Secureworks®

WHITE PAPER

How a Change in Leadership Can Impact Cybersecurity

New Leadership Calls for An Evaluation of Security Strategy, Solutions, and Culture

For many organizations, the tenure of a C-suite executive is often short-lived. A detailed survey of the top 1,000 U.S. companies by revenue revealed some telling statistics: the average tenure for a C-suite executive is 4.9 years.[1] If that number seems low, consider the average tenure of a Chief Information Security Officer (CISO) is around 24 to 48 months.[2] There are many reasons cited for this: long hours, low budgets, and the constant stress of daily new threats to corporate data.

The departure of a CISO or cybersecurity leader can create risk as well as opportunities for an organization. If the CISO's departure was the result of a data breach, it's time to reevaluate the company's cybersecurity strategy. While it might be easiest to assign blame to the departed CISO, there are often other reasons why a cybercriminal was able to penetrate the perimeter and access data. These can include human error, lax security policy, or outdated cybersecurity tools that are sometimes present for the tenure of multiple different CISOs. Whether a CISO's departure is the result of a data breach, or a career-advancing move, a change in leadership can lead to a period of realignment for cybersecurity teams.

From the Board Room to the SOC

When a CISO leaves an organization, the rest of the C-suite naturally worries whether the leadership gap exposes the business to more risk. At the same time, security practitioners lack a clear, guiding strategy to focus their efforts. This is especially pronounced following a breach, where security teams may question the efficacy of how they operated before.

In this paper, we'll look at the business risks and opportunities that organizations need to keep in mind when a new cybersecurity leader takes the helm. A change in leadership could be a defining moment for your organization—an opportunity to review the strategy, solutions, and culture being deployed to protect your business.

Considering Changes to Cybersecurity Strategy

CISOs are increasingly involved in core board decisions. As a recent PwC report notes, the CISO's role is becoming more strategic and no longer just another function within IT.[3] The report goes on to cite that 84% of respondents consider the ability to educate and collaborate across the business to be very important in a CISO. New CISOs are often eager to have an impact. In the process, they bring with them their favored vendors, new solutions, and an emphasis on widespread employee education initiatives.

A key strategic opportunity for CISOs is to evolve their security programs from reactive to proactive. Preemptively identifying weaknesses and vulnerabilities across your network requires full awareness and understanding of an organization's risk profile.

84%

of respondents consider the ability to educate and collaborate across the business to be very important in a CISO.

[1] Korn Ferry, Age and Tenure in the C-suite

[2] ESG and ISSA, The Life and Times of Cybersecurity Professionals 2018

[3] PwC, The CISO in the C-Suite: educator, innovation partner and collaborative risk manager

Secureworks®

Reactive approaches, such as patch management, are focused on fixing an issue after it is identified. It's likely this will continue to consume part of a security leader's role, but a talented leader will strive for a proactive stance, and ensure the organization has everything it needs to manage cyber risk and identify potential threats. If a new CISO is hired because the former CISO wasn't performing adequately, or experienced a data breach, the new leader will likely need to recommend change across multiple areas, as well as prepare for future growth.

Reevaluating the Effectiveness of Current Cybersecurity Solutions

A major data breach often leads to a complete reevaluation of a security operation. In that process, old CISOs are often replaced with a new leader who must review all the cybersecurity tools and solutions currently in use. Here are a few questions to keep in mind during that process:

- What tools does the new security leader have experience with? CISOs often favor tools they are familiar with, and for good reason. The learning curve on new solutions can be steep, so it's essential to consider how bringing in a new tool may affect the analysts who will be managing the day-to-day operations.
- What is the new leader's philosophy on the security stack? Today's market is flooded with new solutions that are intended to simplify security practitioners' jobs, but if implemented without care, they can have the opposite effect. It's important to have a leader who understands the complexity of a security stack and has a plan on how to assess the stack and consolidate, if necessary.
- If there was a recent breach, was it the result of human error, outdated tools, or faulty analytics? In addition to managing the incident response and helping the company recover from a breach's impact on the business, a new leader should also assess any of the tools or resources that may have been at fault in the breach.
- How was the CISO-analyst relationship in the past? Understanding the partnership dynamic of a past CISO can help a new leader get acclimated to the environment and build a strong foundation with the security team from the start. A CISO should know well that new leadership and frequent turnover can affect morale. Before going in and trying to fix things or implement new solutions, a new leader should take time to address and mitigate these pain points among the team.

Influencing A Culture Change

A change in security leadership offers a fresh opportunity to create productive relationships with the corporate board and the security analysts. The security leader can immediately influence the security culture across the organization in several ways:

- **Moving Beyond Compliance:** The role of the cybersecurity leader has gone far beyond simply checking compliance boxes and securing corporate data from threat actors. A great CISO both shapes the cybersecurity posture of an organization, and knows how to elevate the perception of security across the organization.
- **Enabling Digital Transformation Projects:** Today's cybersecurity leader should also be involved from the start of digital transformation projects. With the proliferation of IoT, cloud computing, and the growth of endpoints, cybersecurity should be one of the fundamental building blocks of any digital transformation project. Digital transformation often expands the attack surface for threat actors, so it's critical that CISOs understand how to guide the process.
- **Improving Companywide Communication:** In a survey of the most important qualities of a successful CISO, communication skills ranked the highest – well above technical acumen or operational skills.[4] CISOs are increasingly asked to provide a communication link from the tactical side of the business to the Board. Having a strong and effective communicator in this role – one who can translate key security issues to employees of all levels – can drastically alter the culture of security within an organization.
- **Bringing a Holistic Approach to Security:** Cybersecurity is no longer just the domain of the security leader. A cyber breach has the power to impact shareholder value, public sentiment, and regulatory concerns. As such, cybersecurity should be top of mind for the entire C-suite, every department head, and all employees. It's the CISO's job to make this a reality.

The security leader should reframe how the organization approaches security—from partnering with experienced vendors who have unparalleled threat intelligence and incident response experience, to researching next-generation cybersecurity tools that leverage AI and machine learning to rapidly detect advanced and unknown threats.

The Positive Impact of a New Security Leader—Transforming and Securing the Future

A change in security leadership creates uncertainty, but also enormous opportunity for organizations. Equipped with the right tools and a proactive security posture, a change in leadership can be the critical first step in fortifying an organization's network, creating a security-first culture, and paving the way for a secure future. Sometimes, a fresh start is exactly what an organization needs.

[4] ESG and ISSA, The Life and Times of Cybersecurity Professionals 2018

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