PLAN AND BUILD YOUR SOC

6 Key Considerations Before Setting Up a Security Operations Center

DATAMINR PULSE

Introduction

For many companies, the COVID-19 pandemic exposed physical security and risk management gaps that senior leaders are eager to address in 2021. As a security professional, you might find yourself facing questions like:

- Is it time to build a Security Operations Center (SOC)?
- What people, processes and technology do we need to be successful?
- How much will a SOC cost?
- Should we combine our physical and cybersecurity teams inside the SOC, or keep those teams separate?

Maybe you're leading the charge and actively building a business case around why your company needs to invest in a security operations center in 2021.

If you're reading this book, you've likely worked in a SOC in a previous role or toured SOCs connected to industry-leading companies. You know their benefits—SOCs serve as the organization's central hub for information and action during a crisis. Employees and executives feel safe knowing there's a dedicated group of security professionals tasked with their physical security. Security oversight is centralized and formalized, rather than distributed, ad hoc and siloed.

Here are six key things to consider before setting up a SOC:

Gap analysis

Start by mapping out your company's specific strengths and weaknesses across the risk spectrum.

For companies without a risk management team or a centralized security function, risks can fall into operational silos: Security guards watch surveillance video and maintain access control, logistics teams monitor disruptions to the supply chain, IT teams watch for cybersecurity threats, while the marketing team keeps an eye out for brand risks.

Depending on your company's risk profile, a siloed approach to risk management could be a major weakness, particularly when responding to a complex and fast-moving event that impacts business continuity. Security operations centers serve as a hub for real-time information, which security analysts use to coordinate a fast, cross-functional response to emerging risks.

During your gap analysis, ask yourself, what are your company's strengths and weaknesses around security? Do you have the talented people, robust processes and right tools already in place, and need to scale your existing efforts? If so, a SOC could be a logical next step.

Threat modeling

As you build out the business case for a SOC, try and identify the major risks facing your organization today. Start at the top with the types of risk events that are most likely, and work your way down—which types of risks might have a direct impact on your operations, or could threaten business continuity?

Take a look at past risks your company has faced. Could similar scenarios happen again? Look at risk events that benchmark companies in your industry have faced in recent years—is your company vulnerable to the same risks?

Threat modeling requires a fundamental understanding of six concepts:

1. Identifying your assets: Which company assets will your SOC be in charge of protecting? Which locations will it monitor?
2. Clearly define the SOC's role: Will it handle travel safety? Executive protection? Brand and corporate reputation? Company IP or cyber assets?
3. Threat actors: Who are the individuals or groups capable of carrying out a specific threat, either inside or outside the company? Why might this person or group target my organization?
4. Impact: If this risk event were to occur, what would the impact be to my organization?
5. Likelihood: How likely is this risk event? With risks involving people, how difficult is it to carry out this specific threat, and what could they potentially gain? For more general risks, how often has this risk occurred over the past five years?
6. Controls: What tools and processes do we have in place to mitigate or prevent the risks identified in our threat modeling exercise?

Well-prepared organizations map out the probable risks they face, and perform regular risk scenario exercises to find unexpected gaps in their security planning.

Benchmarking

How does your company's risk management strategy compare to your peers in the industry? How fast have you been able to respond to physical and cybersecurity incidents in the recent past?

Benchmarking exercises are important to understand your current risk tolerance, and whether you might see a marked improvement in your security posture with a SOC.

Remember, security professionals tend to plan for the last risk they faced, rather than the next risk on the horizon. That said, benchmarking gives you a good idea of whether your company's existing security strategies and tools are working.

Here, it can be valuable to lean on your peers in the security industry, asking them for feedback on your organization's security performance benchmarks.

Security professionals managing a SOC have to adapt to the ever-changing needs of their business.

Watch this webinar to see how you can plan for running your SOC during a global pandemic.

WATCH THE WEBINAR

Executive sponsorship

At some companies, security teams are treated like a cost center, and rolled up into massive IT, HR or operational budgets. Identifying and mitigating risk can be expensive, and without a recent, costly internal case study to point to, security professionals can face an uphill battle as they make a case for more resources.

It's important to identify an executive sponsor who understands the value of an integrated security program, and is able to articulate how it ties back to the company's larger strategic and financial goals.

Risk managers inside your company have likely already built a matrix of key risk indicators, highlighting the most likely, and most impactful potential risks on the horizon. Review your company's KRI matrix with your executive sponsor to determine which risks might be better mitigated with an investment in a dedicated security operations center.

Enterprise risk management—a large umbrella that encompasses physical and cybersecurity risk—requires real investment when done right. In a 2019 Deloitte survey of several hundred companies with more than $500 million per year in sales, about two-thirds spent more than $10 million per year on risk management.

However, that investment pays off: Companies that put adequate resources into integrated risk programs typically achieve higher growth and profitability compared to their peers who approach risk in silos, the survey found. Arming your executive sponsor with data will be important as they lobby their peers for more resources.

Pilgrims Risk Management Group uses Dataminr to protect people and assets for clients in some of the world's most challenging environments.

READ THE CASE STUDY

Converged security

Many companies still tend to treat physical and cybersecurity risks as separate entities, with different teams, tools and processes in place to respond to each. During your planning process, it's important to determine whether it makes sense to build a converged security operations center, with analysts well-versed in responding to physical and digital risks working alongside one another.

Depending on your company's risk profile, breaking down the wall between physical and cybersecurity teams could result in greater efficiency, faster response times and an improved overall security posture. Many common risks can affect IT infrastructure and physical safety simultaneously.

For example, a natural disaster that impacts business operations in the area could also threaten the company's technology infrastructure.

Responding to the COVID-19 pandemic required IT professionals to quickly assess the risk of adopting fully remote work environments, while physical security teams made plans to ensure the health and safety of employees.

Taking a phased approach

Successful SOCs typically start with a core set of capabilities and grow over time, winning a greater share of investment after proving their business value.

One Dataminr client described launching their security operations center with a limited geographic and operational scope, with a relatively small budget and tool set. Eight years later, they're running a 24/7 center that provides 18 distinct security services to their company. Growing into that role required strong executive buy-in, a sustained track record of success, and an ROI analysis to support the additional investment.

As part of your gap analysis, lean into what's working in the security function today, and consider building a beachhead around a limited number of services that the SOC could provide immediately. The ultimate goal should be to build out the ability to handle a wide range of emerging risks, across physical and cybersecurity.

Is your company ready for a security operations center?

Security operations centers serve a critical function, by detecting and responding to emerging risks in an organized and centralized manner. They require the right people, processes and technology to process and respond to real-time information, and executive buy-in to support the center's cost.

Dataminr's real-time alerting platform is a crucial tool for hundreds of leading security operations centers worldwide.

Learn more at dataminr.com/pulse

Learn more

Request a demo

Book a demo to see how you can gain earlier insights into high-impact events and emerging risks.

BOOK A DEMO

Contact us

General | info@dataminr.com

Support | support@dataminr.com

Learn more about SOC at our Security Operations Center hub