Whitepaper

CISO strategy guide:

How security leaders can score more budget and transform their position with a seat at the table

Despite economic challenges, CISOs must ensure they can retain - or even increase - their cybersecurity budgets to improve defenses, while articulating value to an organization's key business goals.

SECURE CODE WARRIOR

aws marketplace

Executive summary

Chief Information Security Officers (CISOs) are operating under immense pressure, in an environment that is increasingly complex, regulated, and litigious. Greater threat sophistication coupled with a sharp increase in the number of attacks has proven an overwhelming challenge for some, especially in the face of a deepening shortage of seasoned security professionals. And all the while, a sluggish economy has resulted in everything – even cybersecurity budgets and personnel – being up for examination and possible cuts.

Despite its critical role in supporting the devices, people and platforms that stand between a company and the myriad of threats arrayed against it, cybersecurity budgets are still mostly seen as cost centers by the majority of C-Suite executives and business leaders. On the other side, many CISOs struggle to dispel this notion with fellow executives or members of the board of directors.

But there is a better approach. Smart CISOs who can align cybersecurity investments with their company's business objectives can turn critical thinking about security away from it being a cost center, and instead, position it as a valuable asset worth considerable ongoing investment. This in turn earns those CISOs more respect, a greater voice in cybersecurity planning, and ultimately a reliable budget despite challenging economic times.

Introduction

Chief Information Security Officers (CISOs) have only recently been elevated to the executive level or C-Suite at an increasing number of companies. The reason behind this newfound elevation of status varies, but the recent string of high-profile cybersecurity incidents like the attacks on the Colonial Pipeline, meat supplier JBS and others that crippled hospitals, infrastructure and businesses in all sectors certainly contributed. Even the supply chain was found to be potentially vulnerable, as the massive SolarWinds breach proved. Spurred to action by that unrelenting string of bad news, many firms decided it was a good idea to bring their top cybersecurity official into the fold for more high-level discussions and planning.

And on the whole, this has been a good thing for both companies and their often underappreciated CISOs. Recent surveys have shown that up to 80% of C-level executives now consider advanced cybersecurity programs like zero-trust to be a priority for their organizations, whereas, in the not-so-distant past, security might not even be considered at the board level, where the focus has always been highly targeted on business objectives and profit. Having a CISO present at all relevant planning sessions and meetings will certainly serve to keep cybersecurity top of mind – if a CISO makes the most of these new opportunities.

80%

of C-level executives now consider advanced cybersecurity programs like zero-trust to be a priority for their organizations

While it would be fantastic to say that elevating CISOs to a greater position of authority and responsibility is a fix for all security problems, that is sadly not the case. Giving CISOs a seat at the table when planning the direction of a firm is a good thing, but unfortunately, it's neither a fairytale ending nor the conclusion of the story. In fact, it may be a double-edged sword for many CISOs who now have more authority on paper, but diminished cybersecurity spending power. They have an advanced threat landscape to contend with, long-standing personnel shortages, new legal reporting requirements and a board that – despite the recent changes in organizational structures – may still see the CISO as more of a rank-and-file IT employee instead of a true executive.

It will be up to talented CISOs to overcome these challenges, and pioneer a viable path forward to secure the influence, recognition and funding they need to keep the companies they serve safe in an increasingly hostile digital world.

Modern CISO challenges

The job of a CISO has never been easy. There has always been a struggle between defenders trying to keep their company's data, employees and infrastructure safe, versus the increasingly sophisticated, well-funded and motivated attackers attempting to exploit and disrupt on a wide scale. It takes skill, time and money to keep these relentless attackers at bay, and that job is only getting tougher.

The latest Verizon Data Breach Investigations Report for 2022 spotlights a threat landscape that is more dangerous than at any other point in time. The CrowdStrike 2022 Global Threat Report illustrates a similarly concerning picture, highlighting an 82% increase in ransomware and other attacks compared with last year. And those attacks are costly, too. The recent Cost of a Data Breach Report from IBM and the Ponemon Institute puts cleanup expenses after a cybersecurity breach at an average of $3.8 million per incident.

Even the companies that an organization works with, links in the so-called software supply chain, have become a treacherous potential risk factor that every CISO must consider. Recent research in this area found that many successful cyberattacks these days, 44% to be precise, were first introduced to protected networks through a supply chain that originated outside of a breached organization's direct control. Like other cyber incidents directly involving a company, supply chain attacks can be defended against and ultimately thwarted, but it takes funding and trained security personnel, both of which tend to be in limited supply in even the most advanced organization.

The CrowdStrike 2022 Global Threat Report highlights an **82% increase in ransomware and other attacks compared with last year.**

Another point of consideration is recent movements in US policy, with the new National Cybersecurity Strategy focusing heavily on enterprise accountability for software security, putting software creators on notice. There will be increased scrutiny, and, ultimately, liability in the event that low-quality, vulnerable software sees the light of day.

Fears of a recession, or at least an economic downturn, are also being felt around the world. High-profile layoffs have been announced or completed at top firms including Amazon, Goldman Sachs, Microsoft, Salesforce and many others. And while cutting cybersecurity personnel or pulling back on security program funding may seem reckless given the nature of the threat landscape, the truth is that if the economy continues to get worse, nothing, not even cybersecurity budgets and specialist staff, will be fully protected from the chopping block. If the board only sees cybersecurity spending as a cost center, then budget cuts will eventually find their way there despite its criticality. And that is just one more problem for a modern CISO to face.

One final factor that CISOs will also absolutely need to consider is their level of personal responsibility, and even the potential for legal jeopardy, should the worst happen. CISOs may now have a seat on the board, but that new position of power and influence comes with increased responsibilities. For example, The Strengthening American Cybersecurity Act of 2022, which recently became law, requires reporting of cyber incidents within 72 hours. The Act only applies to critical infrastructure providers, but could be a blueprint for further legislation. Even without specific new laws, the recent conviction of the CISO of Uber for his actions following a security breach clearly demonstrates that CISOs can be held accountable for the choices they make while performing their jobs.

The top CISOs may even see their budgets increase – if they can **clearly tie cybersecurity protections to business objectives.**

It's clear that CISOs, even with their newfound respect and power, will have much to deal with in the coming years. But despite numerous difficulties, at Secure Code Warrior, we believe that the most talented CISOs will not just survive mounting hardship, but can actually thrive. The top CISOs may even see their budgets increase – if they can clearly tie cybersecurity protections to business objectives.

Four ways CISOs can earn budget increases and improve cybersecurity

Learn to speak the language of executives

Having a CISO on a board of directors is a relatively new concept, and other C-Suite executives may not at first know how best to interact with their new colleague. Many CISOs have reported that even after getting a seat on the board, they are still looked at as an IT support person and not a true executive. In fact, the 2021 Global Chief Information Security Officer Survey from executive search firm Heidrick and Struggles found that even with their newfound respect and positions, only 11% of CISOs report directly to their company's CEO. Another 38% reported to the CIO, while the rest were buried somewhere farther down in a company's hierarchy.

What newly empowered CISOs need to realize is that their fellow executives are probably not IT specialists. Chances are, their core expertise will sit outside of the inner workings of cybersecurity. Talking with them about concepts like zero trust, software-defined networking, hybrid cloud computing and other technical terms that roll off the tongue when speaking with the IT staff will likely not be fully appreciated by other board members.

Instead, CISOs should focus on the value of IT and cybersecurity programs, such as how they can assist with a company's growth by facilitating safe expansion into new markets, or serve their customers more efficiently and with less risk.

In other words, CISOs should highlight with other executives core general topics like explaining why cybersecurity programs will help add value to the organization, and leave the deep technical details to discussions with their IT staff. In fact, according to Gartner, over 30% of a CISO's effectiveness will be directly measured against their ability to create value for their businesses in 2023. CISOs should keep this in mind, and at least consider the value of security programs in everything they do.

Merge cybersecurity goals with business objectives

Another factor that works against CISOs when trying to increase their budgets is the fact that cybersecurity programs are often seen as cost centers. Most executives acknowledge that security programs are a must-have in order to protect operations, but may pause at the suggestion of pouring more money into those programs or expanding them. Yes, in the age of digital-first business, it is required, but surely there is little need to spend money beyond what is necessary for basic protections, since those costs are never recovered.

It may be unfair, but the thinking is that cybersecurity spending is different compared to when investing in, say, a new division, store or office. With a physical or business-type investment, the thinking is that there will be a large outlay of initial costs, but that the new division or entity will eventually start making money and provide a return on investment – something that raw cybersecurity spending never does.

So, how can a CISO overcome the idea that cybersecurity spending is a sunk cost? **The key is to align cybersecurity goals with core business objectives.**

So, how can a CISO overcome the idea that cybersecurity spending is a sunk cost? The key is to align cybersecurity goals with core business objectives.

To accomplish that, CISOs must look at their company's overall objectives and the areas the board sees as their organization's greatest strengths. For example, a company might pride itself on having a robust online store where users can purchase specialty products from around the world. A clever CISO could then demonstrate how a certain cybersecurity platform or goal could serve to seamlessly protect all of those transactions, as well as the underlying infrastructure. They could suggest that once such a security program is implemented, the company could market its new, higher level of security to new customers, who will feel safe knowing that their personal and financial data is protected as they interact with the online storefront.

Looping back to the idea of expanding a business into a new area, in that example a CISO could show that higher levels of cybersecurity would be attractive to new customers, perhaps making them more likely to switch over to the new store or office from competitors that offer weaker security protections. That in turn could help the new division turn a profit sooner by merging cybersecurity with business objectives.

It is critical that the modern CISO takes the time to highlight the competitive advantages of security strategy and policy as it relates to ongoing positive customer sentiment and trust; reactive security alone won't have the same impact, and a balanced approach that focuses on protecting privileged assets with every available resource - which may require additional support - can be the ultimate differentiator in the hearts of the consumer.

Leave fearmongering in the past

In the not-so-distant past, CISOs could sometimes get their budgets increased by pointing to the debilitatingly high costs of security breaches. And when CISOs were considered outsiders to the C-Suite, pointing to all the terrible things that could happen in the event of a breach got the attention of the board of directors, who likely increased cybersecurity spending in order to avoid those negative outcomes. While sowing fear, uncertainty and doubt (FUD) could work to get cybersecurity budgets beefed up year after year, it also cemented security as a sunk cost in the minds of many executives – something that CISOs must now combat.

It's true that the costs associated with a cybersecurity incident have continued to increase in recent years. However, many CISOs hold more influence in the boardroom these days, so those old FUD tactics are no longer viable, especially if they serve to distance cybersecurity from business objectives.

Smart CISOs are learning to accentuate the positive aspects of cybersecurity spending. **This includes being able to foster trust and loyalty among customers.**

Of course, CISOs should keep the negative aspects of a cybersecurity breach in mind, however, this should no longer be the sole focus of cybersecurity discussions. Instead, smart CISOs are learning to accentuate the positive aspects of cybersecurity spending. This includes being able to foster trust and loyalty among customers, and even positioning security as part of the brand vision; a key differentiator that can be promoted as a way to improve market share against competitors who don't take cybersecurity as seriously.

Even talking about security breaches should be done in a positive way. For example, instead of lamenting how much a potential breach would cost the company, a CISO should instead explain how avoiding security incidents can have a positive effect and contribute to supporting core business objectives. In this way, CISOs can achieve long-term support for their ongoing, more integrated cybersecurity efforts.

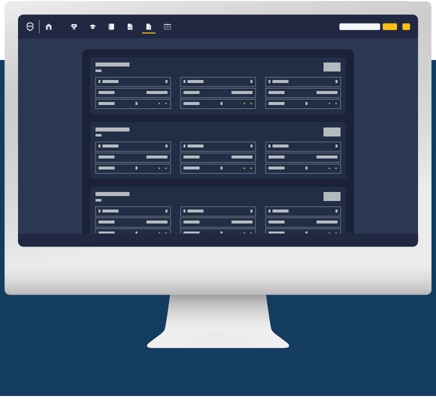
Embrace the magic of holistic, early-stage cybersecurity measures

The primary goal of a CISO is to protect their organization from cyber threats, and in the quest to reveal the value of a comprehensive security program to the wider organization, demonstrating an honest attempt at utilizing every resource to its full potential cannot be underestimated.

Security awareness training is becoming a mainstay of most businesses, and is increasingly rolled out to every person on staff. While this can be a regulatory requirement in some verticals, it does help to elevate the importance of security best practices in the minds of everyone from the sales team, right through to more technical roles. However, what can be missing in a truly transformational, security-first approach to software creation - as is called for in the National Cybersecurity Strategy, no less - is comprehensive upskilling of the development team.

In many scenarios, prevention is easier than cure, and cybersecurity is no different. A holistic security program must extend well beyond reactive measures, and with vulnerability management among the top three considerations for many CISOs, it makes sense that developers are indispensable allies in the pursuit of a cleaner, more secure codebase. However, they need hands-on education to tackle common security bugs head-on, helping them eliminate these issues at the source and ensure they never make it to production in the first place. We're now at the point where we cannot keep excusing low-quality, insecure code, and upskilling the development cohort is by far the most cost-effective, potent remedy for code-level vulnerabilities.

> In many scenarios, prevention is easier than cure, and cybersecurity is no different. **A holistic security program must extend well beyond reactive measures**



It is vital that CISOs fight to retain (or, even grow) existing budget, and detailing the benefits of role-based security upskilling, especially for developers, is a quicker win than adding the next "silver bullet" to an unwieldy security tech stack and hoping it will stem the flow of recurrent vulnerabilities without slowing production to a crawl. It's the sign of a more mature, developer-focused security program that is attempting to put threat actors on notice and stop exploitable issues at the source.

The modern CISO must clearly demonstrate to their fellow executives the direct correlation between better, more mature cybersecurity and increased revenue, market share, or other key business objectives. While it will take time and money up-front to train a development workforce to a state of viable security prowess, this eventually alleviates pressure on worn-out security teams, reduces the impact of skills shortages, and is the best possible chance at achieving consistent security at the speed of delivery.

Conclusion

CISOs who finally earn a spot in the C-Suite of their company or organization will certainly want to celebrate. Many CISOs have complained for years that their constant warnings about cyber threats great and small, as well as their requests for higher budgets, have largely been ignored or truncated. Now, having a spot on the board gives them direct access to company planning, and ensures that their voice is finally heard.

However, achieving that objective can be akin to the dog who, after years of chasing cars, finally catches one. The question becomes one of what to do next.

CISOs may have to work just as hard to ensure that their new executive colleagues understand their concerns, and come to see how increased support for cybersecurity can positively contribute to a company's overall business objectives. That is what the most talented CISOs are already doing, and what will ensure that CISOs are forever thought of as true C-Suite or board-level executives who positively contribute to their organization's bottom line and core business objectives.

CISOs may have to work just as hard to ensure that their new executive colleagues understand their concerns, **and come to see how increased support for cybersecurity can positively contribute to a company's overall business objectives.**

Want to know more about how you can ignite a passion for security in your developers? Please visit Secure Code Warrior to learn how we can help your organization embrace secure coding best practices that reach far beyond the basics.

About Secure Code Warrior

Smarter, faster secure coding

Secure Code Warrior builds a culture of security-driven developers by giving them the skills to code securely. Our flagship Learning Platform delivers relevant skills-based pathways, hands-on missions, and contextual tools for developers to rapidly learn, build, and apply their skills to write secure code at speed.

Established in 2015, Secure Code Warrior has become a critical component for over 500 enterprises including leading financial services, retail and global technology companies across the world.

Request a demo

Try Secure Code Warrior for Free

SECURE
CODE
WARRIOR

securecodewarrior.com

aws marketplace