5 Key Ways

CISOs Can Accelerate the Business

splunk> turn data into doing™

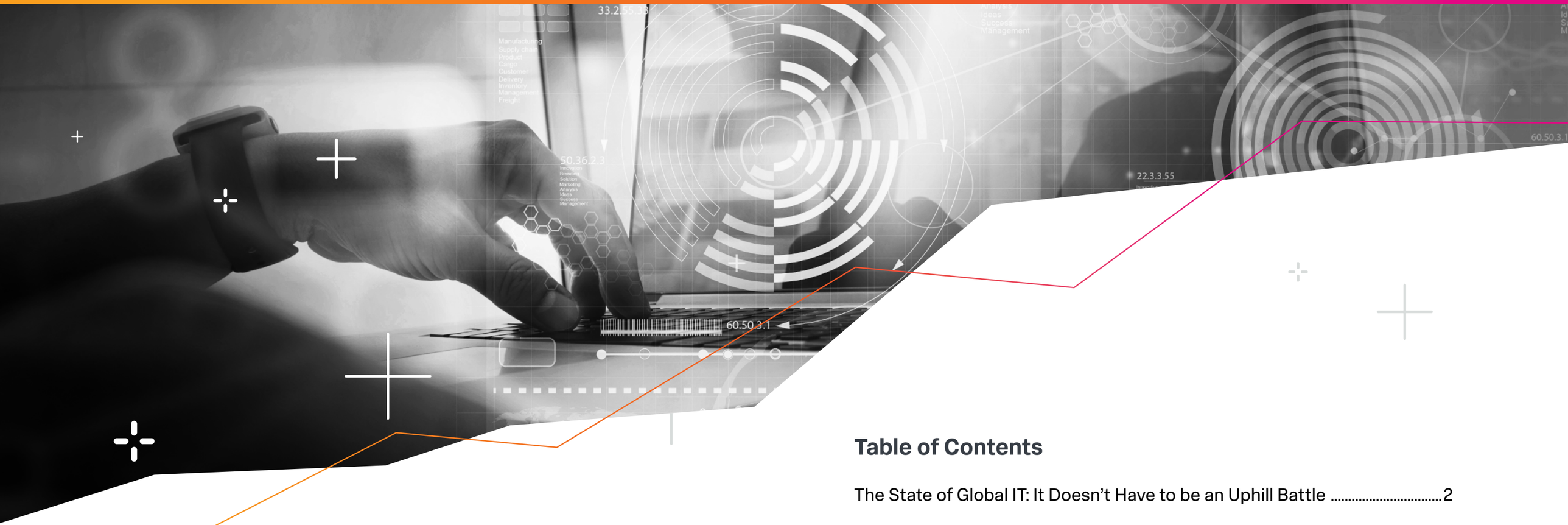


Table of Contents

5 Key Ways CISOs Can Accelerate the Business

Now more than ever, chief information security officers (CISOs) are expected to weigh in on board-level decisions. In an increasingly competitive landscape, business acumen has become just as important as technical know-how, and executives rely on the CISO to map security programs to business objectives to promote growth and generate revenue.

In a report conducted by Forrester, CISOs are encouraged to align security with the enterprise, as well as juggle key innovations and manage the skills gap. Here are five best practices to up-level the business and give the board exactly what they want — a superstar CISO.

01

Understand How
the CISO Role Has Evolved

In the past, CISOs were expected to spearhead their company's security strategy. They gave little thought to profit margins, and if a breach occurred or vulnerability was found, the response was to fix the system rather than fix the business. But times have changed, and the CISO has since become a business role as much as a technical one, with the focus shifting from reactive security measures and technologies to cost-benefit analysis and risk management.

Now, CISOs need to create value, as well as increase revenue, engage customers and drive double-digit growth. They're expected to increase the velocity of business operations (e.g., moving products or experiences quickly and securely to market) to gain a competitive edge and increase profits, as well as minimize risk and any associated monetary loss — or worse yet — damage to brand reputation.

Finally, the board expects the CISO to see security from their point of view, and to communicate and manage cybersecurity along with a long list of other demands (see: digital transformation). According to Forrester, "Security leaders must also add personalization, virtual assistants, edge computing, external API services, and digital process automation to the list of technologies their teams understand."* In essence, a CISO must act as trusted advisor across a number of channels, effectively communicating risk in terms the board understands, so they can swiftly and securely execute on what's best for the business.

02

Know Your Boards Business Needs

Cybersecurity used to be considered part of IT — therefore too technical for executives to understand. On the flipside, CISOs had little knowledge of financial risk, and could rarely answer questions about the bottom line. Yet the board now expects CISOs to be a part of these discussions and to have a seat at the proverbial table. As a result, CISOs need to understand what drives growth and how to speak "security" in practical, real-world terms that the board can understand.

Most executives don't have a technical background. They won't understand the difference between something like "command and control" and "network lateral movement," or might feel intimidated by the intricacies of cybersecurity, especially when conversations consist of tech-speak and manufactured security presentations.

That's why it's critical for the CISO to find common ground with the rest of the C-Suite. To do this, they need to get to the bottom of what the board is concerned with, conveying the value of cybersecurity in metrics the board understands, like time and money saved and incidents prevented. Don't delve into tools deployed or applications tested. They want to see the impact security has had on the business itself — not just how you improved things on an operational level.

Finally, to better prioritize the board's goals, figure out how revenue flows in and out of the organization, and what could potentially jeopardize this (e.g., website downtime for a major retailer). Once you've started to ask these types of questions, you can begin to map initiatives to what's top of mind.

03

Embed Security Into Your Business Strategy

When tasked with a new project, CISOs need to address security from the beginning and then test it through development. Building security into the development process establishes trust with the customer, promotes sales and gets products to market faster, therefore driving revenue. Incorporating security into project and business planning also helps mitigate risk, especially when working in agile environments with short release cycles.

According to Forrester, **"Security strategies that lack alignment miss the chance to insert Security by Design into the earlier stages of the innovation cycle, slowing the firm's plans to tackle large-scale disruption."** Security by Design (SbD) takes a holistic, forward-looking approach to security, versus a retroactive one that only enforces security policies as and when incidents occur (potentially risking downtime and monetary loss).

Thanks to SbD, security professionals can bake security into every stage of the development process, so they can engineer and design the infrastructure from the ground up, as well as automate security controls. In turn, this means CISOs no longer need to be consulted on each and every infrastructure change — meaning less repetition and busy work, and more time to focus on high-level issues.

04

Create a Strategic Roadmap

Roadmaps are hugely beneficial when it comes to long-term planning. They provide a framework for forecasting and coordinating technical developments, effectively mapping security initiatives and solutions to long-term business goals.

First, a strategic plan should assess the current state of security, and outline goals for the next 12 months, midterm goals over 18–24 months, and finally, long-range goals over 36 months. At a high level, the program should verify the mission, vision and goals of the business — that way the CISO can identify where to focus his or her efforts. Not only does this strengthen downstream execution, but this also helps improve overall risk management, preempting potential lapses and lags in technology.

Once a top-level view has been established, the CISO can look at security on a more granular basis, including the company's approach to external and internal threats, data privacy and the integration of cybersecurity as a best practice for day-to-day operations.

Finally, goals should continue to be updated as and when projects are completed, and the CISO should reassess initiatives depending on the organization's needs as well as an evolving technology stack.

05

Determine How Security Solutions Can Help

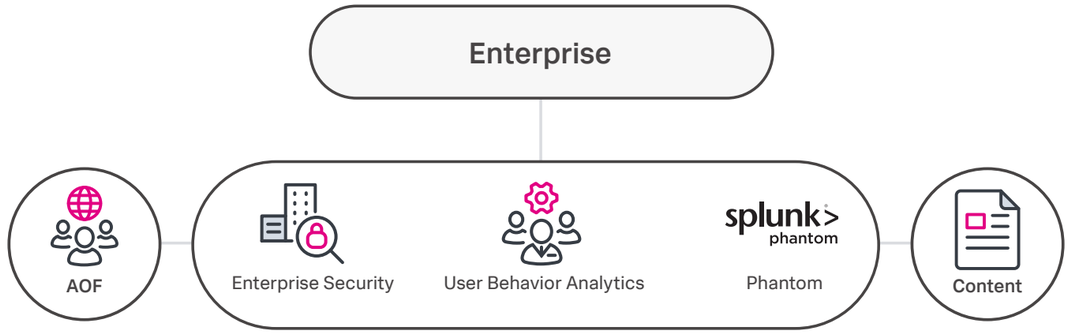
So how exactly can a CISO align security with their organization's business objectives? Especially when they're so busy? Not only do they have to manage up to the board of directors, but also across the rest of the organization — providing solutions, maintaining the status quo and empowering staff where they can. The CISO can hardly do it all, especially when there's a distinct shortage of talent and lack of support. The reality is that there simply aren't enough skilled professionals to analyze the volume of incidents that most organizations face daily.

What the CISO needs is a powerful platform that can ensure security and brand reputation won't be compromised — they need a scalable, overarching security solution. A solution that helps security teams and CISOs better identify important assets or data points within the business, as well as breakdown silos, streamline workflows, and have a global view across IT and security ecosystems. Now, you can automate repetitive tasks to force multiply your team's efforts, and better focus your attention on mission-critical decisions.

The secret is in the SOS — that is, Splunk's Security Operations Suite.

Splunk's Security Operations Suite modernizes security operations and reduces exposure to risk. Our security suite — including market-leading SIEM, UEBA and SOAR solutions — can help improve your cyber defense while accelerating threat management and scaling your security operations.

Find out more about how our security solution can help improve and accelerate your operations, including your organization's security posture.



Get started.

Find out how Splunk's Security Operations Suite can help you on your security journey.

2020-Splunk-SEC-5-Key-Ways-CISOs-Can-Accelerate-the-Business-106-EB

splunk> turn data into doing™