BITSIGHT
The Standard in SECURITY RATINGS

WHITE PAPER

The Evolution of the CISO

The need for C-Suite transformation amidst increased security and cyber risk

The Increasingly Vital Role of the CISO

> In the midst of facilitating organization-wide digital transformation, the CISO also must undergo his or her own professional transformation.

As a newer addition to the C-suite, the role of the Chief Information Security Officer (CISO) is one that is not found in every company. Increasingly, though, it is becoming apparent and essential to the modern enterprise.

While the Chief Security Officer (CSO) often is in charge of physical security, the CISO is differentiated by a range of responsibilities, including:

- Security operations
- Cyber risk and intelligence
- Data loss and fraud prevention
- Security architecture and performance
- Identity and access management
- Third-party and vendor risk management
- Board reporting
- Investigations and forensics
- Governance

The role of the CISO is not without its challenges, both functionally and professionally. In addition to daily responsibilities and pressures, a CISO must demonstrate the communication skills, business savvy, and leadership required of a C-suite executive.

In the midst of facilitating organization-wide digital transformation, the CISO also must undergo his or her own professional transformation to keep up with a world in serious need of cybersecurity leaders.

What Keeps the CISO Up At Night?

15%

of cybersecurity professionals plan to stay in their current roles.[2]

The CISO faces a number of functional challenges daily, especially in today's security climate. As part of his or her core responsibilities, the CISO juggles both technical and managerial duties, including:

Strategic Alignment
The CISO must work to integrate his or her strategy with the mission of the organization so that its goals and appetite for risk are assessed properly.

Changing Regulations
Regulations change frequently as lawmakers pass legislation and new threats emerge. In the wake of GDPR, more governments at all levels are following suit, which means company standards for information security compliance will continue to become more complex.

Cloud Security
As components of the IT stack are moved from the data center to the cloud, the CISO is charged with improving security, identity, and access management across the public and private environments. At the same time, the security of on-premises legacy systems must be maintained.

Team Development
Researchers in the utilities industry estimate that there are fewer than 500 people in the U.S. with the necessary cybersecurity training and expertise to help them comply with regulations.[1] In fact, the shortage of skilled personnel is growing. Plus, only 15 percent of cybersecurity professionals plan to stay in their current roles.[2] With the average time-in-role for security personnel at just two to three years, a CISO must be an engaging, receptive leader that responds to employees' needs and encourages their career growth and development in order to drive down attrition.

Emerging Technology
Security leaders also must keep up with current technology trends, not only to stay vigilant and innovative, but also to take advantage of emerging tools. AI, machine learning, automation, IoT, and 5G capabilities can help the organization achieve true digital transformation. Newer cloud-based security offerings enable security teams to detect threats across multiple parties and prioritize the most pressing issues.

Data Management
With data protection at the top of the priority list, the CISO regularly seeks out stronger data governance practices. At the same time, the CISO regularly must assess and clean data not only to keep it manageable and prevent slowing down the business, but also to reduce the amount of data to protect.

Incident Response and Remediation
Perhaps most challenging of all, the CISO must face the new reality: data breaches can and will happen. Broadening the focus on prevention to include strategic planning enables the CISO to address potential risk introduced by digital transformation and the increasing reliance on third-party providers. In addition, the use of technology to automate and scale security monitoring and other functions minimizes the impact of these efforts on the business.

Common Pitfalls the CISO Faces

> ”
>
> The most prominent CISOs have a good technical foundation, but often have business backgrounds, an MBA, and the skills needed to communicate with other C-level executives and the board.
>
> –**Larry Ponemon, Ph.D.**
> IT Researcher and
> Chairman/Founder of CIPP

1. **The CISO often is a technical performer-turned-manager who focuses too much on the nuts and bolts of security instead of on overall risk management and associated business outcomes.**

   The more urgent need for increased cyber security in the last decade has prompted the role of the CISO to show up more prominently in organizations.

   Naturally, these executives are sought from among security professionals with deep expertise and technical performance skills in the organization. But not every high technical performer is proficient at leadership and management. As a result, an employee can be appointed to the role of CISO before s/he is ready professionally.

   At the same time, the CISO has a tendency to focus more on solving security issues rather than viewing risk management as part of the larger business strategy. Instead of operating in the weeds of how tech security is implemented, the CISO must adopt a broader and more strategic risk management perspective.

2. **The CISO lacks training or mentoring in traditional business skills.**

   Similar to other roles in the C-suite, technical knowledge is not the only skill required to succeed in the job. As a result, the CISO may struggle with the business savvy and communication skills necessary to collaborate with non-technical audiences.

   These skills are crucial, however. Gaining executive buy-in and initiative adoption require the CISO to build collaborative bridges with other business units as opposed to acting as the “software sheriff” – a role that can be viewed as a roadblock instead of an enabler. Without the ability to frame his or her work in terms of business results, the CISO may not be regarded as a true C-level leader, and risks being left out of the decision-making process.

3. **The CISO is subordinate to or fails to differentiate his or her role from that of the CIO.**

   Despite both roles being members of the C-suite, it is common for the CISO to report to the Chief Information Officer (CIO). This can have negative effects on the CISO’s ability to execute freely, as his or her vision can be overshadowed by the CIO’s overall IT strategy.

   The solution may be as simple as making a title change. Security executives with the title of CSO more likely will be considered the same level as the CIO.[3] Regardless, both CISOs and CSOs gain more clout when they report directly to the Chief Executive Officer (CEO), a practice that is becoming more common.[4]

The Need for Professional Transformation

There is enormous pressure for the CISO to manage the risks associated with the organization's digital transformation against the backdrop of an increasingly aggressive attack landscape.

One factor that makes the CISO's role even more challenging and volatile is that it is the rookie among a team of veteran positions whose job descriptions have been defined, honed, and traditionalized over several decades.

Since the initial adoption of the CISO position began only a few years ago, the current crop is among the first to hold the title at their company. It is up to this generation of security pioneers to define the responsibilities and scope of the role of the CISO, and to determine whether it can survive as a differentiated leadership role or devolve into a lower-tier executive position that reports to the CIO or Chief Risk Officer (CRO).

In order to succeed and thrive as a valuable and respected contributing member of the C-suite, the CISO must undergo a transformation of his or her own. Steps toward this professional transformation include:

> The CISO is the rookie among a team of veteran positions whose job descriptions have been defined, honed, and traditionalized over several decades.

Improve Communication and Collaboration

Arguably, one of the most important aspects of the CISO's role is converting other executives into willing collaborative partners in creating a more secure organization.

Yet, only 22% of companies say their organization's security function is integrated with other business functions.[5]

> 22%
>
> of companies say their security function is integrated with other business functions.[5]

Infusing security priorities throughout the company takes regular communication and collaboration with other departments. It also requires understanding and prioritizing what *they* find valuable and worth protecting, from customer data to product innovations to sales leads.

Instead of interfacing only with fellow IT leaders when a security issue arises, the CISO must forge healthy relationships with peers and build collaborative cohorts from the start.

Key areas of focus for the CISO:

- Communicate vital information to non-technical audiences effectively
- Frame information in terms of business outcomes (not just statistics or jargon) in order to gain buy-in and support
- Build alliances with other C-level executives for a clearer picture into other parts of the business, and change the conversation from constantly "fixing problems" to growing and transforming the business proactively
- Prove that the value of the CISO's work not only is to defend the organization against attacks, but also to impact it positively from the top-down by aligning security strategies with business opportunities and goals
- Adopt a broader risk management strategy instead of getting into the "weeds" with security implementation and one-off issues

> In the midst of a serious cybersecurity talent shortage[6] the CISO must prioritize professional development and mentoring to prepare the next class of leaders.

Understand and Convey Business Context

The CISO has spent much of his or her career behind-the-scenes in a technical role with limited exposure to the workings of the business itself – exposure that is vital to the CISO's ability to put the technical aspects of cybersecurity into a business context.

To adapt, the CISO must tap into their soft skills to present cybersecurity performance, risks, vulnerabilities, and initiatives as part of the overall business strategy -- and in terms of their impacts to the business.

Key areas of focus for the CISO:

- Become acclimated with the everyday challenges and vernacular of the business
- Be well-versed in the goals and strategies that the organization is trying to achieve, and demonstrate alignment and commitment to helping realize those outcomes
- Act as a facilitator instead of a roadblock to business development, innovation, and growth
- Identify the metrics that are most relevant and compelling to executives when relaying the impact of cybersecurity performance on the business as a whole

Mentor the Next Generation

As a pioneer of the role, the CISO must prepare the next generation of security executives so that the job not only is more manageable, but revered and valued among fellow organizational leaders.

In the midst of a serious cybersecurity talent shortage[6] the CISO must prioritize professional development and mentoring of his or her team in order to prepare this next generation of leaders, especially as cyber threats continue to increase in prevalence and aggression.

Key areas of focus for the CISO:

- Clearly define the role of the CISO and differentiate it from similar existing positions, such as CIO
- Identify which skills need to be developed within the organization in order to prepare for the future and raise the next generation of leaders
- Develop training programs, evaluations, and/or career tracks around the "business of security" in order to raise awareness and plan for who will take the business into the next era

Shaping the Future of the CISO Role

The CISO must have the most reliable and intuitive set of tools at his or her fingertips to help the business make better decisions about security.

From monitoring data to preparing for board meetings, the role of the CISO includes an ever-expanding list of job responsibilities.

Security leaders must be or become proficient in all of these responsibilities, not only prove their value in the C-suite, but also to lead their teams effectively in the management of today's growing risks, and to prepare those teams for the future of the organization's security.

While the CISO may be accustomed to a narrow or highly tactical focus on data and security based on his or her background, the role of the CISO requires broader perspective and additional skills, including leadership, communication, and a working knowledge of the business itself.

In addition, the modern CISO must have the most reliable and intuitive set of tools at his or her fingertips. These tools can help the business make better decisions about security, prioritize issues, allocate resources, assess cybersecurity performance in context with industry standards, and provide more visibility into the security posture and controls of third-party providers in order to minimize the potential impact of inherited risk.

With a greater focus on the growth of their business, communication, and mentoring skills, the security executives of today can help shape the future of the role of the CISO. Their careful, persistent definition and differentiation of responsibilities will enable the CISO to become the defacto cybersecurity leader that organizations will rely on to align their security controls and practices with their goals for business growth, innovation, and success.

REFERENCES

1 https://rtoinsider.com/naruc-dragos-cybersecurity-scada-86882/

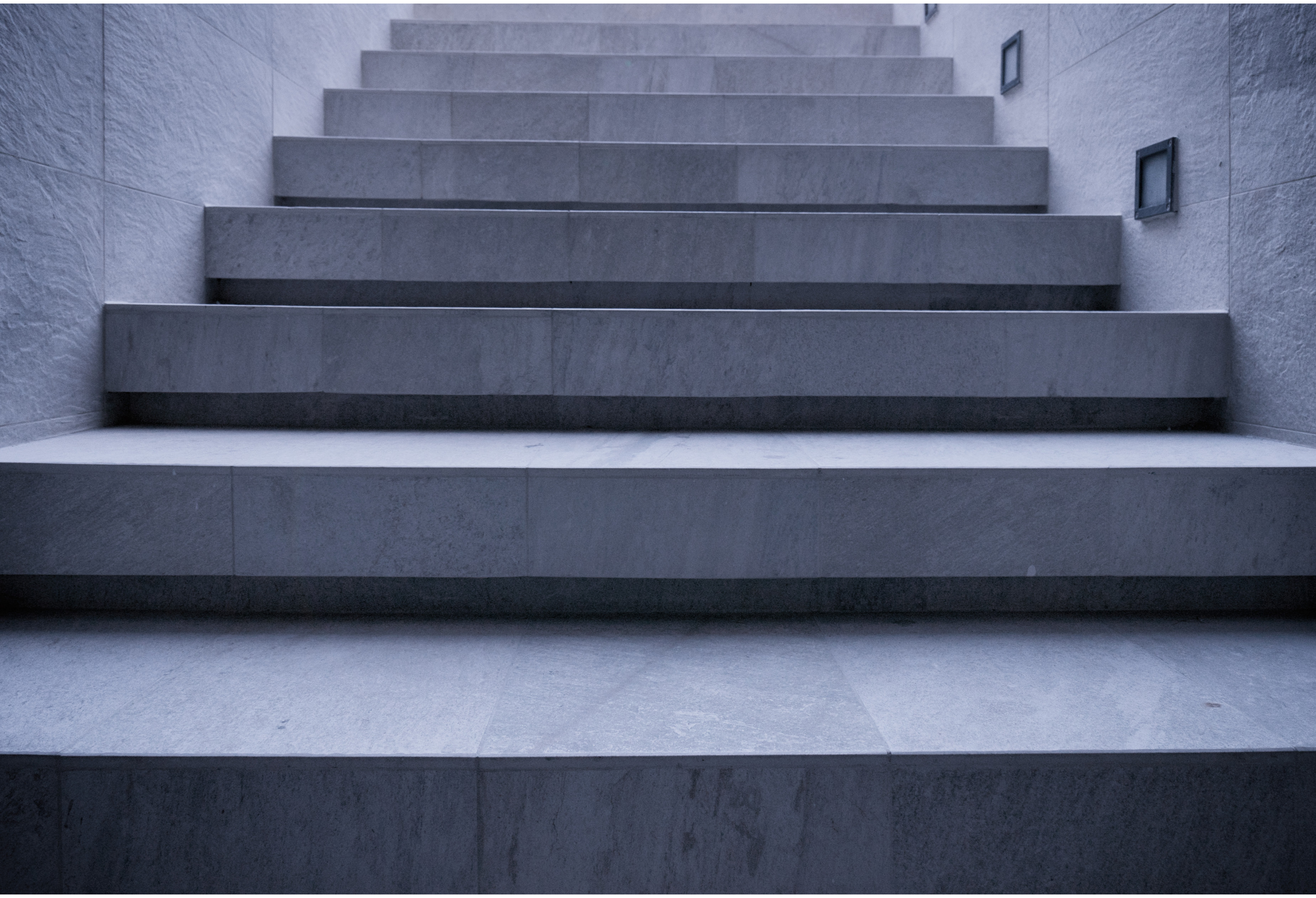
2 https://www.isc2.org/-/media/Files/Research/ISC2-Hiring-and-Retaining-Top-Cybersecurity-Talent.ashx

3 https://www.idg.com/tools-for-marketers/2018-global-state-information-security-survey/

4 https://www.wsj.com/articles/companies-cut-ciso-reporting-ties-with-technology-1524515201

5 https://securityintelligence.com/the-expanding-role-of-the-ciso-seven-attributes-of-a-successful-security-leader/

6 https://www.csoonline.com/article/3331983/the-cybersecurity-skills-shortage-is-getting-worse.html



BITSIGHT®
The Standard in SECURITY RATINGS

111 Huntington Avenue
Suite 2010
Boston MA 02199
+1.617.245.0469

About BitSight
BitSight transforms how organizations manage information cybersecurity risk with objective, verifiable and actionable Security Ratings. Founded in 2011, the company built its Security Ratings Platform to continuously analyze vast amounts of data on security issues. Seven of the top 10 largest cyber insurers, 25 percent of Fortune 500 companies, and four out of the top five investment banks rely on BitSight to manage cyber risks. For more information, please visit www.BitSight.com, read our blog or follow @BitSight on Twitter.