stratascale
An SHI Company

DIGITAL COMPASS.

Your Go-To Resource for Navigating the Ever-Changing World of Technology

Security as a Business Strategy

Thinking Beyond Compliance

Page 4

Three Ways to Position the Value of Cyber to the Board

Page 8

To Build or To Buy a SOC? That is The Question

Page 18

Editor's Note

Effective cybersecurity goes beyond merely protecting a company's key assets; it involves managing strategic risks, safeguarding financial and reputational assets, and integrating cybersecurity into the overall business strategy. Strong cybersecurity practices allow company leaders and boards of directors to meet their governance responsibilities while securing the organization's long-term resilience and success.

We must realize that the significance of cybersecurity extends far beyond protecting assets-it's about managing strategic risks, safeguarding financial and reputational interests, and embedding cybersecurity into business strategy. Effective cybersecurity practices empower leaders and boards to meet their governance responsibilities while ensuring the organization's long-term resilience and success.

Adopting a proactive approach to cybersecurity transforms it from a mere defensive approach into a strategic asset that supports overall business goals and resilience. This shift not only strengthens the organization's security posture but also enhances its competitive edge by:

Aligning Cybersecurity with Business Objectives: Integrating cybersecurity strategies with broader business goals ensures that security measures contribute to the company's success. For example, protecting customer data builds trust and loyalty, directly impacting revenue and market reputation.

Enhancing Resilience: A proactive stance enables organizations to anticipate and mitigate potential threats before they materialize. This foresight reduces downtime, protects critical assets, and ensures business continuity even during cyber incidents.

By integrating these elements, companies can ensure that cybersecurity is not just a protective measure but a strategic component that enhances business performance and resilience. Building a robust cybersecurity program involves selecting appropriate tools tailored to organizational needs, considering business continuity, overall strategy, and future-proofing. Tailoring security solutions ensures they support rather than hinder operations. While consolidating tools and vendor lock-in can offer efficiency and cost savings, they may introduce security gaps and integration issues, limiting flexibility and innovation. Addressing current security needs while planning for future challenges requires a balanced approach.

Kendra Perry
Manager of Emerging Technology
kendra_perry@stratascale.com

CONTENTS

Thinking Beyond Compliance: Security as a Business Strategy

Aligning Compliance & Security Strategies to Reduce Enterprise Risk

Tom Costin
Principal Security Consultant
tom_costin@stratascale.com

Dennis Allen
Director of Security Programs
dennis_allen@stratascale.com

While a critical foundation of strong security strategy, compliance is just the tip of the spear. To truly minimize enterprise risk and become a security-focused organization, it's critical to think beyond compliance.

The Reality of Compliance

Compliance creates a minimally viable standard. A compliant organization is not necessarily a secure one. And vice versa.

Regulations and laws are specifically designed to be broad enough to accommodate a variety of organizations. This means they don't necessarily account for organization-specific data, third party cyber risks, and business continuity plans.

Additionally, regulations and requirements are often behind technology trends, and consumer demands. Becoming proactive against threats requires thinking beyond checkboxes and baseline requirements. Compliance can serve as a foundation to reach a more mature level of enterprise security. The key is aligning compliance to broader security efforts and integrating measures, practices, and policies. In doing so, compliance and security can work together to reduce enterprise risk.

Aligning Compliance & Security to Business Strategy

Aligning compliance and security strategies to broader business goals is critical to minimize enterprise risk. This integration helps organizations build trust with their stakeholders, improve brand reputation, and increase operational efficiency. Which, ultimately, demonstrates a commitment to risk management.

> Here are three steps organizations can take to start aligning compliance and security to broader business strategies:

01

Risk Quantification

Calculating the financial impact of compliance measures and understanding how they influence an organization's risk profile is a great place to start.

There is an inherent risk in non-compliance, which generally manifests as fines, loss of contracts, or other business repercussions. Compliance frameworks do not directly target cyber threats; their primary intent is often to reduce exposure to such threats. However, the business imperative for compliance frequently stems from the necessity to avoid fines and fulfill mandatory requirements.

Quantification aims to identify the potential financial impact of non-compliance compared to the cost of implementing controls. Similarly, the costs associated with data loss, exposure, downtime, and other security incidents must be weighed against the expense of implementing preventative security controls. By putting hard dollars and cents around the impact of compliance on security, leaders can get buy-in and adoption from the business.

02

Control-Based Approach

Organizations often need to comply with multiple frameworks, such as HIPAA, NIST, and ISO standards. By mapping these frameworks to a common set of controls, organizations can streamline their compliance efforts. Many frameworks have overlapping requirements, a controls-based approach allows organizations to test and measure controls once and apply the results to multiple frameworks, reducing effort and ensuring comprehensive compliance. Furthermore, adopting a control-based approach is essential for maturing from a reactive, point-in-time compliance program to a proactive, continuous monitoring posture, which is crucial for most organizations.

03

Cross-Functional Collaboration

To effectively manage enterprise risk, not only should compliance and security leaders collaborate closely but also work cross-functionally with stakeholders from across the business, including legal for compliance, procurement for vendor risk, IT control owners, and business stakeholders who make risk decisions.

By integrating security risk management into broader enterprise risk programs, organizations can ensure a unified approach. This collaboration helps align compliance and security efforts with overall business objectives, ensuring that all measures support the organization's strategic goals.

Ensuring compliance is a crucial starting point for any organization. By understanding and meeting compliance requirements, organizations lay a solid foundation for more advanced security measures. Ultimately, a holistic approach that incorporates compliance and proactive security ensures regulatory adherence while strengthening the overall risk posture of the organization.

Three Ways to Position the Value of Cyber to the Board

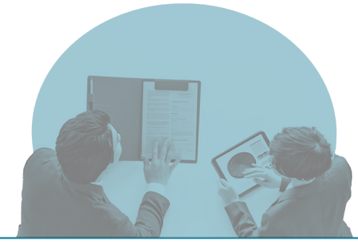
Cybersecurity is often seen as a necessary evil, and something that board members know they must invest in, but it's not something they get excited about. Positioning the value requires shifting mindsets and culture. So, how do you get a board to care about cyber like their bottom line depends on it? (Spoiler alert: it does!) You craft a compelling narrative that aligns with business objectives and demonstrates tangible value. ***Here are three ways to do that.***

Alex Banghart
Research Analyst
alex_banghart@stratascale.com

01 Tell Your Cybersecurity Story

Cohesive Narrative

Imagine, your company's journey through the digital wild west. It's not a dry report, it's an epic adventure in problem solving. Remember that time we narrowly avoided a data breach that could've cost us millions? ***Paint that picture. Make it vivid.*** It's like telling the tale of your greatest escape, but with data. They need to see the drama, the stakes, and the heroics.



Board-Level Reporting

And let's get real about reporting. ***Ditch the jargon and tech-speak.*** Executives want high-level insights, not the technical details. Think of it as translating from geek to sleek. Use visuals—graphs, charts, whatever makes the information pop and ties back to the ROI. It's not just about what you say, it's about how you present it. Keep it sharp, keep it engaging.

Talk Business

Now, for the decisive factor—business impact. If our cybersecurity efforts fail, what happens? Lost data, lost revenue, regulatory fines, and a big dent in reputation. ***Frame it in terms of potential disaster scenarios.*** When you put it in their language, they'll see why it matters. It's not fearmongering; it's reality-checking.

02

Quantify Risk (Talk Money)

Utilize Metrics the Board Understands

Boards live and breathe metrics, so *talk their language.* Convert cyber risks into financial terms they grasp. Potential revenue loss from a breach, cost of downtime—spell it out. Suddenly, it's not just about bits and bytes; it's about dollars and cents.

Talk About Exposure & Risk Drivers

Identify those risk drivers and lay them out. External threats, internal vulnerabilities, whatever keeps you up at night. *Make the board understand exactly what we're up against.* It's like showing them the monsters under the bed. Only these monsters are real, and they've got teeth.

Frame Conversations Around Revenue

Here's a twist: don't just talk about loss. Highlight how robust cybersecurity protects revenue streams. Show them the money saved and opportunities seized because our defenses held firm. *It's about turning a potential negative into a clear, tangible positive.*

03

Showcase Your ROI & Business Alignment

Show How Cyber Can Be a Driver of Revenue

Cybersecurity isn't just a shield; it's a spear. Show how strong cyber practices can drive revenue. Think compliance certifications that open new markets, or robust defenses that build customer trust. *Highlight success stories where cyber strength led to business wins.*

Shift the Cost-Center Mindset

Finally, break the cost-center mentality. Cybersecurity isn't a drain on resources; it's a strategic investment. Show how it reduces operational risks, enhances resilience, and yes, contributes to the bottom line. *Shift their thinking from "necessary evil" to "competitive advantage."*

Enable Other Business

Cyber is the unsung hero behind every successful business unit. Protecting intellectual property, securing customer data, ensuring service availability—it's all interconnected. *Highlight collaborations where cybersecurity made a crucial impact.* Make it clear that cyber is the backbone of business innovation.

In the end, it's about weaving a compelling narrative, speaking the board's financial language, and highlighting the strategic value of cybersecurity. Make it personal, make it relevant, and make it profitable. That's how you get the board to not just listen, but to champion the cause of cybersecurity.

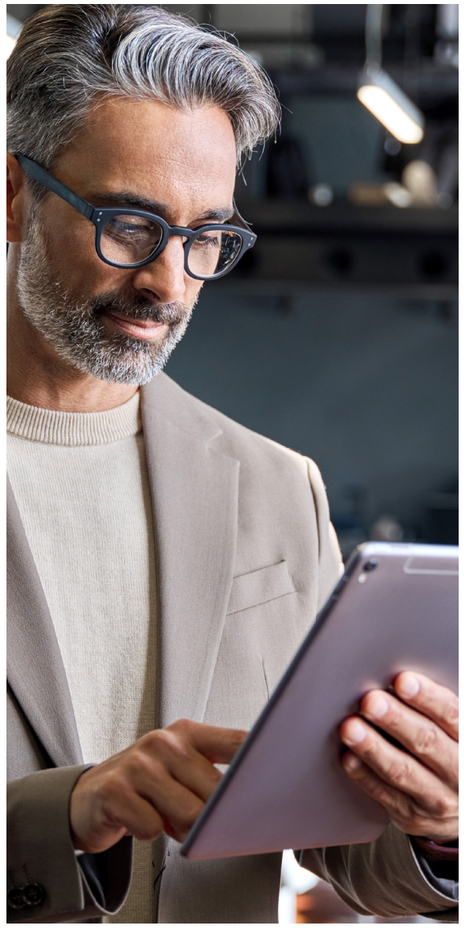
Deep Dive:

The Modern Security Operations Center (SOC)

Beau Ray
Technical Advisor
beau_ray@stratascale.com

What keeps a CISO up at night?

Cybersecurity threats continue to grow in complexity and frequency. Security professionals are bombarded daily with news of new vulnerabilities, breaches, or ransomware attacks, needing to mitigate as many of these threats as possible. This seemingly never-ending cycle of cybersecurity risk leaves most cybersecurity professionals and security stakeholders wondering where the next attack will come from and how it will affect their organization. This constant state of firefighting drives current efforts in modernizing security operations.



The Need for Modernization

When considering security operations center (SOC) modernization, there are many different considerations. Gone are the days of relying solely on an army of analysts sifting through a deluge of alerts and log files. The current state of cyber defense is no longer just about servers and desktops. We must consider everything, including IoT devices and remote employees working from home on unsecured broadband connections. Edge computing management is no longer just about firewalls and switches; we now must consider cloud computing and software platforms as well. All of this leaves every security professional wondering, “How can we possibly protect all of this?”

A Ray of Hope: The Modern SOC

Don’t worry, there is light at the end of the tunnel. That shining light saving you from a state of constant cyber fear is the modern SOC. But what is a modern SOC? There is no specific definition, as it depends on the organization the SOC serves. This allows for many ways to think about the modern SOC and many different models for how it should operate to meet your organization’s needs.

Defining the Modern SOC: The Three Pillars Approach

One way to approach modernization is to conceptualize your modern SOC through three pillars: Proactive Threat Defense, Strategic Security Management, and Centralized Cyber Defense. While separate groups can execute these outcomes, it is more effective to think of these three areas as an integrated strategy. Each pillar has a distinct mandate, with some overlap, to execute a clear roadmap for modernizing security operations.

The Three Pillar Approach

Proactive Threat Defense:

Focuses on anticipating and neutralizing threats before they impact the organization. Leveraging AI and machine learning for advanced threat detection, continuous red-teaming exercises, and utilizing threat intelligence to stay ahead of emerging threats are key components.

Strategic Security Management:

This pillar ensures that the SOC’s activities align with the organization’s overall security strategy. It involves integrating existing and new technologies, driving continuous improvement, overseeing governance and compliance efforts, and operationalizing a proactive approach to neutralizing threats.

Centralized Cyber Defense:

It encompasses the integration of advanced tools, a focus on detection and response, and effective incident response. It involves day-to-day operations using processes and technology identified as strategically valuable, reducing overhead, alert fatigue, and burnout.

Key Components of a Modern SOC

Centralized Cybersecurity Command

A modern SOC serves as the nerve center for an organization's cybersecurity operations. By centralizing threat detection, analysis, and response activities, the SOC ensures that security measures are coordinated and comprehensive. This centralized approach enables a holistic view of the organization's security posture, allowing for more effective threat management and quicker response times.

Continuous, Real-Time Surveillance

One of the defining features of a modern SOC is its ability to provide continuous, real-time surveillance across the organization's entire digital environment. This 24/7 monitoring capability is crucial for early threat detection and swift response. Advanced monitoring tools and technologies, such as SIEM, XDR, and Managed Detection and Response (MDR), are essential.

Integration of Advanced Technology

The modern SOC leverages a range of advanced technologies to enhance its capabilities. Key considerations include Artificial Intelligence (AI), Machine Learning, Automation, Threat Intelligence, Continuous Red-Teaming, CSPM, Continuous Asset Discovery, Security Management, and Identity Security and Posture Management. Emerging technologies in cybersecurity are rapidly evolving, with startups and agile tech companies leading the way with creative ideas, short development cycles, and solid go-to-market plans.

Automation and Artificial Intelligence (AI) are undoubtedly the two most crucial components of any modernization project. By integrating these technologies, organizations can achieve gains in accuracy, efficiency, decision-making, scalability, adaptability, and real-time threat detection. These advancements are essential for any organization grappling with overloaded ticketing systems, employee burnout, and the heightened risk of real threats being overlooked.

Skilled Personnel

Finding, hiring, training, and retaining skilled personnel may be the hardest part of running any security organization. It often feels like a never-ending cycle of hiring, training, and losing good talent.

One key aspect of modernizing the SOC is reducing burnout among analysts and incident responders. Burnout is often cited as a leading reason why an analyst looks for a different opportunity. Modernizing security operations and allowing analysts to be freed from continuous alerting (false or not) and other tedious tasks could help ensure long-term retention of skilled talent.

The combination of advanced technology and skilled personnel allows the SOC to detect, analyze, and mitigate security incidents effectively, providing a robust defense against cyber threats.

Strategic Importance for Executives

For executives, the modern SOC is not just a technical unit but a strategic asset.

Its continuous monitoring and rapid response capabilities are vital for maintaining business continuity and protecting the organization's reputation.

The SOC's ability to provide real-time insights into the threat landscape and the organization's security posture enables informed decision-making and strategic planning.

Furthermore, the SOC's role in ensuring regulatory compliance cannot be overstated. By adhering to industry standards and regulations, the SOC helps mitigate legal and financial risks associated with data breaches and non-compliance.

Modernizing the Security Operations Center (SOC) is crucial in response to increasingly complex cyber threats. Traditional approaches are insufficient, necessitating continuous innovation.

A modern SOC, with real-time surveillance, advanced technology integration, and skilled personnel, centralizes threat detection, analysis, and response, providing a comprehensive view of security posture threat management.

For executives, the SOC is a strategic asset vital for business continuity and informed decision-making. Leveraging existing technologies, fostering continuous improvement, and integrating AI and automation, along with addressing personnel challenges, ensures a resilient and adaptive security framework.

To Build Or To Buy a SOC?

That is The Question

Chris Fountain
Sr. Security Solutions Architect
chris_fountain@stratascale.com

Upleveling your detection and response capabilities to combat threats and manage risk is a no-brainer. Whether to build an in-house SOC or outsource it, is not as clear cut. Designing a security operations center depends greatly on factors like budget, risk profile, organizational goals.

When speaking with security leaders about SOC services, and whether to build in-house, a common theme consistently emerges: “We need to do more with less.”

Talent Acquistion:
One of the biggest challenges security departments faces is being understaffed, making it difficult to address the 24/7 needs of a full SOC. Finding and onboarding talent proficient in multiple security domains is tough, and retaining this talent after significant time and financial investment becomes a business risk.

Technology:
The costs of technology are steadily growing, while technical debt is not being maintained or reduced year-to-year. Additionally, the overlap of disparate tools creates waste in budgets, creating financial strain on security departments.

Budget Constraints:
Security budgets are not growing at the same pace as other enterprise priorities. Obtaining approval for technology procurement, licensing, and headcount requires navigating internal politics and providing justifications, which can be a time consuming and frustrating process. These problems are seen across organizations no matter the size. Often, the conversation leads to whether building or buying SOC operations is the right strategy.

Build vs. Buy:
Understanding the Pros and Cons

To determine ***whether to build or buy SOC services***, business leaders need to weigh the pros and cons of each approach.

Build	vs	Buy
Pros:		
More customizable for “hands on” organizations		Faster time-to-insight: Focus on business insights faster
Technical breadth		Engagement of teams who have “done it before”
Control over technology		Less resource overhead
		Talent growth opportunities to more business centric needs
Cons:		
Need to development talent and resources		Some can see this as “loosing control”
Talent retention may become a business risk		Possible lack of transparency
Alert fatigue		Vendor Management
Longer time-to-value		

Shared Responsibility Model

An approach that has proven to be most effective is the shared responsibilities approach. The shared model can provide organizations with maximum ROI while aligning with business objectives. With a shared model, commodity technologies and capabilities are outsourced while those capabilities and technologies that require significant organizational knowledge are retained.

This approach can provide efficiencies in workflows by leveraging managed service providers in those Tier1-2 SOC services. Managed Service Providers have the expertise, the staffing, security platforms, threat intelligence insights and automations to provide coverage in areas that would normally require “eyes on glass” 24/7 coverage.

Managed Service Providers can leverage automations across their customer base to help with detections, tuning, and reduction of noise from false positives thus reducing overall analyst fatigue.

This allows your in-house staff to focus on escalations and organizational specific responsibilities.

Finally, an MSP (Managed Service Provider) can bring immediate value by bringing security platforms and licensing that offset the costs of procuring them independently. They do this by leveraging partnerships with vendors that can garner cost savings. Additionally, deployment services can be accelerated to increase time to value versus deploying using in-house resources.

	Outsource (Commodity)	Potential (Opportunity)	Retain (Strengths)
Technologies	Firewalls (Network, Web App) Secure Web and Email Gateaways Network Intrusion Detection/Prevention DNS Security	Security Information and Event Management Vulnerability Assesment Endpoint Detection and Response	Data Loss Prevention User and Entity Behavior Analytics
Capabilities	Security Event Monitoring Threat Intelligence Incident Response	Specialized Skills (Operational Technology Security, Threat Hunting)	Incident Handling Remediation

For a Shared Model SOC Before moving to a shared model SOC as part of your cybersecurity strategy, certain considerations should be made to ensure that your organization is prepared.

Before adopting a shared model SOC as part of your cybersecurity strategy, consider the following:

Inhouse vs. Outsource: Assess which capabilities or technologies should be kept in-house versus outsourced. For example, staffing a Tier 1-2 SOC versus outsourcing to an MDR (Managed Detection and Response). Or maybe retaining specialists in the vulnerability management space have been difficult due to the high demand in the market. An MSP can be leveraged to fill these gaps. Evaluate from both financial and operational points of view when making the determination.

CapEx vs. OpEx: Understand how your accounting organization sees licensing and services expenditures. Depending on how your organization sees service contracts and depending upon payment structures, costs can possibly be amortized. Your accounting and finance teams can be leveraged here.

Compliance Requirements: Review any organizational compliance requirements that may be affected by data retention, data residency, and data security. Understand the business risks that are associated with offloading data and licensing. An MSP can aid in helping you understand your regulatory requirements and/or gaps in compliance.

Processes, Policies, and Procedures: Evaluate if your organization has the adequate process, policies, and procedures in place to onboard a managed service provider. Establish SLAs, SOPs, KPIs, and KRIs to set standards and expectations for the provider's service delivery.

Transparency: For outsourced services, ensure that transparency is provided. If possible, co-management of the technology solutions is the best option for visibility and attestations.

The shared responsibility model can help organizations do more with less, addressing the critical challenges of talent acquisition, technology costs, and budget constraints. By carefully considering what to keep in-house versus outsourcing, and ensuring robust processes and transparency, organizations can achieve a balanced and effective SOC strategy.

Women in Tech:

Interview with Dana Carter, Deputy CISO at Sutter Health

Join Stratascale's Emerging Technology Consultant, Mary-Kate Sloper, as she delves into the inspiring journey of Dana Carter, Deputy CISO at Sutter Health. In this conversation, Dana opens up about her path to the C-suite, her innovative approaches to safeguarding patient data, and the cutting-edge strategies she employs to counteract cybersecurity threats targeting healthcare systems.

In this interview you'll discover:

Dana's Inspirational Journey: How she navigated the tech industry to become a leading figure at Sutter Health.

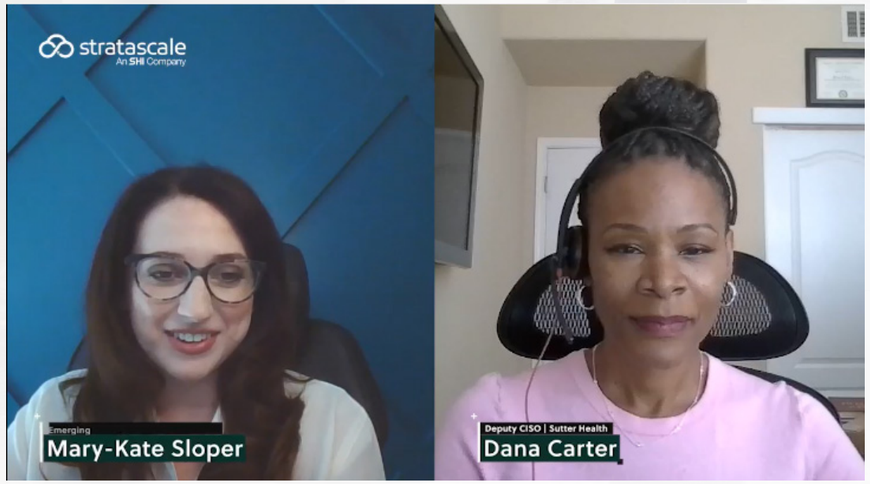
Breaking Barriers: The unique challenges and triumphs of being a woman in a predominantly male field.

Empowering Advice: Practical tips and insights for women aspiring to forge a successful career in tech.

Cybersecurity in Healthcare: The importance of staying ahead of cyber threats facing the healthcare sector.

Building Cybersecurity Culture: Strategies to cultivate a robust security mindset within an organization.

Leadership in the Boardroom: The essential role of cybersecurity leaders at the highest levels of decision-making.



Watch Here

stratascale
An SHI Company

About Stratascale

As a cybersecurity company, we help the Fortune 1000 transform the way they use technology to improve their risk posture, increasing resiliency and operational effectiveness. We help them create a culture of security and infuse it into every layer of their enterprise so they can focus on what's next, not what's standing in their way.

We're securing the digital future.
Come join us.

Learn More