SECURE|ANCHOR

DO YOU KNOW CISO?

Everything You Need to Know for a CISO to be Successful

INTRODUCTION

Step back, if you will, into the time machine and travel with me to 1995. We're visiting the graduating class of Anywhere College.

Ask any of them—go on, ask—what he or she plans to be in 20 years.

How many answer "Chief Information Security Officer?" Probably none.

Yet in just 20 short years, in today's volatile business landscape of cybercriminals and information breaches, the role of the CISO has become a vital part of the C-level executive team.

CISOs bear the mantle of preserving privacy and protecting the critical data an organization considers most valuable. They maintain an exhaustive level of scrutiny throughout a company's network. And they provide an enterprise-wide strategy to support the security infrastructure.

These activities are not only crucial, but exciting—such that students today might certainly aspire to take on the role.

And whether you're thinking of hiring a CISO, or you're a CISO yourself, perhaps you're excited too.

Or nervous, or simply confused.

What is a CISO, really? What makes a good one? And how can you make sure that you or a new hire truly succeed in the position?

This ebook aims to clear up those questions and more.

WHAT EXACTLY IS A CISO?

Although we tend to admire our superheroes for the cars they lift with their bare hands or the other-worldly attributes they display, a superhero doesn't need supernatural powers to live up to the name. Some superheroes are simply everyday people.

Such as your typical CISO, for example.

What they lack in the ability to shoot lasers from their eyes, they make up for in the role they play in protecting innocent data, catching adversaries, and being flexible enough (without stretching their limbs beyond belief) to bring even the most reluctant board members together for a common cause.

In today's cybersecurity landscape of information leak and data breaches of monstrous proportions, the CISO is a multidimensional executive who straddles the boundaries of outdated job descriptions, manages data-driven decisions with lightning speed, and does the heavy lifting of developing and implementing an organization's information security strategy.

TECHIE BY DAY, BUSINESS LEADER BY NIGHT

CISOs maintain two identities—technology expert and business leader—and are particularly gifted at succeeding at both.

Some CISOs come out of school with IT backgrounds and spend a career in technology, but increasingly, the CISO's resume includes leadership and business management acumen that provides enhanced value to an organization.

A successful CISO bridges the communication gap between the IT department and the boardroom. He or she is a translator, a conduit of information. Quite often the CISO is also a diplomat—usually during delicate discussions of budget and return on investment.

Communication is key—not just because information is critical, but because unless both parties speak the same language, neither will understand what the other is saying. Security teams often speak "techie," while their peers at the executive table speak "business." This disconnect requires the CISO to be a translator—to take technical data and convert it to strategic business language that execs can understand, and security metrics that can be tracked in the boardroom.

GUARDIAN OF DATA ASSETS

No matter the size of an organization, data flow and information management are critical to a company's success. Sensitive data needs to be protected to ensure a business preserves its reputation and worth.

A CISO has a bird's eye view of accessibility, permissions, and user behaviors throughout an organization. He or she monitors critical systems and keeps tabs on activities or anomalies that might signify a breach.

But one of the CISO's main roles is gathering key security metrics across the organization in order to be proactive in detecting and controlling the damage from potential security breaches.

Why? Here's an eye-opening statistic: 1 in 4 board members admit to "minimal or no knowledge" about cybersecurity—and only another third say they're *"knowledgeable"* or *"very knowledgeable."*

It follows, then, that the CISO's ability to apply the right intelligence to support an overarching security strategy is both an organization's first and last line of defense against cyberadversaries.

“PLAYS WELL WITH OTHERS”

CISOs need to combine their strengths—much like superheroes, if we can revisit the metaphor—with the other members of a boardroom, to support the overall corporate strategy and vision of a company.

The CISO works closely with the CIO on data infrastructure management and IT regulatory compliance. He or she reviews IT security budgets and forecasts with a Chief Financial Officer (CFO). And, of course, a CISO provides the Chief Executive Officer (CEO) with a security strategy that defends the organization from cyberattacks and strengthens its ability to stay agile and in control of its data.

However, since the role of CISO is still evolving, many organizations don’t quite grasp how to fit the position into an existing corporate structure, which can cause political friction or divergence among department heads. The good news is that as the functions of a CISO mature and standardize, organizational issues often subside.

WHAT MAKES A GOOD CISO?

There isn't just one answer—there are many.

A GOOD CISO IS A TECHIE. UNLESS HE OR SHE ISN'T.

Historically, CISOs needed a highly technical background in order to rise through the ranks to take over the reins as a C-level security executive.

Many still do. Gaining a degree in computer science and collecting certifications in CISSP or CISM gives a future CISO a solid foundation of IT expertise. After all, an understanding of security technology – from firewalls to IPSs – forms a critical piece of a CISO's perspective on strategy and policy.

But as the CISO role has evolved to focus more and more on business requirements, CISOs have also come to need a strong understanding of corporate structure and communications.

That means CISOs wear multiple hats, including those of *"relationship-builder"* and *"organizational leader."* A good CISO bridges the gap between technology and business, and needs a resume to support strength in both.

Today's CISO might just as likely have an MBA as an IT degree, or more experience as a manager than a hands-on technical administrator. Either set of experience can help build a foundation for success.

Relationship-building Skills

Organizational Leadership

MBA Degree

IT Expertise

Corporate Structure Understanding

Communications Experience

A GOOD CISO NEEDS TO ANTICIPATE, ASK AND ASSURE.

Who worries about everything that might go wrong?

That's right. The CISO. His or her primary job is to anticipate potential security threats throughout an organization's network infrastructure.

And to succeed here, CISOs must always maintain proper visibility, prioritize continually, and ask the right questions.

Additionally, CISOs must maintain comprehensive risk management practices. They report on potential threats and propose policy to reduce the overall risk levels within the company. That requires regular presentations on security strategy that assure the executive board that everything is under control.

AN EFFECTIVE CISO NEEDS TO ACT “GOOD”—WHILE THINKING “BAD”

How many movies or television shows have you watched that feature a former hacker or cybercriminal reformed and recruited to work with a government agency to track down the REAL bad guys?

I certainly wouldn’t recommend this career path, but life does imitate art in one respect— a good CISO must often think like an adversary to track potential risks.

Employing penetration testing techniques or advanced threat modeling to view an organization from a cybercriminal’s point-of-view allows CISOs to recognize a latent threat before it happens.

And beyond maintaining a tactical focus, CISOs must develop a global perspective on information security, with an eye to issues such as politics, natural disasters, or regulatory compliance.

A GOOD CISO... ALSO NEEDS TO KNOW HOW TO DO EVERYTHING ELSE

Because the role of CISO is an evolving one, there's little agreement across industries on a *"standard"* job description. For this reason, when hiring their first CISO, many organizations look to bring on someone who has already held the title at another company.

At a minimum, a CISO must possess a broad range of executive level characteristics that demonstrate a commitment to leadership, strategy, and forward thinking. He or she must understand how to align technology with business goals, support information technology infrastructure with security policy and protocol, and communicate on progress and risk reduction.

WHAT CHALLENGES DOES A TYPICAL CISO FACE?

A typical CISO is responsible for maintaining enterprise-wide security strategy, educating the organization on protocols, and communicating success to the executives in the boardroom.

Yet as demanding as that sounds, it gets worse—an evolving technology landscape, increasingly sophisticated cybercriminals, and publicly scrutinized security breaches create a plethora of additional challenges for CISOs. Facing any one of these issues on your own would be daunting—but for a CISO, they're all just part of an average work-day.

No matter what trials a CISO faces today, odds are high that tomorrow will bring new challenges, and the critical role of CISO will continue to evolve.

Today's CISO must:

Bridge the gap between technology and business, facilitating communications about security risk and protocol throughout the organization.

Develop a clear and consistent state of security awareness in order to build employee comprehension and compliance and help prevent insider security attacks, whether deliberate or accidental.

Continually transform their approach to security strategy to stay on top of advances in technology—from hardware-based networks to the explosion of the internet to the increasingly common virtual systems invisibly housing company data in the cloud.

Measure and prove the efficacy of their security efforts in the face of varying definitions of risk, fluctuating levels of trust from executive leadership, and little consensus on the basic language of security terms.

COULD SECURE ANCHOR'S CISO SERVICES HELP YOUR ORGANIZATION?

Many organizations now realize a CISO is necessary, but the exact requirements of the role are not clear. That means—if they're hiring—that finding a CISO with enough experience is challenging, and fitting them into the organization can be difficult. And make no mistake: even if there's already a CISO in place (whether that's you, or you want it to be you) the struggle doesn't get easier.

However, the increasing number of public security breaches that damage reputations and rock corporate foundations are creating a ticking clock. Unless there is a capable CISO at the top tier of the business, with accountability for the overall

security strategy, leadership may need to take the fall—like Target CIO Beth Jacob and CEO Gregg Steinhafel did after a damaging security breach in 2014.

This means that executives are increasingly acknowledging the critical need for a CISO in the boardroom—and looking to any and every means to make sure they have the best one in place.

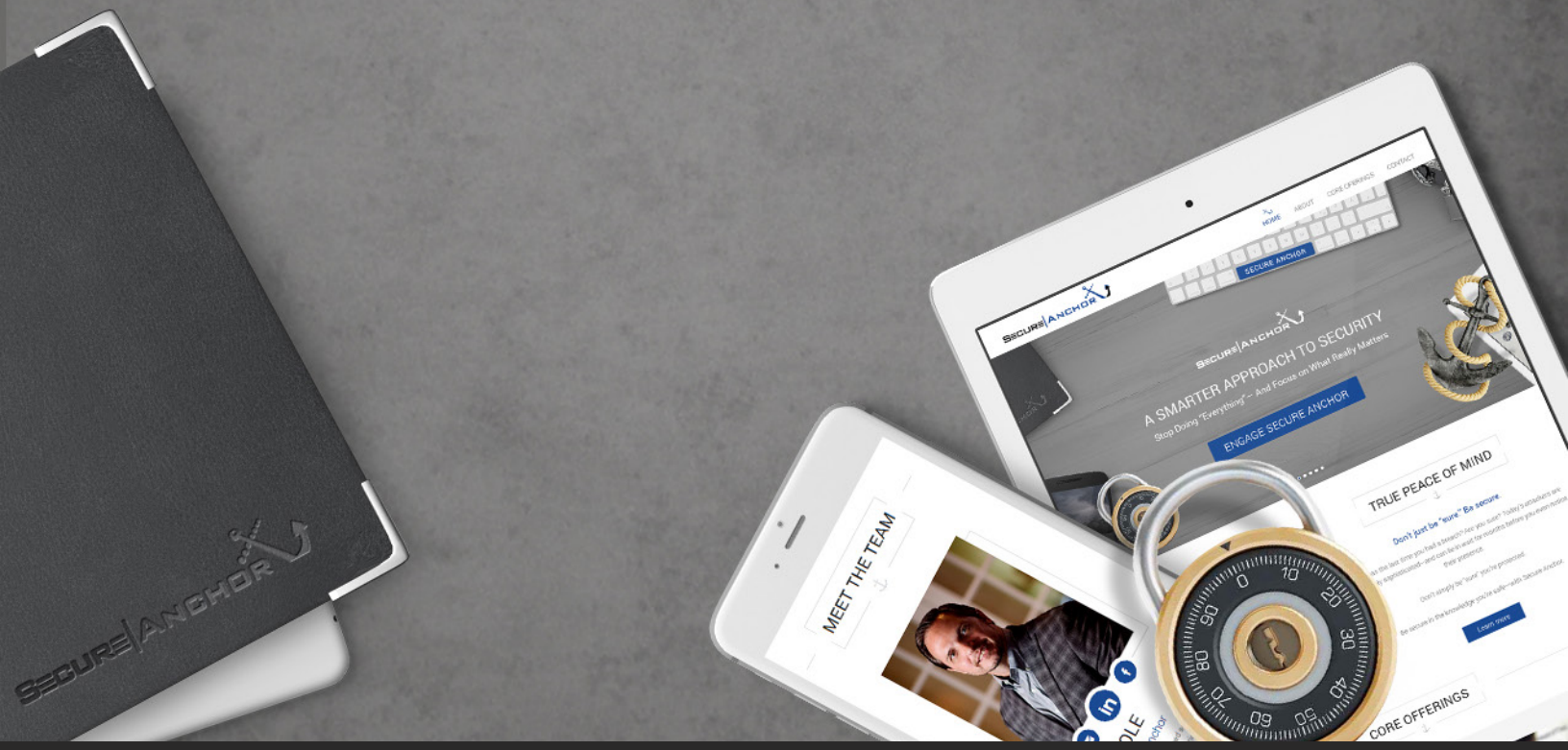
The CISO is now an essential function, and one requiring significant investments and dependable leadership—which means organizations are feeling intense pressure to get it right.

Whether you need a temporary CISO while you recruit a permanent candidate, or you'd like training and coaching to become the best CISO you can be—or even if your organizational budget simply can't afford a full-time hire—we can help.

Schedule a consultation today to learn more about putting our CISO expertise to work for you.

SECURE|ANCHOR

A worldwide leader in information security services for public and private enterprises, Secure Anchor Consulting is well-versed in the latest best practices, experienced in countless *"worst-case"* security scenarios, and well-equipped to transfer knowledge to your own security staff.



SECURE|ANCHOR 703.675.2055 info@secure-anchor.com www.secureanchor.com