Google Cloud

Google Research Survey

A Comparative Study on Cyber Risk: Business vs. Security Perspectives

2023 Survey Results

Commissioned by Google Cloud

ISMG
INFORMATION SECURITY
MEDIA GROUP

Introduction

Welcome to the report summarizing the survey: **A Comparative Study on Cyber Risk: Business vs. Security Perspectives.**

In Q3 2023, we surveyed 343 senior executives at major enterprises globally, divided into two groups of respondents: cybersecurity professionals and executive board members who are not cybersecurity professionals, to compare and contrast their perspectives on the role of cybersecurity in relation to organizations achieving their business or mission goals.

Areas we are keen to identify include:

- Views on current board capabilities and understanding of cybersecurity's role in addressing business risk;
- Board advice to CISOs on what they need to hear from their security teams compared to what the cybersecurity teams think they should be communicating;
- CISO advice to boards on what they need to ask of their cybersecurity teams versus what their boards think they should be asking;
- Perspectives on priorities and mitigation strategies in relation to cybersecurity threats;
- Board and CISO perspectives on the risks and opportunities presented by generative AI.

More than just survey results, this report offers expert analysis of what both boards and cybersecurity professionals perceive to be the main challenges around communicating cybersecurity risk and addressing or mitigating vulnerabilities. This report benchmarks what the industry is doing in regard to boards addressing cybersecurity so that you can use these results to replicate best practice and avoid common errors in approach.

Tony Morbin

Executive News Editor, EU
Information Security Media Group
tmorbin@ismg.io

Table of Contents

About this survey:

This survey was conducted in summer 2023. It attracted 343 responses from board members and senior cybersecurity professionals globally.

About Google Cloud:

Learn more at:
https://cloud.google.com/solutions/security/board-of-directors

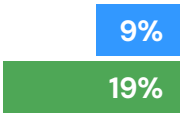
Google Cloud

By the Numbers

STATISTICS THAT JUMP OUT FROM THIS STUDY INCLUDE:

Business Security

12% of business leaders and 31% of security leaders believe they have no cyber experience on their board.



9% of business leaders and 19%, of security leaders say cybersecurity is only discussed at board meetings if an issue arises.

49% of business leaders and 33% of security leaders say they are very confident in their understanding of AI risk.

Executive Summary

Business leaders and security leaders agree on the importance of cybersecurity, but there are significant differences in how the two groups perceive and prioritize the threats and view the role of the other party.

Business leaders have greater confidence in the cybersecurity capabilities of their organization and their board members than do security leaders. These perceptions extend to new technologies such as generative AI and the level of preparedness required to tackle related tential new threats.

Board members may consider an issue resolved once the strategy has been agreed on, while cybersecurity professionals are tasked with operationally implementing that strategy.

More concerning, board members may have unjustified confidence in their cybersecurity, while cybersecurity professionals can be unwilling or unable to accurately communicate risks faced to the board.

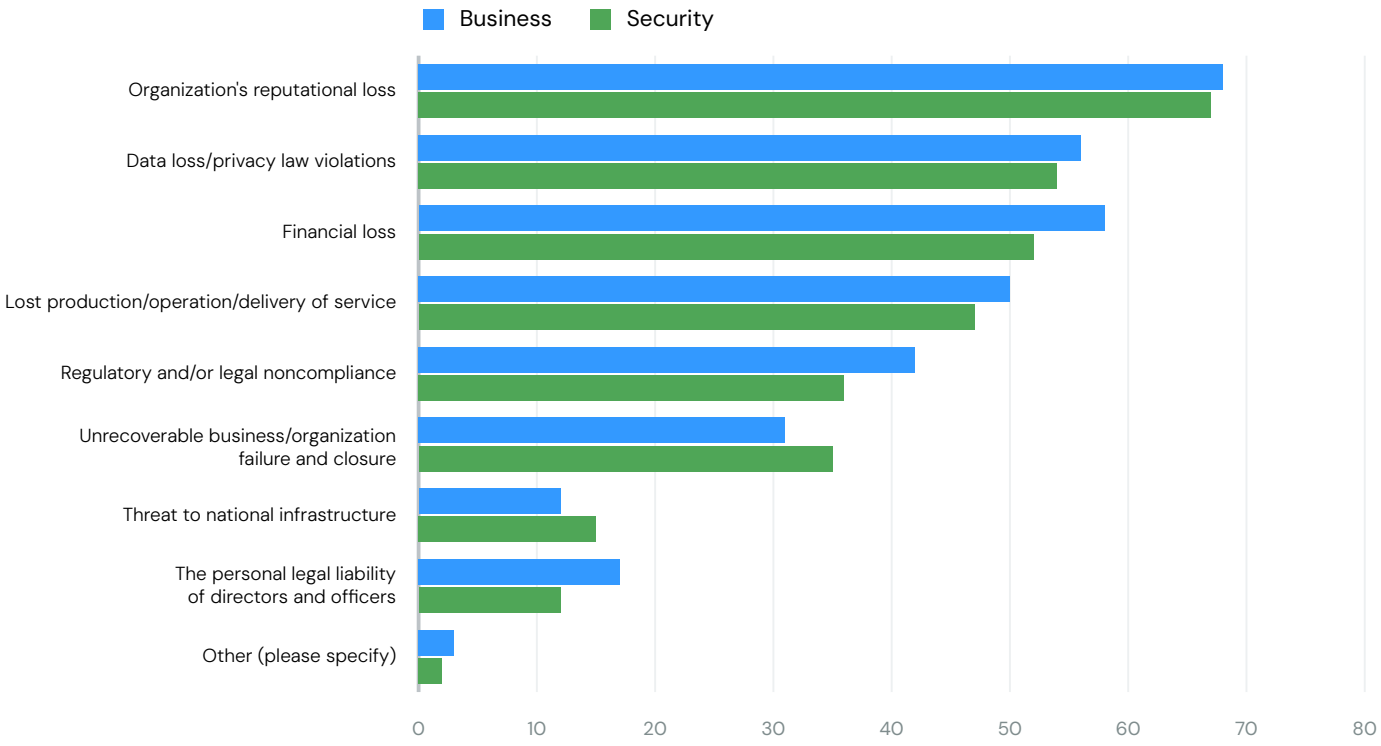
There is a need for greater communication so that each group might aid the other in their understanding. Board members' advice to CISOs reporting to the board includes: "Keep it short and to the point, but don't pull any punches. They [the board members] need to understand the risk," and, "Don't provide assurances that you can't back up and always be honest. Tell the truth."

In contrast, CISO advice to the board members includes: "No matter how bad the CISO makes it sound, it's worse," and, "Listen carefully."

On a more positive note, the two groups agree that reputational loss is the most concerning consequence of a successful cyberattack, business professionals understand how a cyberattack can affect the business, and cyberprofessionals appreciate the board members' role in ensuring the resiliency of the enterprise as a whole.

Survey Results

What are you most worried about in the event of a cyberattack? (Please select your top 3 concerns)



Business leaders are explicitly tasked with protecting the wider interests of their organization as a whole, whereas traditionally cybersecurity leaders were once perceived as having a narrow view of their remit, which was technically focused on managing cybersecurity controls. Whether that criticism was ever justified or not, our figures suggest that security leaders have realized that they include greater business awareness in terms of the impact of security lapses.

In fact, there were almost identical scores for business and security leaders when asked what is the biggest concern around cyberattacks. Both strongly agreed that it is the organization's reputational loss, with 68% of business leaders and 67% of security leaders putting it in first place.

There was a little more divergence in opinion for other threats, with second place for business leaders being financial loss, at 58%. Business leaders then put data loss/privacy law violations narrowly behind in third place, at 56%.

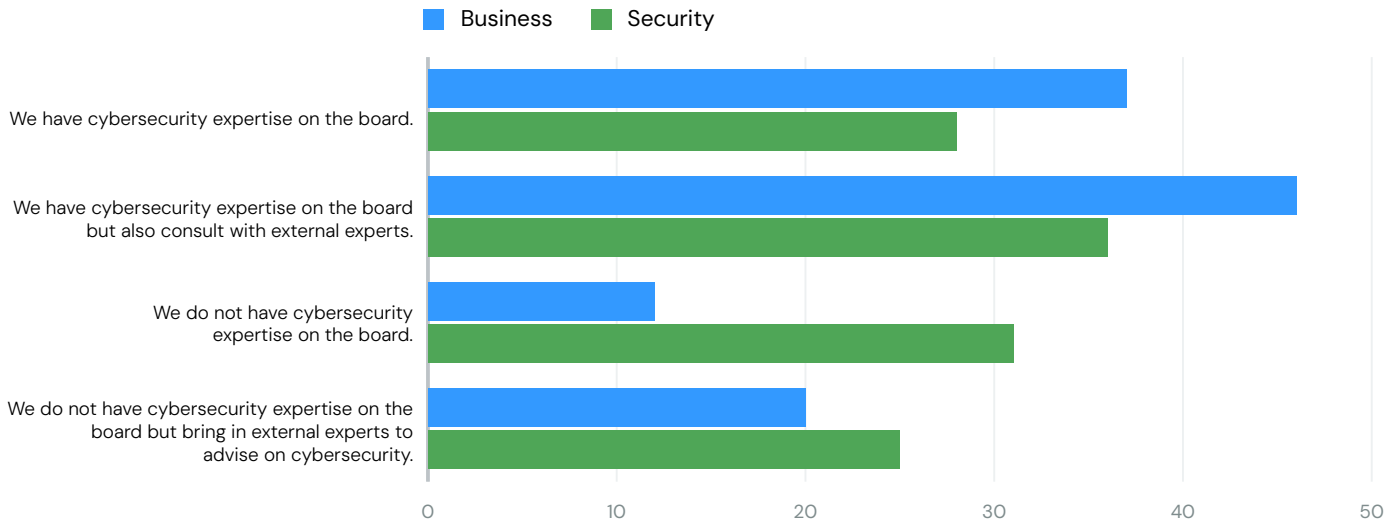
While the figures for security leaders was similar, the actual prioritization was reversed, with data loss/privacy law violations put in second place, at 54% and financial loss in third place, at 52%.

It is perhaps no surprise that business leaders should put financial loss higher than data loss given their targets, incentives and reputations are more likely to be tied to how well the organization is doing financially. Similarly, security leaders will be directly held responsible for data loss/privacy law violations, and see that as a primary part of their role. In fact, the surprise here is that the extent of divergence between the two is so narrow, with business leaders putting data loss so high, and security leaders putting financial loss so high – suggesting that each group appreciates the overall business impacts entailed in the other's concerns.

As would be expected, senior business leaders rate the personal legal liability of directors and officers higher - 17% - than do security leaders - 12%. But that may change as security leaders increasingly find themselves implicated when there is a material impact from a breach under SEC rules in the U.S., as in the current case of the CISO at SolarWinds being deemed liable by prosecutors for negligence, and similar regulations internationally, including named personal liability for noncompliance under the EU's NIS2 directive.

Comparing previous anecdotal commentary about business and security leaders' perspectives of each other's concerns with the statistical results of this survey, it would appear the gap has narrowed when it comes to business leaders now appreciating the business impact of a security fail and security leaders understanding the business responsibility of the security function. But there is still some way to go for security leaders to appreciate the growing potential personal impacts of legal liability for senior company officers.

Which of the following do you have? (Please check all that apply)



One area where there is a glaring difference in perception between business leaders and security leaders is in assessments of the board's security experience and competence.

Twelve percent of business leaders simply say their organizations have no cyber experience on the board – while a further 20% qualify that by saying they have no cyber experience on the board but they bring in external experts to advise on cybersecurity. That means 32% don't have cybersecurity experience on the board – a frighteningly high figure considering cyberthreats are now a tier one threat with the potential to close a company for good.

Yet the situation may be even worse with security leaders, with 56% of them saying their organization has no cyber experience on the board. Thirty-one percent simply say there is no experience there, and 25% say there is no experience but qualify it by saying cybersecurity expertise is brought in.

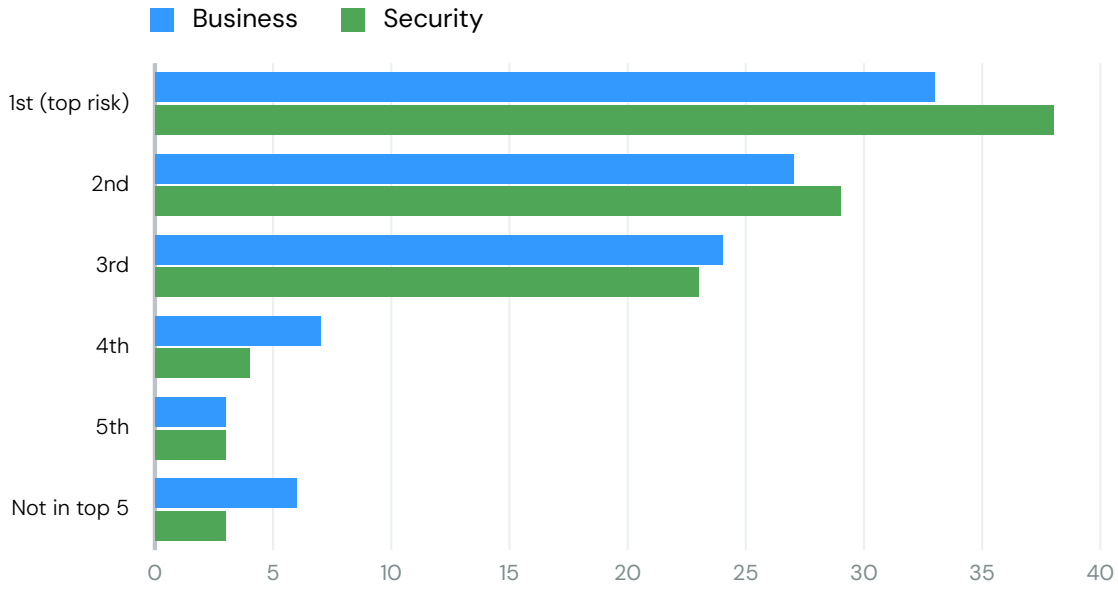
When looked at in terms of what experience they thought they had, 37% of business leaders say they have cybersecurity expertise on the board, and 46% say they have experience on the board and also bring in expertise. Thus 83% believe they have cyber experience on the board.

Again, in contrast, only 28% of security leaders say they have cybersecurity experience on the board, and 36% say they have cyber experience and bring in outside expertise, thus a total of 64% believe they have cyber experience on the board.

This huge discrepancy – 86% of business professionals and 64% of cybersecurity professionals believing they have cybersecurity expertise on the board – speaks of a gulf in perception of what it means to have cybersecurity expertise. Of course, cybersecurity professionals will have higher expectations of what it means to have cybersecurity experience, and business professionals covering a broader remit of expertise are likely to play up more limited knowledge. As the question invite respondents to check all answers that apply, there is some double counting and thus totals exceed 100%. But these figures are not even close.

The obvious conclusion is that boards have far less cyber expertise than business leaders believe they have.

How significant is cybersecurity risk relative to the organization's overall risk posture?



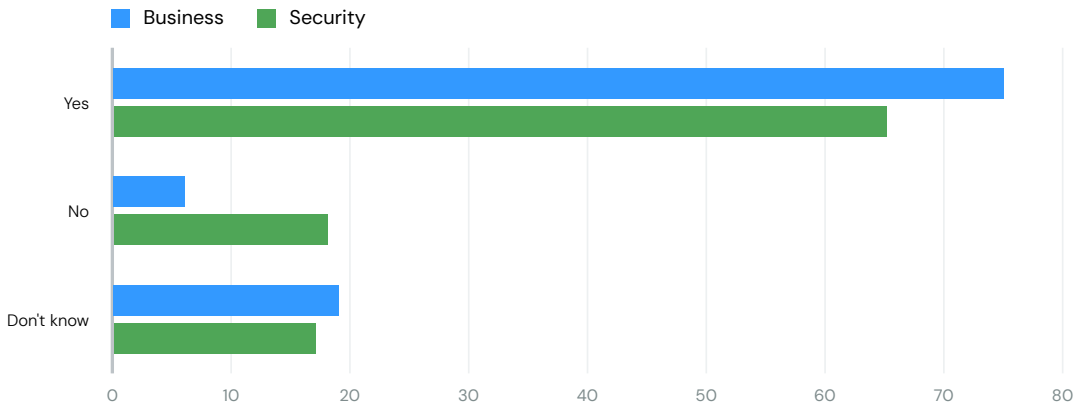
Remarkably, more business leaders put cybersecurity as their top risk - 38% - than do cybersecurity leaders - 33%, which may speak to fear of the unknown, but it contradicts a widely held view among security leaders that business leaders don't appreciate just how great a risk cyberthreats are to their organization.

In fact, the opposite appears to be the case when looking at those who do not put cybersecurity risk in their top five, and while the numbers are low – at 3% for business leaders and 6% for cybersecurity leaders –twice as many security leaders minimise the risk compared to business leaders.

For the bulk of respondents, the results are very similar, thus it's the second-greatest risk for 29% of business leaders and 27% of security leaders, and in third place for 23% and 24%, respectively.

Frankly, the downplaying of cybersecurity risk by cyberprofessionals is a counter-intuitive response. It was not expected and is not easily explained.

Is your cybersecurity risk within your organization's risk appetite?



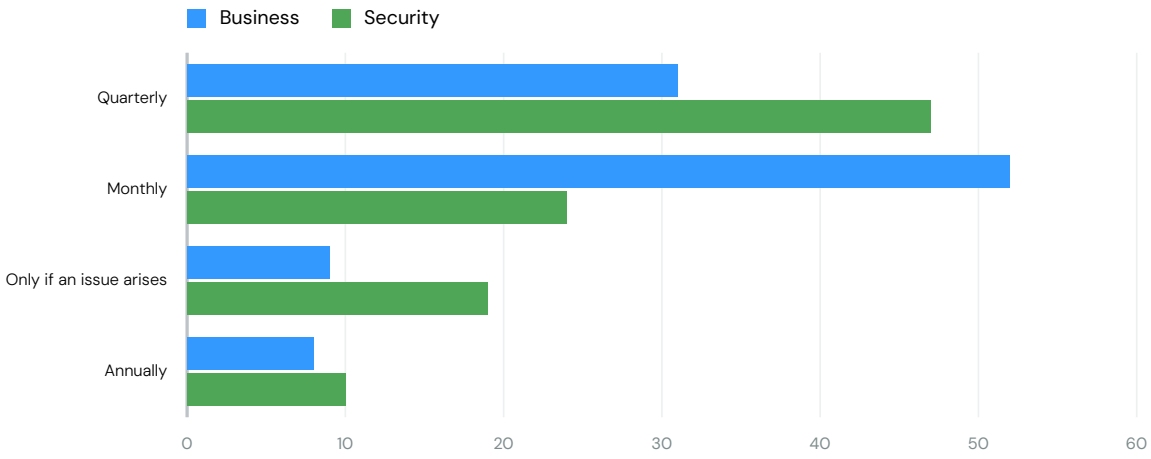
Seventy-five of business leaders say that their cybersecurity risk is within their organization's risk appetite, compared to 65% of security leaders. It is likely that business leaders will have a better appreciation of the bigger picture in terms of what the organization's appetite for risk is, whereas the cybersecurity professionals are expected to have a better understanding of what the risks faced actually are, with either factor contributing to this divergence.

A nearly equal percentage – 19% of business leaders and 18% of security leaders – say they don't know their cybersecurity risk within their organization's risk appetite – again, the business leaders likely have less knowledge of actual risk, and the cybersecurity leaders likely have less knowledge of the organization's risk appetite.

Only 6% of business leaders say their cybersecurity risk is not within their organization's risk appetite – suggesting concern about specific issues, but 17% of cybersecurity professionals say it is not – suggesting knowledge of a greater number of specific concerns, or implications, that may not have been communicated to management.

The inference is that cybersecurity professionals are aware of more cybersecurity concerns than are communicated to management.

How frequently are cybersecurity issues a topic in board discussions?



The largest number of business leaders - 52% - say cybersecurity issues come up in the board room monthly, but less than half that number of cybersecurity professionals agree, with only 24% saying it is discussed monthly.

For security leaders, the largest number - 47% - say it comes up quarterly, whereas just 31% of business professionals say it is discussed quarterly.

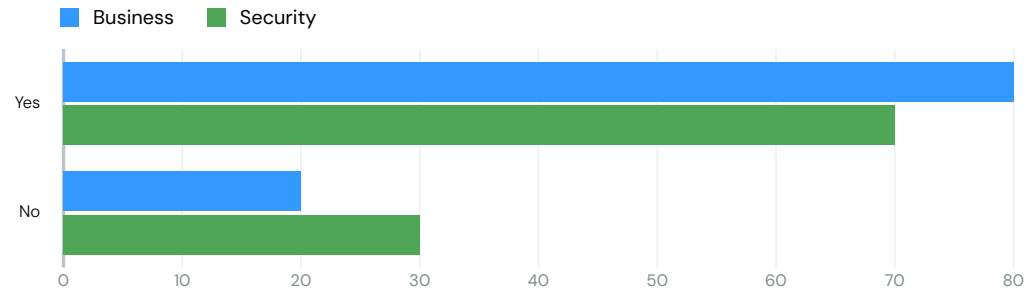
Another huge discrepancy is that just 9% of business leaders say cybersecurity is only discussed if an issue arises, compared to more that double that number - 19% - of security leaders who say the same thing.

It is also shocking that 8% of business leaders admit cybersecurity is only discussed annually, and slightly more cybersecurity professionals - 10% - believe that is the case.

The clear implication is a divergence of perception in how frequently and in what context cybersecurity is discussed. Business professionals believe it is discussed frequently on a planned regular basis, and cyber professionals believe it is discussed as much as half as often and is twice as likely to simply be addressed on an ad hoc basis, presumably when an incident occurs that has to be addressed. Lack of discussion suggests lack of prioritisation/ importance attached to cybersecurity.

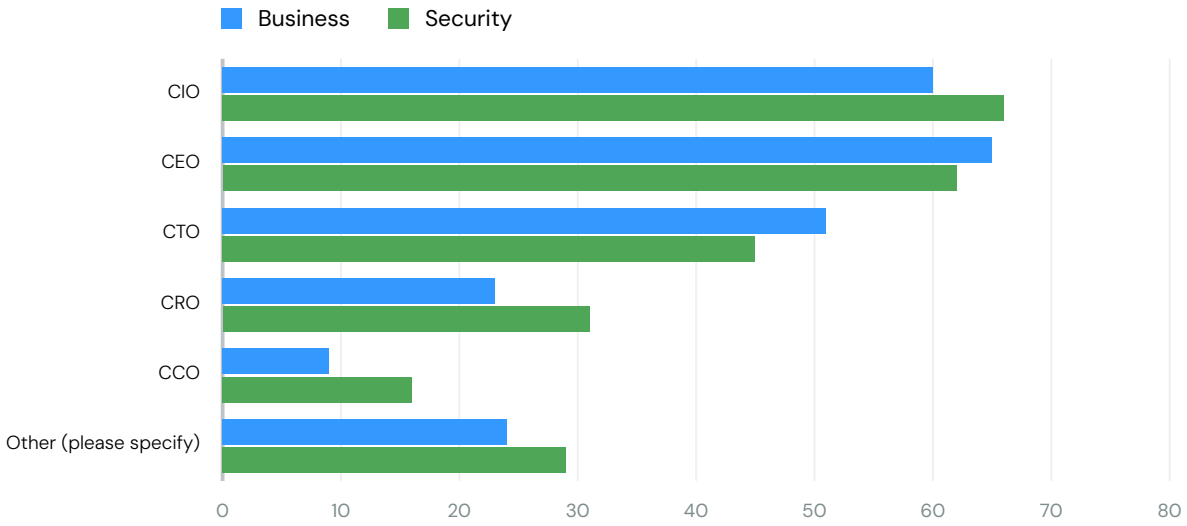
Bridging the divide between business leaders and cybersecurity will require better communication, and our results show that the cybersecurity professionals do not believe current communication is as good as business professionals seem to believe it to be, hence prioritization of cybersecurity is not as high as business professionals believe it to be.

Do you participate in ad hoc meetings on cybersecurity topics with the board members and/or other executives?



Eighty percent of business leaders report participation in ad hoc discussions of cybersecurity, which is noticeably greater than that of security leaders, at 70%. This demonstrates that business leaders are discussing cybersecurity issues without their cybersecurity leaders present. One-third of cybersecurity leaders report never being engaged in such meetings – and this exclusion reduces authoritative information flows to the board.

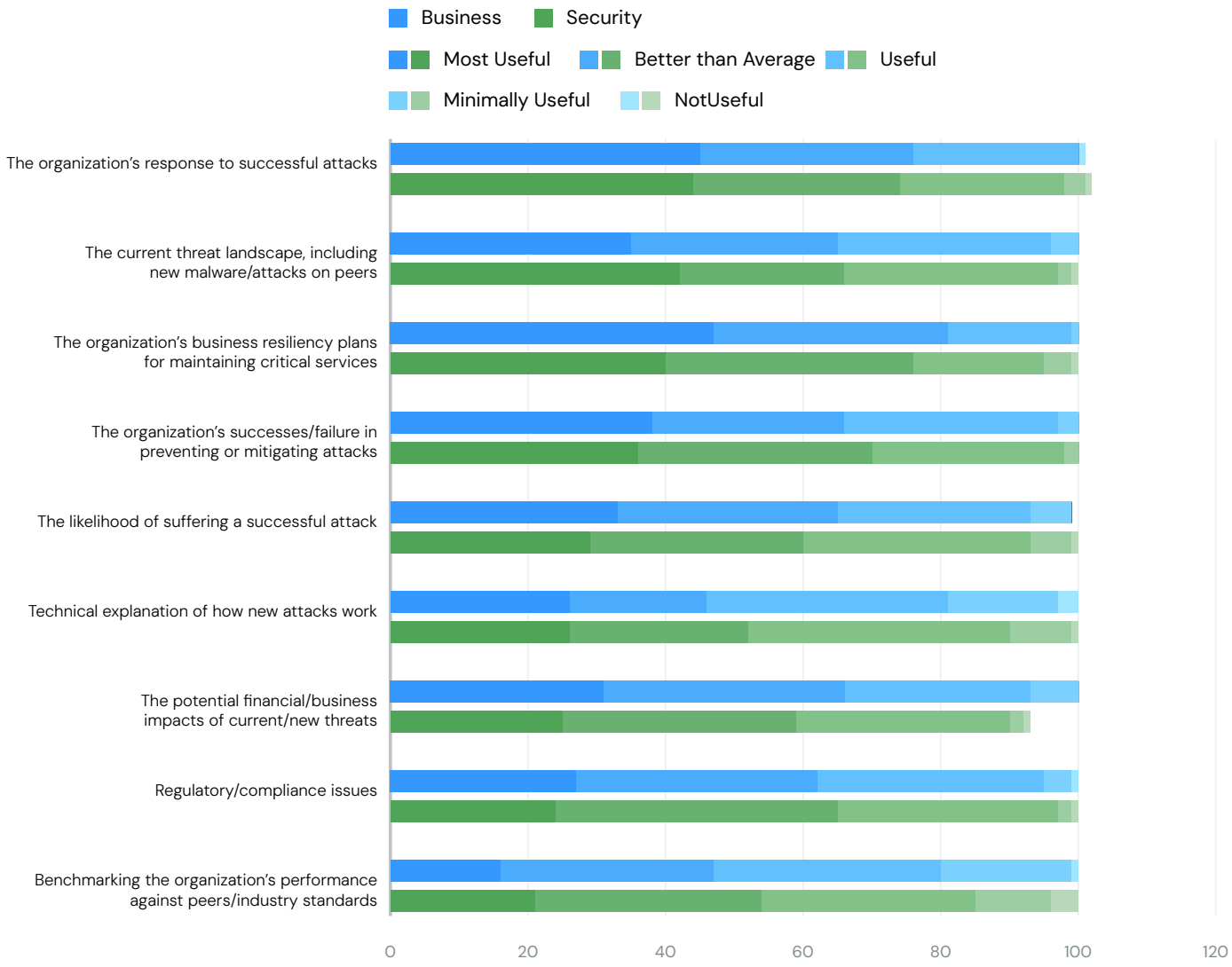
If yes, with whom do you discuss the cybersecurity topics? (Select all that apply; if No to previous, skip)



Where these discussions do occur, there are the expected differences in who business leaders and security leaders speak with. Business leaders say they most often speak with the CEO, at 65%, compared to 62% for security leaders.

Security leaders say they most often speak with the CIO, at 66%, compared to 60% for business leaders. The next most likely candidate for discussion with both groups is the CTO, at 51% for business leaders 51% and 45% for security leaders.

What cybersecurity-related information is most useful to you?



By looking at what cybersecurity-related information is most useful for each of the cohorts, we are able to get an indication of priorities and concerns, or pain points.

As would be expected, there is considerable overlap in areas of shared concerns, but equally, given the different roles, there are also differences in emphasis between the two groups.

Business leaders say the most useful information is the organization's business resiliency plans for maintaining critical services, at 47%, which would fit in with their big-picture strategic concerns. Of course there is no "right answer" – but if there were, business resiliency might well be it – yet security leaders rank it third, at 40%.

Security leaders say the most useful information is that which helps the organization's response to successful attacks, at 44%. No doubt this reflects their day-to-day operational concerns rather than organizationwide strategic concerns.

Business leaders did not neglect that issue and ranked it second, at 45%.

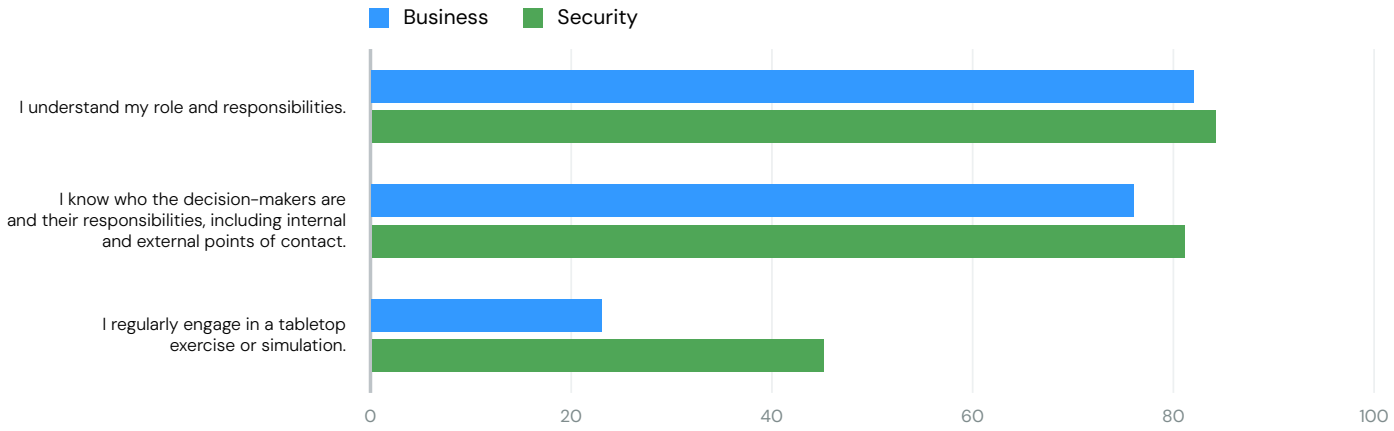
In second place for security leaders is information on the current threat landscape, including new malware/attacks on peers, at 42%. Again, this reflects an operational rather than strategic approach, in line with the remit of the role.

In third place for business leaders is the organization's successes/failure in preventing or mitigating attacks, at 38%.

At the other end of the scale, 1% of business leaders describe benchmarking the organization's performance against peers/industry standards as not useful, compared to 4% of security leaders. Three percent of business leaders say technical explanations of how new attacks work are not useful, as do 1% of security leaders.

In general, it would appear that cybersecurity professionals adopt a practical, operational perspective of areas where further cyber-related information is sought, while business leaders, often wanting much of the same information, prioritise in terms of strategic threats.

If your organization had a cyber incident, such as a ransomware attack, which of the following would apply? (Please check all that apply)



With the option to check all that apply, double counting may occur, but 82% of business leaders and 84% of security leaders say they understand their role and responsibilities if a cyber incident occurs. Seventy-six percent of business leaders and 81% of security leaders say they know who the decision-makers are and their responsibilities, including internal and external points of contact.

The biggest discrepancy is in the number who regularly engage in tabletop exercises or simulations. Forty-five percent of security leaders say they do, compared to only 23% of business leaders.

What qualifications does a CISO need to effectively articulate cybersecurity risk at the board level?

The responses from business leaders include having deep technical knowledge, understanding of the business and the business impacts of attacks, financial understanding and the communication skills needed to articulate risk in business terms to a nontechnical audience. Some respondents emphasized practical experience over formal qualifications while others specified qualifications such as CISSP.

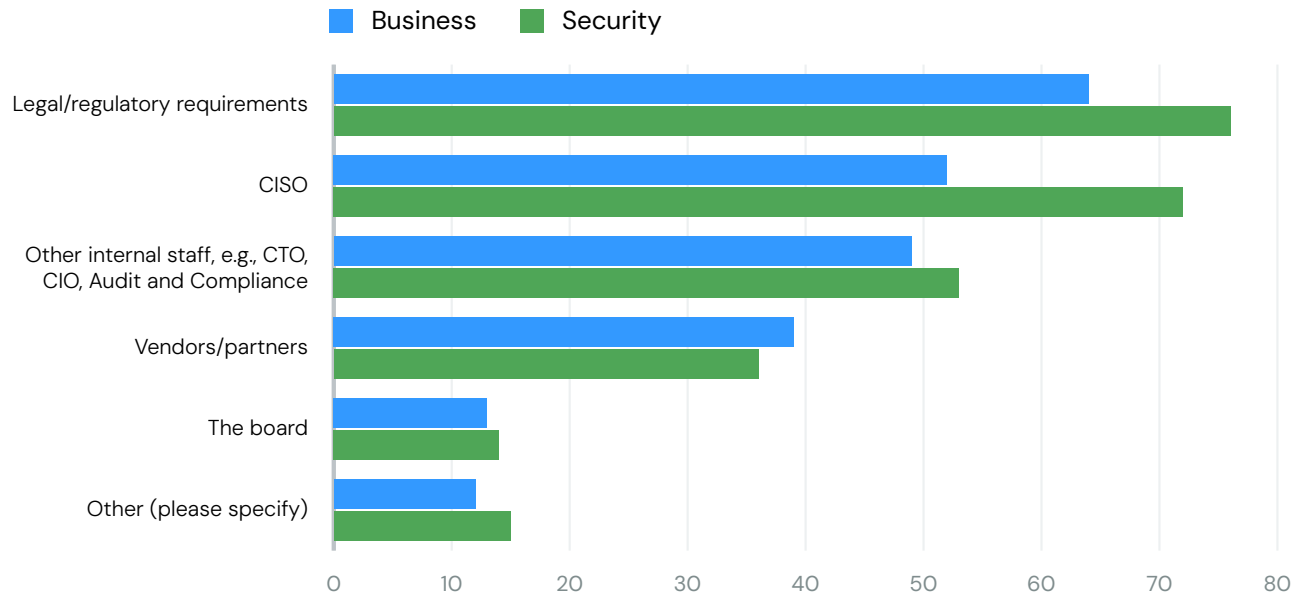
The responses from security leaders include the understanding that a CISO needs a combination of technical expertise, business acumen and strong communication skills to articulate risk to the board. Some advocate formal qualification but others are more in favor of hands-on experience.

What key piece of advice would you give to the board when it comes to asking the CISO about cyber risk?

Security leaders say questions from the board should reflect understanding of the consequences of decisions. The board should also ask questions to identify exactly what it is that they don't know. Then, they should be prepared to listen to answers that they might not want to hear, such as, "You will need to spend to fix this."

Business leaders say questions from the board should be brief, simple, realistic, truthful and relevant to the business.

Where does the organization source its cybersecurity standards from? (Please check the top 3)



Both business leaders and cybersecurity leaders have the same order of prioritization of sources of cybersecurity standards for the organization.

The top response from both groups is legal/ regulatory requirements, but cybersecurity leaders give it a higher rating, at 76%, compared to 64% from business leaders.

CISOs come in second for both groups, but again security leaders give it a higher rating at 72% compared to 52% for business leaders.

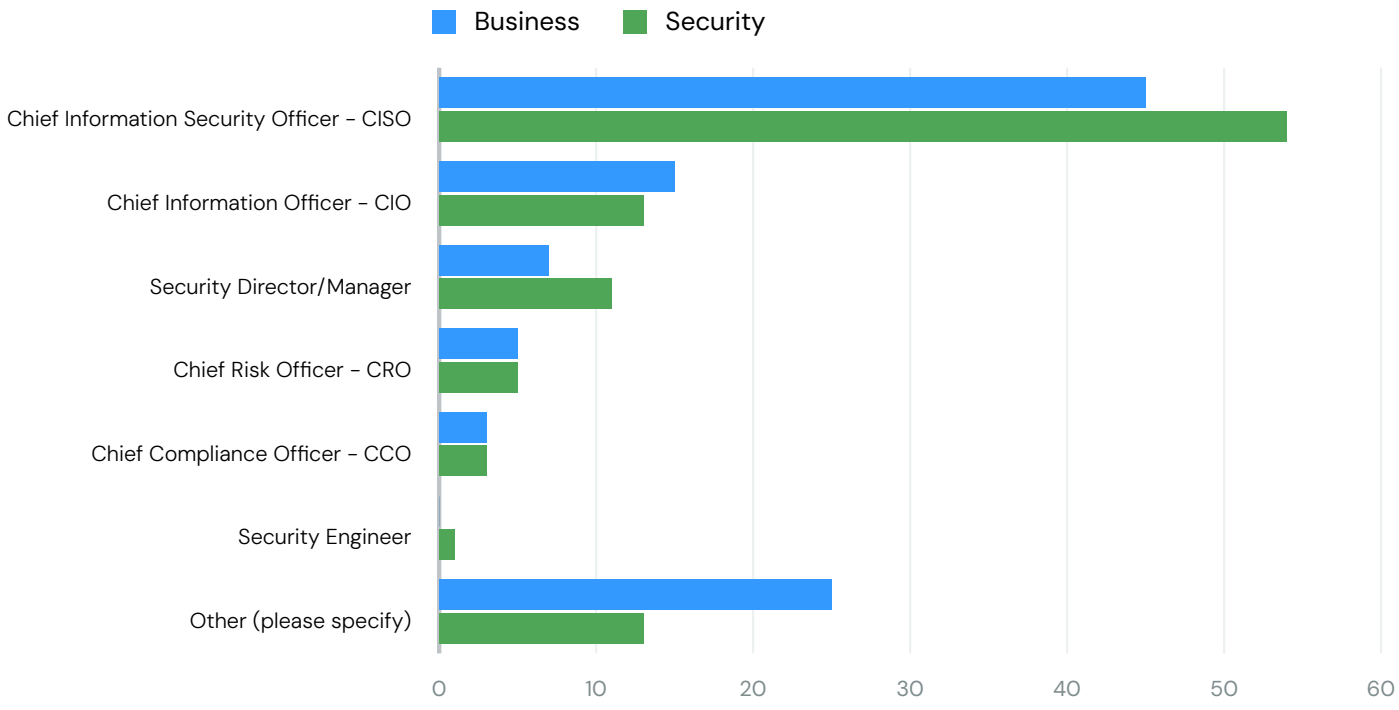
For business leaders, other internal staff comes in at 49% compared to 53% among security leaders.

Perhaps surprisingly, business leaders are more likely to get standards from vendors or partners than security leaders are, at 39% and 36%, respectively.

The board scored just 13% from business leaders and 14% from security leaders.

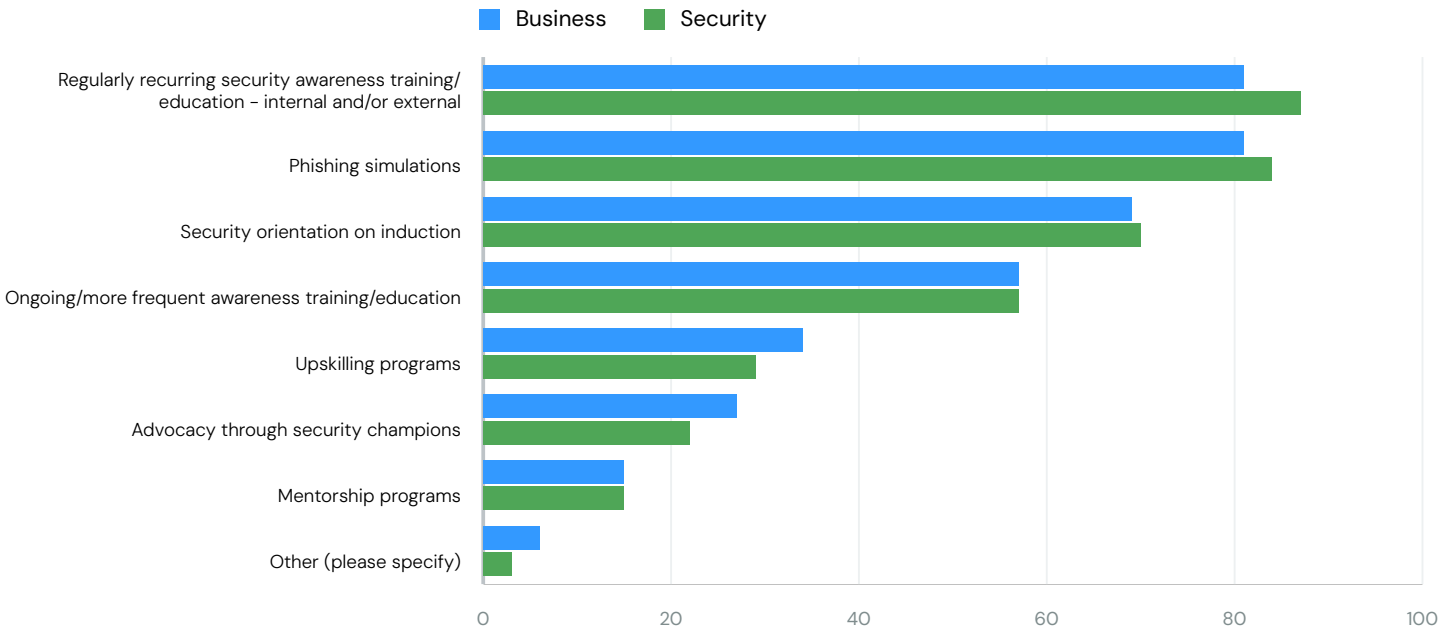
Conclusions include that while the two cohorts are aligned in terms of where standards come from, security leaders appear more vested in those standards by having a higher engagement in them and more direct responsibility for delivering and conforming to them.

Who is responsible for leading the charge to create/mature a security culture in the organization?



Business leaders and security leaders are in strong agreement. The top choice for 45% of business leaders and 54% of security leaders is CISOs, and the second choice for both groups is CIOs, at 15% for business leaders and 13% for security leaders. Twenty-five percent of business leaders say others are responsible and the most frequently cited individual is the CEO. Other choices include legal, the CTO, the board, the IT director or h of IT, the CTO, and the head of audit.

Which of these approaches do you use? (Please check all that apply)



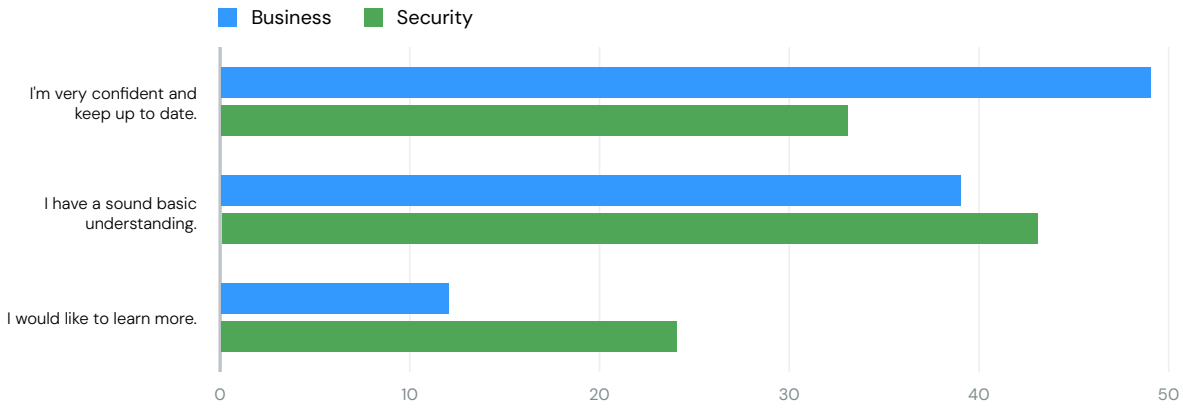
Both business leaders and security professionals are in general agreement when it comes to approaches used to maintain information security in terms of priorities/most used, though specific scoring differs.

The most popular security approaches for business leaders are phishing simulations and regularly recurring security awareness training/education, in a tie for first place at 81%.

Among security leaders, regularly recurring security awareness training/education is in first place at 87%, followed by phishing simulations at 84%.

Security orientation on induction comes third in both groups – at 69% for business leaders and 70% for security leaders.

Relative to your peers, how would you assess your understanding of the risks of AI/ emerging technologies?



Thirty-nine percent of business leaders say they are very confident and keep up to date with the risks of AI/emerging technologies, compared to 33% of security leaders, and 39% of business leaders say they have a sound basic understanding, compared to 43% of security leaders. Twice as many security leaders - 24% - say they would like to know more, compared to 12% of business leaders.

It may simply be that business leaders need a more optimistic outlook than security leaders, whose role calls for a higher level of scepticism.

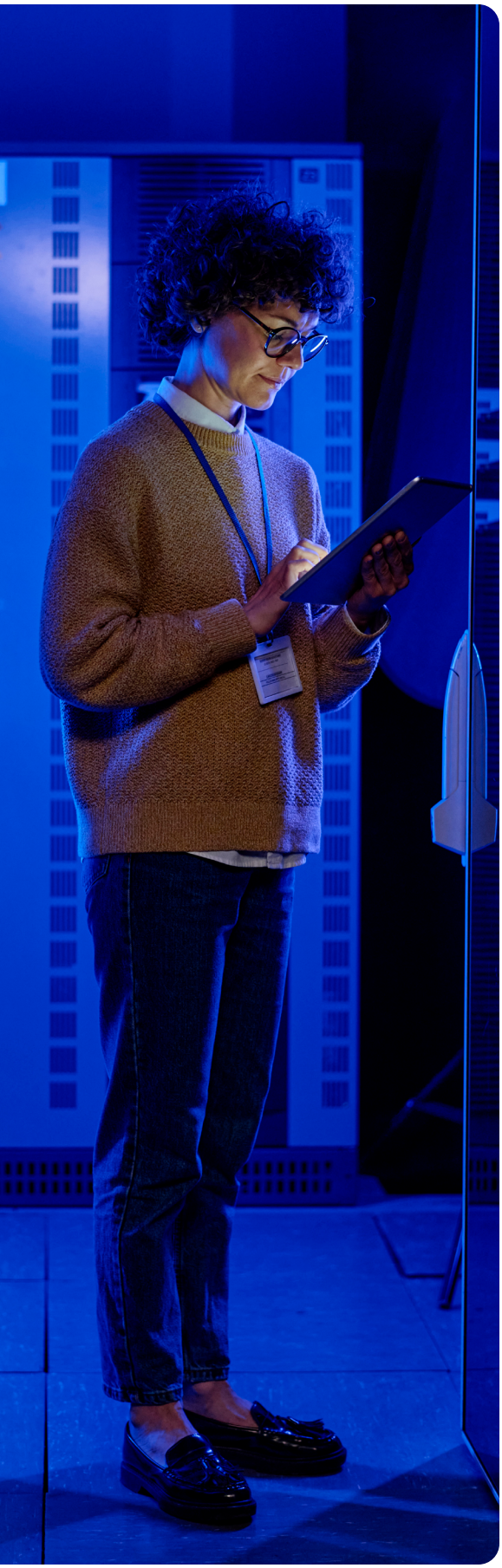
In addition, the nature of a tech-oriented role necessitates constant learning and keeping up to date with new developments, thus the surprise should not be that twice as many security leaders say they want to know more, but that the figure was only 24%.

What AI-related risks are most concerning to you?

The respondents expressed wide-ranging concerns, and while the security leaders put more emphasis on specific attack types, generally, they and the business leaders have the same concerns, including ease of attacks, loss of visibility, misuse by staff with unintended consequences and ethical issues. Clearly, security issues are proliferating and are expected to increase in line with usage and understanding of what AI can do and is doing.

Responses from business leader responses address data leakage, faster attacks, erroneous information, and the unknown.

Responses from security leaders cover a range of specific attack enhancements and the simplification of attacks when AI is used by adversaries, plus misuse by staff, unintended consequences, bias within the system, accidental errors or poisoned learning, and the unknown.



Conclusions

Moving Beyond Stereotypes

Often stereotypes exist because they contain a kernel of truth, but stereotyping is a lazy way to categorize as it cannot provide the full picture. People are not one-dimensional; they are complex and individual, even within categories.

Negative stereotypes of business leaders seen from a cybersecurity perspective include that they simply see cybersecurity as a brake on innovation, slowing speed to market and incurring unlimited cost with no tangible return, and they lack understanding of business imperatives and the need to describe risk in business terms.

On the opposite side, security leaders can be accused of sometimes viewing business leaders as being incautious in their pursuit of profit and growth and having no understanding of technology or the impact of a successful attack and cybersecurity's role in reducing business risk.

In this survey, we have a wide range of views expressed via responses to set questions, and we received perceptions of both business leaders and security leaders from their counterparts. We found that both stereotypes are wrong. Business leaders demonstrate an appreciation of the role played by cybersecurity and acknowledge that security leaders have a better understanding of business needs than they are often given credit for. But differences of perspective do exist.

Playing Offense vs. Defense

Both business and security leaders recognize that they are on the same side, striving to ensure the business succeeds, and the reputation of the business is a leading concern for both. But while business leaders are playing offense, trying to increase their score, security leaders are playing defense, minimizing opportunities for their opponents.

Each group needs to acknowledge the part the other plays. In many areas, this survey suggests significant room remains for greater communication and understanding of the other party.

The role of the business leader is to take calculated risks – within the risk appetite of the organization - through innovation to grow the business. Our survey shows how business leaders are experimenting with a far wider range of AI than security leaders, in a wider range of use cases.

Optimism vs. Understanding

Business leaders have a more optimistic outlook and express greater confidence in the cybersecurity capabilities of their organization and their board compared to security leaders. They believe they have more discussions about cybersecurity, and they say their understanding of AI risks is higher than what security leaders report.

But twice as many security leaders say they conduct simulation exercises, as compared to business leaders. And slightly more business leaders than security leaders say they do not understand their role and responsibilities or who the decision-makers are and their responsibilities in the event of a cyberattack – at 18% for business leaders and 16% for security leaders.

This lack of comprehensive understanding of roles and responsibilities by both parties suggests a lot more needs to be done in the areas of implementing playbooks and preparing for attacks via simulation exercises.

Different Priorities

Understanding and prioritization of security risks including AI risks is similar across both groups, although security leaders understandably rank data loss higher than financial loss. When looking at AI threats, although there is significant overlap – for example, in data loss and AI hallucinations, business leaders tend to worry about strategic threats while security leaders are concerned about specific operational threats.

Business leaders say that the most useful information for them is the organization's business resiliency plans for maintaining critical, and security leaders say it is the organization's response to successful attacks, again reflecting the divide between strategy and operations.

Honest Communication …

On communication between the two groups, and advice to their counterparts, one telling comment in the survey is from a security leader to business leaders: "No matter how bad the CISO makes it sound, it's worse. We really need to invest more in basic maturity and security hygiene." The commenter calls on business leaders to "listen" and understand the impact of an attack. Yet, in their comments, business leaders call for honest explanations, even if they will be hard to take.

Taken together, the comments show that business leaders suspect and security leaders confirm that security sometimes sugarcoats bad news and business sometimes turns a deaf ear to difficult truths. Both sides know the solution – security needs to be frank, and business needs to acknowledge and respond to the concerns raised.

… Leads to Effective Action

Comments on the survey show that each side has an acute awareness of the concerns and pain points of the other side. The negative is that more work needs to be done to bridge the gaps between statements of understanding and actions that demonstrate that understanding.

Business leaders need to ensure that in pursuing their overarching strategy, they do not ride roughshod over the practical realities of operations that security leaders face. Security leaders need to ensure their operational activities are aligned with the overall business strategy of their organizations. And the two need to communicate more to address joint concerns and achieve optimum results for both.

Expert Analysis Based on Interview With Google

David Homovich

Office of the CISO, financial services, Google Cloud

In an interview with Information Security Media Group, David Homovich, Office of the CISO, financial services, Google Cloud, discussed the key survey findings.

Cybersecurity Expertise

TONY MORBIN: What was the most significant finding of the report for you, and did it confirm what you expected?

DAVID HOMOVICH: One of the interesting findings in the report is around boards' expertise and understanding of cybersecurity. Thirty-one percent of security leaders say that their organizations have no cyber expertise on the board, and 36% say they have expertise on the board but also bring in external counsel or experts to advise on cybersecurity. In contrast to that, 12% of the business leaders say that their organization has no cyber experience on the board, and 20% say they don't have it bring in cyber experience externally to help advise on cybersecurity.

There is a disparity between how much cybersecurity expertise an organization thinks they have versus what they actually have. This aligns to what we're seeing happening now globally from governments, which are increasingly implementing regulatory measures to raise compulsory cybersecurity baseline standards, including for boards to be able to demonstrate oversight of cybersecurity risk. And that aligns with why Google Cloud developed our Board Insights Program and why we're publishing our quarterly perspectives for the board on security.

"There is a disparity between how much cybersecurity expertise an organization thinks they have versus what they actually have. This underscores how important it is to incorporate security into all business initiatives."

It also underscores how important it is to incorporate security into all business initiatives. Everyone needs to understand that cybersecurity is everyone's responsibility, from interns to the boardrooms.

Readiness for a Cyber Incident

MORBIN: Was there anything in the survey that surprised you?

HOMOVICH: There really was. Eighty-two percent of the business leaders and 84% of security leaders believe that they understand what they need to do in the event of a cyber incident, and we're seeing more and more cyber incidents occurring every day. At the same time though, when we ask those respondents if they participate in a cyber simulation or an exercise to test those capabilities, only 23% of the business leaders said that they do, while 45% the security leaders said that they do. So while a significant part of the population surveyed says they know what to do in the event of a cyber incident, they're not preparing for a cyber incident via a simulation or an exercise.

Individuals that aren't testing the playbooks and best practices that need to be followed during a cyber incident may not understand fully the impact an attack is going to have on the business and what the business's response and recovery process is. The best way to prepare to respond to a cyber incident is to ensure that your business is resilient, meaning that your services can be brought up in little or no time without impact to the customer. That requires testing to be in place. I encourage individuals to go through simulation-type exercises to build that muscle memory, so that when there is a cyber incident, they'll be able to respond.

CISOs vs. Boards on Optimism

MORBIN: The board were generally more optimistic in their responses. What would you say are the reasons for that, and what concerns does that raise?

HOMOVICH: It's the old saying, "Where you stand is where you sit." Based on the responses, boards are concerned about their

organizations' reputational loss and financial loss; those are the issues that boards of directors care about. Security professionals cite data loss and privacy regulations as some of the top concerns for them. Boards of directors say that their cyber risk was within the overall business risk appetite, and that number is lower for security professionals. That's where boards are a little more optimistic than the security professionals.

Boards continue to think about the reputational risk to their organization, and they don't necessarily think about the security repercussions. CISOs are more pessimistic in order to be able to get the resources they need from boards of directors to meet the changing threat environment. The survey shows different levels of cybersecurity knowledge within the organization – security professionals tend to be more pessimistic because they're dealing with cybersecurity on a day-to-day basis.

Who Is Responsible for Security Culture?

MORBIN: What did the responses to our survey tell you about who is responsible for security culture and routes to achieving or maturing that?

HOMOVICH: Business leaders and security leaders are pretty much in strong agreement, citing that the top source is their CISO, followed by the CIO and then security directors and managers. It's essential that security is incorporated into all business initiatives. To achieve that effectively, boards should promote more in-depth collaboration among the C-suite members, particularly with your CISO, CIO, CTO and CCO – the whole C-level suite – but also with your business leaders, to make sure you're incorporating better security into all products and services rather than thinking of security as an afterthought. The culture comes down from the top, but cybersecurity is everybody's responsibility.

Implications of AI

MORBIN: We had a question about the implications of AI. What stood out for you about those responses, and why?

"The survey shows different levels of cybersecurity knowledge within the organization – securityprofessionals tend to be more pessimistic because they're dealing with cybersecurity on a day-to-day basis."

HOMOVICH: The difference between business and security leaders stood out. Among the business leaders, 49% say that they are very confident and are keeping up to date on AI, and 33% of security leaders say they are. Thirty-nine percent of business leaders say that they have a basic understanding of AI, compared to 43% of security leaders. So, it would appear that business leaders know more about AI, but arguments could be made that security leaders are more focused on the security implications of AI. They are mitigating to those solutions, and that requires a deeper level of understanding. Boards may think that they understand AI – particularly from reading about it in the news – but security professionals think about the underlying security concepts that go with implementing AI solutions.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 36 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® · CU INFO SECURITY® (Just for Credit Unions) · GOV INFO SECURITY® · HEALTHCARE INFO SECURITY®

infoRisk TODAY · CAREERS INFO SECURITY® · Data Breach TODAY (Prevention. Response. Notification.) · CyberEd.io

CIO.inc · DeviceSecurity.io · PaymentSecurity.io · FraudToday.io

CYBER THEORY · CyberEdBoard · Xtra mile LIFECYCLE MARKETING · GREYHEAD

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io