SecurityScorecard

CISO ACTION PLAN

Align with your Board to Strengthen Security

Introduction

A challenge exists in modern organizations: to improve the quality and effectiveness of formal and informal communications between the Chief Information Security Officer (CISO) and other senior executives, including the C-suite and board members. This publication presents action plans to help CISOs and senior executives find common ground.

Understanding the Challenge

We've all witnessed the struggles that technology experts often have when trying to communicate with less technical colleagues. The image comes to mind of the IT help desk expert attempting in vain to explain to a confused employee how a task might be accomplished. The reverse is also common, where an employee tries to make a request from technical staff, but struggles to explain what they are actually trying to accomplish.

A similar communication challenge exists between senior executive staff and enterprise security leadership teams. Generally, business executives and CISOs have different backgrounds, and as a result, often speak in much different languages. The result is that communication between CISOs and senior executives is often lacking–hence, the need for this discussion.

On the following pages we offer some practical tips for both groups in the form of recommended action plans. The presumption is that the communication gap is not the fault of either group, but rather stems from the differences in how each type of executive developed their skills. By focusing on proposed action plans for both CISOs and senior executives, an organization nurtures the possibility that this information-sharing gap might be minimized, and this will reduce risk.

Action Plan for CISOs

The action plan recommended for CISOs is focused primarily on curating their communication skills, but perhaps not in the manner one might expect. Most advice for CISOs to date has been to simplify their explanations of cybersecurity, presumably because senior executives are ill-equipped to understand complex technical issues. While aspects of this view might be true, our advice to CISOs actually follows a somewhat different path.

Instead of “dumbing down” complex technical and compliance issues related to cybersecurity for senior executives, CISOs are encouraged to improve the quality of their presentations. Discussions held with senior executives should be clear and correct, but they do not require hand holding as if they are Luddites. Instead, communications should be improved and sharpened. Senior executives are intelligent, and they can keep up.

Most senior executives recognize the risk an immature cybersecurity program poses to their company. Recognizing and quantifying, however, are two different things. For example, a decade ago, building a robust security infrastructure and program involved creating a fortress around on-premises data centers. CISOs felt more in control because data was contained within their own environments. The rise of digital transformation and cloud-based resources changed the CISO’s security model. Today, an organization’s security posture relies on their technology partners’ security postures.

The specific action plan recommended for CISOs to improve their communications with senior executives includes three points, each of which can be initiated immediately. All three can be curated by the CISO, with emphasis on continual improvement.

ACTION

#1

Never underplay the real challenges of cybersecurity to executives.

More than ever before, technology drives collaborative business processes. The rise of turnkey cloud technologies creates a hyperconnected ecosystem, shifting the IT model from data fortress to data ecosystem. Additionally, to enable their workforces, companies give various levels of access to a number of clients, suppliers, and consultants.

Every new access point—whether human or technology—increases the challenges that CISOs face, and they need to give their senior leadership team a realistic picture of these new risks. They also need to find metrics and key performance indicators that make sense in this new hyper-connected ecosystem. Explaining these challenges can be difficult, but it is not impossible.

Each connected location is a domino in the middle of that IT infrastructure. If one domino falls, the ones around it become less stable and can topple. The hyper-connected ecosystem works the same way, which is why security ratings provide valuable insight for senior leadership teams and boards of directors. Organizations can use security ratings to track their safest and riskiest business partners as a way to gain insight into the stability of each partner "domino" throughout the supply chain.

As a member of the C-suite, a CISO must bring business acumen along with security expertise to bridge the divide between security functions and the C-suite. CISOs can accomplish this by providing their leadership and directors with visibility into ecosystem complexity using business language, such as risk and financials, to get everyone on the same page. Giving the team an understanding of risk in a way that aligns with their objectives is a way to move toward a more robust cybersecurity posture.

ACTION #2

Ensure that cybersecurity reports provide the right information for the audience.

CISOs, senior executives, and directors all understand the importance of cybersecurity. CISOs need to remove technical jargon from their reporting and provide security reports that offer value. Security reporting should be simple, objective, and actionable. A simple board report is one that provides easy-to-understand prescriptive and measurable remediation activities. For example, a CISO might want to create metrics that align with a cybersecurity framework, such as NIST, and use the high-level categories of Identify, Protect, Detect, Respond, and Recover. The report does not need to get into the technical details but provide data that enables informed decision making. The focus should be on understanding current maturity as compared to target maturity, using technical details as illustrative examples.

Reports must provide objective, independently verifiable analyses. Even in its most simple form, a board report needs to align security maturity with technical weaknesses. An audience-aware report uses the metrics as the supporting documentation for the business-level highlight. If leadership or directors want to drill down into how the CISO determined the maturity level, the evidence should enable independent analysis.

The most difficult part of creating a business-audience report is making it extensible across the complex, hyper-connected ecosystem. Gaining visibility into third- and fourth-party risks is the primary challenge organizations and CISOs face in a digitally transformed world. Security ratings provide the visibility that organizations need by going beyond traditional point-in-time reports. With continuous monitoring that takes an outside-in approach, security ratings offer at-a-glance visibility into a given vendor's or vendor ecosystem's risk.

When CISOs take an audience-centric approach to discussing security risk, they build stronger internal stakeholder relationships and enable better security outcomes.

ACTION

#3

Become a true business partner to drive value.

In order to become a true business partner, the job of the CISO is not to say no but to help their peers come up with secure solutions to business problems. The CISO who approaches their relationships from a value-generation perspective for their company's customers will succeed.

For example, when SecurityScorecard Co-Founder and CEO Aleksandr Yampolskiy was CISO at Gilt Groupe, he was concerned with not only securing the company's digital assets, but also with delivering value to the customers shopping on its public site. Alex and his team integrated a service which would notify users if their passwords and accounts were compromised so they could change their passwords immediately. Alex and team further drove value for the company by putting a secure NortonLifeLock badge on the checkout site, which improved its purchase conversion rate. At every turn, Alex's aim as a CISO was to not only be a support function, but to help the business from a profits and loss perspective.

As a Team Lead for Security Engineering at Goldman Sachs, he took a similar approach. When the opportunity arose to launch a Chinese internet trading service, he generated millions in new revenue by applying security expertise.

Cybersecurity is now a business-critical initiative, and it's up to boards and members of the C-suite to work together to drive value for their organizations.

Action Plan for Senior Executives

Just as CISOs must be attentive to their communication approach with the senior executives in the organization, the reverse obligation is also true. This prompts the recommended action plan listed on the following pages for C-suite executives and board members. The objective is to improve the quality of all formal and informal discussions, information sharing sessions, feedback processes, and other forms of interaction with the enterprise security team—which includes the CISO.

Just as with our advice for CISOs, the specific action plan recommended for executives includes three points–each of which can also be initiated immediately. Unlike CISOs, however, who come to the communication with the expectation that they will need to make adjustments, it might be more difficult for experienced executives to adjust their approach. If this becomes too big of a hurdle, some introspection is recommended.

ACTION

#1

Take the time to self educate on cybersecurity using all available resources.

Just as CISOs must meet executive leadership where they are in their cybersecurity journey, leadership has a responsibility to gain a better understanding of technology. At a high level, leadership needs to understand the basic elements of digital transformation so they can make informed decisions around choosing technologies.

For example, this might mean understanding, on a basic level, that a device is an access point that malicious actors can exploit. It also means understanding why—not necessarily how—applying security patch updates to software and firmware mitigates risk.

Just as senior executives and directors have learned to extract the important findings in financial reports, they need to be able to extract fundamental data from security reports.

ACTION

#2

Embrace cyber resilience.

While it might be tempting to require that a CISO promise complete security, the hyper-connected ecosystems necessary for maintaining modern business operations make that an impossible dream. Just as CISOs need to set up their senior leadership and boards for success, the same must be done in return.

CISOs need a leadership team that understands data breaches are inevitable. Rather than looking to drive risk to zero, senior leadership teams should make sure that CISOs focus on cyber resilience. This means giving them the tools necessary for improving detection and recovery times. Senior executives and directors should ensure they fund initiatives that reduce recovery time, enhance communications, and provide clarity over proper recovery steps.

ACTION

#3

Encourage CISOs to share complexity if such detail is relevant.

Modern CISOs need to be business-aware, but their value to the company is their technical knowledge. As much as they need to step away from technical jargon, they still need to meaningfully explain technical issues.

Technical issues have a large impact on the choices companies make. For example, most organizations use cloud-based applications. Each connection point, or API, is a potential risk. If a CISO suggests that the company not deploy an application, the senior leadership team needs to ask why.

Senior executives and directors must question their CISOs purposefully, and they can do that by understanding the reasoning behind their suggestions. Senior executives need to work with their CISOs to understand risk, not to simply defer on all technology decisions.

Finding Common Ground

The ultimate goal for improving communications between CISOs and senior executives is to reduce enterprise cyber risk–and this should be the primary focus. To properly identify, assess, measure, and optimize decisions regarding cybersecurity threats, the CISO and executive team must be on the same page. Several other benefits, however, do result from this improved communication, including the following:

Expanded employee career options

When the CISO communicates more effectively with the senior executive team, the result can be a more intimate alliance between the security team and rest of the company. This has the effect of opening and expanding career options for security team members in other parts of the organization —and the reverse is also true.

Improved diversity in decision making

Improved communication between the CISO and senior executive team improves the diversity in decision making for the organization. Security-related matters have often been left out of major decisions, such as mergers with insecure companies and outsourcing to insecure suppliers. These problems can be avoided by improving diversity of input.

Accelerated enablement of digital transformation

The ultimate goal of digital transformation requires avoidance of bad outcomes from hackers and enablement of safe operation for bold new means of automation. Including the CISO in this high-level discussion will improve the odds that the digital transformation initiatives will avoid any negative security consequences.

Successful organizations are built on a foundation of trust and respect. Most companies adopt technologies that enhance collaboration which ultimately reinforces these fundamental characteristics.

Create your FREE account today,
take control of your security score,
and start managing your security posture.

GET STARTED

SecurityScorecard.com
info@securityscorecard.com

United States: (800) 682-1701
International: +1(646) 809-2166

About SecurityScorecard

Funded by world-class investors including Evolution Equity Partners, Silver Lake Waterman, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings with more than 12 million companies continuously rated.

Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 30,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight. SecurityScorecard is the first cybersecurity ratings company to offer digital forensics and incident response services, providing a 360-degree approach to security prevention and response for its worldwide customer and partner base.

SecurityScorecard continues to make the world a safer place by transforming the way companies understand, improve and communicate cybersecurity risk to their boards, employees and vendors. Every organization has the universal right to their trusted and transparent **Instant SecurityScorecard** rating. For more information, visit **securityscorecard.com** or connect with us on **LinkedIn**.

SecurityScorecard