Getting more out of your relationship

How boards and CISOs can secure a strategic partnership

IBM Institute for Business Value

How IBM can help

Cybercrime is an insidious threat that has reached crisis levels. Though hard to quantify with precision, estimates of its costs to the global economy range from USD 375 to 575 billion per year.[1] No geography or industry is immune. IBM's broad, integrated portfolio is helping organizations outthink threats with an integrated and intelligent security immune system, incorporating the very latest in cognitive, cloud and collaboration technologies.

To get the latest insights from IBM Security, please visit **ibm.com**/security/ciso.

Building a secure future – as partners

In today's hyper-connected world, a strategic relationship between Chief Information Security Officers (CISOs) and their boards of directors is critical. It enables organizations to better prevent, respond to and recover from incidents and helps mitigate cyber-risks. Board members and security leaders tend to approach security from their own vantage points. Building a strategic partnership, however, requires aligning their viewpoints to determine the best way to support the overall organization. Our research revealed a group of security leaders who have successfully built supportive, trusting and communicative partnerships with their boards, enabling a clear focus on the greater needs of the business.

In it together

Although not yet a fully mature business process, cybersecurity is and will continue to be a board room issue. As cybersecurity ingrains itself into the strategic agenda of boards of directors, challenges are emerging and successful practices are being codified. Today, CISOs and other security leaders are faced with increased personal responsibility. They not only have to manage their own teams and operations, they must also guide and advise their C-suite, as well as educate and collaborate with their boards of directors – who may have varying levels of experience and knowledge on the topic.

The relationship between boards of directors and security leaders is an important one that needs more care and attention. According to a recent *Harvard Business Review* study, among 23 board processes assessed, those related to cybersecurity were rated dead last in effectiveness by directors surveyed.[2] For this to improve, interactions between CISOs and their boards need to occur more frequently – and time spent together must be used more effectively. Some CISOs appreciate this need for more face time with directors. According to a study by the Enterprise Strategy Group (ESG) and Information Systems Security Association International (ISSA), 44 percent of information security professionals surveyed believe that CISO participation with executive management is not at the right level today and should increase in the future.[3] Work needs to be done on both sides of the equation.

65% of board members
suffer security fatigue

79% of board members agree they need to
improve support of their CISO

63% of CISOs indicate they
should improve collaboration
with their board

83% of more strategic security leaders say
close collaboration
with the C-suite and board can
help mitigate risk

In researching this important issue, we didn't stop at simply identifying the problem; we dug deeper to understand what is really happening between board members and security leaders worldwide:

- Are board members and security leaders on the same page?
- Are boards supportive of their security leaders and providing them enough time and resources?
- Are security leaders providing their boards enough education and expertise?
- Do security leaders have a mutually beneficial relationship with their boards – one that enables them to make well informed decisions?
- What are the benefits and barriers in the relationship?
- What kinds of frameworks, tools and communication methods are being used to manage cyber-risk?

Seeking answers to these questions, we surveyed over 300 board members and 300 security leaders in 28 countries representing 18 industries about their views and practices. In the process, we identified a group of security leaders whose approaches have enabled strategic partnerships with their boards and helped increase their value to the business.

Security through a different lens

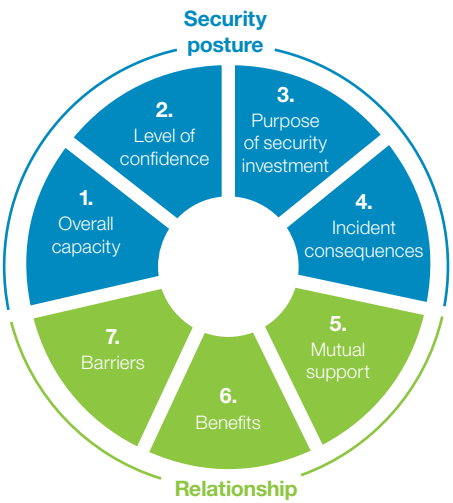
The good news is that boards are paying attention to and getting involved in security strategies. The clear majority (over 75 percent) of both directors and CISOs have seen the involvement of boards increase over the past two to three years, and they expect it will continue to increase in the next two to three years. With this growing involvement, it is essential to understand what is happening between the two functions. In our analysis, we found seven critical areas relating to the overall security posture of organizations and the relationship between boards and CISOs (see Figure 1). We discovered that, although the importance of cybersecurity is well recognized, boards and security leaders have a long way to go before they can build a true strategic partnership and reap its benefits.

We discovered that boards of directors are feeling the pressure from cyber-risks and an increasing responsibility to protect the organization, with many bordering on being overwhelmed. We also found that board members have significantly more confidence in their organizations' security capabilities than security leaders do. They are also generally more worried about the consequences of an incident.

On the other side, security leaders say they are providing enough support to their boards. And compared to the directors, more security leaders view investment in cybersecurity as more than just a cost of doing business. Both groups say there are opportunities to improve the relationship and better support one another. They also agree that a strong partnership can provide significant tactical and strategic benefits – though each group identifies relationship barriers from its own perspective (IT versus business issues).

Figure 1

Seven critical areas of partnership



Source: IBM Institute for Business Value analysis.

"With the external cybersecurity threat, we know and believe quite a lot, but we don't know everything. It's a continuous race. Do we really know what risks we are facing? We are sometimes surprised by the speed of things. How can we cope with that complexity and speed? We can give it all of our attention and focus."

Managing Board member for a global banking and financial services company

1. Overall capacity

Board members feel growing pressure related to cyber-risks and their increasing responsibility to help manage them. The majority of board members surveyed say they are experiencing "cyber-fatigue." Sixty-five percent agree they suffer from too many requests for resources, too many programs, and too much dedicated time and energy. However, only 49 percent of security leaders think their board members suffer from cyber-fatigue. Security leaders should be sensitive to this gap. And, on top of the fatigue, 60 percent of board members say that the cost of cybersecurity is "out of control" compared to only 43 percent of security leaders.

2. Level of confidence

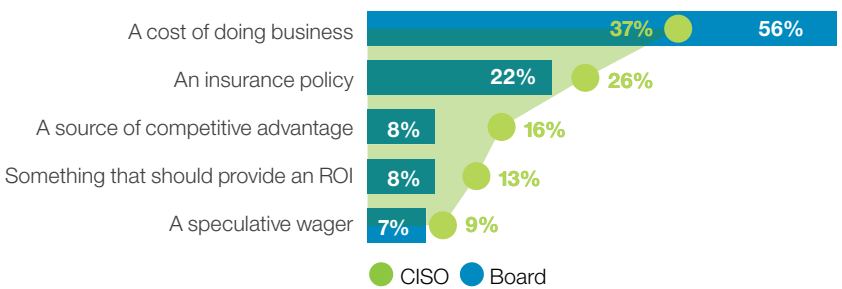
Board members are also much more confident today in their organizations' security capabilities than security leaders are. Forty-one percent of board members say their organization's overall cybersecurity preparedness is significantly better compared to others in their industry. Only 16 percent of CISOs feel the same way – a much more moderate view. This large gap exposes either a potential overconfidence by board members in their organizations' security capabilities, which is dangerous, or a lack of true understanding about their security capabilities. Either way, security leaders must address the issue.

3. Purpose of security investment

We asked both sets of respondents how they view cybersecurity investment – in other words, why they think their organizations are spending money on cybersecurity. We already know that boards see overall costs as an issue, so we wanted to see if security expenditures were viewed as simply a necessary business cost or an investment that could enable the overall business. When asked to select one answer that best describes how they view cybersecurity

investment, well over half of board members say they consider it simply a cost of doing business compared to 37 percent of security leaders (see Figure 2). Security leaders want to contribute more to the business where they can, with over a quarter viewing cybersecurity investments as a source of competitive advantage (16 percent) or something that should provide a return on investment (13 percent).

Figure 2
View of cybersecurity investment



Source: IBM Institute for Business Value analysis.

4. Incident consequences

Board members are generally more worried than security leaders about the consequences of a security incident – whether considering reputational damage, loss of competiveness or enterprise liability (see Figure 3). This increased concern is even more evident when looking at legal consequences, which would naturally be top of mind for board members.

Figure 3

Worried about consequences

Source: IBM Institute for Business Value analysis.

The biggest gaps between the two groups are around things like liability, lawsuits and government action. Security leaders seem to understand the impact of a security incident to reputation, investors and customers. However, they may not think about the legal consequences as much as they should if they want to be on the same page as their board members.

5. Mutual support

Both board members and security leaders say there is still work to do to improve their relationship, even though they agree security leaders are providing good support. It is important to realize that both groups aren't satisfied with their current relationship, and both recognize the need for change. Seventy-nine percent of board members agree they need to improve their level of support for their CISO, and 63 percent of CISOs agree they should improve their level of collaboration with their board. Both groups appear to want to take the relationship to the next level. A large majority of board members indicate they are getting enough access to cybersecurity expertise (71 percent) and being presented the right information by their security leadership (79 percent). However, they are looking for a deeper partnership.

6. Benefits

Both groups see significant tactical and strategic benefits from a strong relationship – with board members suggesting there is more benefit to be had overall (see Figure 4). The top benefit for both groups is tactical – a better ability to respond to incidents. At the end of the day, the whole organization should be prepared. When something bad happens, the entire organization – from top to bottom – needs to mobilize to address it. The more strategic benefit of reducing overall enterprise risk ranks high for both as well. The biggest discrepancy relating to benefits is around obtaining proper resources for initiatives and technology. Board members are almost twice as likely to rate that a significant benefit than security leaders.

"The board makes sure we have done the right things, that there is some oversight, that various committees have looked through our work, and that we are spending money wisely. In addition, they ask questions to make sure we are lined up with what other organizations of similar size and scope are doing."

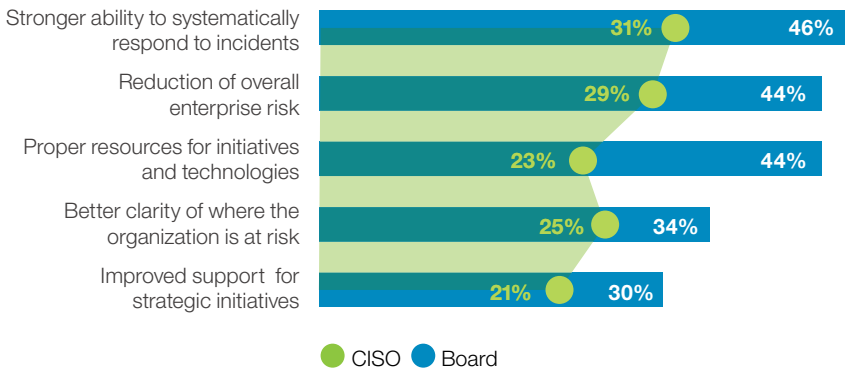
CISO for a leading Canadian financial protection, wealth and asset management firm

"One of the challenges we have is the nature of the relationship with the board itself; it is a 'quarterly relationship.' Trust takes time to build, and you need to develop personal relationships… at some level, meeting infrequently is a barrier to building a deeper, more meaningful relationship."

Security leader for a major global retailer

Figure 4

Benefits of a strong relationship



Source: IBM Institute for Business Value analysis.

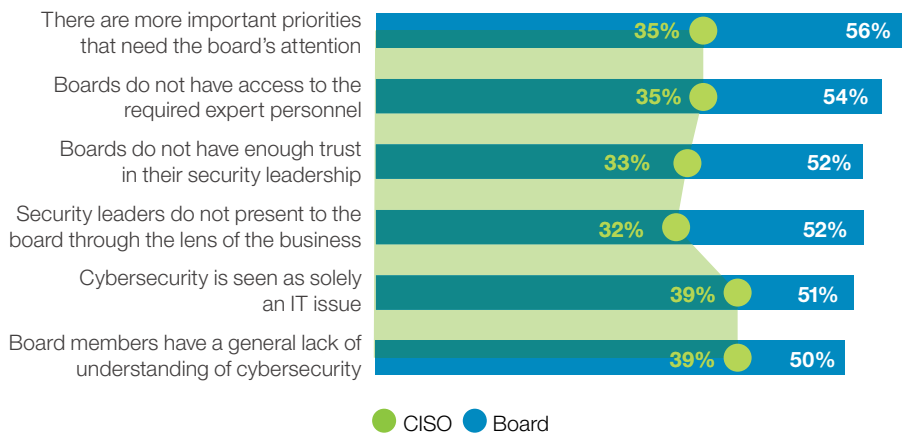
7. Barriers

Finally, we explored potential roadblocks to a good relationship between the two groups. Just like with benefits, board members react more strongly when identifying barriers to the relationship than security leaders (see Figure 5). No barriers are ranked significantly higher than the others, but the top barrier for board members is the fact that they have more important priorities than cybersecurity demanding their attention. The top barriers for security leaders are cybersecurity being seen solely as an IT issue and board members having a general lack of understanding of cybersecurity.

This is a bit of a conundrum for security leaders since they should be the ones providing the training and expertise to board members so they have a good enough grasp on the topic to have meaningful conversations. The most important point is both board members and security leaders need to recognize what might prevent each other from fully realizing the value of their partnership – and what steps they can take to correct the situation.

Figure 5

Barriers to a strong relationship



Source: IBM Institute for Business Value analysis.

"I am not sure the board really always understands the risks. When they ask questions, they say, 'What are your programs? Do you have enough money?' I tell them it is not a money problem; it is an awareness problem. I have to link awareness to programs, and then link to the money."

CISO at a global energy and automation company

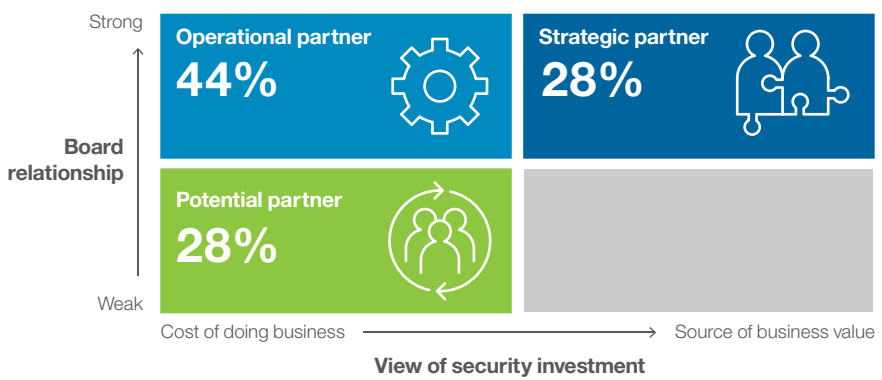
The road to partnership

In addition to determining the similarities and differences between security leaders and board members, we also identified a group of security leaders who exhibit a good relationship with their board – who have successfully strengthened the relationship. How do they partner for success? Do they employ different practices than the others? Do they believe or do something fundamentally different?

To answer these questions, we profiled the 300 security leaders based on their self-described board relationships, the details of those relationships (for example, providing enough expertise, understanding impacts of cyber-risk, etc.) and how they viewed the rationale for security investment. Analysis of their responses revealed three distinct archetypes (see Figure 6).

Figure 6

Partnership archetypes



Source: IBM Institute for Business Value analysis.

Potential partners, 28 percent of the sample, don't have a strong relationship with their board and indicate that security investment is just a cost of doing business, an insurance policy or, at worst, a speculative wager. They report their board relationships as less cooperative, less conversational and less trusting than the other two groups. They are also more unsure of the strength of their board relationship principles. Potentially, this could be because they don't have enough access to the board, their board is more skeptical or uncooperative, or they are simply frustrated by the current nature of the relationship.

Operational partners, the largest group at 44 percent, have strong confidence in their overall security capabilities and indicate they are doing better than their industry peers. They also rate their board relationship, in general, as more cooperative, conversational and trusting than the potential partners do. They have the fundamentals down and are cultivating a strong board relationship. Like the potential partners, they see security investment as a cost of doing business and approach their board relationship from that perspective.

Strategic partners, 28 percent of the sample, are very similar to the operational partners, except in one fundamental way. They see security investment as something greater than simply a cost of doing business. Many say it should provide a return on investment or serve as a source of competitive advantage. They not only want to protect and defend their organization, they aspire to go beyond and show that security can contribute to the business – by enhancing customer and client confidence, helping develop new products or solutions, or enabling a platform innovation. These security leaders want to show their boards the true value of security.

"The keys to a strong relationship with my board have been establishing a level of transparency, demonstrating return on investment and being a bit forward thinking."

CISO for a leading Canadian financial protection, wealth and asset management firm

"I think the board expects our financial officers to hold us accountable – to make sure we are spending money wisely and not just layering technology on top of technology. It is my job to connect the dots. I have to show them the data and prove that without what we do, we wouldn't be able to serve our customers in the right way."

CISO for a leading Canadian financial protection, wealth and asset management firm

Strategic partners know that the more the board is involved and the stronger the relationship is, the better they can manage risk together (see Figure 7). Almost all strategic partners report their board has gotten increasingly involved in the past two to three years (92 percent), compared to 80 percent of operational partners and only 63 percent of potential partners. A larger percentage also agree that collaborating with the board and C-suite is an effective way to help mitigate risks. More strategic partners also report having overcome the challenge of not presenting security issues through the lens of the business. Generally, strategic partners are better positioned to leverage the board relationship as part of the security strategy. So, how do they approach developing board agendas, risk reporting tools and breach responses?

Figure 7

Characteristics of strategic partners

Source: IBM Institute for Business Value analysis.

Board agenda

Nearly 90 percent of both operational and strategic partners regularly report to their boards. This compares to only 65 percent of potential partners. These potential partners aren't getting the access they need to build strong relationships like the other groups. What cybersecurity and cyber-risk-related information is presented in these regular meetings? Strategic partners report more on the organization's current risk profile, new and emerging threats, and necessary future improvement areas than operational or potential partners do. They present much more than simple updates on current performance and status; they provide their board members a view of the entire security landscape so they can better understand the issues.

Risk reporting tools

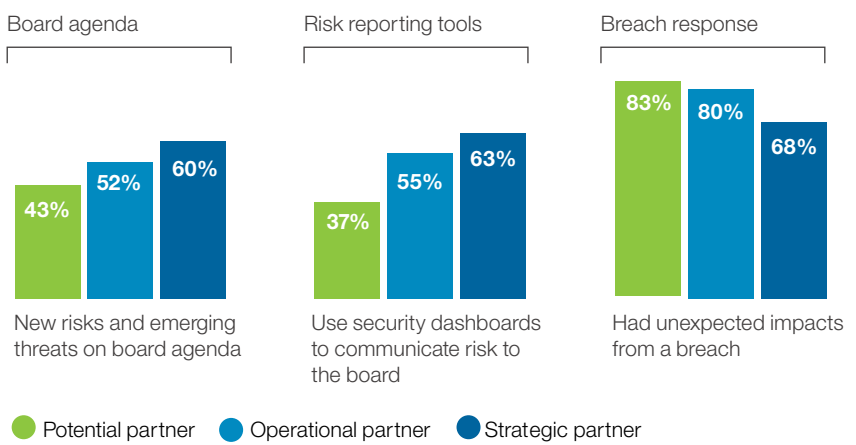
Strategic partners also use more advanced risk reporting tools more frequently – things like automated tools and dashboards. These enable a more detailed, continuous conversation. Sixty-three percent of strategic partners use security dashboards that provide real-time reporting and visualization versus only 37 percent of potential partners (see Figure 8). A larger percentage of strategic partners use automated business intelligence tools and reports from security products – 58 percent compared to only 38 percent of potential partners. The top communication tool used by potential partners is slide presentations (at 47 percent), something more suited to simple, one-way reporting. On the other hand, because strategic partners want to enable an active discussion with their board, they do more than just present; they also embrace tools that promote dialogue.

Breach response

Roughly a third of respondents in each group had a security breach in the past two years. The vast majority of those with a strong board relationship (over 80 percent) indicate that regular practice and simulation enhanced their response, their response plan worked as designed and worked well, and they had good internal communications. Potential partners didn't fare as well, with only 71 percent saying their response plan worked well and 58 percent saying they had good internal communications. Additionally, 83 percent of potential partners had unexpected consequences from a breach compared to only 68 percent of strategic partners (see Figure 8). This is significant since both board members and security leaders cite improved incident response as the top benefit of a good relationship.

Figure 8

Practices of strategic partners



Source: IBM Institute for Business Value analysis.

Recommendations

Although progress has been made, there is still work ahead for both security leaders and board members to build the sustained confidence and effective practices necessary to secure their organizations for the long term. A good way to start is by looking at the guidance provided by the National Association of Corporate Directors. The organization offers five recommendations for boards, which are supported by our research: Treat cybersecurity as an enterprise-wide issue, not just an IT one; understand the legal implications of cyber-risk; make enough time for the topic and have access to enough expertise; develop and maintain a well-supported enterprise-wide cyber-risk management framework; and plan to identify and address what risks to avoid, accept and mitigate.[4] Going beyond those five, we recommend the following for board members and security leaders seeking to improve their security relationship:

For board members

Board members should get smart and get active

- Participate in incident response and table-top exercises to understand your role in the process. Just like the C-suite, board members should be involved.
- Tour your security operations. Talk to the actual people involved in security in your business. Have them walk you through what they do on a day-to-day basis.
- Take the same security awareness training as employees. In addition to specialized training, board members should be subject to the same education requirements and testing (for example, understanding phishing techniques) as the rest of the business.

"What has contributed to our good relationship? We have solved a few big problems together. We built the trust and solved the problem. We have demonstrated skills and have a proven track record."

CISO at a global banking and financial services company

"We are now at a point where we are trying to shift the relationship with the board – to make it more strategic, more about risk. What are the risks? How are they manifesting? What are people doing about them? We want to provide a roadmap for the future."

Security leader for a major global retailer

Boards should understand that security leaders want more than just resources

- Realize security leaders want to be partners with the business. Work together to understand the cyber-risk you face – more technology and financial resources aren't always the solution, and security leaders understand that.
- Know that security doesn't have to be just a cost of doing business. It may be difficult to prove traditional ROI at times, but your security leaders can bring value to the business with better customer relationships and help evaluate risk for new business initiatives.

Boards should focus on transparency and accountability to forge a better partnership

- Require your security leaders to be open and transparent, even if there are issues. In turn, agree to give them the time and support they need to address those issues.
- Don't always treat a breach as a failure. It can be an opportunity to grow as an organization. A breach can provide a chance to reassess risks and review and improve your business strategy as well as your cybersecurity strategy.

For security leaders

Security leaders should provide easy access to insights on the total security environment

- Provide board members a view of the entire security landscape in the language of the business. Help the board understand how the company compares to industry competitors and the rest of the global market. Educate the board on emerging threats and cyber-risks, and detail what you are doing to address them. Give boards the information that is relevant in a way that is relevant.

- Give board members access to information outside of board meetings, without overwhelming them. Don't just present to the board; use tools like infographics, maturity models, frameworks and dashboards to enable an ongoing conversation about cyber-risk and how best to mitigate it.

Security leaders should think like board members

- Think beyond the technical. Don't address only what you are worried about; think about what you would want to know if you were a board member. Board members say they are overwhelmed and worried about a greater number of issues – help them overcome their fears through education, and engage them in program decisions to address cyber-risks.
- Build relationships with one or two savvy board members. Use them to test new ideas and to gain an understanding of areas of strategic importance for the entire board – try to break the "quarterly relationship." These board members can act as your delegates and translators.

Security leaders should be grounded and trustworthy to build the board's confidence

- Make cybersecurity a team sport by engaging the board in incident response simulations or table-top exercises to offer board members insight into your strategies. This provides an opportunity to demonstrate your organization's strengths and challenges, while helping to build stronger relationships with members.
- Take a proactive stance and pursue dedicated cyber-risk education sessions outside of normal board meetings. These can include security awareness exercises and relevant guidance, such as updates on changes to international privacy laws and potential impacts to business.

The path to partnership

For board members

Get smart and get active

Understand that security leaders want more than just resources

Focus on transparency and accountability to forge a better partnership

For security leaders

Provide easy access to insights on the total security environment

Think like board members

Be grounded and trustworthy to build the board's confidence

How will you get more out of your relationship?

- Do you understand what your board members or security leaders think about needs, challenges and priorities? Can you see things from each other's point of view?
- Do you have a common understanding of each other's view of cybersecurity and how it can enable the business to achieve its strategic objectives?
- Are you providing each other enough information regarding your concerns and the actions needed to address them?
- Are you making enough time available and using the right communication tools to enable a continuous dialogue?
- Are you taking time to educate one another on your processes and how you view risk?

About the authors

Diana Kelley is the Global Executive Security Advisor (ESA) for IBM Security. As ESA, Diana leverages her 25 years of IT security experience to provide advice and guidance to CISOs and security professionals worldwide. Diana can be reached on LinkedIn at linkedin.com/in/dianakelleysecuritycurve, via Twitter @dianakelley14 and at drkelley@us.ibm.com.

David Jarvis is the Security and CIO Lead at the IBM Institute for Business Value. He is responsible for developing and executing a research agenda that explores emerging business and technology topics for those areas. David can be reached on LinkedIn at linkedin.com/in/davidajarvis, via Twitter @dajarvis and at djarvis@us.ibm.com.

Contributors

Lisa van Deth, Campaign & Thought Leadership Strategy, IBM Security

Shamla Naidoo, Vice President, IT Risk & IBM CISO

Christophe Veltsos, Associate Professor, Department of Computer Information Science at Minnesota State University, Mankato

Demographics and methodology

To better understand the evolving relationship between CISOs and boards of directors, the IBM Institute for Business Value (IBV) and the Economist Intelligence Unit (EIU) surveyed a balanced distribution of 302 CISOs and other security professionals and 302 board members (CEOs and board members) in 28 countries, representing 18 industries, between February and April 2017.

To determine our security leader archetypes (potential, operational and strategic partners), we applied a k-means clustering algorithm that revealed three distinct behavior patterns. These behavior patterns were based on questions relating to overall board relations, principles of the relationship and security leaders' views of the purpose of security investment.

For more information

To learn more about this IBM Institute for Business Value study, please contact us at iibv@us.ibm.com. Follow @IBMIBV on Twitter, and for a full catalog of our research or to subscribe to our monthly newsletter, visit: ibm.com/iibv.

Access IBM Institute for Business Value executive reports on your mobile device by downloading the free "IBM IBV" apps for your phone or tablet from your app store.

To learn more about IBM Security, please visit ibm.com/security/ciso.

The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research and technology to give them a distinct advantage in today's rapidly changing environment.

IBM Institute for Business Value

The IBM Institute for Business Value, part of IBM Global Business Services, develops fact-based strategic insights for senior business executives around critical public and private sector issues.

Notes and sources

1 "Net Losses: Estimating the Global Cost of Cybercrime." Center for Strategic and International Studies and McAfee. June 2014. https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

2 Cheng, J. Yo-Jud, and Boris Groysberg. "Why Boards Aren't Dealing with Cyberthreats." *Harvard Business Review*. February 22, 2017. https://hbr.org/2017/02/why-boards-arent-dealing-with-cyberthreats

3 Oltsik, Jon. "The State of Cyber Security Professional Careers: An Annual Research Report (Part I)." Jon Oltsik. Enterprise Strategy Group (ESG) and Information Systems Security Association International (ISSA). October 2016. http://www.esg-global.com/hubfs/issa/ESG-ISSA-Research-Report-State-of-Cybersecurity-Professional-Careers-Oct-2016.pdf

4 "NACD Director's Handbook on Cyber-Risk Oversight 2017." National Association of Corporate Directors. 2017. https://www.nacdonline.org/cyber

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
July 2017

GBE03841USEN-00