THE EVOLVING ROLE OF CISO

NETWORK INTELLIGENCE
The Digital Security Company

According to Wikipedia, a Chief Information Security Officer (CISO) is the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy and program to ensure information assets and technologies are adequately protected. The role of the CISO has evolved considerably over the past few decades. While in the 80s and even the 90s, CISOs may have been a rare breed, today CISOs are often seen leading their organization's cybersecurity effort from the front.

Some interesting nuggets:

- **Up to 50% CISOs reportedly come from an IT background. The converse is that 50% do not. This reflects a very interesting aspect of cybersecurity – you don't necessarily need to be from an IT background to do well here.**
- **The position emerged in the 1980's. Steve Katz, probably the world's first CISO was appointed by Citibank in 1985. He says, "99% of becoming a CISO was serendipity and being open to a new career opportunity where there wasn't a career".**

Typical responsibilities of a CISO

A CISO has a wide-ranging set of responsibilities. As the primary executive accountable for cybersecurity within the enterprise, various aspects of their job might entail:

- Understanding compliance requirements for their business depending on the industry, countries they operate in, and type of data that their business handles.
- Carrying out effective risk assessments and determining a feasible risk remediation plan that has buy-in from the C-Suite
- Monitoring implementation and operation of security controls aligning with globally accepted cybersecurity frameworks such as NIST-CSF, ISO 27001, etc.
- Running a security awareness training program that covers employees as well as contractors
- Addressing third party risk via a security monitoring program
- Handling cybersecurity incidents and coordinating actions via a Cybersecurity Incident Response Team (CIRT)
- Monitoring global trends, new attack vectors and determining how these impact their organization's cybersecurity posture
- Putting together a team, motivating them, ensuring their skills are upgraded
- Keeping up with business transformation and ensuring cybersecurity aspects are being addressed in the age of DevOps, containers, rapid cloud adoption, etc.
- Reporting regularly to the C-Suite, to the Board and to regulators the organization's cybersecurity posture via the careful selection of metrics

That's quite a bit! And in the midst of all this, the CISO also has to meet multiple vendors, understand solutions that are on offer, evaluate them, and monitor their successful implementation within the organization. Today, the role of a CISO has become more "proactive" rather than "reactive". It involves a deep partnership with all lines of business and ensuring their team is connected more than ever with the business. As the new dimensions are in spotlight, priorities need reshuffling.

The facets of a modern CISO

Sratregist- Drive business and cyber risk strategy alignment innovate and instigate transition change to manage risk through valued investments.

Advisor- Integrate with business to educate, advice and influence activities with cyber risk implications.

Guardian- Protect business assets by understanding the threat landscapes and managing the effectiveness of cyber risk program.

Technologist- Assess and implement security technologies and standards to build organizational capabilities.

CISOs need to be "trusted business advisors". A world class CISO must be a business enabler who finds creative ways to help the business say "Yes" to new opportunities.

Evolution of the CISO

The CISOs transition within an organization from their original role to that of an innovator is not without challenges. Some of the challenges and the ways to overcome them are:

Lack of resources and effective team structure.

- Identify your team strengths and improve them.
- Determine what motivates them and assign them that role.
- Outsource effectively - choose the right cybersecurity partners to work with
- Adopt automation as far as possible and move team members aware from routine and mundane tasks.

Weak relationship with the business units within the organization.

- Change roles towards advisor figure. (requires getting to know the business really well)
- Speak their dialect - skip the jargon as much as possible.
- Report business-aligned metrics

Ineffective communications/ reporting among stake holders and throughout the organization.

- Inform all relevant stakeholders about all the achieved milestones - you're the main evangelist for cybersecurity wihtin the organization.
- Get to know audience, then prepare the message. End-users versus the Board - a very different messaging is required.

Lack of support and trust from executive leadership and stake holders.

- Use business centric, risk focused approach. Identify the key 20% of information that moves 80% of business.
- Justify cybersecurity investments from a business risk perspective

Inadequate senior management commitment

- Keep everybody who needs to be involved into the game.
- Articulate your risks without leveraging Fear Uncertaininty and Doubt (FUD)

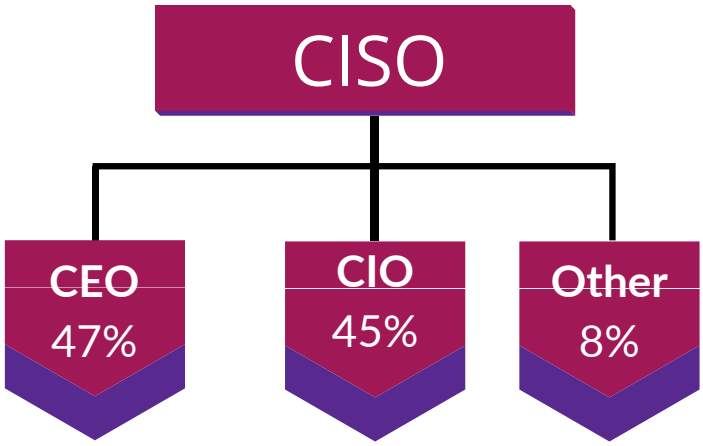
Insufficient funding.

- Again, use business centric, risk focused approach.
- Demonstrate ROI by using statistics from cost of data breach statistics published in the Ponemon Institute Report
- Determine weak spots in the organization. Start investing internal resources, leveraging existing infrastructure.

Going back to **Steve Katz**, who says "***What I see with many CISOs is that too many CEOs have no idea who the CISO is and there's no means of communications. You have to be out there evangelizing and be part of the company. You are either a part of the C-level of management or you are not.***"

Organizational placement of CISO

As the role of the CISO evolves, so does their line of reporting. Initially, the security function is totally embedded into the IT organizational structure. It then evolves to come under the Risk Department or the CISO might end up reporting directly to the CEO. According to "Threat Track CEO survey"



CEOs operate according to risk. A CISO should be able to explain risks in a business language and from business perspective.

What to report to the board/ Senior Management:

- Top cyber risks
- Emerging threats
- Program maturity
- Audit and regulatory concerns
- Compliance status
- External collaborations/ Special projects

What do we expect them to ask?

- How much could we lose if we don't manage this risk intelligently?
- What is the likelihood of the risk occurring?
- What is our vulnerability to this risk?
- If I mitigate this risk, how does this change the likelihood and impact?
- How much can we gain if we accept this risk- provided we manage it properly?
- How much is it costing us (or will it cost us) to manage this risk?
- If there a potential reputational risk impact from this risk?

Looking towards the future

As the role of the CISO has changed, what companies look for in a CISO has changed, too. Finding the right CISO has become a challenge. Companies want someone who understands both the technology landscape and the business implications of technology. Some of the challenges are:

- CEOs/CXOs are looking to hire or develop a senior security leader and aren't sure how to identify the best candidate.
- Existing security leaders are looking to develop their talents.
- Organizations are looking to optimize their security plans and move from a tactical position to a more strategic one.

CISOs have to step outside of the security domain and see what value they can add throughout the organization. The CISOs should be focused on three specific areas:

- Ensuring that the organization is extremely disciplined in the things that are known. If you can't deliver on the basics, you can't deliver.
- Becoming proficient in addressing today's more expansive expectations. For example, CISOs can talk about risk management, but they need to actually define it and articulate it for their organizations, so decision-makers understand what they are investing in, and why.
- Analyzing, predicting, and preparing for the future. We know that IT consumerization will continue to redefine customer expectations.

Conclusion

CISO's do not succeed on their own. They must take the initiative to bridge silos that may exist within organizations. In the end, it comes to basic relationship building so that CISOs are recognized as valued contributors to C-suite. And the job continues to evolve.
The Digital Age isn't waiting for anyone. CISOs who lean in to guide their organizations through this period of unprecedented technology change and opportunity can rise from good to great.

ABOUT NETWORK INTELLIGENCE

We are a global cybersecurity provider founded in 2001 with more than 600 team members working out of our New York, Amsterdam, Sydney, Riyadh, Dubai, Mumbai, and Singapore offices. We offer cybersecurity services using a comprehensive framework – ADVISE. The ADVISE framework empowers us to Assess, Design, Visualize, Implement, Sustain, and Evolve your cybersecurity posture as a long-term partner to your organization. By incorporating AI technologies, we revolutionize the way organizations approach security. We serve customers across industry verticals such as Banks and Financial Services, Technology and Media, Oil & Power, Airlines, E-commerce, Retail, Healthcare, etc.