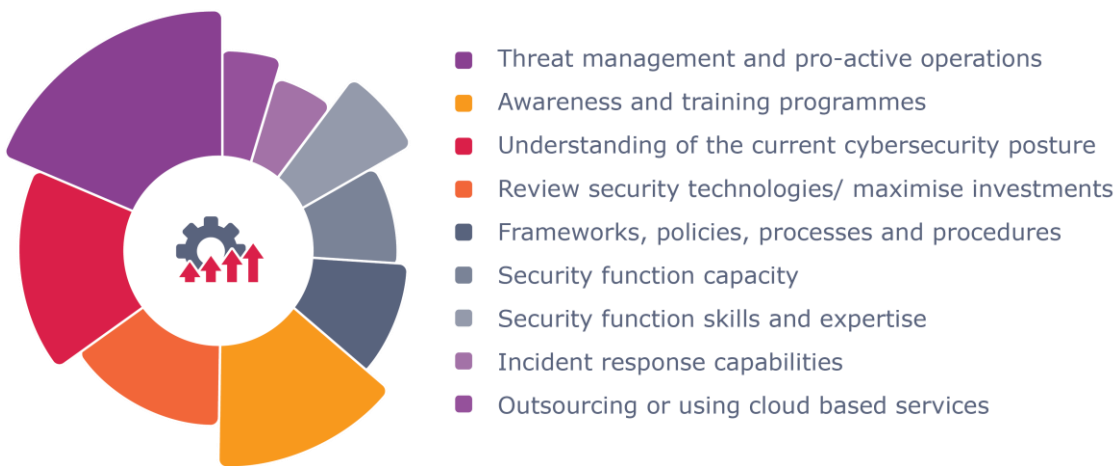
FRAMEWORKS USED BY ORGANISATIONS



IMPROVEMENT INITIATIVES

Most organisations have developed a cyber improvement programme. Although awareness is still a high priority, most organisations have threat management as the highest priority. Knowing the organisational security posture remains a key initiative. Optimising the use of existing security technologies, instead of investing in additional technologies, remains high on the programme as cyber security functions are expected to maximise the return on technology investments and reduce costs.

PRIORITISED IMPROVEMENT AREAS



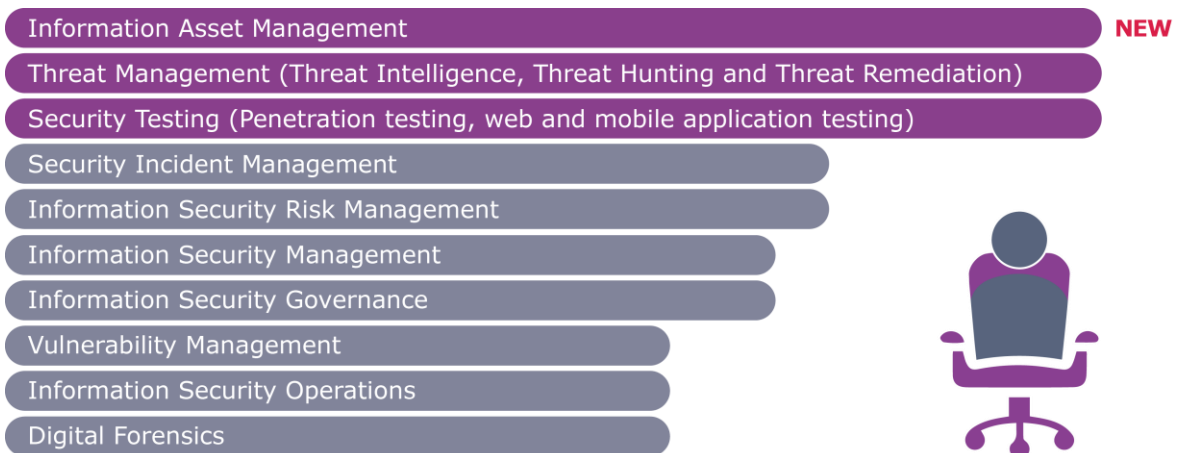
The survey also canvassed respondents to rank the initiatives they believe will positively impact their cyber posture. The statistics support many other areas of the survey which show that organisations are focusing on proactive measures and preventative controls, namely:

- proactive threat management practices
- awareness and training
- better understanding of current cyber security posture and threats

STAFF AND SKILLS

The survey highlighted the continued growing demand for cyber skills, with just under half (49%) of organisations indicating that they did not have adequate staff capacity. A new category of skill that most organisations are looking for is Information Asset Management. This is due to the masses of new data volumes being captured and used by organisations as part of their digital strategies. This data is not only being stored, processed and used in centralised data lakes and digital platforms, but also exists as unstructured data that is spread throughout the organisation. This data is being used in business-led systems and solutions as well as modern technologies such as User Data Analytics, RPA, AI, and others. There is a growing trend to be able to use Information Asset Management tools and techniques to manage and secure the sprawl of data.

SECURITY SKILLS SHORTAGES





ADDRESSING THE CYBER CHALLENGES

The Mobius approach to addressing the risks, threats and challenges highlighted in our survey is based on three fundamental tenets:



KNOW YOUR RISK LANDSCAPE

Let us confidently accelerate your digital journey by helping you know your risk landscape.



DEVELOP YOUR DIGITAL RESILIENCE

We work with you to develop sustainable data risk resilience into your business systems.



SECURE YOUR DIGITAL JOURNEY

Have confidence in your secure digital risk landscape.

At Mobius, we believe organisations cannot confidently accelerate their digital journey without trust. That's why we work with our clients to develop sustainable data risk resilience into their business systems, building and implementing practical and relevant solutions that ensure they know and can secure their digital risk landscape.

GOVERNANCE, DRIVERS, MANAGEMENT AND SKILLS:

The survey highlighted the need to ensure that cyber has full support across the organisation, that it is risk-based, and is sufficiently resourced and skilled. Consider utilising an Information Security Management System (ISMS) based on ISO standards as the basis for driving your cyber security programme. The Mobius Consulting teams across Africa and Europe have extensive ISO experience and can guide you on how to start your ISMS journey.

THE NEED FOR SECURITY TESTING:

Many organisations cite a lack of testing skills and an understanding of their cyber security vulnerabilities. We recommend that you utilise external experts, such as Mobius Binary, to perform your security testing and to obtain an unbiased view of your vulnerabilities.



UNDERSTANDING THREATS, AND BEING BETTER PREPARED:

The key to effective and efficient cyber security is firstly to understand the threats that apply to your organisation and to implement controls tailored to your environment. Incident response readiness was also highlighted as an ongoing theme by participating organisations. Consider using the Mobius approaches to cyber security to help address these challenges and to improve digital trust.

THE AWARENESS CHALLENGE:

Lack of awareness remains the number one root cause of cyber threats and the most important cyber initiative for most organisations. Address this challenge with interactive awareness programmes tailored for your business and team. Get in touch with us to arrange an awareness programme discussion with our experts.

MANAGING CYBER RISKS:

Many organisations indicated that they strive to consolidate cyber security management systems and use solutions that support their overall risk and compliance processes. We recommend you adopt a leading practice framework to mature your cyber security posture. Our experts can work with you on this journey.

THIRD-PARTY-RELATED RISKS:

Inadequate third-party security was the second-most common root cause of breaches and major cyber incidents. To combat this, consider solutions that focus on identifying and managing third-party security based on the actual risks presented by the third parties. Many organisations do not have the capacity or systems to manage third-party risks and are turning to specialist service providers like Mobius to provide a fully managed service as well as customised solutions to track and report on third-party risks.

PRIVACY REMAINS A KEY CONCERN:

Both customer and employee personal data is considered the most valuable type of data across all industries and is a primary target for malicious attackers. Additionally, a malicious data breach would have the biggest negative impact on most organisations. You can learn more on how to practically address privacy gaps by contacting the Mobius team.

INSIDER BREACHES:

A top concern for many organisations across industries is insider breaches. In response, a robust Identity and Access Governance (IAG)-based approach to users is essential. We recommend you adopt a holistic approach that considers all factors to offer a long-term solution to user access. Contact Mobius to learn more about our extensive Identity and Access Management methodologies and services.

MEET THE MOBIUS GROUP EXPERTS

**PATRICK RYAN****Group Strategist | Mobius Group**

Patrick Ryan is a leader in the Information Risk and Compliance sector and has led teams and projects across multiple industries in his 25 years of experience. Patrick's vision for the Mobius Group is to build a global network of like-minded people who collaborate and innovate to help clients tackle their information risk needs.

**LYNN MARTIN****Group Strategist | Mobius Group**

Lynn Martin (CRISC, CISA, CDPSE, CIPP/M, CIPP/T) has over 20 years of experience in the consulting world and a passion for the business side of consulting, which allows her to apply a diverse approach to technical and operational solutions. Lynn is currently focused on growing new markets for the Mobius Group worldwide.

**GRAEME HUDDY****Director | Mobius Binary**

Graeme has over a decade of experience in IT operations, Information Security consulting and auditing. Today, he leads Mobius Binary and a team of highly skilled penetration testers as they help organisations worldwide determine whether they are clearly secure.

**SANDHYA MOHAN-PILLAI****Managing Director | Mobius Consulting South Africa**

Sandhya Mohan-Pillai (CGEIT, CISA, CISM) has over 20 years of IT Consulting experience. She has successfully driven business growth in targeted markets across South Africa by leveraging her strong leadership skills, and is passionate about adding value in everything she does.

**AMANDA HECHTER****Senior Managing Consultant | Mobius Consulting United Kingdom**

Amanda Hechter (ISO 27001 Lead Implementer, ISO 27001 Lead Auditor, Systems Security Certified Practitioner) has 11 years of experience in Information Governance, Risk and Security. Amanda's vision is to be known as a problem solver in the Information Security industry and she hopes to instil this thinking and passion in the next generation of Information Security leaders.

**LOVENA J REDDI****Director | Mobius Consulting Mauritius**

Lovena J Reddi (BSc (Hons), MBA, CISM (CISA), CDPSE) has over 15 years of experience in the field of Information Technology. Lovena's role at Mobius Consulting Mauritius is to drive Mobius Consulting to be the leader and trusted partner in Information Security, Risk and Compliance both locally and internationally.

**RAYMOND DU PLESSIS****Director | Mobius Consulting South Africa
Cyber Security Service Line Lead**

Raymond du Plessis (CISSP, CISA, CISM, CRISC and CSX) has over a decade of experience in Information and Cyber Security. His vision is to help organisations become more proactive to counter modern cyber-attacks by developing pragmatic approaches and solutions to cyber threat management.

**YOLANDI MOODLEY****Director | Mobius Consulting South Africa
Information Security Service Line Leader**

Yolandi Moodley (ISO 27001 Lead Auditor and Implementer) has over 13 years of experience in Information Security and IT Risk Management. Yolandi understands the importance of Information Security Awareness in today's increasingly digitised world and is passionate about driving this for her clients as she sees first-hand the impact of effective awareness campaigns.

**CANDICE JACKSON**

Principal Consultant | Mobius Consulting South Africa Information Privacy Service Line Leader

Candice Jackson (CIPP/E, CGEIT, CISA, CRISC) has over nine years of IT consulting experience. Candice helps drive the maturity of the Information Privacy service line by applying a practical, compliant approach that is underpinned by intuitive technological innovation.




**CANDICE JAMIESON**

Principal Consultant | Mobius Consulting South Africa Technology Assurance Service Line Leader




Candice Jamieson (CIPM, CDPSE, CISM, CISA, CIA) is an experienced audit and risk specialist with 15 years of experience in Information Risk, Privacy and Security. Her goal is to drive sustainable change in organisations that will achieve Governance, Risk and Compliance targets by implementing practical steps to improve day-to-day operational processes.

CONTACT US




SOUTH AFRICA

-  info@mobiusconsulting.co.za
-  www.mobiusconsulting.co.za
-  [mobius-consulting-south-africa](https://www.linkedin.com/company/mobius-consulting-south-africa)




MAURITIUS

-  info@mobiusconsulting.mu
-  www.mobiusconsulting.mu
-  [mobius-consulting-mauritius](https://www.linkedin.com/company/mobius-consulting-mauritius)




UNITED KINGDOM

-  info@mobiusconsulting.co.uk
-  www.mobiusconsulting.co.uk
-  [mobius-consulting-uk](https://www.linkedin.com/company/mobius-consulting-uk)

MOBIUS BINARY

-  info@mobiusbinary.com
-  www.mobiusbinary.com
-  [mobius-binary-clearly-secure](https://www.linkedin.com/company/mobius-binary-clearly-secure)

PHINITY RISK SOLUTIONS

-  info@phinityrisk.com
-  www.phinityrisk.com
-  [phinity-risk-solutions](https://www.linkedin.com/company/phinity-risk-solutions)