Raconteur

Cybersecurity: the boardroom agenda

panaseer

panaseer

Panaseer is a cybersecurity automation and data analytics company that helps organizations identify and fix gaps in their security controls to optimize their cybersecurity posture and stop preventable breaches. Panaseer's Continuous Controls Monitoring platform gives a complete, trusted view of security controls, with best practice metrics and measures guidance that improve collaboration and prioritization.

Contents

Cybersecurity in the boardroom: the new dynamic

Boards are becoming more attuned to cyber risks and security chiefs must speak their language to impart the right messages

SUCHANDRIKA CHAKRABARTI

The relationship between the corporate board and the chief information security officer (CISO) is becoming ever more cooperative – because it needs to. Effective teamwork between the two parties is crucial if firms are to be resilient to the proliferation of cyber attacks and comply with strict legislation on digital resilience that's coming into force in both the US and the EU.

"The most successful CISOs stay close to larger corporate strategy efforts and objectives, as laid out by the board and executives." So says Curtis Simpson, CISO, Armis.

The onus is on the CISO to relate their team's work back to the organization's overall strategic goals, stresses Dan Boresjo, CTO at White Bullet, a provider of anti-piracy tech. He adds that they cannot expect board members to possess a high level of technical knowledge.

"Communicating IT issues with a non-technical board is always going to be difficult. If possible, illustrate the risks using real anecdotes as well as potential scenarios," Boresjo advises. "It's important to bring this all to life."

A research report published in the journal Computers & Security last October probes the evolving relationship between CISOs and boards. The authors single out the external factor that's been most responsible for pushing the two parties closer together.

They write: "We conducted 18 interviews with non-executive directors from 43 organizations to cast light on current cybersecurity practices and on the factors that drive directors' engagement. Our findings emphasize that regulations are the most influential driver."

They suggest that worries about non-compliance and its consequences have been a key reason for boards' increasing interest in cybersecurity. This fear factor can often adversely affect their strategic decision-making, rendering their approach less proactive, far-sighted and holistic than it could and should be.

The report goes on to note: "Directors are not always completely aware of their duties and liabilities concerning cybersecurity oversight."

With the advent of tougher regulations from the US Securities and Exchange Commission (SEC) and the Digital Operational Resilience Act (DORA) in the EU, boards potentially face criminal liability with respect to security breaches. The pressures that such developments place on the board-CISO relationship mean that it is developing apace.

"This is a fast-moving area that requires more than a one-off conversation," Boresjo notes. "It's an ongoing evolution."

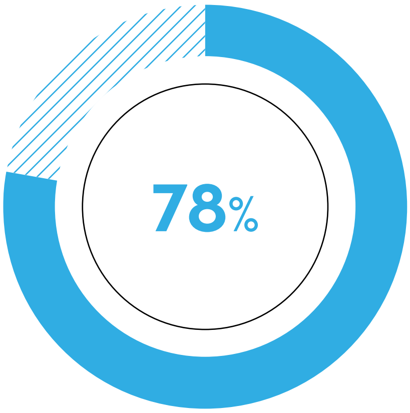
The relationship is likely to function effectively if CISOs can learn how to translate the metrics underpinning their function into stories that resonate with board members and their priorities.

Professor Peter Cochrane is an eminent academic, consultant and non-executive director who worked as British Telecom's CTO in the late 1990s. He believes that the CISO "has to have a seat at the table and feel as much a member of the board as the CFO does. They must learn 'board speak' and get to the point clearly in expressing the risks of failure and its potential costs."

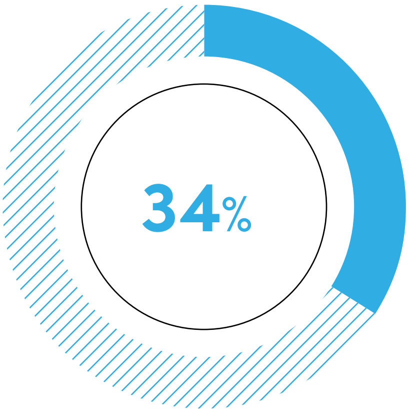
Communicating the gravity of cyber risks

CISOs can often find that, despite having a seat at the boardroom table and bringing compelling

> **Communicating IT issues with a non-technical board is always going to be difficult**
>
> DAN BORESJO, CTO AT WHITE BULLET



of board members agree that their organisation is at risk of a material cyber attack in the next 12 months



of CISOs agree that their organisation is at risk of a material cyber attack in the next 12 months

MIT Sloan, 2022

data to meetings, cybersecurity can fall to the bottom of the agenda. This is an oversight that needs to be tackled urgently – but how?

"Recommended strategies should refer to how operations will be improved, costs will be avoided and risk will be reduced – in that order," Simpson advises. "A combination of technical and commercial metrics – such as loss of business in dollar terms – that highlight how key risks could affect critical business priorities, should keep everyone's attention in the room."

Boresjo agrees, adding: "I find that it can help to communicate in analogies. Things can develop so quickly, so it's important to convey the potential speed and scale of a possible event."

Cochrane advocates strategic relationship-building. His advice to CISOs would be to "approach the chairman and give a one-on-one explanation. Remember that, generally, no board members will understand anything about technology, let alone the cyber threats."

A lack of knowledge at the top level is about to become a liability under the new US and EU legislation. To deal with this threat, Cochrane suggests bringing in "a consultant to corroborate the views of the CISO and explain further what's at risk and what's to be done about it, in plain English."

This move also provides an intelligence-sharing opportunity. To a certain extent, a seasoned consultant will be able to bring in real examples of effective cybersecurity strategy from other organizations they've advised.

"Often there is a central function, such as enterprise risk management, that establishes the central program and supporting collateral used to communicate risk with the board," Simpson says. "Depending on the size of the organization and committee, it may also be in the CISO's best interests to discuss the risk with other members of the committee before the formal review meeting."

Both cyber attacks and the new legislation being enacted to tackle them are creating huge new challenges for businesses. Boards must accept that such risks affect every element of the business, while CISOs must ensure that these always have a prominent place on the agenda.

Focusing on the data that matters most

Security chiefs have a host of data at their disposal, but they risk turning their boards off a key subject if they spout figures without a care for what this audience really needs to know

SUCHANDRIKA CHAKRABARTI

Cybersecurity can sometimes suffer from an image problem at board level. In September 2022, a research report co-published by the MIT Sloan School of Management advised CISOs to "avoid jargon and overly technical language and instead speak the language of the board and the business. Then they will be seen as business partners who understand the broader impact of their work and respected colleagues of their executive peers."

Unavoidably, cybersecurity presents boards with new metrics to consider, but which of these are the most deserving of the leadership team's attention. And which, if any, can be left on the back burner?

Given that cyber attacks tend to be targeted, agile and fast-developing, the simple answer to the second question is 'none' – constant vigilance is crucial. Yet there are ways in which CISOs can apply all the data they obtain from monitoring, testing and repairing the company's cybersecurity program to tell the board a story that translates all this material into business impacts.

"The best metrics are the ones that actually matter to the business, so seek out measurements that narrate how security helps the enterprise to achieve its objectives," says Curtis Simpson, CISO at Armis.

This requires cultivating a close working relationship with the board and understanding the overall business strategy.

Focus on metrics that show the impact of cyberattacks

Simpson would advise CISOs not to "focus on parroting the number of cyber attacks the company is experiencing, because that figure has no measurable outcome that the board can relate to. Instead, use those metrics to show the measured impact that those attacks could have on areas such as productivity."

While the MIT Sloan report acknowledges that the "traits most desired of the CISO by their boards differ depending on location and industry", it adds that, "in general, board members reported that they most value cybersecurity experience (49%), technical expertise (44%) and risk management (38%). These findings suggest a heavy focus on protection over resilience."

CISOs need to widen this view of their work. They clearly have a job to do in emphasizing the proactive nature of cybersecurity, which relies upon the constant monitoring of the firm's digital environment.

The importance of storytelling

Peter Szyszko is the founder and CEO of White Bullet, a provider of anti-piracy tech. He believes that many boards view cybersecurity "as a type of insurance – an unnecessary one – even though our vulnerabilities are increasing dramatically, given that so many of us are no longer operating on a secure network in one office. As well as testing, it's important to highlight the horror stories concerning the potential liabilities."

It can be helpful to explain some of the metrics being scrutinized before combining them into a narrative for the board. That's the recommendation of Greg Hatcher, founder-CEO of White Knight Labs, a cybersecurity consultancy specializing in penetration testing.

He says: "Some of the most important metrics include: the number and severity of security incidents; the time it takes to detect these and respond to them; the percentage of systems that are up to date with patches and other security measures; and the percentage of employees who have completed cybersecurity training."

Added to such complexity is the fact that, as Hatcher says, these metrics can be "difficult to interpret. For example, the time it takes to detect incidents and respond to them can be affected by a wide range of factors, including the sophistication of the attack and the effectiveness of the company's incident-response processes."

By prioritizing those metrics that the board needs to know about immediately, and presenting data in an easily digestible way, CISOs can achieve their aims.

Szyszko believes that "boardroom meetings are a valuable opportunity to share such insights and raise the profile of cybersecurity. We must not wait for a crisis but instead work proactively."

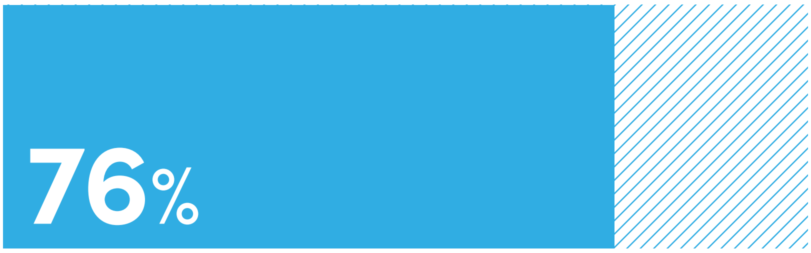
Translate the numbers into board-speak

Ensuring that this topic remains on the senior leadership agenda is an important task for the CISO. It's therefore crucial to contextualize the metrics to retain the board's attention.

As Simpson says: "Letting the board know what's important in cybersecurity terms isn't just a question of your ability to produce the most shocking numbers. It's also about using those numbers to tell a story that illustrates the commercial impacts in a way that matters to boards. CISOs who can translate these metrics into a meaningful narrative will find it easier to obtain the resources they require to fund their cybersecurity programs and better protect their businesses."

High-level conversations about cybersecurity "must take place regularly and in the language of business, rather than the tech jargon of security," stresses the MIT Sloan report.

By translating the numbers into board-speak, the most effective CISOs are strengthening relationships at the top level and providing vital insights into how cybersecurity is working at their firms. Such efforts will be amplified by the leadership team's understanding and support, because, as the report points out, "the more the board makes cybersecurity a priority, the more other leaders will do the same".



of boards discuss cybersecurity once per month and found a disconnect between the CISO's understanding of their organisation's cybersecurity capability and that of the board

Panaseer, 2023

COMMERCIAL FEATURE

What new US and EU legislation means for boards and cybersecurity

New legislation will put the onus on firms to improve their own cybersecurity strategy, or face the consequences

In 2022, global cyberattacks increased 38% from 2021, according to figures from Check Point Research. By country, the most attacked were the US, which saw a 57% escalation, and the UK (77%). Such alarming statistics cannot be ignored; consequently, both the US and the EU are bringing in legislation that puts the onus on firms to improve their own cybersecurity strategy, or face the consequences.

In March 2023, the Securities and Exchange Commission proposed requirements for organizations to address their cybersecurity risks. In the same month, the Biden-Harris Administration released the National Cybersecurity Strategy (the NCS) – it sets out an ambitious vision for digital resilience, and has a 2030 deadline. The implementation period for the EU Digital Operational Resilience Act (DORA) is even more urgent, at just two years, which kicked in this year. Financial entities in the European Union (EU) and their critical Information and Communication Technology (ICT) providers must be ready to comply with DORA by January 17, 2025.

The US strategy aims to build cyberspace resilience. The NCS sets out five pillars that clarify its aims – to defend critical infrastructure; disrupt and dismantle threat actors; shape market forces to drive security and resilience; invest in a resilient future; and to forge international partnerships to pursue shared goals.

How to improve security posture

The NCS will shift cybersecurity responsibilities from front-line users, such as individuals, small businesses and local governments, to larger and better-resourced organizations, such as software developers and hardware manufacturers. Above all, the NCS will renew efforts to penalize entities that, in its view, fail to properly protect data. Boards need to consider their new liabilities, and ensure that their company has strong digital resilience.

So where do board members and security leaders begin when it comes to tackling the changes that need to be made? Charlotte Jupp, head of customer success and security performance management at Panaseer, a cybersecurity automation platform, says: “To start with, it’s important to understand your assets, and your control coverage across those assets. They could be devices, applications, people. Are you testing the logins onto your network for risks? And are you training the people who use it on the risks?”

Answering these basic questions is the first step towards testing the maturity of your existing security program. Panaseer’s continuous controls monitoring platform delivers an overview of current security controls, providing metrics and measures guidance for the CISO to bring to the board. Access to an overview of the current program’s strength is key; no one metric will convince a board to act.

Instead, as Jupp says, “As CISO, you want to take a set of metrics to the board, relating them to the real world, and to the business impact that they will have. If you’re a bank and your trading server goes down and the market starts shifting, how much money are you losing every single day?

“It’s about looking at your most business-critical assets, putting financial value against it, and presenting what the risk is on those particular assets,” continues Jupp. “The board should be left asking: what resources does the CISO need to fix this problem as soon as possible?”

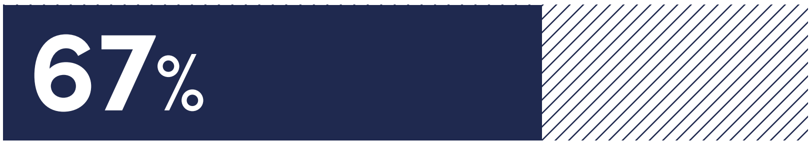
Technological research and consulting firm

Gartner says that metrics need to be 'outcome-driven', meaning that the numbers must translate into meaningful action. Therefore, a useful cybersecurity metric should: inform priorities, resourcing and investments; align to business context to provide actionable insights; support evidence-based ways of working to drive accountability – and celebrate success.

Panaseer identifies 18 crucial benchmarks that must be considered, and which can be tracked via their automated security measurement platform. Essentially, these numbers feed into the CISO's main role for the board: storytelling and translation. It's about showing the board that, where the firm's cybersecurity health intersects with the SEC and/or DORA, there is an opportunity to strengthen the business. Performing gap assessments will identify those areas where they may not comply with the new laws.

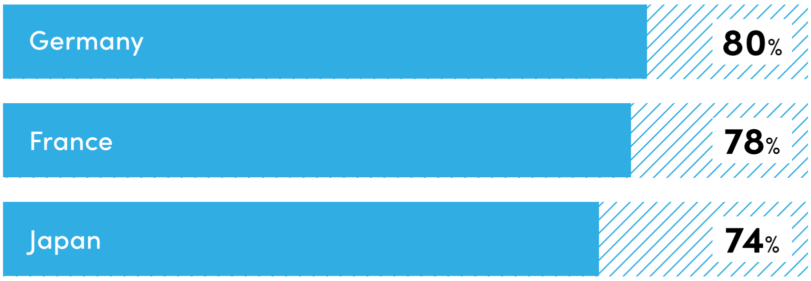
Reporting requires boards to disclose cybersecurity risk to investors

For many companies, the diagnosis will be that there are several necessary steps they ought to consider, in order to bolster their cyber resilience. As Jupp explains: "You can start to build a plan for maturing your security program, because the metrics help you identify where the issues sit, where process improvements need to be implemented, and what level of risk your team and the board can agree on."



Two-thirds of board members **(67%)** believe human error is their biggest cyber vulnerability

This is most keenly felt in traditionally stricter corporate cultures such as



MIT Sloan, 2022

The SEC will impose new reporting requirements on organizations, which will require boards to disclose their level of cybersecurity risk to investors. It also calls for improved sharing of information between the government and private sector when it comes to cybersecurity threats, vulnerabilities and risks. The reporting requirements add urgency to the board's new responsibilities around digital resilience.

In the EU, DORA will require major operational resilience benchmarks and board oversight requirements on financial entities. In fact, member states are required to provide for individual civil liability for board members, and may also provide for criminal liability if they wish.

The introduction of such serious repercussions for having weak cybersecurity fundamentally changes the relationship between the board and the CISO. As Jupp explains: "CISOs want boards engaged in understanding the impact and supporting the CISO team; boards need to become more cyber-literate."

Panaseer's cybersecurity monitoring platform will keep track of the metrics that CISOs need to build their stories upon, as they step into their newly-enlarged roles in advising boards on how to mitigate ICT risk.

For more information please visit
WWW.PANASEER.COM

The six golden rules of handling cyber risks at board level

Here are a set of rules that CISOs would be well advised to remember when engaging with their firms' strategic decision-makers

SUCHANDRIKA CHAKRABARTI

01 Integrate cybersecurity into the organization

A successful cyber attack can easily wreak serious financial and reputational damage on any enterprise. Cybersecurity must be threaded through every aspect of your organization. The board needs to have a comprehensive and resilient strategy as part of the overall business plan to mitigate risk.

The board must understand the cyber risks that require management. To this end, call in an independent consultancy to assess these risks. The resulting informed overview of your organization's cybersecurity posture and data will aid effective decision-making.

Also, every department in the business must take responsibility for its part in the overall digital resilience of the firm. Help them to do so by providing training and clear guidelines to work to.

02 Build a dashboard to help the board understand trends

A 2022 research report co-published by the MIT Sloan School of Management has revealed that two-thirds of board members view human error as their biggest cyber vulnerability, even though figures compiled by the World Economic Forum suggest that this factor contributes to 95% of all cybersecurity incidents.

The report is based on interviews with 50 board directors working across a wide range of sectors in 12 countries, including the US and the UK. The disconnect between boards and CISOs is a global problem. A translation job is needed. This can be done by building a dashboard that displays metrics in such a way that board members without IT expertise can understand their organization's digital resilience.

03 Discuss security in every board meeting – and not only at the end

Current levels of funding and awareness at board level generally don't translate into preparedness for cyber attacks, according to the MIT Sloan report. Just under half (47%) of the interviewees consider their organizations to be unprepared to deal with a cyber attack in the next 12 months.

The key to improving this figure lies partly in the relationship between boards and CISOs. While 69% of board members believe that they see eye to eye with their CISOs, only 51% of CISOs feel the same way.

04 Aim for security, not compliance

Cyber attacks evolve constantly – and quickly. All organizations need a tailored approach to digital resilience. Any given company will have a unique set of needs, priorities, technology and data. It therefore requires security programs that can be monitored and updated easily.

Boards must keep asking their CISOs the important questions. These are: what kinds of data are we keeping and why? Where are we keeping that material? Do our policies and procedures adequately protect our data? Do our security practices actually conform with those policies and our public statements? And is our spending on security appropriate to the level of risk the business is facing?

05 Maintain the incident response plan

It's crucial to build organizational resilience to respond to attacks as they happen. As recent breaches have shown, it's important to have both a strong data security program and a robust incident response plan.

Time is of the essence when tackling a breach. The time that employees must spend on flagging down senior executives and getting them to focus on an emergency is time taken away from the crucial tasks of taking appropriate countermeasures and minimizing the damage.

This is where an effective security program helps. It ensures that, when appropriate, an incident can be swiftly elevated to the appropriate level of the hierarchy.

06 Explore cyber risks in the supply chain

While you might be confident in your own organization's digital security, its assets may still be exposed to numerous risks if your suppliers have failed to take sufficient precautions. Of the businesses responding to the UK government's 2022 Cybersecurity Breaches Survey, only 13% reported reviewing the cybersecurity of their immediate suppliers, while only 7% said that they'd gone deeper into their supply chains.

Such oversights need to be tackled at board level by encouraging collaborative relationships between organizations and their suppliers. Any enterprise is only as resilient as the weakest link in its supply chain.

The ability to demonstrate a good level of cybersecurity is fast becoming a key component of supplier and provider bids. Indeed, it is already a requirement for many government contracts.

> “An effective security program ensures that, when appropriate, an incident can be swiftly elevated to the appropriate level of the hierarchy

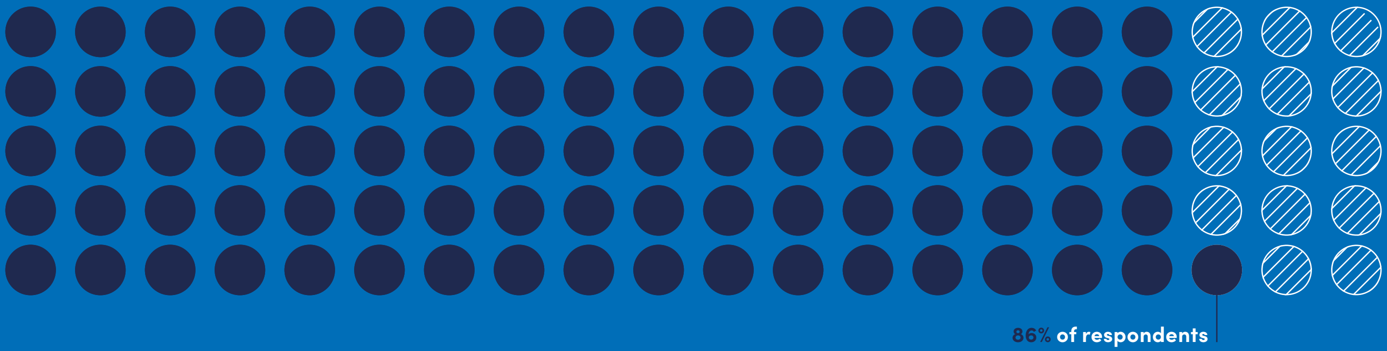
A robust, cohesive security culture will help reduce cybersecurity breaches and risk

Cybersecurity breaches are challenging and expensive, but with the right security culture in place, fewer breaches and disruptions occur

TOP OF THE LIST FOR SECURITY LEADERS IS A CRACKDOWN ON RANSOMWARE

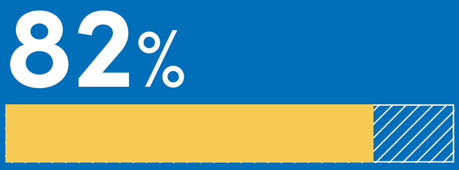
Panaseer, 2023

Ransomware mitigation is a budgeted priority in 2021 and 2022 for the majority of security leaders

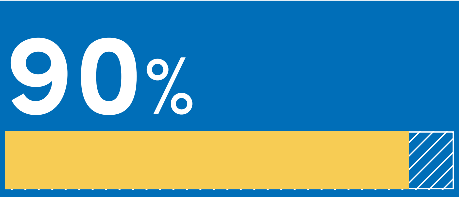


BUT EVEN WHERE CYBERSECURITY MEASURES ARE IN PLACE, BREACHES OCCUR

Panaseer, 2023



82% of security leaders have been surprised by a security event, incident, or breach that evaded a control they thought was in place



90% of security leaders see the failure of controls expected to be in place as the primary reason for data breaches

79% of enterprises have experienced cyber incidents that should have been prevented with existing safeguards

AND KNOWING THE RISKS DOESN'T NECESSARILY PREVENT BREACHES

Gartner, 2022

90% of employees who admitted undertaking a range of unsecure actions during their work activities knew that their actions would increase risk to the organization and undertook the actions anyway

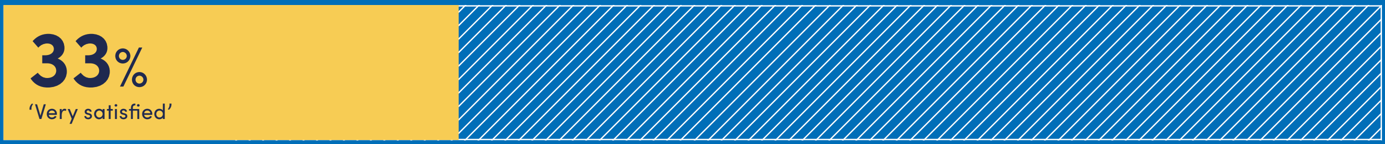
The top reasons for this were:

#1 Speed and convenience

#2 Perceived benefits outweigh perceived risk

WHILE 91% OF CISOS ARE REPORTING TO THEIR BOARD ON RANSOMWARE PROTECTION LEVELS, ONLY ONE-THIRD ARE VERY SATISFIED WITH THE TIME, RESOURCE, ACCURACY AND DETAIL OF THEIR RANSOMWARE BOARD REPORTING

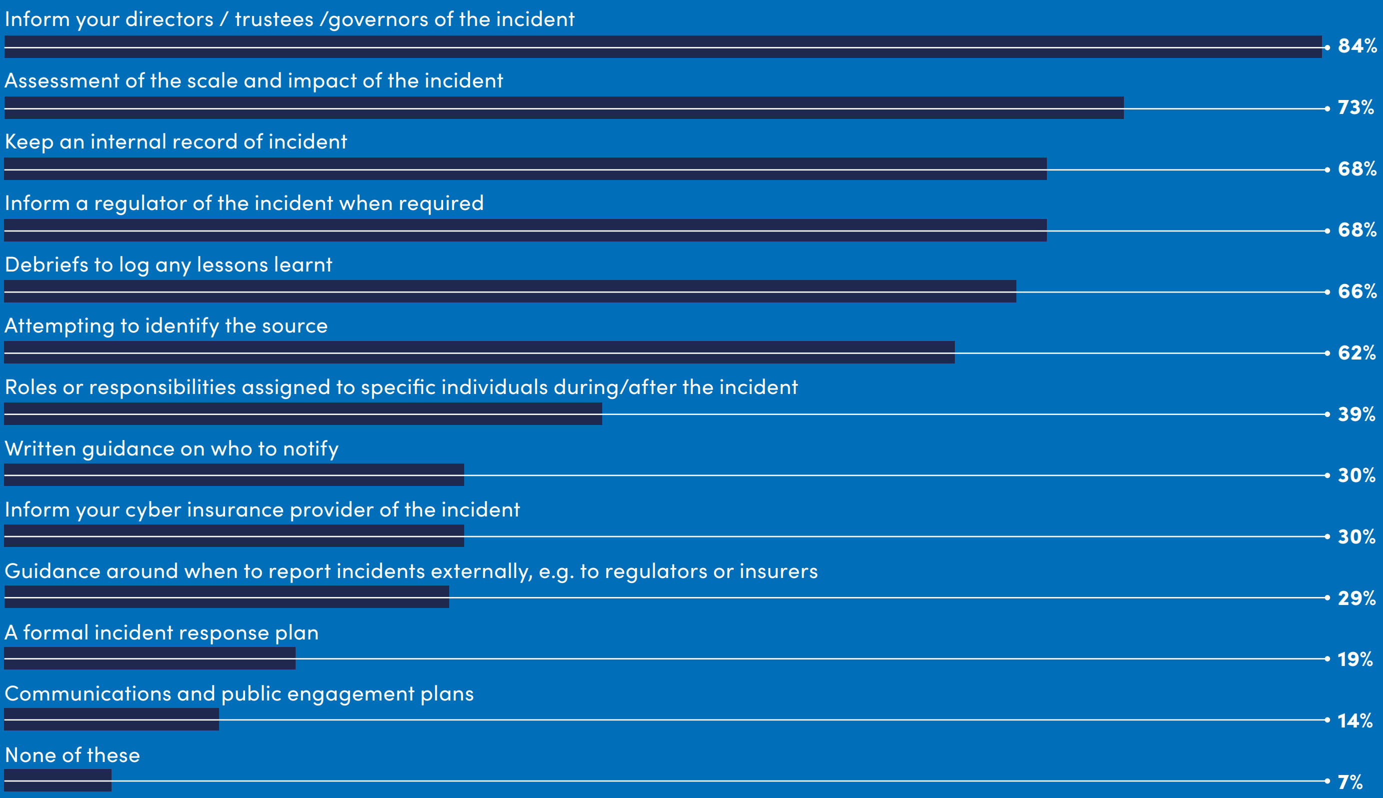
Panaseer, 2023



WHEN THERE IS A BREACH, THE MEASURES TAKEN BY BUSINESSES VARY, WITH FEWER THAN TWO-THIRDS OF BUSINESSES ATTEMPTING TO IDENTIFY THE SOURCE

gov.uk, 2022

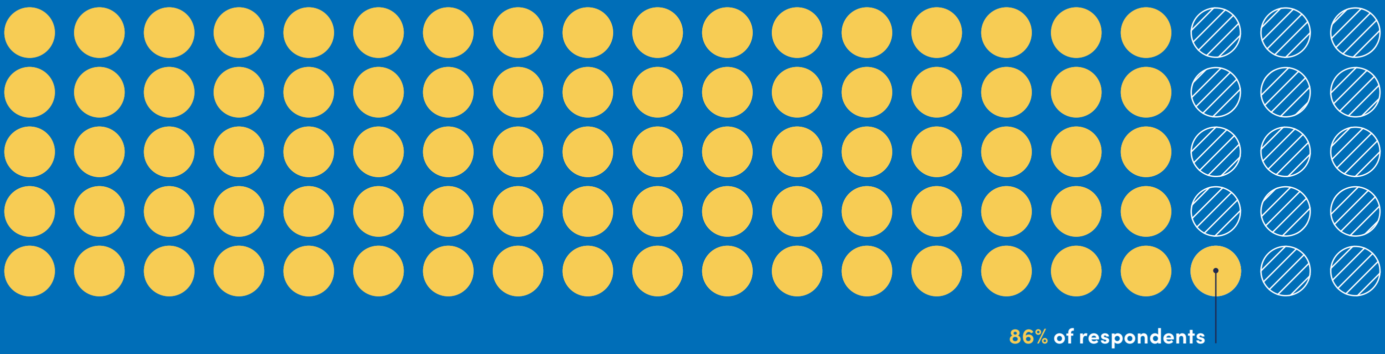
Percentage of organisations that take the following actions, or have these measures in place, for when they experience a cyber incident



BUT, SECURITY LEADERS ARE DRIVING CHANGE, AND THE PROSPECT OF SAVING MONEY VIA LOWER INSURANCE PREMIUMS IS A FACTOR IN DRIVING CYBERSECURITY PROGRAMMES THAT PRODUCE DATA-DRIVEN METRICS

Panaseer, 2023

Nearly all security leaders want to prove the strength of their cybersecurity programme to insurers



Raconteur

panaseer