Secureworks®

WHITE PAPER

The Business Executive's Guide to Cybersecurity

Keys to Improving your Relationship with the CISO

Once primarily the role of a small group of security experts, cybersecurity is now established as a business-wide concern that becomes increasingly important every year.

The increasing prevalence of high-profile breaches and security incidents has emphasized the critical role cybersecurity plays in protecting a company's valuable assets and its reputation. Many organizations and C-suite leaders are increasingly accustomed to a level of suspicious events and incidents that make the importance of cybersecurity hard to ignore. At the same time, digital transformation initiatives harness new technologies that are critical for business evolution, yet introduce new and different forms of risk for the organization to address. These factors have contributed to a realization that security is now the responsibility of the entire C-suite.

In addition to the CISO, CTO, and CIO, non-technical business leaders within an organization must understand cybersecurity in terms of potential risk to the business and have a high-level grasp of how their cybersecurity framework protects against threats. 79% of global executives rank cyberattacks and threats as one of their organization's highest risk management priorities in 2020, according to a 2019 Marsh & McLennan survey of 1,500 executives.[1]

Organizations that do not have clear insight into threats will face the following risks:

- Recovery: the financial cost of recovering from a data breach can be in the millions.
- Reputation: the cost to an organization's reputation can be devastating. Once a breach is exposed, customers may lose faith that their data will be protected by an organization and choose to do business elsewhere. Employees and investors may also lose confidence in the business, leading to further financial damage.
- Regulatory compliance: governments across the world are ramping up their regulations around consumer data and privacy. Violating these regulations can lead to monetary fines, the inability to do business in certain markets, and may even create legal issues such as lawsuits from shareholders.

79%

of global executives rank cyberattacks and threats as one of their organization's highest risk management priorities in 2020.

What to Expect from the CISO

Executives should look to the CISO – or equivalent role within an organization – to regularly and clearly communicate key risk factors to the business. To do this, it's vital that the C-level team builds a strong relationship with regular check-ins to discuss important changes and emerging issues. During these risk assessment meetings, non-technical executives should feel comfortable discussing the organization's cybersecurity program at a high level, ask questions of the CISO about risk for their specific business segment, and offer a perspective on third-party security vendor selection.

[1] Marsh & McLennan, 2019 Global Cyber Risk Perception Survey

The entire C-suite should collaborate to identify what key pieces of data they expect their CISO to provide, as they will vary from company to company. But as a guideline, the CISO should be equipped to share guidance on the following questions:

- What is the cybersecurity risk for the company?
- How well is this risk being managed?
- Are we dedicating the correct amount of resources to cybersecurity?
- Is the security program performing at a level that we need it to, commensurate with the risk we're carrying?
- What types of analytics should business leaders have access to, and how should we establish a regular cadence of reporting for those analytics?
- What is our incident response plan? This is a part of risk management, and any mature organization should have a response plan that is regularly rehearsed. Those rehearsals should include key members of the C-suite and other stakeholders who may be impacted.

The executive team needs to understand what the technologies and techniques mean for mitigating risk to the business, not what each of the technologies do and how they work.

Common Communication Errors

Simple communication issues between the CISO and the rest of the executive team can derail progress and leave the business open for greater risk. Those errors include:

- Lack of Regular Information Sharing
  The responsibility for keeping the lines of communication open and mitigating risk weighs equally on the CISO and the rest of the C-suite, so it's critical that all parties are committing to regular information sharing. Ideally, this risk committee should meet once a month to get updates on the data, address outstanding questions, and discuss strategy for handling emerging issues.
- Business vs. Technical Information
  Although non-technical executives should have a high-level understanding of cybersecurity as it relates to business risk, the onus is on the CISO to be familiar with the business and share information in a way that focuses on business-related risk – not for the C-suite to understand security.

CISOs that present overly technical information that focuses on technology, processes, individual security controls, and other minutiae must consider their audience.

Choosing a CISO

There may come a time where an organization needs to hire a new CISO. What are the key qualities that the hiring committee needs to consider?

- An expertise in security and a strong security background.
- Well-versed in risk management. Every discussion between the CISO and executive team should be a risk-based discussion, and everything the CISO does should be focused on managing risk to the business.
- Business expertise. The CISO must be a business partner and enabler and should be able to demonstrate how their risk management program will enable the business to accomplish its goals.
- What framework has the CISO adopted to manage cybersecurity risk? Are they mapping to one of the well-known frameworks such as NIST, creating their own, or using a proprietary one? The framework should be easily communicated and have good industry acceptance.

The Technology Selection Process

In addition to building a strong relationship with the CISO that includes regular risk committee meetings and reporting, non-security executives should also have a stake in the third-party security vendor decision-making process.

When searching for a new security partner, there are several key technologies and support aspects that the vendor must be able to provide:

- A consultative approach to risk management strategy, with the ability to help build a program from the ground up or work within the already established framework.
- Expertise with the technology they're proposing to deploy, and 24/7 monitoring and response capabilities.
- Broad enough reach and collective knowledge that they can use their data to protect your organization. Smaller companies with a limited customer base won't have the same expertise and "lessons learned" to bring to bear for your organization.
- World-class analytics with a proven track record. Not only should they have the data to perform meaningful analytics, but a proven track record in this area with the people and processes to present them.

The right partnership can help you prioritize the actions that yield meaningful, measurable outcomes and validate the capabilities and value security brings not only to IT but to the entire business.

In order to understand what the third-party is bringing to the table, this set of questions can help executives determine whether the vendor is a good fit:

- **Incident Response**
  - How will the third-party expert respond when there is a cybersecurity incident?
  - Can they share more information about how many customers they have, how long they've been operating in the industry, and case studies that illustrate how they work closely with customers to mitigate risk?
- **Third-party validation**
  - What external validation does the third-party have? External validation is part of how an organization manages risk, so it's essential that the proper credentials and certifications are in place.
- **Interoperability**
  - Does the third-party technology work well with what we already have in place, or will there be a need for further investment from the organization on upgrading technology?
  - Will their platform enable us to grow with future technologies?

Security is the responsibility of an organization's entire leadership team, and it's important to understand how a variety of security risks may impact the business.

Mitigate risk across your organization by building a strong relationship with the CISO, encouraging establishment of a risk committee that enhances information sharing, asks informed questions around consultative capabilities, collective knowledge, and metrics during the technology selection process.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp