2021 AUSTRALIAN CYBERSECURITY RISK REPORT

Understanding Australian businesses and their approach and attitudes toward cybersecurity

CONTENTS

VARONIS

ABOUT THE REPORT

The 2021 Australian Cybersecurity Risk Report is our inaugural report into the cybersecurity landscape across small to large businesses in Australia.

This report focuses on the approaches businesses are taking towards securing their systems and data and reveals the concerns individuals have around the business impacts of a potential cyber-attack within their organisation.

This report was compiled from over 515 responses from individuals in C-Level and Senior Management roles that have a key or final decision-making role in businesses covering a number of industries, including IT & telecoms, financial services, government, manufacturing, professional services, education and healthcare.

This results are nationally representative and weighted to the 2016 ABS Census to ensure accurate representation.

The report aims to help businesses better understand their cybersecurity landscape and provide valuable insights into what businesses can do to minimise the risks and repercussions of a potential cyber-attack.

Our Approach

10 questions

A detailed exploration of approach and attitudes to cybersecurity

N=515 sample

A robust sample of Australian businesses

Weighted data

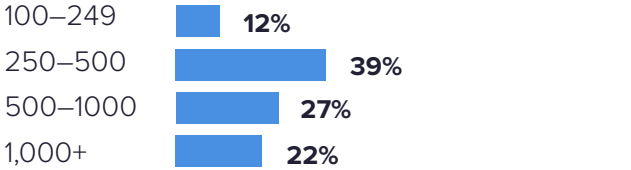
Sample weighted to the 2016 ABS census to ensure representivity

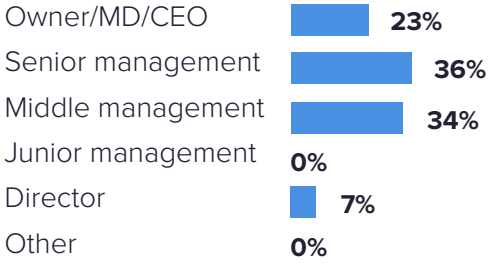
Nationally representative

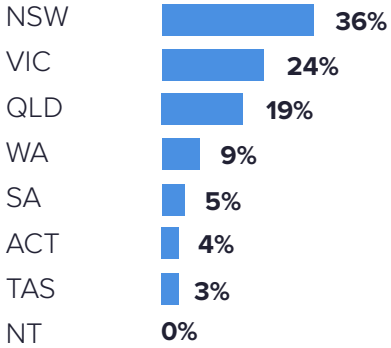
Talking to Australians in all states and territories

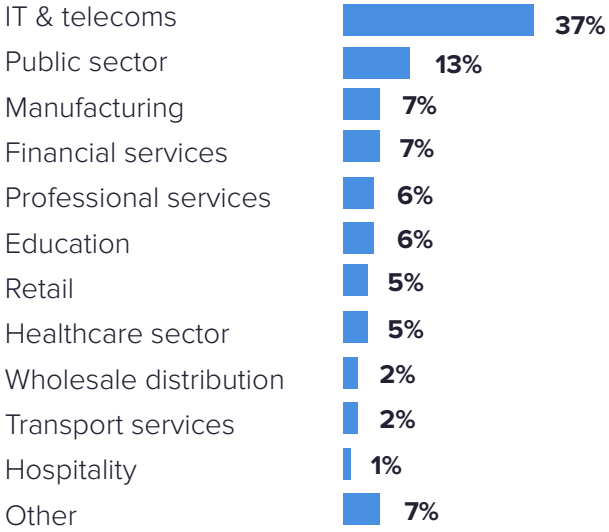
UNDERSTANDING OUR SAMPLE

Demographics









*Percentages rounded to the nearest decimal.

STATE OF THE INDUSTRY

Data breaches and cyber-attacks have been rising steadily in Australia since the beginning of the COVID-19 pandemic. Ransomware attacks in particular have proliferated across the world and are growing in sophistication and maliciousness.

Under Australia's Notifiable Data Breach scheme, more than 1,000 data breaches were reported between January and December 2020. Data breaches are becoming more costly and time-consuming to recover from. IBM reported the average cost per data breach in 2020 was AUD $3.35 million, an increase of 9.8% from the previous year, and took an average of 211 days for businesses without security automation to recover from.

Notably, data breaches resulting from human error have increased significantly, accounting for 38% of all notifications and rising by 18% from June 2020.

Despite the rising proportion of breaches attributed to human error, malicious or criminal activity is still the most common cause of data breaches in Australia, accounting for 58% of incidents in the second half of 2020.

Under Australia's Notifiable Data Breach scheme, **more than 1,000 data breaches** were reported **between January and December 2020.**

STATE OF THE INDUSTRY

It is important to note that some industries are disproportionately affected by data breaches. Data obtained from the Office of the Australian Information Commissioner (OAIC) revealed the health sector maintains the highest incidence of data breaches, reporting 23% of all breaches. Healthcare is followed by finance, which reported 15% of all breaches. For the first time, the 'Australian Government' sector, which refers to all federal government agencies, entered the top five affected industry sectors, reporting 6% of all breaches.

Identity information was exposed in 45% of the total reported data breaches, while financial details, such as bank account or credit card numbers, were exposed in 40% of breaches. Furthermore, health information was exposed in 26% of breaches, while tax file numbers were exposed in 18%.

The consistent rise in data breaches and the increase of security incidents caused by human error demonstrates that more action should be taken at a board and executive level to improve cybersecurity awareness and organisational resilience against cyber-attacks. Cybersecurity must be included as a board-level agenda item to ensure organisations maintain compliance with ever-changing regulations.

Cybersecurity Risk Report
Key Findings

Data theft and loss, human error and insider threats are the biggest cybersecurity concerns for one in two businesses.

Around **one in five Australian businesses are less than confident** about the storage of their organisations' sensitive information.

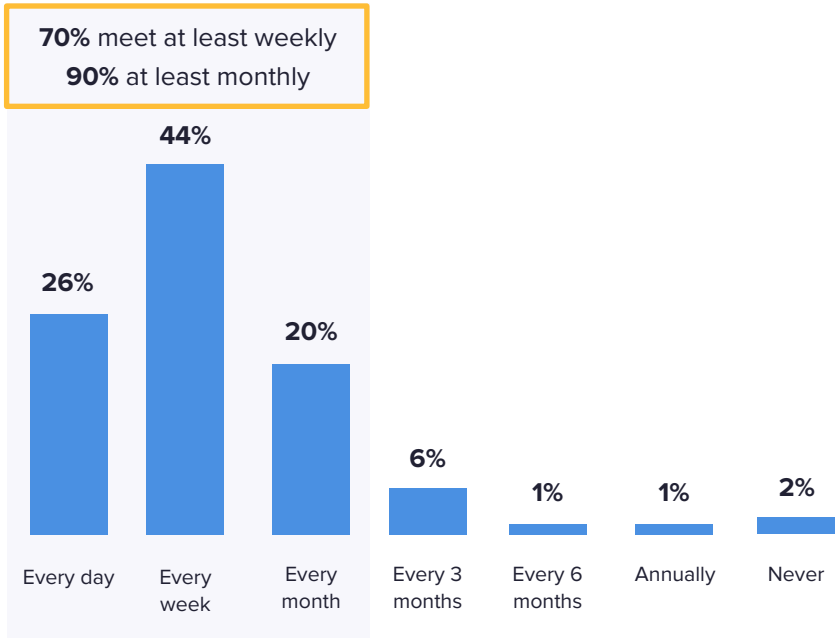
Personal data and financials from a business and its customers are anticipated to be the **most likely targets for a cyber-attack.**

Four in five Australian businesses are confident in their organisation's ability to withstand a cyber-attack.

Despite this confidence, almost **two-thirds think a potential cyber-attack on their organisation is likely** in the next 12 months.

ORGANISATIONAL AWARENESS

How often does your team meet and communicate on IT security issues, risks, and organisational initiatives?



Cyber risk awareness and discussions

A quarter (26%) of all respondents meet with their teams daily around security and IT issues. 44% meet at least once a week, while 20% only meet once a month.

It's positive to see a large proportion of organisations prioritising collaboration.

The pandemic and the move to remote working drove organisations to increase investments in cybersecurity and IT infrastructure. Furthermore, the recurring theme of ransomware attacks in the news cycle, including high-profile breaches within global corporations and critical infrastructure, have amplified the need for improved security protocols within organisations. Collectively, these factors may have resulted in increased communication on cyber risk.

Organisations need to introduce strategies that help them understand and address the threat landscape, today and in the future. It is evident that organisations must take real preventative action to reduce the risk of data breaches.

KEY BUSINESS CONCERNS

The biggest cybersecurity concerns facing Australian businesses

It is unsurprising that respondents listed data loss or theft as the biggest cybersecurity concern facing their organisations (53%). Following this closely is 'human error' (40%) and 'insider threats' (37%). While many organisations place their main focus on warding off external attackers, internal actors can put data at risk, whether through careless accidents or malicious intention. This human element is an area that many organisations forget to focus on.

The survey results demonstrate that organisations recognise the significant role human error plays in data security. However, the fact that it remains so high on their list of concerns may indicate the need for increased cyber education in the workforce, which could reduce the incidence of attacks caused by human error.

A study by IBM found that human error was a major contributing cause in 95% of all data breaches. This means that without human error, the majority of cyber-attacks can be avoided.

Over a third (37%) of organisations recognise rogue insiders as one of the greatest cybersecurity threats facing their organisations, however protecting against insider threats can be particularly challenging. An internal attacker has a strong head start on any external player: they often know what data is valuable and where to find it, and they don't need to gain access and insert malware to gain access to systems.

Having a good data management policy is key to spotting attempted insider attacks and identifying the perpetrators. Conversely, poor or non-existent data management policies enable internal attackers to go unnoticed.

Thinking about the biggest cybersecurity concerns facing my organisation, which of the following are the three greatest concerns?

Data loss or theft	**53%**
Human error	**40%**
Insider threats	**37%**
Ransomware	**33%**
Hacktivism	**28%**
Breaches	**24%**
Foreign threat actors	**22%**
Intellectual property theft	**21%**
Data alteration	**19%**
Mobile	**13%**
Cloud	**9%**

BUSINESS IMPACTS AND ISSUES

Loss of brand reputation is a greater cybersecurity concern for organisations than loss of IP

Overall, loss of brand reputation is the biggest concern for organisations surveyed.

In fact, if a breach is poorly managed, customers are likely to lose trust, dissociate from the business or service and shop with a more secure competitor.

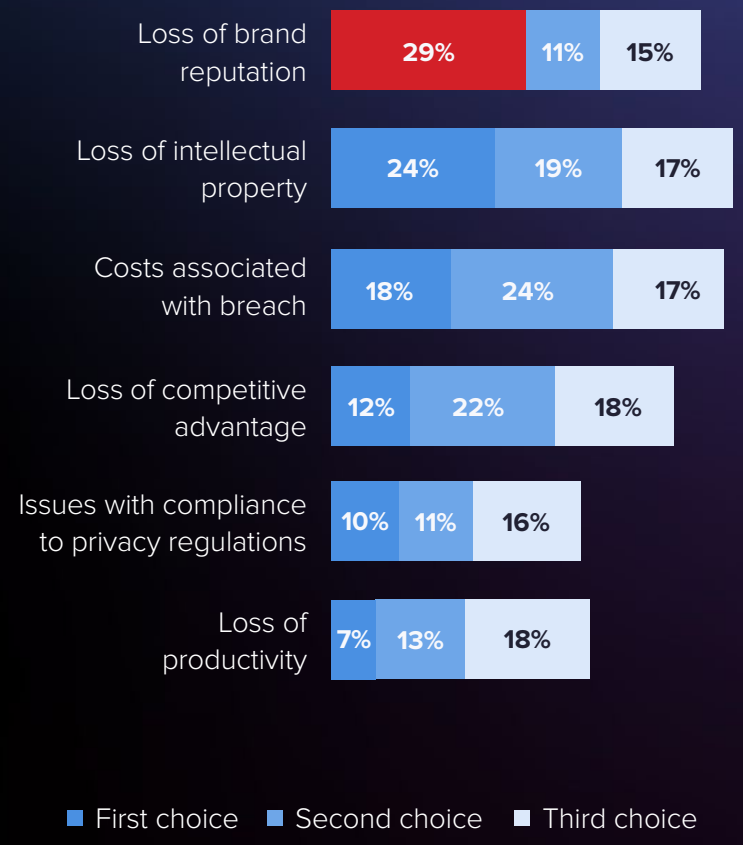
Loss of intellectual property is the second most important issue marked by respondents. Any company's intellectual property is valuable. Unfortunately, it's also one of their most vulnerable assets, making a tempting target for attackers.

Unsurprisingly, cost is the third biggest issue identified by respondents. The period following a data breach is not an easy one for companies. Time and money are spent to effectively manage a crisis, with even more time and money spent on the aftermath. These expenses include upgrades to security solutions and the cost of external security consultants.

It is important to note that loss of brand reputation, loss of intellectual property, and costs associated with the loss of current customers and competitive advantage are significant as well.

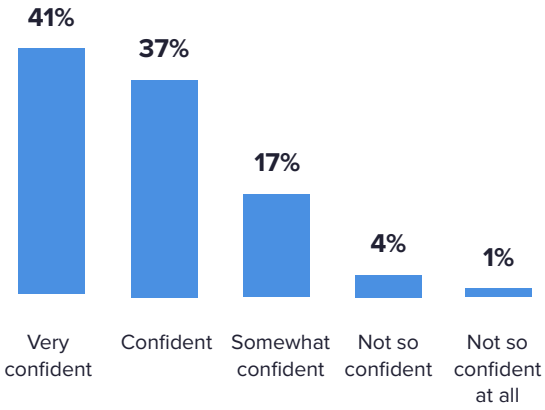
With significant updates to the Australian Privacy Principles due to pass through as legislation in the near future, data security and protection of personal information should be center stage within organisations. It is crucial that all businesses take cyber security seriously to protect not only their client's information, but their reputations as well.

Thinking about a possible breach in cybersecurity, please rank in order of importance the following business issues.

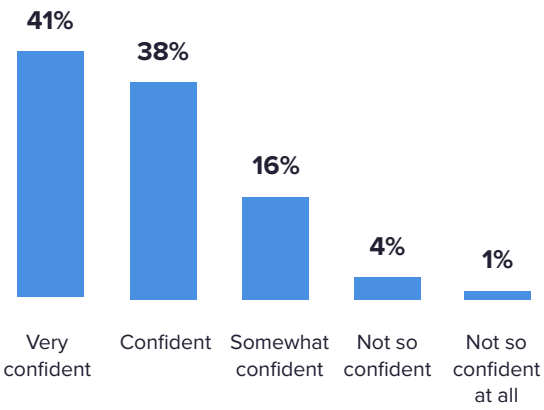


MEASURING BUSINESS CONFIDENCE

How confident are you that you know where all your organisation's structured and unstructured data is kept (DMS, PMS, Network drives, cloud, on-prem)?



How confident are you that you know where all your organisation's sensitive data (customer and employee personal information, customer and business financial information, PHI, etc) is kept?



*Structured data is stored in a predefined, fixed format, usually a relational database (RDBMS). It is organised in rows and columns and is easy to analyse and search, and can include items like phone numbers, names, and postcodes, such as in an airline reservation system. Unstructured data is essentially everything else—data which is not organised in a predefined way and is stored in its original format, such as videos, mp3s and emails. Unstructured data requires more work to process and understand, due to the different formats its stored in.

One in five businesses aren't confident about where their sensitive data is kept

One in five (21%) respondents are less than confident about where their unstructured and structured data is kept. One in five respondents are also less than confident about the location of their most sensitive data, which includes customer and employee personal information, customer and business financial information, personal health information etc. This presents organisations with a critical level cyber risk.

However, this risk is further exacerbated by remote working, which has connected a new range of personal devices to the corporate network. For example, employees are using VPNs to connect to the corporate network with their mobile phones, personal laptops and more, which frequently lack the same level of protection as company devices.

With so many more places for data to end up, it is imperative that organisations improve visibility into the locations of their most important information and assets. The high value of sensitive data, combined with the lack of knowledge over WHERE this data is located, and WHO has access to it, makes these organisations prized-targets for threat actors.

STORING SENSITIVE INFORMATION

Almost three quarters of Australian businesses store sensitive information in Microsoft 365

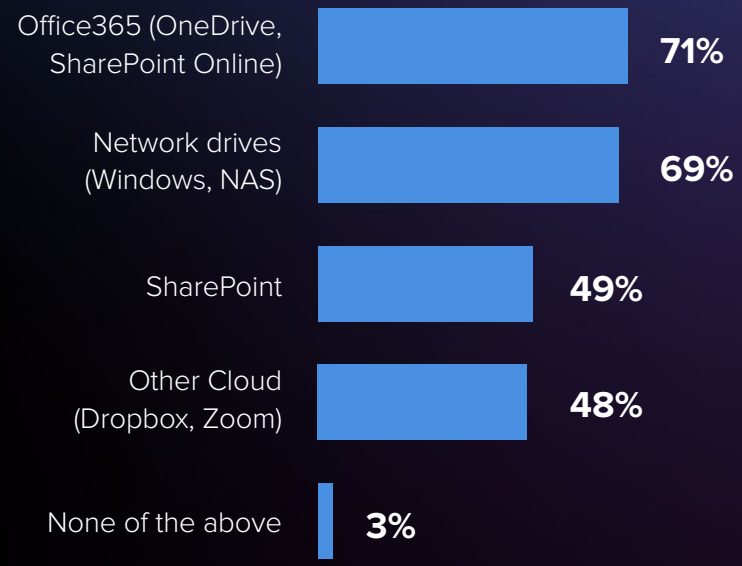
71% of organisations store sensitive data in Microsoft 365. With the onset of COVID-19, many organisations rushed to implement cloud-based services such as Office 365, which allow workers to collaborate remotely.

While these services facilitate collaboration, they also expose organisations to a new range of security vulnerabilities, significantly increasing cyber risk. Furthermore, these cloud-based programs are frequently accessed by BYO devices that are far less secure compared to corporate devices, further increasing cyber risk.

Many Australian organisations rely on a hybrid model in which some data is stored in the cloud and some on-premises. Some enterprises are adopting a cloud-first approach while continuing to store at least a portion of their environment on-premises.

Your security must address who's accessing your data on-premise and in the cloud, and provide visibility to ensure that only the right people have access to data at all times, all use is monitored, and abuse is flagged.

How many different locations does your organisation store sensitive information?



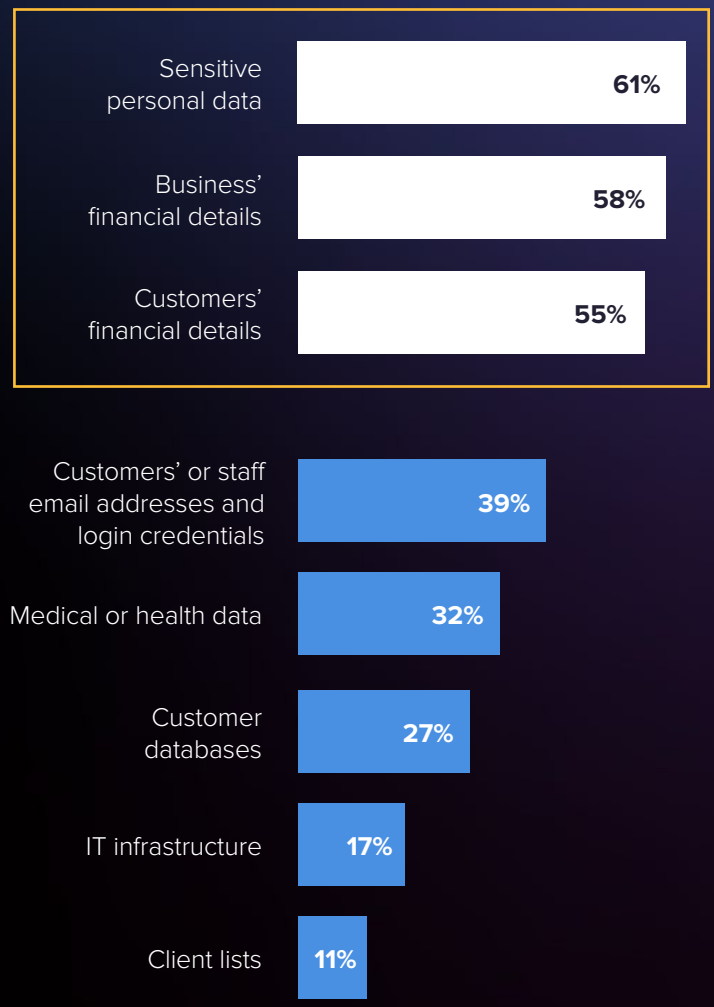
WHAT'S THE MOTIVATION BEHIND AN ATTACK?

Organisations believe employee's personal data is just as much of a target as business-related data

Respondents believe the most likely target for a cyber-attack is sensitive personal data, such as employee information (61%), followed very closely by the organisation's financial details (58%) and customer financial details (55%).

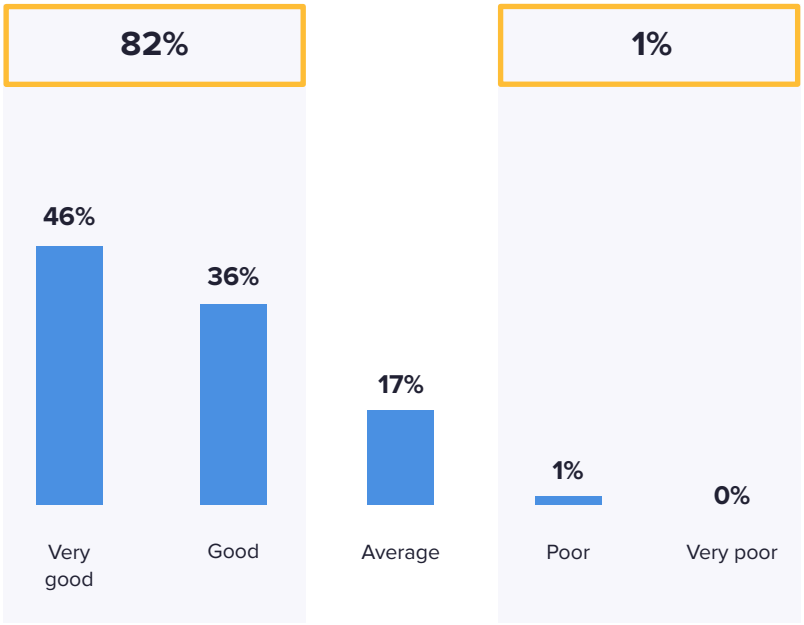
Today's threat actors are big-game hunting: once they get inside an organisation's systems they will silently gain high-level access to Active Directory (aka "the keys to the kingdom")–which makes it possible for them to go wherever they like and do whatever they like. They can steal information before unleashing a ransomware attack. If a victim doesn't pay, cybercriminals can still turn a profit by selling the data. Some may publicly release a portion of the stolen information to extort victim organisations into paying the ransom.

If your organisation were to be the target of a cyber-attack, what do you think would be the primary motivation to attack your organisation?



HOW PREPARED ARE BUSINESSES?

How do you rate your organisation's ability (staff, resources, technology) to protect itself or respond to a cyber-attack?



Resilience or overconfidence

82% of respondents rated their ability to protect themselves from a cyber-attack as good or very good, yet businesses take an average of 233 days to detect and contain a data breach.

The steady rise in data breaches in 2021, combined with organisations' long breach detection time-frames and the undeniable factor of human error, points to a serious overconfidence in organisations' ability to protect themselves against a cyber-attack.

This also points to an underestimation of the sophistication of ransomware. Attacks are evolving. Zero Day attacks leverage known flaws in software. In supply chain attacks like SolarWinds, attackers place malicious code in software disguised as legitimate updates.

This overconfidence is a key issue preventing cybersecurity from becoming a more prominent issue at the board and executive level. Organisations may remain confident until a breach happens to them, when it's already too late to act.

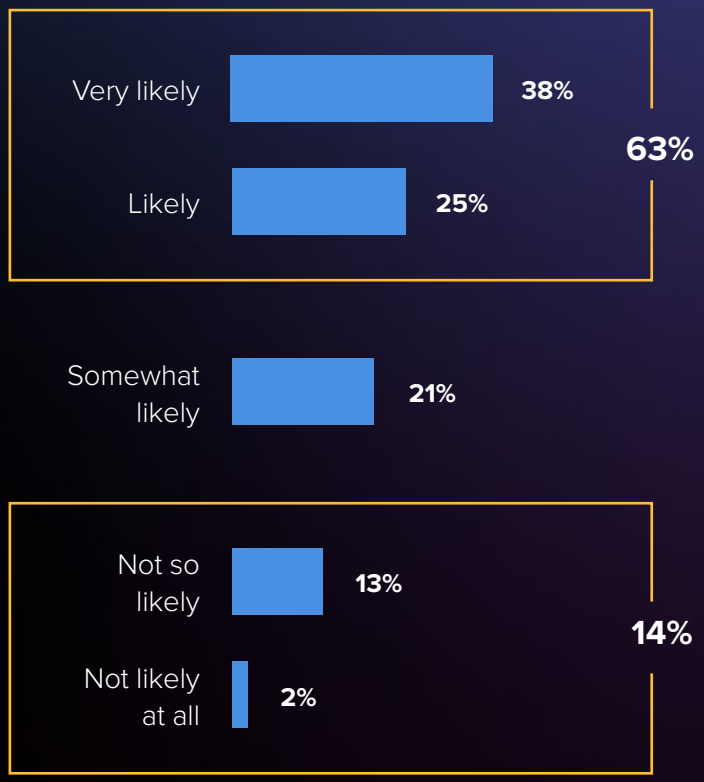
IS YOUR BUSINESS A TARGET?

Cyber risk over the next 12 months

Almost two thirds (63%) of respondents reported it is very likely or likely that their organisation would be the target of a cyber-attack/ threat in the next 12 months. This indicates strong awareness on cybersecurity threats, which is the first step in securing an organisation's data.

The key to reducing damage in the inevitable event of a cyber-attack is to implement a policy of Zero Trust. Zero Trust means to trust no one within the organisation. This approach can be supported with the use automated security tools which can prevent an attacker from moving laterally throughout the network, and gaining access to the most important or sensitive information.

How likely do you think it is that your organisation will be subject to a potential cyber-attack/threat in the next 12 months?



Don’t let remote work **put your data at risk.**

Get a free risk assessment.

GET STARTED

About Varonis

Varonis is a pioneer in data security and analytics, specialising in software for data protection, threat detection and response, and compliance. Varonis protects enterprise data by analysing data activity, perimeter telemetry, and user behaviour; prevents disaster by locking down sensitive data; and efficiently sustains a secure state with automation.