thycotic

CYBER SECURITY TEAM'S

GUIDE

TECHNOLOGY DECISION MAKING

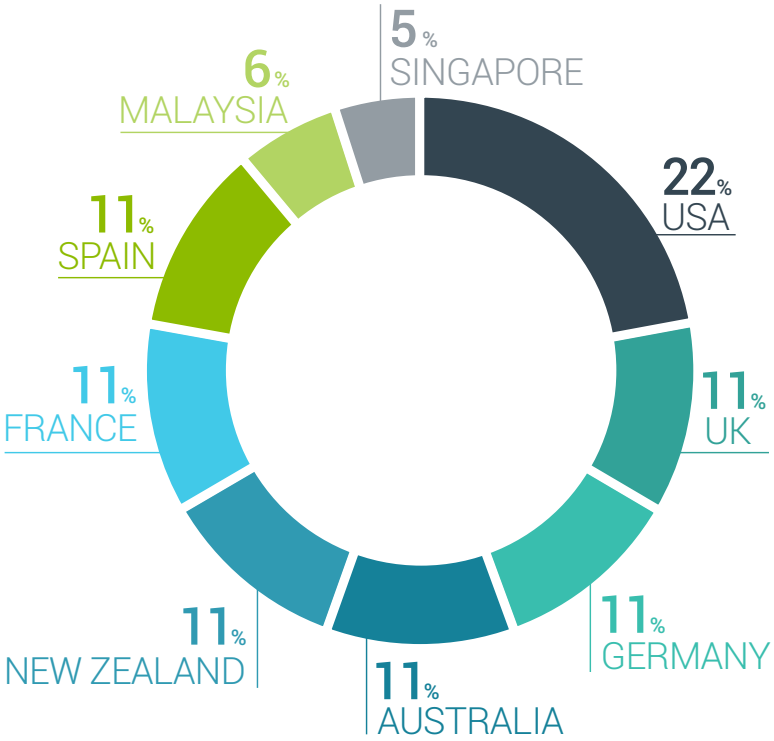
Avoiding pitfalls, evaluating solutions, overcoming barriers

EXECUTIVE SUMMARY

Security decision-makers today are faced with a myriad of choices when it comes to security investments: and increasing risk means making the right and most informed decisions has never been more critical. Some IT and security leaders, however, complain there are too many security solutions, a shortage of skilled resources, and lack of budget – in some cases, even causing them to leave brand new products on a shelf, untouched.

With competing demands, how do these leaders make real-world decisions about where and when to allocate finite resources in a way that best serves the interest of their organization, both now and in the future? Are decisions made on facts or fear? What kind of evaluation criteria are needed from vendors to help them make the most informed decisions?

To get answers to these questions, Thycotic, in conjunction with Sapio Research, conducted a survey in August 2020 that gathered responses from more than 900 Senior IT security decision-makers working within organizations of 500+ employees in the following countries:



Results from the survey reveal major factors influencing the way cyber security executives and top managers are making decisions when purchasing technology solutions to help protect their organizations.

31% of respondents held CEO/CSO/ CISO/CIO positions

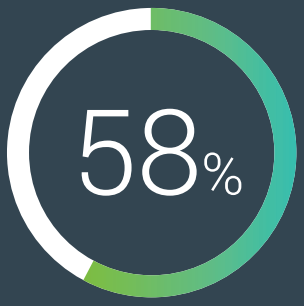
37% of respondents held Head of IT Dep/IT director positions

32% of respondents held IT Manager/ Security Manager position

KEY TAKEAWAYS

This report identifies three key takeaways based on the responses from IT security leaders in these global organizations.

say security incident/ audit failure convinced the Board to make new security investments



claim to be getting more security budget due to COVID-19

of cyber security investments get fully utilized

1 In the wake of COVID19, spending on cyber security is expected to increase, with organizations adding more technology and many moving to cloud solutions. Yet with all this new investment, half of organizations admit that new technology solutions they purchase are never fully utilized.

2 Most companies consider themselves “In the Pack” when it comes to adopting new technologies. They make decisions on technology purchases based primarily on benchmarking and analyst reports, with Proof of Concept (PoC) as the preferred method of evaluation. In making a purchase decision, they look at minimizing risk, Total Cost of Ownership (TCO), integration, and the reputation of the provider. IT operations and security teams have nearly equal say in the final selection.

3 Boards appear to support increased cyber security investments, frequently motivated by internal security incidents and compliance audit failures. However, barriers to securing cyber security investments remain, including technology purchases outside the scope of compliance needs, low perceived threat, and lack of ROI.

KEY TAKEAWAY #1

In the wake of COVID19, spending on cyber security is expected to increase, with organizations adding more technology and many moving to cloud solutions. Yet with all this new investment, half of organizations admit that new technology solutions they purchase are never fully utilized, commonly referred to as "shelfware."

SURVEY RESULTS

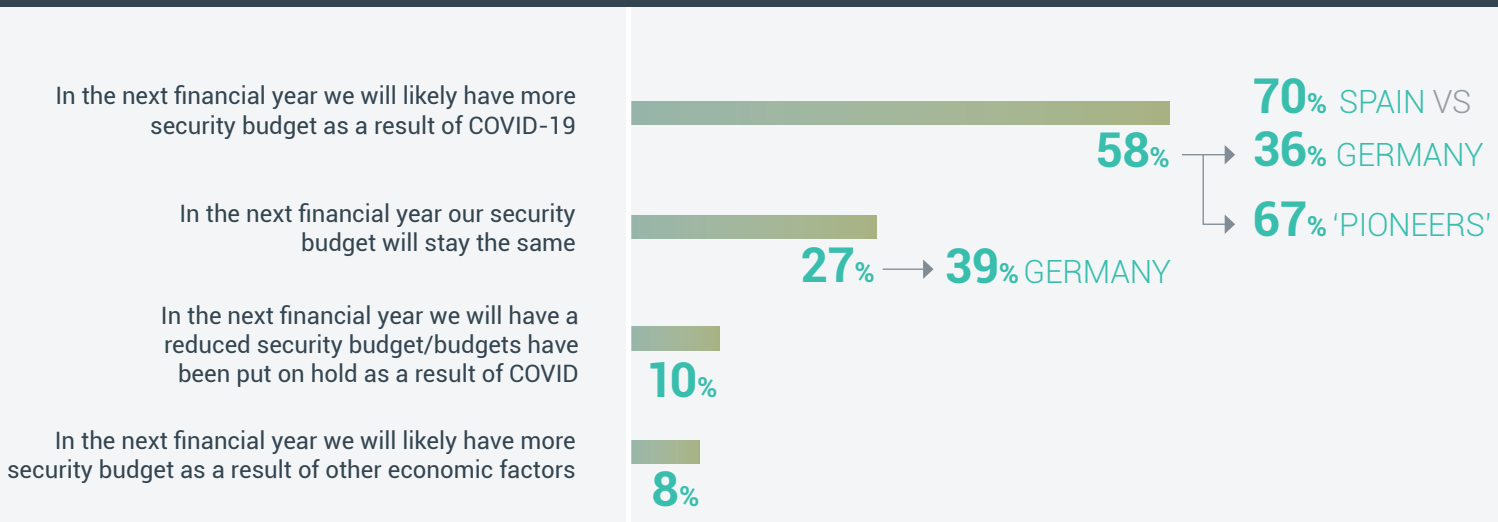
Almost 3 in 5 believe that in the next financial year they will have more security budget as a result of COVID-19 (58%)

2020 has been a very different year for many, and no one predicted a global pandemic would shut down the entire planet. It will be a year to remember or for many, a year to forget. Many companies had some percentage of employees working remotely or from home offices, typically approx. 5-10% of the workforce, depending on the industry and country. Not many companies were prepared to switch to 100% remote working. Companies who adopted cloud and had experience in Cloud Digital Transformation were quick to transition to a remote workforce while others who failed to adopt a cloud strategy early struggled.

This major shift in the work environment put company's IT and Security infrastructure to the ultimate test on as to whether they could continue providing critical business services and functions while keeping the company secure from cyber threats.

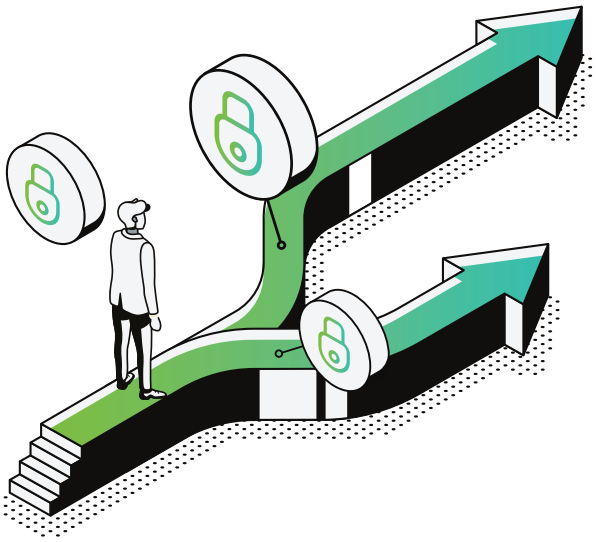
Companies who were already on the path to Identity and Access Management, as well as Privileged Access Management implementation, have been effective in enabling remote privileged users with the ability to continue performing critical tasks remotely and reducing the risk of cyberattack.

Q7 | When thinking about budget for the next financial year, which of the following statements describes your situation best?

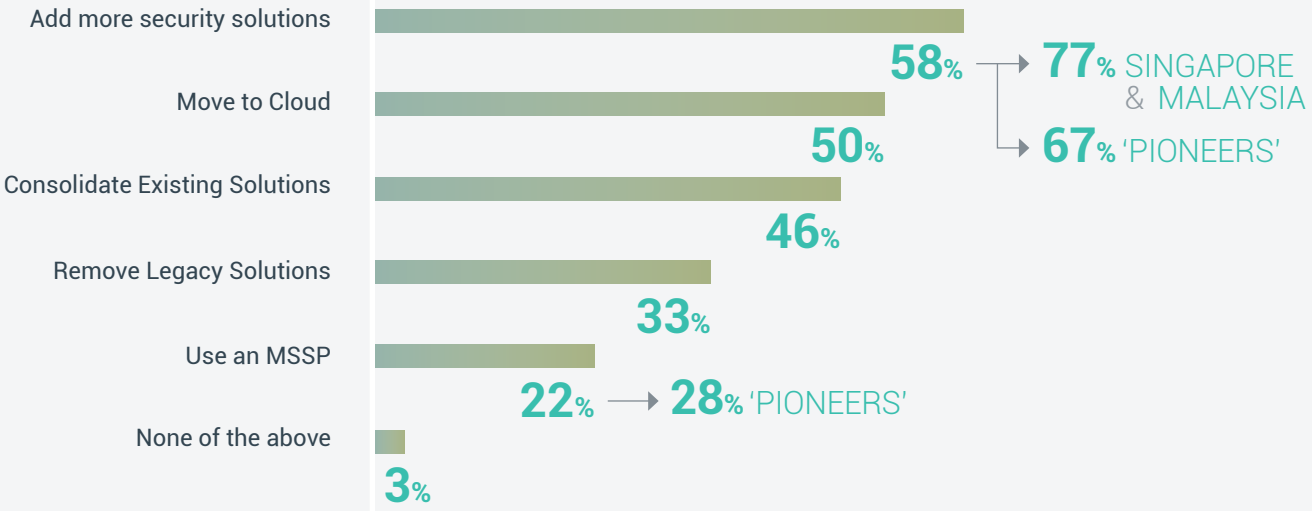


Nearly 3 in 5 IT security decision-makers are planning on adding more security solutions in the next 12 months; 50% are planning to move to the cloud

Many organizations have adopted a cloud-first approach. This means they must first consider cloud deployment options unless the services do not exist, it is not technically possible yet, or legal issues prevent a cloud option. In today's modern era of cloud computing, some companies are ALL cloud, meaning they completely consume and deliver all of their business services from the cloud, and they don't own any physical servers or locations to place them.



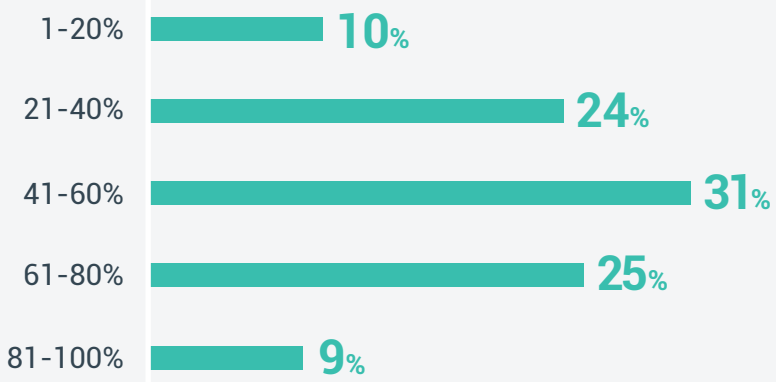
Q17 | Which of the following are you planning to do in the next 12 months?



However, with increased spending expected, IT and security professionals admit only 50% of cyber security technology investments gets fully utilized!

A disturbing finding among survey respondents indicates that 50% of cyber security solutions never get fully utilized. This situation is very likely due to a lack of sufficient resources to fully use the solution, or companies are frustrated when trying to expand the implementation beyond the initial deployment. It is also a sign that too many security solutions are still overly complex, or do not integrate well with legacy technologies.

Q12 | Approximately what percentage of cyber security technology that you invest in gets fully utilized?

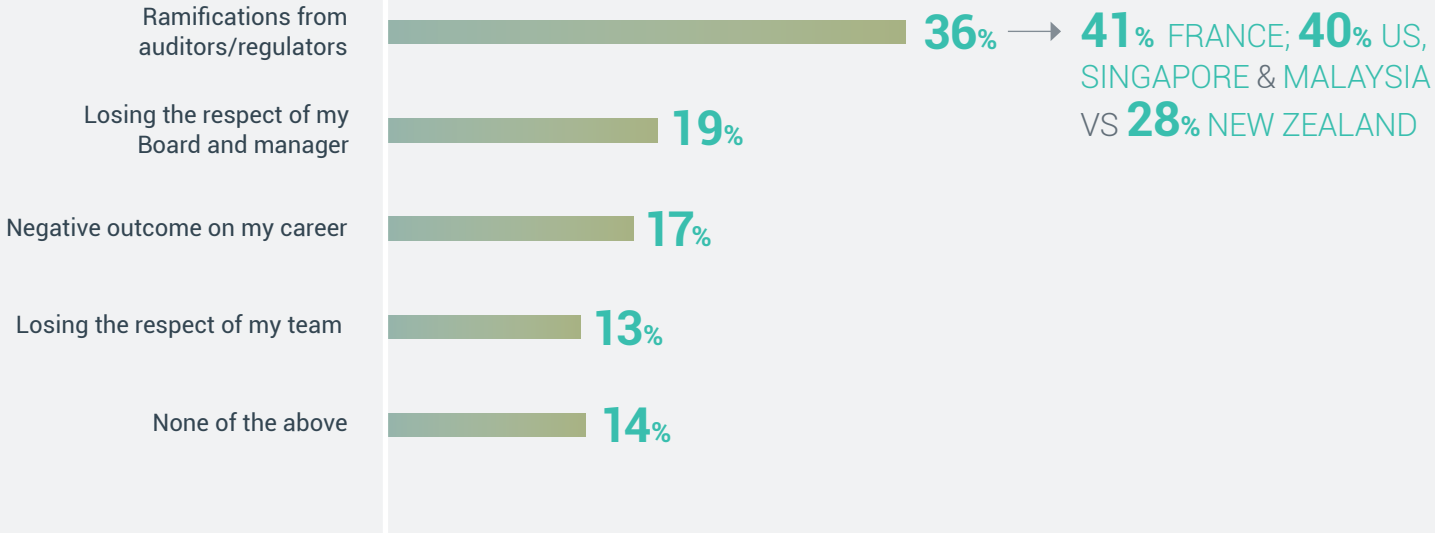


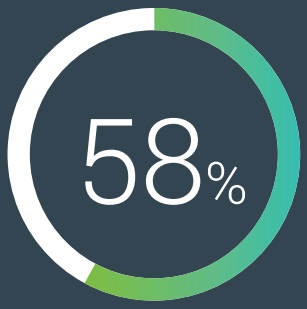
UK	50.1
Germany	49.12
US	56.65
Australia	49.72
New Zealand	44.42
France	55.1
Spain	44.23
Singapore/Malaysia	44.9

One in 3 respondents believe that ramifications from auditors or regulators would concern them most when adopting new cyber security technologies (36%)

All superheroes have fears, and for IT Security superheroes it is the auditors and regulators they fear. If Superman has kryptonite, then IT Security leaders have the auditor. 36% of IT Security respondents fear ramifications from auditors/regulators when deciding on new security solutions. Another 19% are concerned with damaging their reputation with the Board, and 17% are concerned about the negative impact on their careers. Thus, it's understandable that IT Security decision-makers frequently rely on the recommendations of industry analysts or industry peers to help minimize the risk of making a poor decision.

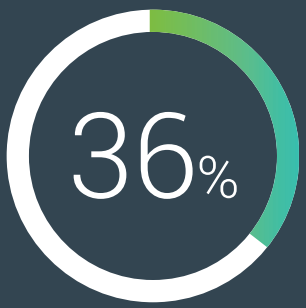
Q13 | On a professional level, which of the following would concern you most about new cyber security technology adoption?





getting more security budget due to COVID-19

of cyber security investments get fully utilized



fear ramifications from auditors/ regulators when making security purchase decisions

RECOMMENDATIONS

The global pandemic has generally accelerated industry trends, including increases to security budgets as highly publicized incidents grow, a greater reliance on cloud solutions, and an expansion of regulations that seek to protect privacy and force compliance with more stringent security standards.

1 Prepare and protect your organization for a remote working environment that has become the "new normal" with cloud-ready solutions.

A Privileged Access Management (PAM) program, for example, can help support this "new normal" by enabling privileged users to access critical business systems remotely without requiring them to come into unsafe environments that would be a risk to their health. To achieve this, security solutions must be "cloud ready" to the greatest extent possible, so that they can be managed securely from any location and accessed 24x7.

2 Prioritize "usable" security solutions that are readily adopted by security teams rather than more complex products that may require extensive training or constant professional services to realize their value.

With 50% of security solutions at risk of becoming "shelfware," organizations need to place a premium on ease of use and rapid time to value. The goal should be to implement security solutions that enable and encourage self-sufficiency, backed by timely technical support as needed, as opposed to costly professional services as a requirement.

3 Choose solutions with a built in "compliance bias" that allows security executives and managers to satisfy auditors and meet regulations without adding to their already heave workload.

Security solutions should make demonstrating compliance as easy as possible with flexible policy-guided execution along with reports design to satisfy auditors with a minimum of effort. Out-of-the-box reports can greatly reduce the time and resources required to meet common regulatory and compliance mandates.

RESOURCES

Remote Worker Cyber Security Toolkit https://thycotic.com/solutions/free-it-tools/remote-worker-tools-cyber-security/

PAM Software Vendor Checklist helps evaluate the simplicity and usability of PAM solutions

Critical Controls for Modern Cloud Security explains how to use Privileged Access Management (PAM) to mitigate vulnerabilities across the cloud attack surface.

Expert's Guide to PAM Success describes the people, process and technology needed to develop an advanced PAM program.

KEY TAKEAWAY #2

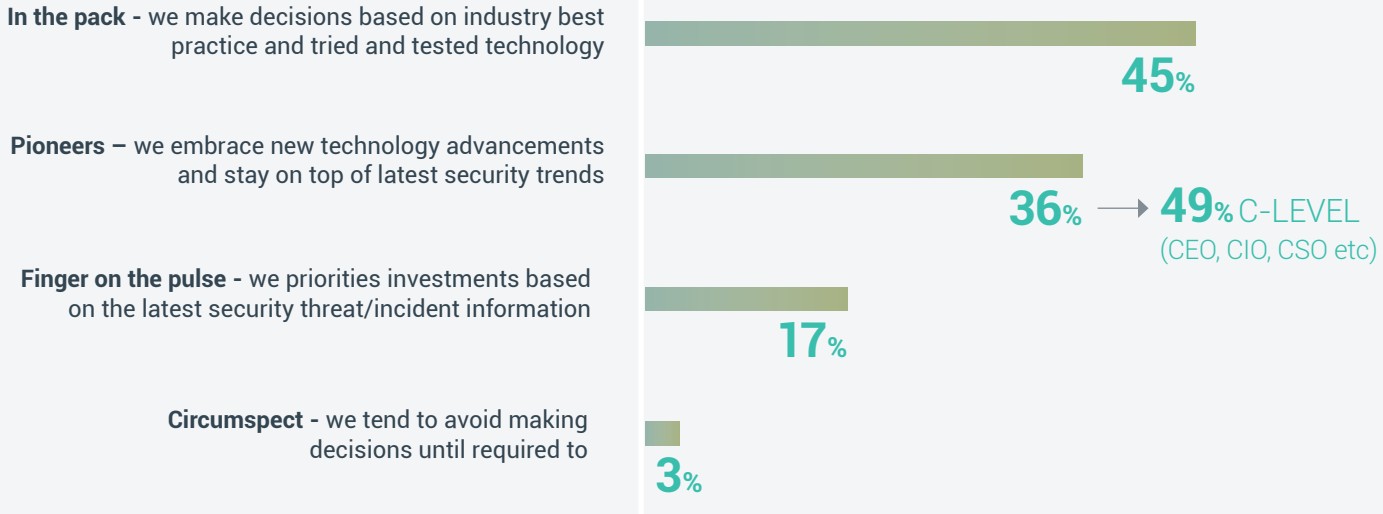
Most companies consider themselves "In the Pack" when it comes to adopting new technologies. They make decisions on technology purchases based primarily on benchmarking and analyst reports, with PoC the preferred method of evaluation. In making a purchase decision, they look at minimizing risk, TCO, and integration along with the reputation of the provider. IT operations and security teams have nearly equal say in the final selection.

SURVEY RESULTS

Almost half of respondents describe their organization as 'in the pack' (45%) while a third consider themselves 'pioneers' (36%), when it comes to investment in cyber security projects.

Security leaders must strike a fine balance between using proven technologies and choosing the latest cutting-edge security solutions with products touting capabilities such as quantum computing, blockchain, AI, and ML. 45% of respondents stick with proven best practices when choosing security solutions, while 36% consider themselves as pioneers that embrace new technologies.

Q2 | Which of the following best describes the risk profile of your organization when it comes to investment in new cyber security projects?



Leaders in new technology adoption by country

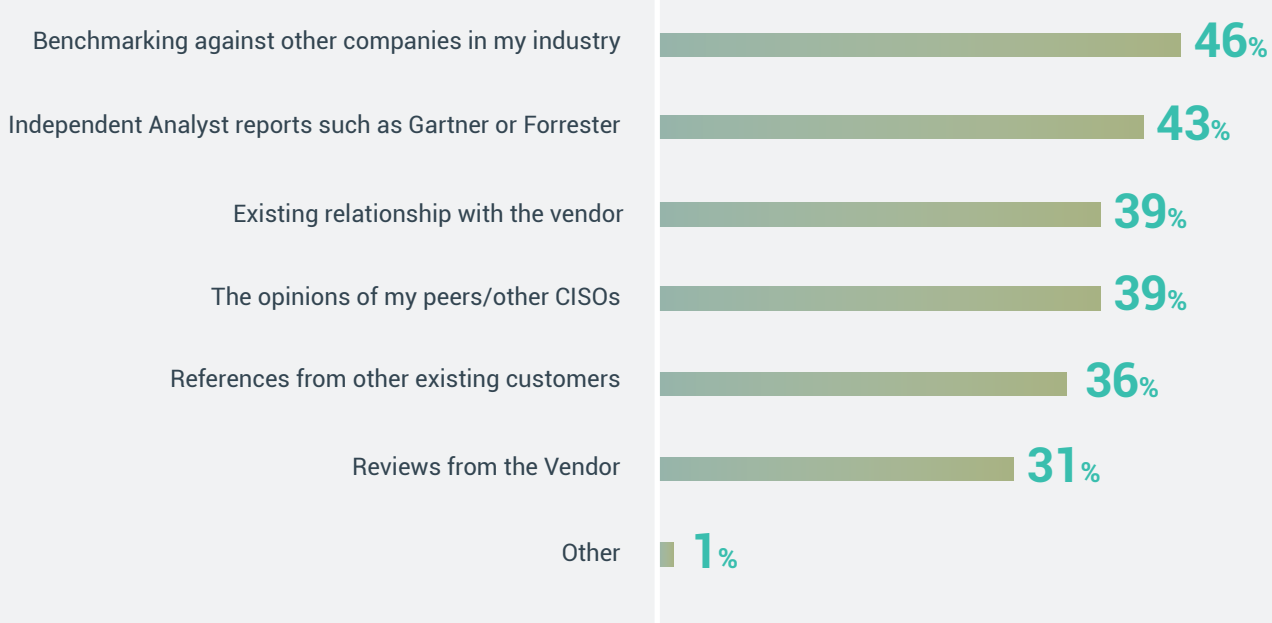
The US and France appear to be leading the way as pioneers with the UK, Germany, Australia, New Zealand, Spain, Singapore and Malaysia sticking with best practices and proven technology.

	UK	Germany	US	Australia	New Zealand	France	Spain	Singapore/ Malaysia
In the pack	51%	49%	38%	43%	54%	33%	59%	41%
Pioneers	31%	27%	47%	32%	28%	45%	30%	34%
Finger on the pulse	14%	20%	14%	21%	14%	22%	10%	23%
Circumspect	4%	4%	2%	4%	4%	0%	1%	2%

Before investing in new cyber security products, survey respondents said the most important sources of informed decision-making are benchmarking against other companies in the industry and independent analyst reports.

Not surprisingly, senior IT security decision-makers look to their peers for guidance. Benchmarking with other companies in their industry was the top method in decision making with 46% of respondents looking to peers for answers, 43% look to industry analysts, and 39% relying on existing relationships with vendors.

Q8 | When thinking about information you source before investing in new cyber security solutions projects, which of the following are most important in your decision-making process?



Most important sources of information by country

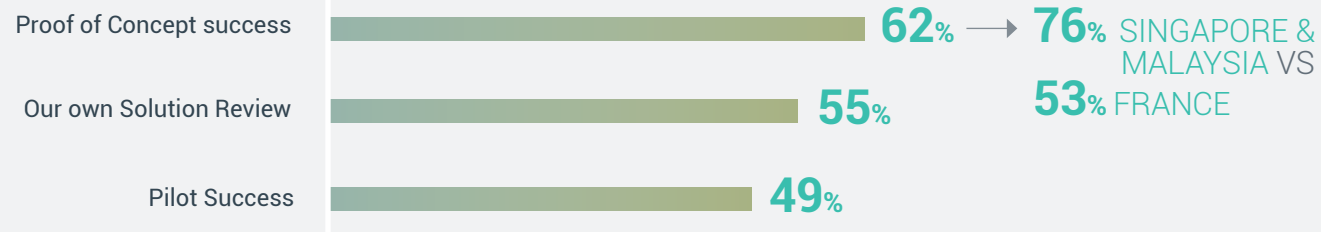
The US and France appear to be leading the way as pioneers with the UK, Germany, Australia, New Zealand, Spain, Singapore and Malaysia sticking with best practices and proven technology.

	UK	Germany	US	Australia	New Zealand	France	Spain	Singapore/ Malaysia
1st	Benchmarking against other companies in my industry (48%)	Existing relationship with the vendor (42%)	Existing relationship with the vendor (45%)	Independent Analyst report such as Gartner or Forrester (47%)	Benchmarking against other companies in my industry (40%)	The opinions of my peers/ other CISOs (53%)	Benchmarking against other companies in my industry (48%)	Benchmarking against other companies in my industry (59%)
2nd	The opinions of my peers/ other CISOs (43%)	Independent Analyst report such as Gartner or Forrester (41%)	Independent Analyst report such as Gartner or Forrester (45%)	The opinions of my peers/ other CISOs (43%)	Independent Analyst report such as Gartner or Forrester (39%)	Benchmarking against other companies in my industry (51%)	Independent Analyst report such as Gartner or Forrester (45%)	Independent Analyst report such as Gartner or Forrester (50%)
3rd	References from other existing customers (39%)	Benchmarking against other companies in my industry (40%)	Benchmarking against other companies in my industry (42%)	Benchmarking against other companies in my industry (40%)	The opinions of my peers/ other CISOs/ Existing relationship with the vendor (38%)	Existing relationship with the vendor (40%)	References from other existing customers (40%)	Existing relationship with the vendor/ References from other existing customers (42%)

3 in 5 use PoC success when evaluating a new security solution (62%).

As much as possible, senior IT security decision-makers test drive security solutions before committing to purchase. PoC is the most favored method for evaluating solutions (62%) followed by an internal solution review (55%) and piloting the solution (49%) in a production environment.

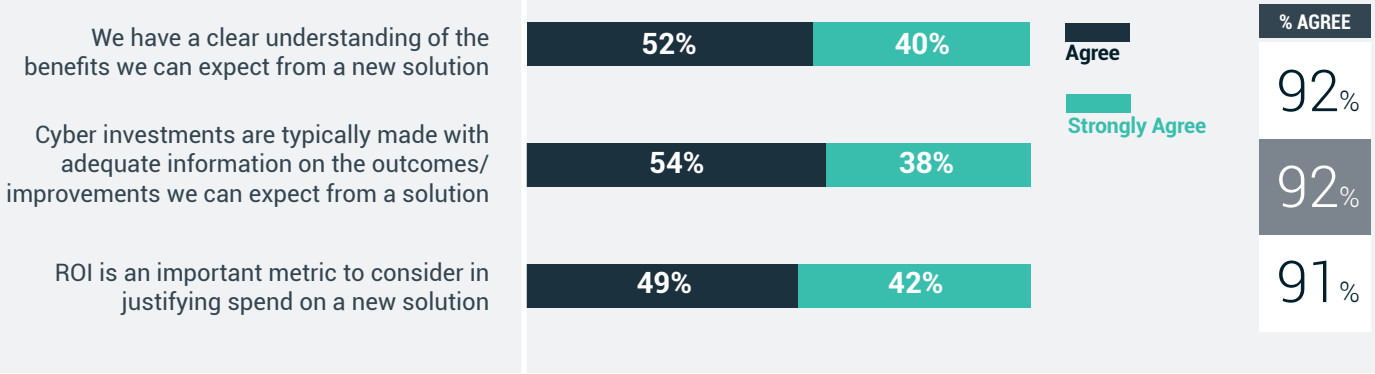
Q9 | When thinking about the practical measures you employ to evaluate the results of a new security solution, which of the following do you use?



92% have a clear understanding of the benefits they can expect from implementing a new cyber security solution.

The good news for IT security teams is executive management and Boards listen and back them with investments. This is a major change from only a few years ago when security teams struggled to get Board approval for cyber security initiatives. It appears after several years of major cyberattacks, increased risk of ransomware and business email compromise, Boards have become much more involved and aware of the need for such investment. Security teams are doing more research when making decisions and have a clear understanding of the need for measurable security performance goals/KPIs.

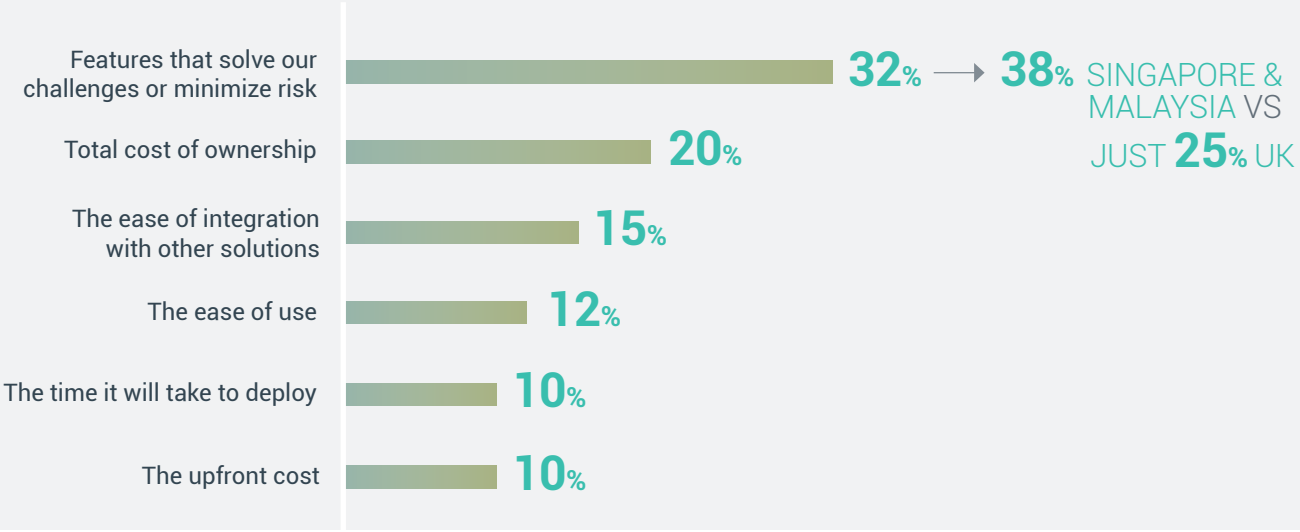
Q10 | Thinking about the expectations of implementing a cyber security solution, to what extent to you agree with the following?



When making decisions about specific security solutions, features that solve challenges or minimize risk are considered to be of highest importance.

32% of respondents say they choose solutions that help them solve specific challenges while another 20% factor in the TCO, as well as ease of integration with other solutions (15%) and ease of use (12%).

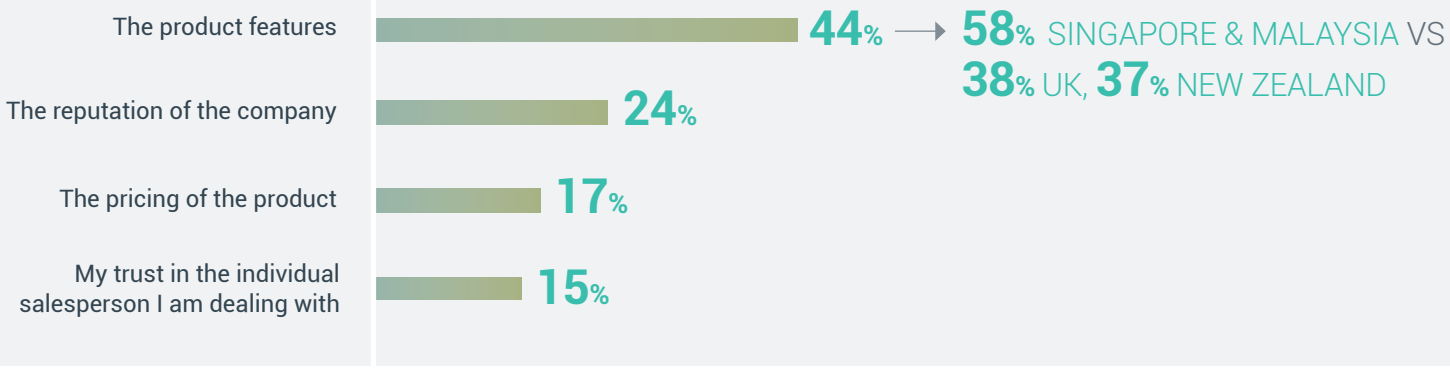
Q11 | When making decisions about a specific new security solution, what factor is of highest importance?



Product features make the most difference in making the final buying decision (44%), yet 24% of respondents consider the reputation of the company to be the most decisive factor Further, 15% consider their trust in the individual salesperson to be most important.

As in many business decisions, "soft" criteria such as vendor reputation and trust in an individual salesperson still play a critical role in any final decision. While prioritizing the justification of a purchase based on demonstrable product features (44%), the less tangible reputation of a company (24%) and trust of the salesperson (15%) also play a substantial role.

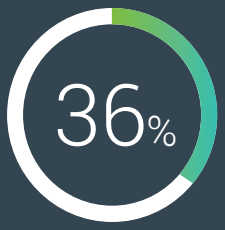
Q18 | Which of the following is the most decisive factor in your buying decision for a new cyber security solution?



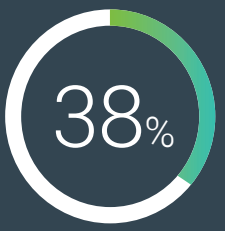
IT Operations is the most likely department to be involved in the decision-making process for new cyber security investments, and slightly more likely to have the final say (38%) as compared to security teams (32%).

IT Operations shares a significant portion of the decision-making process with security teams, and actually has the final say in decisions (38%) among survey respondents compared to the security team and CISO (32%). France appears to counter this trend, where Operations have much less influence in the final say (18%).

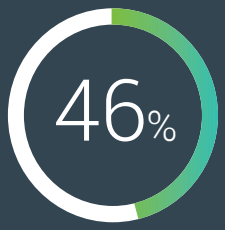
Q15 | Which departments are involved in the decision-making process for new cyber security investments?
Q15b | Which department has the final say in the decision-making process of new cyber security investments?



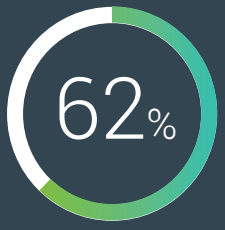
consider themselves "pioneers" in adopting new technology



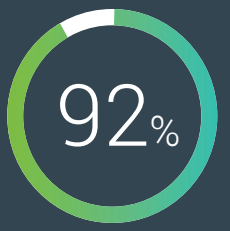
indicate IT Ops has final say on technology purchases



say benchmarking is the top evaluation method



test new products with a PoC



understand benefits from new cyber security solutions

RECOMMENDATIONS

1 | Use analyst reports and colleague references to help prepare your shortlist of vendors/solutions.

Very few organizations have the time or resources to explore all possible security solutions available. The IT security industry has several major analyst firms continuously issuing opinions and reports. While there is often a cost to access their analysis, in many cases leading vendors provide analyst reports free of charge on their websites. Professional colleagues also provide an invaluable resource for shared experiences with specific solutions as well as avoiding pitfalls based on the experience of others.

2 | Conduct a PoC or Pilot before making any major decision.

The PoC means evaluating a security solution in a controlled test environment. A pilot evaluation requires putting the solution to work in a production environment with limited scope. In either case, decision-makers should use these techniques to answer the following types of questions:

- How easy is it to deploy the solution?
- How intuitive is the User Interface?
- Do I have the skilled resources to operate and maintain?
- Will this require additional professional services? And at what cost?
- What are the underlying requirements or hidden costs?
- Does it work in my specific environment?
- Does it integrate with my existing solutions?
- What kind of support options are available with the solution?
- Can we try logging some support calls just to test the response?
- Will it make our day-to-day tasks easier and more efficient?
- Does it offer more value for future priorities and business plans?
- Will it adapt and scale as our business grows?

RESOURCES

'Gartner's 2020 Magic Quadrant for Privileged Access Management and Gartner Peer Insights Reviews

CM-Alliance: Thycotic Tops CyberArk in PAM Vendor Evaluation

KuppingerCole: Executive View Secret Server

State of PAM Maturity Report highlights disturbing results based on more than 450 responses worldwide to our online PAM Maturity Assessment.

PAM for Dummies eBook provides an excellent overview of the PAM lifecycle.

Privileged Password Vulnerability Benchmarking Tool assessment and report.

KEY TAKEAWAY #3

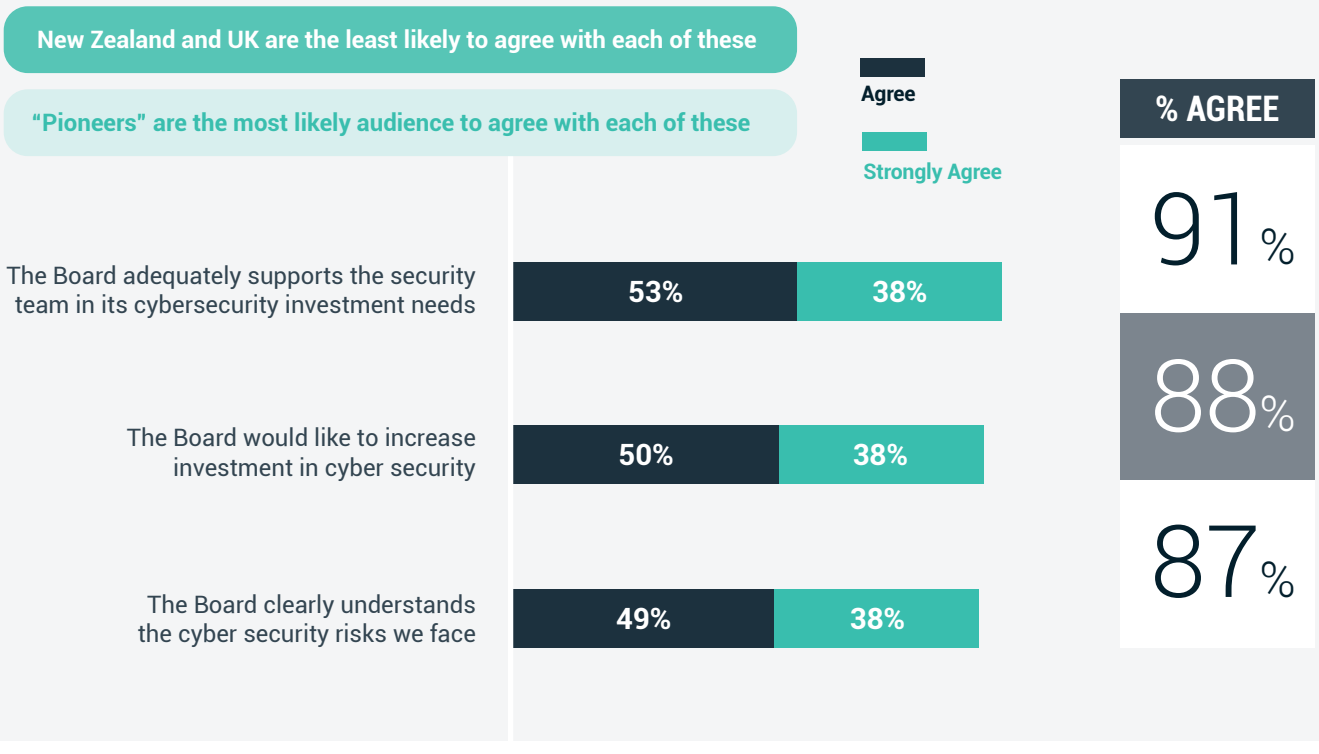
Boards appear to be supportive of increased cyber security investments, frequently motivated by the cost of internal security incidents and compliance audit failures. However, barriers to securing cyber security investments still remain. This includes technology purchases outside the scope of compliance needs, low perceived threats, and lack of ROI.

SURVEY RESULTS

More than 90% or 9 in 10 respondents believe their Boards adequately support the security team in its cyber security investment needs.

This is good news for IT security teams since past research has indicated getting Board awareness and support for investments was a struggle for many organizations. The COVID 19 pandemic may have contributed to growing support as it has accelerated the path to digital transformation and put the security of remote workers into much sharper focus.

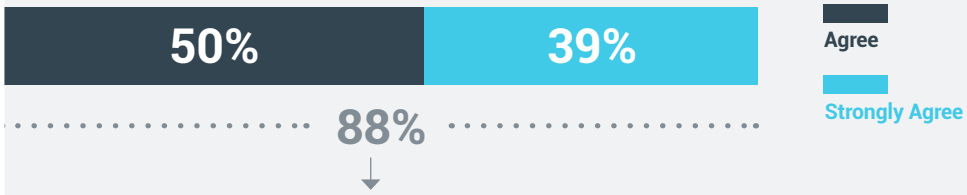
Q5 | Thinking about the Board approval for decisions on cyber security, to what extent do you agree with the following statements?



88% believe that they generally get Board approval for the level of cyber security investment they recommend.

Q6 | When thinking about the decision-making process for cyber security investment, to what extent do you agree with the following statements

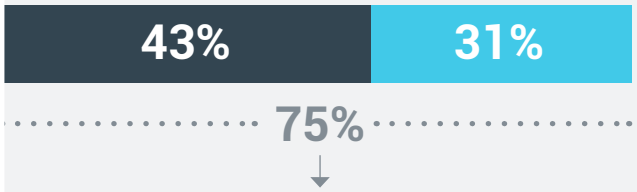
We generally get Board approval for the level of investment we recommend



JUST **81%** NEW ZEALAND, GERMANY

JUST **81%** IT/SECURITY MANAGERS

We want to try out innovative new tools but are not given the budget to do this



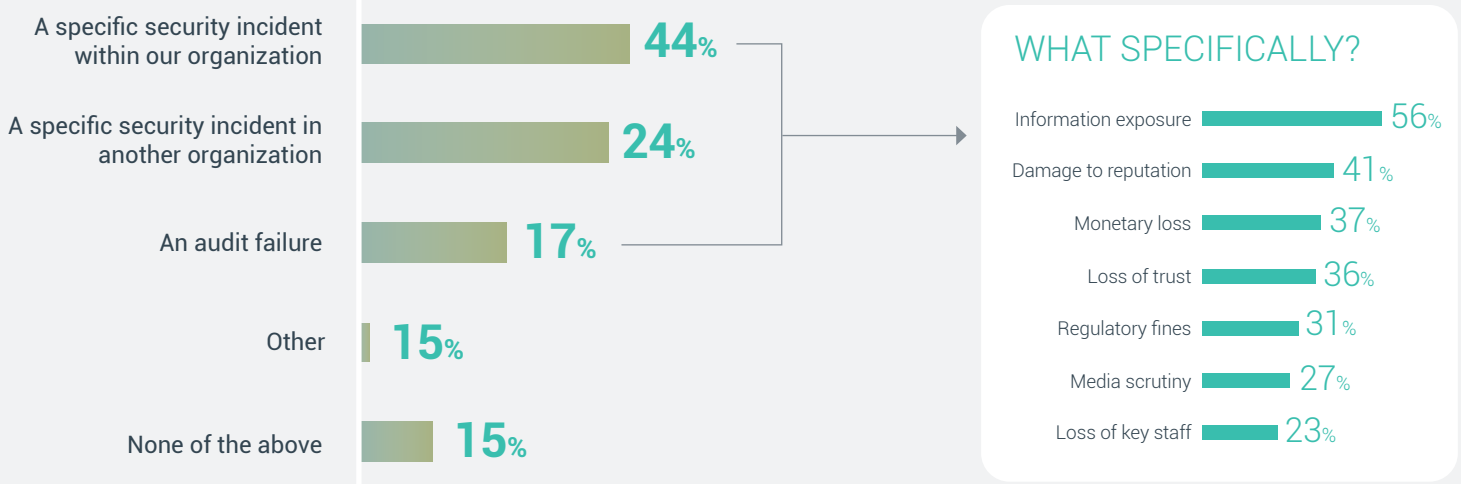
84% NEW ZEALAND, SPAIN

77% of respondents have experienced either an incident in their organization or an audit failure which convinced the Board to make investments in new security projects; specifically, information exposure and damage to reputation is reported to have triggered this.

The pervasiveness and publicity surrounding cyberattacks across the globe and a heightened regulatory environment have both contributed to a willingness by executive management to commit more funding to cyber security. Nothing focuses the attention of top management more than the occurrence of a security incident in their own organization. Given incident reporting requirements, it becomes difficult to hide or ignore incidents that have an impact on the 'organization's reputation.

Q3 / Q4

Have any of the following events/incidents convinced the Board to make investments in new security projects? What was it about the incident that specifically triggered the Board to change their mind?

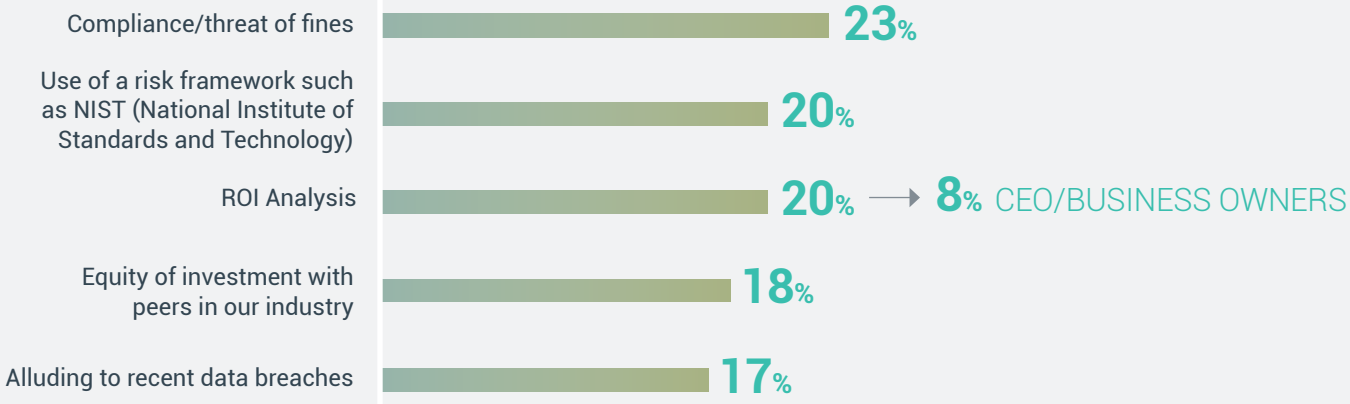


Almost a quarter of respondents believe that compliance or threats of fines have been the most effective in persuading Boards to invest in cyber security (23%)

The fear of compliance fines is a significant factor in convincing executive Boards to invest in cyber security, according to survey respondents. The EU GDPR, for example, has seen several companies receive significant fines in millions of € Euros resulting from a data breach or failure to be compliant. No one wants to be the next victim of a cyberattack or a failure in compliance. Therefore 23% of decision-makers use this fear factor as an effective motivator to help convince their Boards to invest in cyber security. Another 20% use best practices and standards to persuade Boards, with 20% focusing more on ROI by showing how cyber security can contribute to business value.

Q14

Which of the following strategies has been the most effective in persuading Boards to invest in cyber security?



Country comparison of most effective strategies in persuading Boards to invest

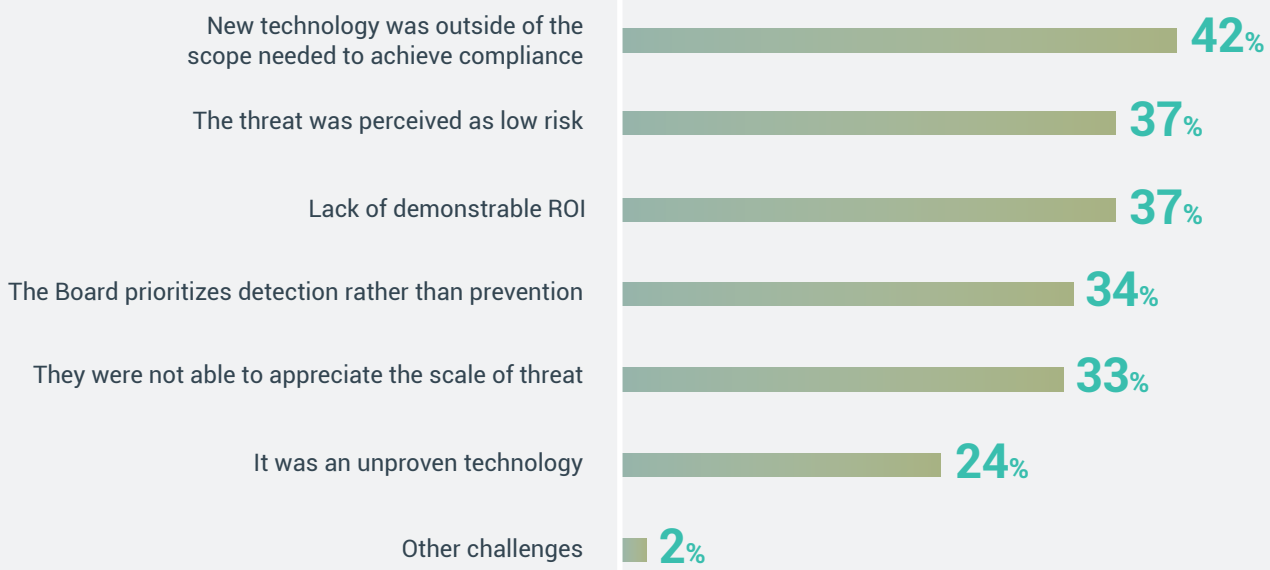
In the UK, Germany and France, compliance is top reason used to persuade the Board. Whereas in the US and New Zealand IT teams lead benchmarking against peers. Surprisingly, Australia, Singapore, and Malaysia lead with ROI.

	UK	Germany	US	Australia	New Zealand	France	Spain	Singapore/ Malaysia
1st	Compliance/ threat of fines (27%)	Compliance/ threat of fines (33%)	Equity of investment with peers in our industry (24%)	ROI Analysis (28%)	Equity of investment with peers in our industry (26%)	Compliance/ threat of fines (32%)	Use of a risk framework such as NIST (National Institute of Standards and Technology) (24%)	ROI Analysis (27%)
2nd	Use of a risk framework such as NIST (National Institute of Standards and Technology) (21%) / Alluding to recent data breaches (21%)	ROI Analysis (21%)	Compliance/ threat of fines (22%) / Use of a risk framework such as NIST (National Institute of Standards and Technology) (22%)	Use of a risk framework such as NIST (National Institute of Standards and Technology) (20%)	Alluding to recent data breaches (24%)	Alluding to recent data breaches (20%)	Compliance/ threat of fines (22%) / ROI Analysis (22%)	Use of a risk framework such as NIST (National Institute of Standards and Technology) (26%)
3rd		Use of a risk framework such as NIST (National Institute of Standards and Technology) (20%)		Equity of investment with peers in our industry (19%)	Use of a risk framework such as NIST (National Institute of Standards and Technology) (18%)	ROI Analysis (18%)		Compliance/ threat of fines (19%)

The biggest challenge IT security decision makers have faced when getting approval for investments on previous cyber security projects related to new technology purchases that fall outside the scope needed to achieve compliance (42%). Other barriers included low perceived threat risk (37%) and lack of demonstratable ROI (37%)

These survey responses indicate that compliance remains a top driver for security solutions with 42% of citing compliance, followed by 37% saying the threat was perceived as low risk and 37% naming a lack of ROI.

Q1 | **Thinking about your last one or two cyber security projects, what were the biggest challenges in getting approval from the Board on your cyber security investment?**

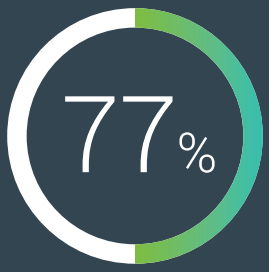


Most important sources of information by country

The US and France appear to be leading the way as pioneers with the UK, Germany, Australia, New Zealand, Spain, Singapore and Malaysia sticking with best practices and proven technology.

	UK	Germany	US	Australia	New Zealand	France	Spain	Singapore/ Malaysia
1st	New technology was outside of the scope needed to achieve compliance (46%)	The threat was perceived as low risk (48%)	New technology was outside of the scope needed to achieve compliance (43%)	New technology was outside of the scope needed to achieve compliance (51%)	New technology was outside of the scope needed to achieve compliance (51%)	The Board prioritizes detection rather than prevention (40%)	The threat was perceived as low risk (46%)	Lack of demonstrable ROI (58%)
2nd	They were not able to appreciate the scale of threat (41%)	New technology was outside of the scope needed to achieve compliance (36%)	Lack of demonstrable ROI (35%)	The threat was perceived as low risk (41%)	The Board prioritises detection rather than prevention (37%)	The threat was perceived as low risk (38%)	The Board prioritises detection rather than prevention (33%)	New technology was outside of the scope needed to achieve compliance (50%)
3rd	The Board prioritises detection rather than prevention (38%)	Lack of demonstrable ROI (32%)	They were not able to appreciate the scale of threat (34%)	Lack of demonstrable ROI (39%)	Lack of demonstrable ROI (36%)	Lack of demonstrable ROI (33%)	Lack of demonstrable ROI/It was an unproven technology (29%)	The Board prioritises detection rather than prevention (44%)

believe their Boards support cyber security investment needs



say security incident/audit failure convinced the Board to make investments

Most significant barriers to investment approval?

42% cite "outside the scope of compliance needs"

37% claim "low perceived threat"

37% can't demonstrate ROI

RECOMMENDATIONS

1 Move beyond a compliance checklist approach. Satisfying compliance mandates does not assure security.

Since businesses must typically satisfy the security requirements and controls mandated by legal regulations, meeting compliance goals can certainly help with getting budget approval. The risk of fines for regulation violations provides a tangible cost that executives understand. However, meeting audit requirements helps organizations get certified or become compliant, but that does not mean they are secure. Compliance is usually defined as a snapshot in time, that satisfies the lowest common denominator. True cyber security requires a continuous process of reducing business risks on a daily basis to meet the ever-evolving threat landscape.

2 Build the business case for cyber security investments with agreed upon ROI criteria.

Security solutions must also help add value to the business, not just be considered a cost. Leading with an estimate ROI when seeking budget approval can help reassure Boards when making investment decisions. How does a particular security solution help the business? In what ways does the solution help employees achieve their goals, improve productivity and accelerate digital business innovations?

To compare the cost of software, make sure you factor in all the variables. Consider what it costs to get up and running and to maintain and grow your solution over time.

The right decision can increase your competitive advantage and prepare you for the future. The impact of making the wrong decision may be felt for years.

To assist organizations in this step, Thycotic has created The PAM TCO Checklist to identify critical questions and weigh all the cost factors, so you can compare options and budget before you buy your software.

RESOURCES

Global State of Privileged Access Management Risk & Compliance shows privileged credentials at risk even as compliance requirements increase.

Resources to help you pass your next compliance audit you must demonstrate effective privilege management

CISO's quick Guide to Access Control Compliance

NIS compliance and Privilege Access Management

Customizable cybersecurity Incident response plan template helps IT operations, security and incident response teams form a united front against an attack to coordinate actions and maintain business continuity.

Least Privilege Discovery Free Tool

2019 WAS THE YEAR EU GDPR ENFORCEMENT GOT SERIOUS.

Having completed the introduction phase, EU GDPR enforcement came to the forefront in 2019 as several companies experienced a breach and suffered substantial penalties. More than 30 major fines were issued with over €400 million in financial penalties. Google was the first company to come under GDPR focus and was fined €50 million for lack of consent and transparency, including preselected opt-in for personalized ads.

Several hospitals, government agencies, and education institutes also received fines for poor Privileged Access Management. They either failed to protect personal information with appropriate authentication or stored data without proper consent. British Airways and Marriott, who were breached in 2018 (or at least discovered they had been breached that year) received the largest fines issued to date. British Airways was fined €204 million after 500,000 'customers' records were stolen and Marriott was fined €123 million after it discovered its reservation database had been hacked between 2014 and 2018.

There were several causes behind companies receiving EU GDPR fines:

- Not having adequate security protection, such as Privileged Access Management, authentication and multi-factor authentication for accessing personal information
- Not having appropriate consent for mass collection of personal information, such as having pre-checked opt-in or ignoring opt-out requests
- Failure to inform DPA within 72 hours of breach discovery

Companies that cooperated more closely with a DPA investigation were generally fined less for violations.

CONCLUSION

IT security and operations leaders face a daunting task when it comes to making cyber security technology investment decisions. The proliferation of vendors and products continues to grow especially as threats escalate and grow in sophistication.

By sharing the opinions and feedback of colleagues, this research survey report (and others like it) seeks to provide leaders with the knowledge and insights necessary to make more informed decisions. With cyber security budgets expanding to meet the rapidly changing needs of organizations worldwide, it is critical IT security decision-makers work diligently to ensure a safe and secure path for the accelerating digital transformation of a global marketplace.

This report is one of a series of global research survey reports from Thycotic focusing on critical issues facing cyber security professionals. Previous reports include:

The CISO Challenge: Aligning Business Enablement with Enforcement highlighting the internal challenges cyber security leaders must work to overcome in achieving recognition and resources.

The Cyber Security Team's Guide to Success sharing insights executive insights into how cyber security leaders measure results, secure budget and avoid stress.

Expert's Guide to Advanced PAM Success defining the people, processes and technologies CISOs, IT operations, and cyber security professionals need to plan and execute an advanced PAM program.

ABOUT THE SURVEY

Sapio Research conducted research in August 2020 among 908 Senior IT security decision-makers working at organizations with 500+ employees, within the following countries: UK (100) Germany (102) USA (200) Australia (102), New Zealand (102) France (100) Spain (102) Singapore (46) and Malaysia (54). At an overall level, survey results are accurate to ± 3.3% at 95% confidence limits, assuming a result of 50%.

Sapio Research is a London based B2B and consumer market research agency with an experienced team of researchers offering qualitative and quantitative research services and tools to help clients gain deeper insights. https://sapioresearch.com/

ABOUT THYCOTIC

Thycotic is the leading provider of cloud-ready privilege management solutions. Thycotic's security tools empower over 10,000 organizations, from small businesses to the Fortune 100, to limit privileged account risk, implement least privilege policies, control applications, and demonstrate compliance. Thycotic makes enterprise-level privilege management accessible for everyone by eliminating the dependency on overly complex security tools and prioritizing productivity, flexibility, and control. Headquartered in Washington, DC, Thycotic operates worldwide with offices in the UK and Australia. For more information, please visit www.thycotic.com.