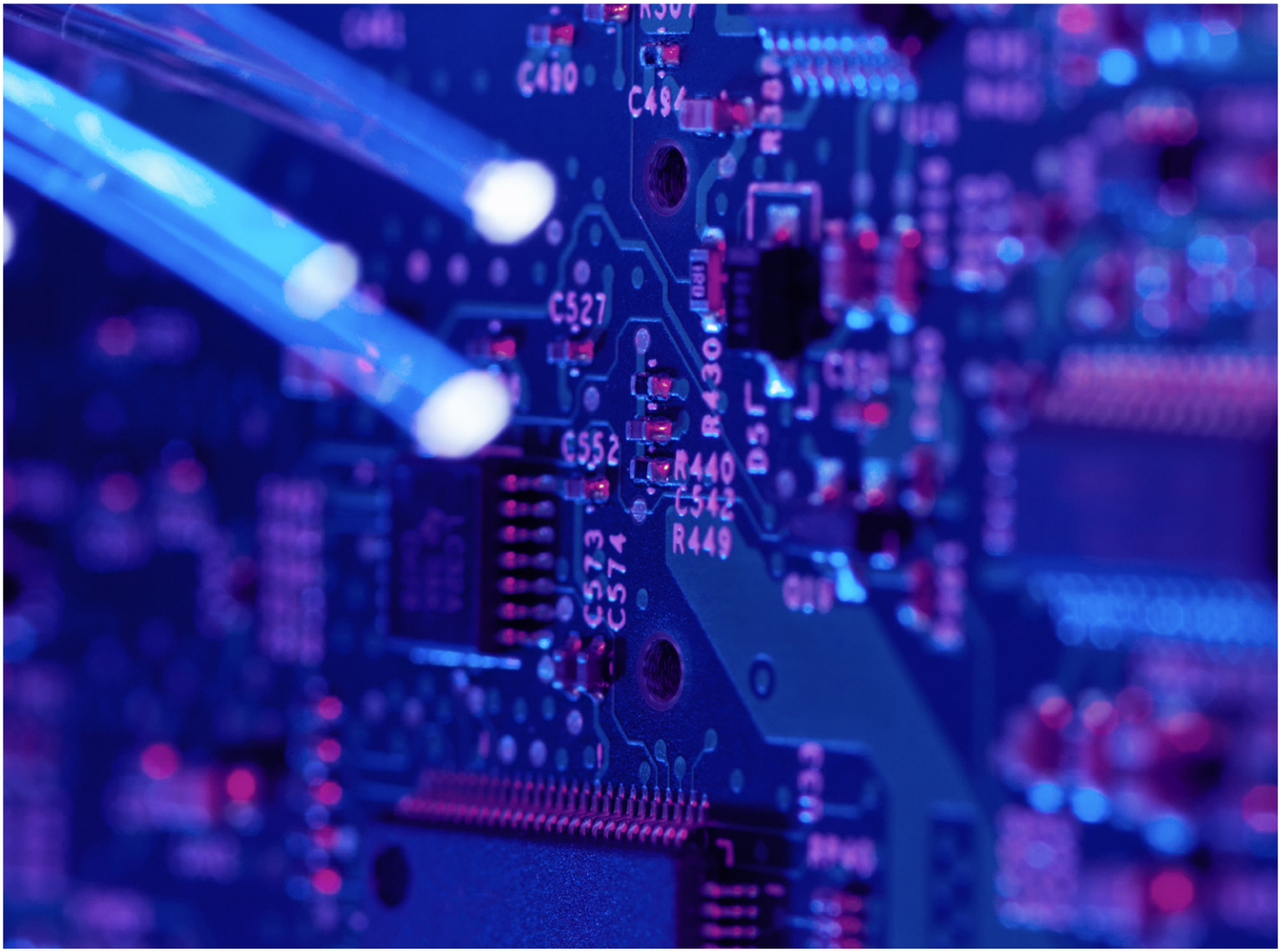
Secureworks®

WHITE PAPER

Roadmap to the CISO

Will you be C-level or just have the title?



The role of a CISO is evolving from a technologist to a business leader whose responsibilities include partnering with many aspects of the business to communicate and mitigate risk across the organization.

Taking on this management advisory role, the modern day CISO is required to be a security advocate on a wide range of topics that affect business performance including HR, digital and physical security, vendor and partner management, and regulatory compliance. What's more, they are called upon to report to Boards and the C-suite in language that non-technical business leaders can understand and act upon. They must translate very complex technology metrics into plain English about levels of risk and the capabilities used to reduce risk and crisis management when a breach occurs.

In short, the CISO is following the same evolutionary trajectory as the Chief Information Officer and Chief Financial Officer by continuing to take on and be responsible for more strategic organizational responsibilities. In this white paper, you will learn more about the evolution of responsibilities for the modern CISO, the technical and business skills that provide a foundation for aspiring CISOs, and recommendations to set yourself on a trajectory to become a successful CISO.

The role of a CISO is evolving from a technologist to a business leader whose responsibilities include partnering with many aspects of the business to communicate and mitigate risk across the organization.

Ev·o·lu·tion

The gradual development of something, especially from a simple to a more complex form.

Let's look at a hypothetical human example, a college graduate who finished their degree top of their class with honors, earning high distinctions in all of their assessments and examinations. They successfully land their dream job and start evolving themselves to manage the practical elements of their studies to integrate well with that business's needs. The question becomes could this individual continue to evolve and self-educate to match the changing horizon of the industry in which they work?

A 50/50 Shift

Much like our example above, a CISO's evolution is the same.

It's no surprise that a majority of CISOs come from an information technology and computer science background. In fact, out of today's top Fortune 100 security leaders, half (50 percent) of the CISOs had information technology/security and/or computer science as their main area of study. Additionally, F100 security leaders hold an average of 2.86 certifications to keep their credentials up-to-date.[2]

Anatomy of a CISO[1]

85%
Bachelor's Degree

40%
Master's Degree

3%
Doctor of Philosophy

2%
Juris Doctor

Availability varies by region. ©2018 SecureWorks, Inc. All rights reserved.

Secureworks®

While there is no question that a keen technical acumen is necessary for the CISO role, the increased levels of public scrutiny and greater need for visibility from business leaders and the Board of Directors has resulted in a required skillset that is equal parts technical and business leader. Further solidifying this point, if you look at the latest job postings for large enterprise organizations, you see a reoccurring need for a business skillset that falls into key areas outside the typical technologist's realm. Below are examples of enterprise-level CISO job postings from LinkedIn. The responsibilities are grouped together by functionality (edited for anonymity).

Collaboration, Implementation, Process Improvement:

- Understand information technology systems and business practices to be able to identify risks and prepare detailed risk analysis deliverables and executive summaries, including business impact and cost/benefit analysis.
- Partner with business leaders to develop a cohesive Information Security Strategy, and a roadmap (schedule, cost, effort, benefit model) for strategy implementation.
- Drive and instill continuous improvement discipline within information security and in the business. Strive to identify opportunities to reduce the overall cost to serve and operate new solutions and help the business find new ways to reduce their overall cost and improve efficiency.

Compliance, Privacy, Audit, and Risk:

- Report the levels of IT compliance risk and control effectiveness to key stakeholders such as IT-business unit management, senior management and internal/external auditors.
- Re-enforce and reward focus on XYZ's vision, and ensure information security's solutions that support the organization's quality system within their teams are compliant.
- Supervision of a Risk and Compliance team, including mentoring, crafting development plans and delivering performance reviews.
- Collaborate with the Chief Privacy Officer to protect data subject to data privacy regulations.

Legal, HR:

- Advise Legal, IT, and business leaders on third-party risks related to information technology and make recommendations related to contractual provisions, SLAs, etc. to mitigate identified risks.
- Liaise with other risk management functions (e.g., Legal, Compliance, HR) to ensure compliance with local, state, and federal laws and regulations as they relate to information technology or areas affected by information technology.

Availability varies by region. ©2018 SecureWorks, Inc. All rights reserved.

A Hybrid Emerges

Though these responsibilities are rooted with the CISO, they very much blur the line between technical and business focus. The desire for business acumen, in addition to technical knowledge, has become commonplace with a majority of employers preferring a post-bachelor education ranging from master's degrees in computer science to business and law degrees.

- Bachelor's Degree – 85%
- Master's Degree - 40%
- Doctor of Philosophy - 3%
- Juris Doctor - 2%

For the companies that required a bachelor's only, many of them listed both business and law degrees alongside of security or technical degrees. In fact, business was the largest independent area of study (40 out of 100) by the top F100 security leaders.

What does this tell us? A need for a hybrid skillset that is both rooted in security but has evolved to look at the business and the effects decisions and collaboration have on achieving the ultimate success of the company.

The resulting question is: how do you become a CISO given the evolving preferred skillset? The answer really is based on whether you want to be a security practitioner or a hybrid with both a security background and eye on the business? Remember back to our graduate student example? That failure to evolve and continue to self-education could be detrimental to their aspirations in their professional life. The same thing can apply to someone aspiring to be a CISO who fails to evolve from the technician to the hybrid. It's really easy to have a security issue and get pulled right back into the technical world you know.

The point being, there are two types of CISOs: those that have a strategic balance of technical vs. business risk and those that just have the C in their title. Think of it in this scenario: The Board has asked the CISO of a major firm to present where the greatest areas of risk are for a new expansion. This expansion will entail bringing on new vendors, new applications, new employees, new processes and a lot of unknowns. How would each react?

Technical focused: This CISO would likely focus on limitations. There would be a large focus on technology needs, people needs, the disruption of processes, etc. There would be a discussion about increasing budget to accommodate the changes and calculated tactics to show vulnerabilities. The discussion would likely take a more technical turn than what executive leadership is able to comprehend or need to know; thus, leading to a lack of understanding from the decision makers on what the real risk is and how to mitigate it.

Hybrid: This CISO would likely focus on what we should and shouldn't do from a risk taking perspective. The discussion would focus on each part of the implementation, the potential vulnerabilities the new expansion opens them to, which parts to consider based on the risk to the organization, and the respective departments (HR, IT, Legal,

Availability varies by region. ©2018 SecureWorks, Inc. All rights reserved.

Compliance). The CISO becomes the advisor and works with the decision makers to determine which areas require more investment and which areas they are comfortable with absorbing risk. Thus, enabling the expansion by having the business knowledge and relationships that communicate effectively what executive leadership needs to know and can turn into an actionable plan moving forward.

Granted, this is a very high-level scenario but the point is, it is two different discussions with different outcomes when the CISO is focused on empowering the business and mitigating risk vs. looking at it from a purely technological and investment standpoint.

Stepping outside of your comfort zone is key. Think to yourself, if I want to become a CISO that is both technical and business oriented, who on the business side will provide me with insight that will help me make better future decisions.

Designing your path

So, now you understand a bit more about how the modern CISO is shaping up. You aspire to become a CISO one day and you want to ensure your career is on the right track. But what is the right track? Drop everything and get an M.B.A.? Go to law school? Get more technical? Not necessarily. Chances are there is no perfect answer based on each individual situation; however, there are some key things anyone aspiring to be a CISO can do to develop the necessary skills and relationships in order to stand out from other candidates when the opportunity knocks:

Find an executive sponsor/business ally: Almost everyone has a mentor at work; however, those mentors usually work in the same organization/field that you operate in. Stepping outside of your comfort zone is key. Think to yourself, if I become a CISO that is both technical and business oriented, who on the business side will provide me with insight that will help me make better future decisions by considering all aspects of the business. You may find yourself looking to executive leadership in the C-suite but that's not the only move. Instead, look toward a leader in HR, Legal, Sales, Marketing, Risk Management or another part of the business that a CISO's decisions would impact. Opening these relationships not only expands your knowledge of the business but shows you are looking at things from a big picture. Get to know the board, what motivates them, their decision tendencies, their outlook, etc. Develop business allies at the top of the organization who manage risk (CFO, Legal, risk managers, etc).

Know your business, know what your company is protecting and why: Understand the strategic value of the assets. Don't look at it from a technical standpoint of protecting information but rather what that information does to serve the greater good of the company and clients.

Get versatile: Are you poised to be a business manager or a technologist? If you can't answer both, it's time to build your business/risk management acumen as well as infosec acumen. Some great areas to build are: risk management, resource allocation, strategic prioritization, ability to engage all parts of the business in the security strategy and enforce requirements, budgeting and most of all, leading conversations on security risks as an enterprise risk management issue.

Availability varies by region. ©2018 SecureWorks, Inc. All rights reserved.

Develop your communication skills: CISOs must be capable of reporting to the board, business partners externally, security and IT vendors and other business leaders within the company to advocate for security requirements and budget. Communicating in a way that non-technical leaders can understand and puts issues into perspective for their understanding is key to creating advocates for security considerations. Developing these skills can be done internally or externally through training or for example, getting the CFO in your corner to help you translate security risk mitigation into financial risk mitigation terms.

Communicating in a way that non-technical leaders can understand and puts issues into perspective for their understanding is key to creating advocates for security considerations.

Keep one eye on technology: Thus far, we talked about the need for a greater business acumen; however, make no mistake about it, staying on top of how companies are organizing for security practices is still just as important. Know about the latest threat intelligence, government intervention, development of technologies for prevention and defenses are still key to securing your company and client's valuable assets. The goal is not to shift entirely away from a technical focus but to develop the business skillset that complements that technical acumen to make security decisions based on business need.

Conclusion

If you take one thing away from reading this paper, it's to do things that take you out of your comfort zone. You have to be versatile and develop advocates for your cause. Remember when you got your bachelor's degree and you couldn't understand why you had to take astronomy, sociology or a bunch of other classes that were unrelated to your primary focus? Think of this as much the same. You will be required to know many areas of the business and make decisions while looking at the big picture in order to mitigate risk. For those areas of strength it will come easy. For areas of weakness you will need those relationships and background in the very things you will have to consider when communicating to executive leadership.

Understand that the modern day CISO role may not be for everyone. Before embarking on the journey, ask yourself if you like being out front, taking risks and being forward facing in the business. If not, the CISO role may not be for you, and you may prefer to be the technologist – for which there will continue to be a very strong demand as the sophistication of defenses strives to keep pace with the sophistication of the adversaries. If this sounds like a journey you are willing to take, remember developing this discipline takes time. It will require taking chances and maybe even job roles along the way that you never thought of. Just keep in mind that all mountains have many routes to the top. How you get there and your ability to stay there is up to you.

Source:

[1-2] Digital Guardian, The Anatomy of a CISO: A Breakdown of Today's Top Security Leaders

Availability varies by region. ©2018 SecureWorks, Inc. All rights reserved.

Secureworks®

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

We combine visibility from thousands of clients, 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 clients 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
www.secureworks.fr

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
UK House, 180 Oxford St
London W1D 1NN
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

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
www.secureworks.com.au

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

Availability varies by region. ©2018 SecureWorks, Inc. All rights reserved.