Securing the C-suite

Cybersecurity perspectives from the boardroom and C-suite

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 the cost of cybercrime to the global economy may range from $375 billion USD to $575 billion per year.[1] No geography or industry is immune. Financial losses, reputational damage, national security concerns, to name a few, characterize some of the core risks the C-suite is taking serious notice of. Historically considered a technical issue within the domain of the IT department, security is now a central topic within operations, across the C-suite and elevated at the board level.

IBM's broad, integrated portfolio of security software and services addresses prevention, detection, response and remediation that can help organizations anticipate and take early action to mitigate the impacts of cybersecurity risks.

To learn more about how IBM works with organizations to secure their digital infrastructure, please visit

ibm.com/security

Why the C-suite should care about cybersecurity

Ninety-four percent of CxOs believe it is probable their companies will experience a significant cybersecurity incident in the next two years. And while 65 percent of C-suite executives are highly confident their cybersecurity plans are well established, only 17 percent are actually "cybersecured" – demonstrating the highest degree of preparation. The cybersecured have made significant progress to define and implement their cybersecurity strategies. As a result, these organizations have a more effective cybersecurity risk mitigation profile. At the C-suite level, cybersecured organizations stand out for being more engaged in threat management. They work cross-functionally on cybersecurity issues, are more likely to have appointed and empowered a Chief Information Security Officer (CISO) and they collaborate with external entities to share incident information.

Executive summary

Cybersecurity issues are no longer limited to the IT department; instead, they threaten every aspect of the organization and pose a significant threat to ongoing business continuity and reputation. These issues extend well beyond the technical environment and reach across the entire business ecosystem. Cybersecurity solutions must encompass not only technical fixes, but also changes in business processes, controls, management and employee behavior.

To get a deeper view into the specifics of the C-suite's concerns and perspectives on cybersecurity, IBM conducted a survey of more than 700 C-suite executives from 28 countries, across 18 industries. Participants spanned traditional C-suite roles, compliance officers and legal counsel. This report will provide insights into the executives' assessments of risks and challenges, as well as how these assessments align with actual threats.

Cybersecurity is important, but it's not always clear who the enemy is

Two-thirds of the C-suite views cybersecurity as a top concern that must be addressed. However, they are not clear about which elements of security present the greatest risk. Fifty-four percent of those surveyed acknowledge risks from organized crime groups. However, many tend to over-emphasize the risks from opportunistic "rogue" actors and discount the dangers from other sources, such as industry spies, national and foreign governments and personnel within the business ecosystem (employees, vendors, partners). Understanding the enemy helps optimize risk management and investment in security solutions.

Collaboration is essential to level the playing field

It's generally acknowledged in the security domain that collaborative sharing of incident information is a powerful weapon to combat the bad guys. In fact, the most successful cyber-criminals are known to collaborate by sharing information on the "dark web," the seedier side of the Internet in which those with ill intent can interact anonymously. The "good guys," however, are more reticent to collaborate. Over two-thirds of CEOs in our study said they are

65%

of C-suite executives are very confident their cybersecurity plans are well established, yet only 17 percent demonstrate the highest levels of preparedness and capability.

68%

of CEOs are reluctant to share security incidents externally, yet external collaboration is recognized as a powerful offensive capability against cyber-criminals.

60%

The CFO, CHRO and CMO feel the least engaged in cybersecurity threat management activities, yet are the stewards of data most coveted by cybercriminals.

reluctant to share their organizations' cybersecurity incident information externally. Equally concerning, internal, cross-functional collaboration is weak, particularly among the three specific C-suite roles –Chief Human Resources Officer (CHRO), Chief Marketing Officer (CMO) and Chief Financial Officer (CFO)– that have stewardship for the most coveted data sought by hackers (employee, customer and financial information, respectively). These three executives are also the least confident their organization's cybersecurity plans are well thought out and executed.

Organizations can benefit from the lessons of those who have prepared well

Cybersecured organizations have implemented a comprehensive cybersecurity program to detect breaches, prevent incidents and remediate risks. Most telling, these companies have established an Information Security Office, appointed a Chief Information Security Officer (CISO) and have implemented a cross-functional governance model that engages the organization from the boardroom, to management, to employees. They are also more open to collaboration and external sharing of incident intelligence.

C-suite considerations

Organizations ready to increase cybersecurity capabilities can look to emulate the cybersecure elite. First, clarify which actors present the greatest risks and assess the organizational commitment to risk aversion. Next, improve awareness and drive a more risk-aware culture across the entire organization. Institute regimens for cybersecurity governance, continuous monitoring, incident reporting and response preparation. Last, use collaboration both internally and externally to manage threats and secure the organization's most valuable digital assets. Enforce security standards across both the IT infrastructure and business processes.

The C-suite view of cybersecurity

It's important

IBM's 2015 Global C-suite study surveyed more than 5,600 C-suite executives across a broad range of strategic issues and emerging trends.[2] Sixty-eight percent of study participants cited IT security as their top concern with respect to technology likely to revolutionize their businesses over the next three-to-five years (see Figure 1). Heightened concern about the IT security risks of emerging technology is important; however, security vulnerabilities also exist within existing legacy infrastructure and integration points with vendors, customers and partners.

In this context, it's critical to understand what a solid cybersecurity plan should include. A significant majority of the executives in our study strongly agreed IT security consists of four critical components:

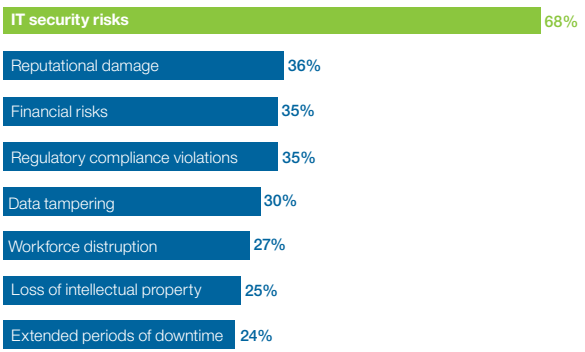
- Prevention (77 percent): a strategy, plan, training and technology to mitigate potential threats
- Detection (76 percent): real-time systems and processes to monitor and detect breaches, coupled with forensic analysis capabilities to perform root cause analysis
- Response (74 percent): forensic analysis, communications, who is in charge, pre-written statements, actions coming out of analysis
- Remediation (78 percent): plans in place to rapidly address and close gaps in security (technical, process, training, etc.)

… but will it happen to me?

Fifty-one percent of CxOs surveyed believe a one-in-four chance exists of a breach occurring that will have a material impact on their organizations. That's a significant acknowledgement of the risk and is consistent with a recent study that suggests "the likelihood of a data breach involving a minimum of 10,000 records is estimated at approximately 22 percent over a 24-month period."[3]

Figure 1

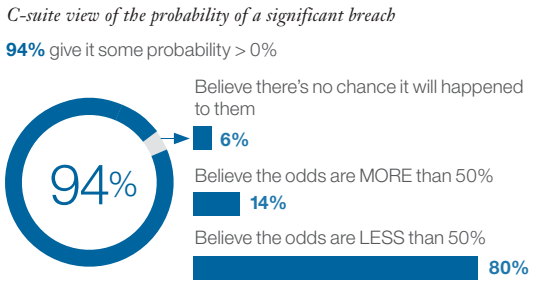
C-suite view of technology risks over the next 3-5 years.



Source: IBM Institute for Business Value.

Figure 2

C-suite view of the probability of a significant breach



Source: IBM Institute for Business Value.

The other 49 percent of CxOs vary widely in their opinion of the probability of a breach. Thirteen percent of CxOs have already experienced a significant breach or see it as inevitable (5 percent and 8 percent, respectively). Surprisingly, 6 percent reported they believe no possibility exists for a breach that would materially impact their organizations. (see Figure 2).

While the C-suite as a whole has mixed opinions of the likelihood of a breach, CISOs – those on the front lines of cybersecurity – are much more concerned. In fact, many CISOs report that they consider the threats so great they feel they are losing the fight. According to the 2014 IBM CISO Study:

- 83 percent of CISOs say the challenge posed by external threats has increased in the last three years (42 percent said dramatically)
- 59 percent strongly agree the sophistication of attackers is outstripping the sophistication of their organization's defenses
- 40 percent say that sophisticated external threats are their top challenge.[4]

Admittedly, it's as much art as science to evaluate the probability that a security breach will materially and adversely impact the organization, particularly in light of the variety of threat actors, their motivations, nuances by industry or geography, and specifics of existing security gaps at a particular organization. Perhaps most concerning is that months– or even years – may pass before an incident is discovered. By then, it's usually too late, as the damage has likely been done.

Where are the IT risks?

When asked about their views of specific risks in the IT infrastructure, 57 percent of the C-suite assigned the highest risks to employee mobile devices – those employees who bring and use their own mobile devices to work (BYOD) and 54 percent to social media/channel systems, (such as surfing the Internet and responding to emails at work (see Figure 3). Enterprise mobile, cloud and integration points within the business ecosystem (partner/vendor integration points) are also considered high risk. However, legacy infrastructure presents many security risks as well and should not be discounted. The number of mobile-device originated incidents is still fairly small by comparison to other legacy vulnerabilities, so C-suite concerns may be prematurely elevated.

Significant breaches over the past few years reveal some legacy infrastructure components have high risk potential, particularly if there is:

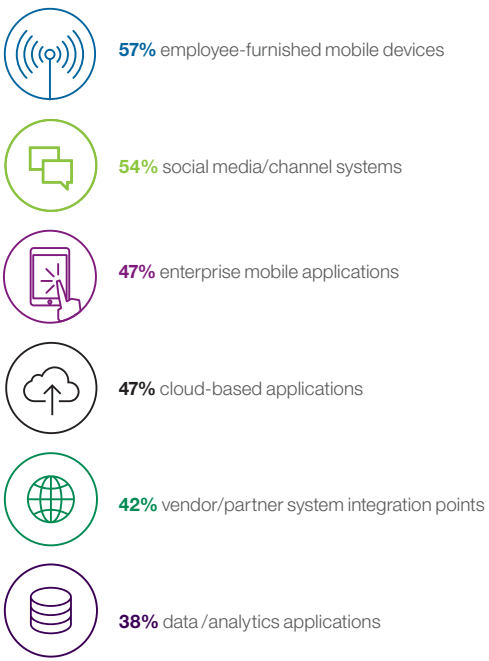
- A lack of awareness among employees and management
- A common vulnerability has not been addressed (for example, not staying current with software patches)
- Basic protections are not implemented or updated regularly, such as anti-virus programs and malware detection.

Who is the enemy?

Knowing the enemy requires understanding the different threat actors, how they operate and their sophistication levels, all of which can be used to assess degree of risk. Security experts understand the continuum of threat actors well, based on monitoring and analysis of incidents. A variety of actors with different motivations and objectives are constantly looking for vulnerabilities. These players range from the "inadvertent actor" with no malicious intent to the "advanced persistent threat" (ATP) –a sophisticated, well-funded and resourceful character that presents a much higher risk of significant impact.

Figure 3

C-suite view of riskiest IT infrastucture areas



Source: IBM Institute for Business Value.

We asked our study participants to indicate what actors they believe represent the top three threats of risk to their enterprise. Seventy percent of the C-suite selected rogue individuals as among the highest, with 38 percent selecting them as the most threatening actor. Organized crime groups were second and suggest the C-suite is aligned on the risk these actors represent. Protection of intellectual property is clearly a concern, with industry competitors viewed as the third most significant threat actor.

Executives' perception of risk may not align with the potential impact from each type of actor. Actors have different threat profiles based on their intent, level of sophistication and the proportion of incidents attributed to them. Some external rogue individuals have a relatively low threat profile due to lower sophistication, limited funding and using mostly known vulnerabilities that are easier to secure. Focusing too much effort on that group may not yield a comparable risk reduction for the investment made, compared to addressing more sophisticated actors, such as national governments, industrial spies and organized crime groups. Greater risks may exist from malicious insiders and other external agents (employees, vendors, partners).

The IBM 2015 Cybersecurity Intelligence Index report provided sobering numbers from an analysis of incidents: 31.5 percent of data breaches are attributable to malicious insiders and 23.5 percent are due to insider errors or non-adherence to processes and policies that lead to inadvertent data breaches or disclosures.[5] Only 32 percent of CxOs in this study selected current/former employees and 8 percent current/former vendors as among the top three threats. Analysis of incident data can provide insightful profiles of actors, and this improved awareness can help executives make more informed decisions about where to focus their security strategies.

Governance and collaboration

An effective tactic to combat cybercrime is transparency and collaboration, sharing incident information internally and externally. Forensic analysis of breaches reveals intrusion methods, practices and origins. Sharing this information cross functionally within the organization and externally helps to build a collective knowledgebase of actors and their methods, which, in turn, informs solutions.

Executives should engage and collaborate on cybersecurity internally, and organizations should engage other members within their business ecosystem when necessary, such as vendors, partners and industry competitors. The most successful cybercriminals are known to collaborate by sharing information on the vulnerabilities they have uncovered on the dark web. Failure to collaborate puts an organization at a disadvantage against cyber-criminals who, as a practice, collaborate and share information about vulnerabilities they uncover.

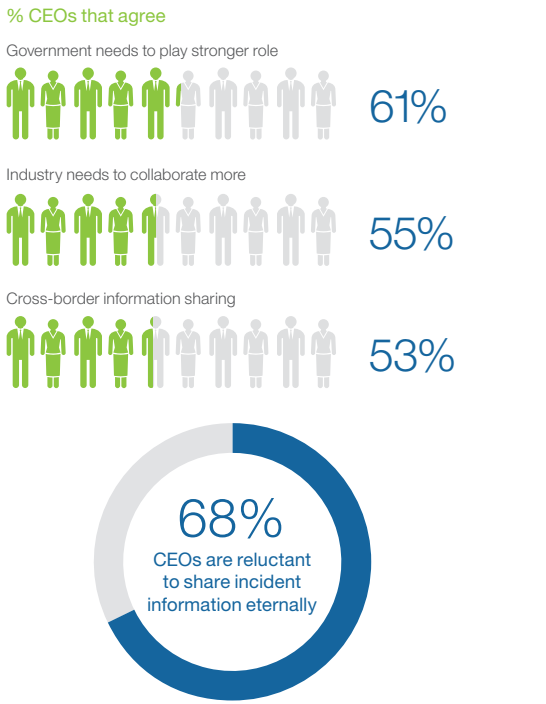
The CEO dichotomy

CEOs appear conflicted about sharing incident information externally. While the decision to do so can be uncomfortable, with the right controls, sharing incident information can level the playing field.

When presented with a series of statements about an external party's role in combating cyber-crime, 61 percent of CEOs agreed that governments need to play a stronger role, 55 percent said more industry collaboration is necessary and 53 percent indicated cross-border information-sharing is necessary (see Figure 4).

Figure 4

CEOs importance placed on external support versus willingness to collaborate externally



Source: IBM Institute for Business Value.

Yet, when we asked CEOs to what extent they were willing to disclose cybersecurity incidents to a variety of stakeholders (both internal and external), 68 percent of CEOs expressed an aversion to share incident information externally. However, greater external collaboration among organizations can speed the development of collective knowledge and insights on threat actors and their strategies. Leadership needs to address the aversion to responsible sharing with appropriately vetted external parties, creating the opportunity to leverage analytics and apply increasingly sophisticated cognitive capabilities to strengthen and automate security solutions and help to mitigate risks.

The confidence paradox

Sixty-five percent of C-suite respondents say they are confident that their organization's cybersecurity plans are well established. However, this view is not consistently shared across all C-suite roles. Seventy-seven percent of Chief Risk Officers (CROs) and 76 percent of Chief Information Officers (CIOs) report their organization's cybersecurity plans are well established. But, among CEO's, only slightly more than half agree. The Chief Marketing, Finance and Human Resources Officers join the CEO in the bottom half of this "confidence index" relative to peers (see Figure 5). This is significant because these three executives are ultimately the stewards of customer, financial and employee data – information highly coveted by cyber-criminals.

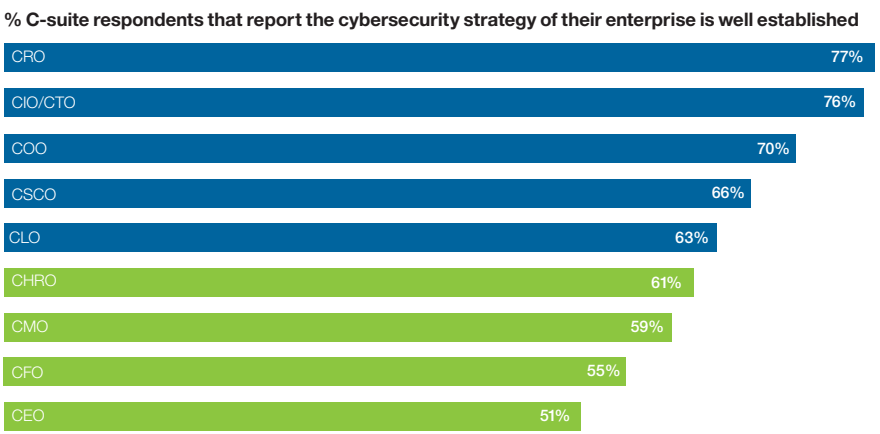
CIOs and CROs may have a higher degree of confidence because of their specific roles. Since, historically, cybersecurity has been largely an IT responsibility, CIOs may believe that they have addressed the technical aspects and implemented solid defenses across the corporate network, within applications and for access remotely via laptops and mobile devices. Assuming that is sufficient without engaging the business has the potential to miss areas in business process, information management and third-party solutions. Cloud exemplifies this concern and may account for the C-suite's differing views on the security risks. Business discretion to

leverage third-party cloud offerings, without engaging IT/security– or considering the provider's cyber-risk posture – adds risk.

Similarly, the CRO, with responsibility for assessing and planning around enterprise risk, may have incorporated cybersecurity risks into the enterprise risk management (ERM) framework. However, that does not necessarily translate into actual "fortification" against the risks. ERM is geared toward after-the-fact risk event response plans. Plans should be examined for specific tactical steps that can be taken to mitigate risk by enhancing security. The CRO may feel confident the plan and actions are formulated, but C-suite peers across the business need to actually address the specific risks.

Figure 5

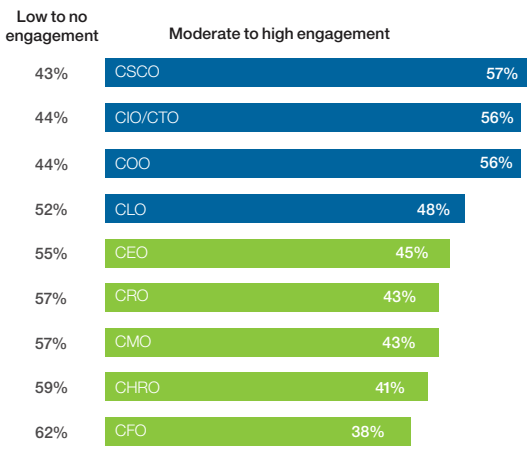
Strength of cybersecurity plans by role



Source: IBM Institute for Business Value.

Figure 6

Degree of C-suite engagement in cybersecurity threat management activities by role



Source: IBM Institute for Business Value.

C-suite collaboration – From IT to the business

Alignment across the C-suite, particularly between IT and the line-of-business owners, is increasingly important to building a mature security posture. We examined responses to specific survey questions to ascertain the degree to which alignment exists between roles.

Compared to the CEO, Finance, Marketing and Human Resources executives, the CIO is nearly twice as confident that cybersecurity plans encompass a cross-C-suite approach and collaboration.

The CIOs confidence may be due to progress made from an IT perspective in understanding and taking steps to secure what IT considers to be the highest risk areas. However, the CIO's focus of concern is more on IT legacy systems, such as the network, operations systems and financial systems, and less on Marketing, Human Resources and vendor/partner ecosystem.

While CIOs expressed confidence, 69 percent of C-suite participants indicated that cybersecurity plans fail to adequately incorporate cross-C-suite collaboration. At the role specific level, almost three-fourths of CEOs, CHROs, CMOs and CFOs indicate they do not believe the cybersecurity plans include them in a cross-functional approach.

In a related question focused on tactical execution of cybersecurity plans, we asked to what degree functional executives participate in security threat management activities in C-suite meetings (see Figure 6). Almost 60 percent indicated they did not feel included in the topic or participate during C-suite meetings. By role, 57 percent of CMOs, 59 percent of CHROs and 62 percent of CFOs indicate they are not involved in those topics and discussions within the C-suite.

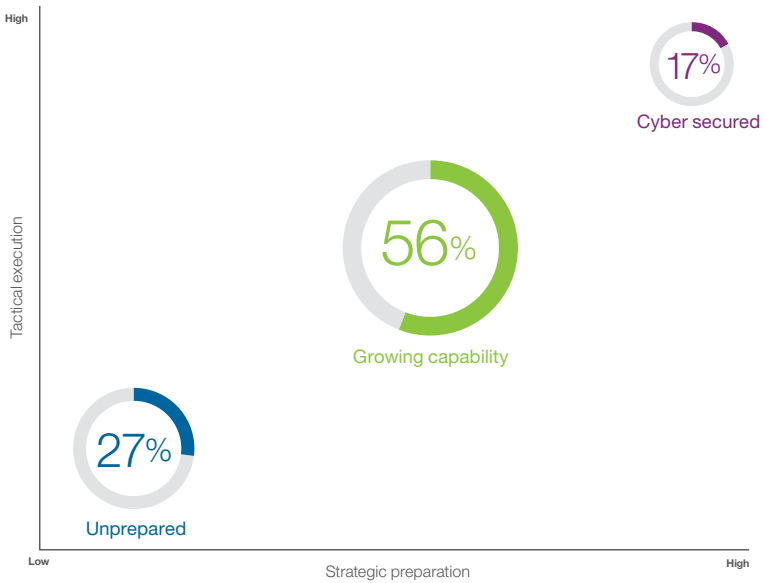
Considering C-suite level interaction is the primary forum within which the surveyed executives indicated they collaborated with peers on cybersecurity, the low level of engagement by these three key executives is concerning.

Being cybersecured

We analyzed responses to questions designed to indicate strategic and tactical cybersecurity preparation. From that analysis three profiles emerged. One group that we call "cybersecured" provide some insights into what the most capable organizations have done to implement a security strategy and tactically execute on that plan to mitigate cyber risk. They represent 17 percent of study participants and have significant differentiators (see Figure 7).

Figure 7

Cybersecurity C-suite capability model



Source: IBM Institute for Business Value.

Cybersecurity capability model

One group of respondents emerged as most capable and prepared on cyberSecurity at the C-suite level. We call this group the cybersecured. They have the most sanguine views of the risks, the need for cross-functional governance, and they incorporate these risks in the organization ERM plans more than any others. Most important, among this group, the C-suite engages in a more balanced and collaborative fashion.

The analysis was done on several questions in the survey instrument designed to capture the completeness of cybersecurity plan and the degree of tactical execution on that plan. Each question asked the respondent to rate their organization, on a scale of 1 to 5, with 1 being "not effective at all" and 5 being "extremely effective," on each of these elements.

The strategic dimension of the capability model requires progression along three areas of focus:

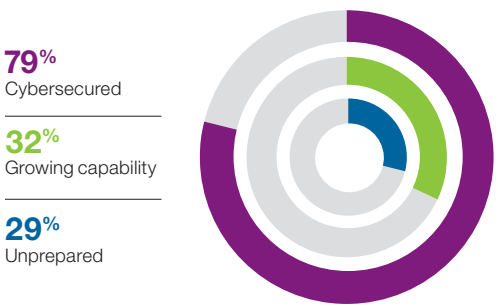
1. Establishing a governance model for security, including enterprise-wide collaboration
2. Identifying and protecting critical data and applications and
3. Developing and implementing an effective response plan.

The tactical dimension of the maturity model considers the degree to which respondents indicated the level of effectiveness on each of four elements of the cybersecurity plan.

Figure 8

Prevalence of CISO role by capability group

Have established an office of information security and appointed a Chief Information Security Officer (CISO)



Source: IBM Institute for Business Value.

The cybersecured team usually picks the CISO for captain

An important factor leading to greater capabilities in cybersecurity is directly correlated to having established an office of information security and an appointed CISO. Cybersecured organizations are 2.5 times more likely to have done this (see Figure 8).

Among cybersecured, the C-suite collaborates as a team

Executives in cybersecured organizations understand the value of a holistic and cross-functional approach to cybersecurity. Recognizing the importance of engaging the business side, they are five times more likely to have incorporated cross-C-suite collaboration into their cybersecurity plans compared to unprepared organizations. For the cybersecured, C-suite collaboration is far more likely to be built into cybersecurity governance (see Figure 9). They are also governing cybersecurity better than other groups, with 61 percent indicating cybersecurity is a regular topic in C-suite meetings, compared to just 31 percent for others. Most important, we find the level of engagement, by role, to be much higher on average, especially with the Chief Marketing, Human Resources and Finance Officers.

At the board level, cybersecurity is almost two times more likely to be a regular agenda topic for the cybersecured (56 percent) than for other organizations (27 percent). Board members do not have to become experts on cybersecurity; however, they should be informing themselves regarding cybersecurity risks to the degree necessary to:

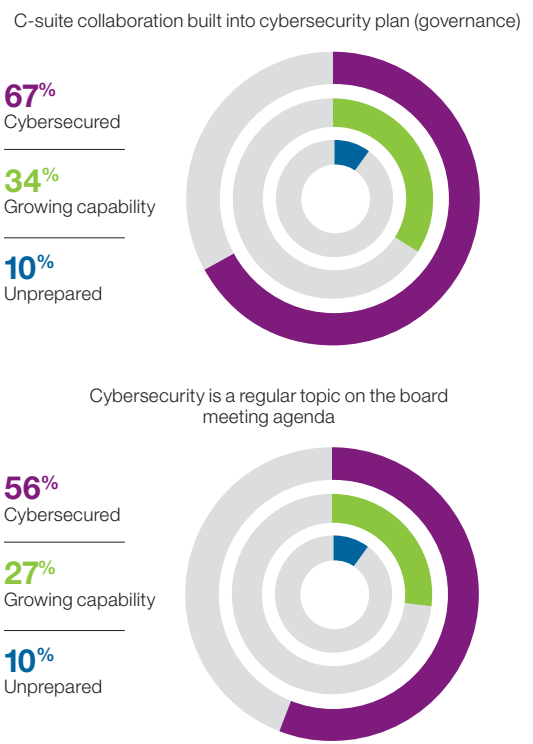
- Request that management describe and update the board on the appropriate controls in place
- Monitor controls periodically to make sure they are functioning as intended
- Request reporting on significant incidents quickly.

Cybersecured organizations collaborate more with external parties

Considering that successful cyber-criminals are known to collaborate among themselves, it stands to reason collaboration on security management and incidents among organizations would contribute to risk reduction. Among cyber-criminals, that collaboration takes the form of one actor discovering a weakness and making the knowledge available for sale for others to exploit. CEOs of cybersecured organizations are much more likely to share incident data with external parties. They are three times more likely than others to collaborate with industry competitors and twice as likely to collaborate with third-party security services firms and vendors/partners. To level the playing field, executives should consider the value of external collaboration as a powerful offensive tactic. Incident data about actors, origins and strategies is growing rapidly. The more organizations collaborate to gain knowledge of cyber-criminals and their activities, the better prepared they can be to put mitigating solutions in place.

Figure 9

Prevalence of collaboration and board transparency by capability group



Human Resources' integral cybersecurity role

Only 57 percent of CHROs reported they have rolled out cybersecurity training for employees. As the stewards of sensitive employee personal information, which is highly coveted by hackers, CHROs should be at the forefront of their organizations' cybersecurity efforts. Some of these include:

Protecting sensitive employee personal information
HR needs to own the governance of protecting employee sensitive personal information and the business processes of using and maintaining that data, across the hire-to-separation lifecycle.

Cybersecurity training and enforcement
The proliferation of personal mobile devices with access to corporate systems is increasing in prevalence and creating new vulnerabilities. Human Resources can help establish clear security policies and disciplinary actions for employees that are enforced, up to and including termination.

Hire to separation practices
HR can assist stakeholders to establish clear job roles and career paths, then help with the search and screening process, including candidate screening for security risks to defend against inadvertently hiring what might become an "insider" threat. HR should help to evaluate roles for their sensitivity and apply additional scrutiny as needed when hiring into those positions.

Recommendations: Securing the C-suite in 2016 and beyond

Understand the risks

- Evaluate your industry, geography and business ecosystem/partners for risk
- Conduct a security risk assessment or update any assessment that is over a year old
- Ascertain which areas present opportunities for threat actors and invest to defend accordingly
- Incorporate the security assessment into the enterprise risk plan as appropriate
- Develop education and training for employees, make it mandatory, update it regularly and enforce compliance rigorously.

Collaborate, educate and empower

- Establish a security governance model and program to encourage enterprise-wide collaboration
- Empower the CISO with the mission of managing information security risk across the enterprise, as well as lead the initiative among the C-suite
- Elevate and regularly discuss cybersecurity at C-suite and board meeting agendas and engage Risk, Finance, Marketing, Human Resources and Supply Chain at a minimum
- Craft foundational materials for executive level education
- Include the C-suite in developing an incident response plan and share it with the board for input.

Manage risk with vigilance and speed

- Implement continuous security monitoring software and build or leverage third-party security services to conduct incident forensics
- Share incident data with appropriately vetted external parties, such as competitors, vendors/partners and security experts, and leverage analysis of threat events to continuously secure the environment
- Identify your organization's digital assets (i.e., data, applications, systems and infrastructure) and develop a mitigation plan for each, based on risk level and appetite
- Develop and enforce cybersecurity policies, including workplace behaviors for employees, contractors and vendors, including mobile-device management, particularly employee mobile devices (BYOD)
- Make cybersecurity an intrinsic part of business processes and decisions.

What is the CISO's role?

Having a CISO or the equivalent function in the organization has become a standard in business, government and non-profit sectors. The CISO role has become vital to the operation of large organizations because security has become too important to be a task for a CIO.

The number of organizations that have a CISO has grown steadily since 2006, at a rate of about 10 percent per year. In 2006, 22 percent of organizations reported having a CISO, and by 2011 that was up to 8 percent.[6] On average across all participants in this study, 71 percent report their organization has a CISO. Among the cybersecured, (see sidebar, Cybersecurity capability model, page 11) almost 80 percent have a CISO, and the CISO has an average tenure with the organization that's almost two years longer.

At the board level, CISOs are expected to give visibility to and quantify the risks to the organization. At the C-suite level, the CISO is tasked with formulating and executing a comprehensive cybersecurity framework to mitigate risk.

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.

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.

About the authors

Diana Kelley is the Executive Security Advisor (ESA) at IBM Security and the manager of the IBM Security Newsroom. As ESA she leverages her 25-plus years of IT security experience to provide advice and guidance to CISOs and security professionals. She has contributed to the IBM X-Force report and frequently publishes thought leadership pieces on the Security Intelligence blog. She is a current faculty member with IANS Research and serves on the Advisory Board for InfoSec World and the Content Committee for the Executive Women's Forum. Diana is a frequent speaker at security conference and has been quoted as a security expert in The New York Times, TIME, MSNBC.com, Information Security Magazine and The Wall Street Journal. She co-authored the book Cryptographic Libraries for Developers. Diana can be contacted at drkelley@us.ibm.com.

Carl Nordman is the Research Lead for Cybersecurity and Finance Transformation in the IBM Institute for Business Value. He is responsible for conducting primary research in both domains. He leads studies to uncover current trends and perspectives on current strategic issues. Carl has over 25 years of experience in Finance Risk and Fraud. Previously he has held positions in IBM's Consulting Services practice, delivering engagements for CFOs at Fortune 1000 companies, and running Finance and Accounting BPO services as an Account Executive for several clients. Carl can be contacted at carl.nordman@us.ibm.com

Contributors

John Lainhart, Partner, GBS Public Sector, Service Area Leader, Cybersecurity& Privacy;
Gretchen Marx, Program Director, IBM Security Portfolio Strategy, IBM Security;
Lisa van Deth, Program Marketing Manager, Campaign & Thought Leadership Strategy, IBM Security.

Acknowledgments

Peter Allor, Senior Security Strategist, IBM Security; Michelle Alvarez, Threat Researcher, Publisher and Editor - Managed Security Services; Chuck Carney, Vice President Security Services, IBM Security; David Jarvis, Manager, IBM Center for Applied Insights, Market Insights; Bob Kalka, Vice President Strategic Accounts and Enablement, IBM Security; Charles Kolodgy, IBM Security Strategist, IBM Security; Jason Kravitz, IBM Techline Specialist for Internet Security Systems and Services; Christopher Poulin, Research Strategist - X-Force, IBM Security; Michaela Santa Barbara, Program Director, Security Consulting & Systems Integration.

Notes and sources

1 "Net Losses: Estimating the Global Cost of Cybercrime," June 2014.Center for Strategic and International Studies. http://www.cyberriskinsuranceforum.com/sites/default/files/pictures/rp-economic-impact-cybercrime2.pdf

2 "Redefining Boundaries: Insights from the Global C-suite Study." IBM Institute for Business Value. November 2015. http://www-935.ibm.com/services/c-suite/study/study/

3 2015 Cost of Data Breach Study: Global Analysis. Benchmark research sponsored by IBM, independently conducted by Ponemon Institute LLC, May 2015.Page 20, figure 15. http://www-01.ibm.com/common/ssi/cgi-bin/sialias?subtype=WH&infotype=SA&htmlfid=SEW03053WWEN&attachment=SEW03053WWEN.PDF

4 "Fortifying for the future: Insights from the 2014 IBM Chief Information Security Officer Assessment." IBM. December 2014. www.ibm.com/ibmcai/ciso

5 IBM 2015 Cyber Security Intelligence Index - https://securityintelligence.com/economic-espionage-the-global-workforce-and-the-insider-threat/

6 PricewaterhouseCoopers' annual information security survey, 2011, 2006

IBM Global Business Services
Route 100
Somers, NY 10589

Produced in the United States of America
February 2016