DATAMINR PULSE

NextGen Security Operations: A Roadmap for the Future

Best practices to future-proof security operations in 2022 and beyond

There's no doubt that the security threat landscape has become increasingly complex and sophisticated. The question is no longer if an organization will be impacted by a significant crisis or disruption, but when. It's a reality that today's security leaders have to contend with—no matter their size, industry or location.

And as the COVID-19 pandemic taught us, today's security leaders must move from being crisis managers to crisis leaders. This requires them to leverage the latest tools and technologies, develop the most relevant skill sets in their people, and build processes and cultures that are future-proofed for accelerating threat trajectories.

Here we explore some of the major themes shaping the future of the security industry: cyber-physical risks, types of security models and frameworks, and remaining resilient in the face of new and unexpected challenges and change.

Mitigate and Manage Cyber-physical Risks More Effectively

The greatest enemy of rapid response is complexity and fragmentation. Yet, this is precisely what a siloed view of physical and cyber risks introduces into the security and risk management of an organization. Security leaders and teams need a holistic view of their threat landscape—now more than ever, given that cyber-physical threats have become more pervasive and our world hyper-connected.

In fact, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has called for more formal means and standards of collaboration between cyber and physical security. But how to put that into action remains a challenge for many. Some organizations have responded by converging their cyber and physical operations into a single, unified security function. While this is not the prevailing model, it is frequently touted as the solution to improving risk mitigation for cyber-physical threats.

It's not the only answer. Better cooperation and communication between physical and cyber teams is key. When done right and on a consistent basis, the teams are better able to see the full picture of their organization's security risks. Also key is ensuring the physical security function gets the attention and investments it needs to identify and mitigate cyber risks inherent in its industrial control systems (ICS).

Benefits of cyber and physical security teams working in close partnership:

- A stronger, more holistic security posture
- Faster identification of, and assessment and response to, threats that fall within both the cyber and physical domains
- Better communication and sharing of information and technology
- More efficient resource allocation

Improve communication and collaboration between cyber and physical teams

Despite the clear need for, and benefits of, better communication and collaboration between the two security functions, it remains a challenge. Here are four ways both teams can work to overcome barriers.

1: Get to know each other. Because cyber and physical security teams often work in complete silos—especially at large enterprises—they have fewer opportunities to meet and get to know the key players on the other side. Knowing the names and faces of counterparts goes a long way in forming meaningful partnerships.

2: Understand the other's responsibilities and challenges. Both physical and cyber security leaders should create a baseline awareness of the other's intelligence and how they work within the organization. They can start by providing practical resources and relatable context so that both sides of the house understand how the two security functions intersect.

3: Maintain regular, productive communication. Establish a standard, disciplined routine of communication and coordination, such as meetings and check-ins. Most importantly, both cyber and physical security leaders need to communicate frequently to maintain real-time situational awareness.

4: Proactively prepare for future threats. Even if there is no active risk, it's imperative that the physical and cyber teams work together to prepare for future threats. This includes role-playing via tabletop exercises and conducting assessments of past risk incidents where there was a cyber-physical convergence.

Protect ICS against cyber attacks

ICS are systems that automate and control industrial processes, as well as support critical infrastructure such as energy, transportation, health, manufacturing, food and water. Today's ICS are more vulnerable than ever, with a 41% surge in reported ICS vulnerabilities in the first six months of 2021. This is in large part due to the shift toward managing ICS via remote access and the fact that an increasing number of systems are now connected to the Internet.

It's an added challenge for physical security teams already tasked with managing a larger surface area of risk. And trying to shield all ICS from cyber risks is an enormous undertaking. However, the following practices can help improve organizations' security posture:

- Maintain a complete and up-to-date inventory of your Internet-connected ICS; this is the most basic starting point for securing ICS.
- Stay abreast of new developments from regulators and government agencies, such as the advisories on ICS vulnerabilities to be patched issued by the U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and the Industrial Control Systems Cybersecurity Initiative launched in April 2021.
- Leverage Dataminr Pulse's real-time information related to cyber vulnerabilities and threat actor activities to increase your visibility of the risk landscape.

Industrial control systems: a new target for cyber crime

Take for instance the 2021 water treatment plant hack in Oldsmar, Florida. A hacker gained access to the plant's control system, turning a cyber attack into a physical one that threatened to poison the city's water supply with dangerous levels of lye.

Dataminr alerted customers, in real time, to the scale of the attack, the affected software and the exposed municipal-level IP addresses at risk of exploitation—enabling customers to be more proactive in securing their systems and guarding against this vulnerability in remote management tools.

Ensure You Have the Right Security Framework

The current state of risk has turned well-run security operations into a key competitive differentiator. Companies must keep pace with today's evolving threat landscape or risk becoming more vulnerable and unequipped to tackle future risks.

This means that security leaders need to ensure they have the right security model in place to meet the specific requirements of their organization. While each business will approach security operations differently—taking into account size, age and industry— most settle on one of two security models: decentralized or centralized.

Organizations that adopt a decentralized model rely on dispersed security teams to manage risks, usually at the local and/or regional levels. Their security operations are self-contained and the decision-making process is kept within particular business units, typically based on geographic location. This model is often initially adopted by smaller organizations with a narrow physical footprint and less mature security operations.

As organizations put more resources and capital into their risk operations, they tend to become centralized. Typically these organizations are large enterprises with multiple locations in one or more countries. For them, this security model allows for a dedicated, centralized team that continuously monitors all business locations, traveling employees and other assets.

A key benefit is reduced stress levels and improved coordination among all security analysts. The potential downside is the inherent risk of having a single point of failure. It's why some organizations opt to have not just one but several centralized security teams.

In many instances, enterprises that centralize their security function do so by creating a security operations center or SOC, which serves as a hub for real-time information used by security analysts to coordinate fast, cross-functional responses to emerging risks and crises. This sophisticated operating model allows for a stronger security posture and better visibility of potential risks in each continent or region in which an organization operates.

What to consider when setting up a SOC

1. Gap analysis: Map out your company's strengths and weaknesses across the risk spectrum. What are they? Do you have the talent, processes and tools needed to scale existing efforts?

2. Threat modeling: 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 ones have a direct impact on operations or threaten business continuity?

3. Benchmarking: Use benchmarking exercises to understand your current risk tolerance, whether a SOC significantly improves your security posture and if existing strategies and tools are working.

4. Executive sponsorship: Identify an executive sponsor who understands the value of a centralized security program and is able to articulate the link between it and the company's strategic and financial goals.

5. Converged security: Should your SOC focus on physical or cyber security only, or should it bring the two together to create an integrated team? Improved communication and collaboration between the teams creates greater efficiencies and a stronger overall security posture.

6. A phased approach: Start with a core set of capabilities that will grow over time. The first step is to consider a limited number of services that can be provided immediately.

No matter the type of security model chosen—be it centralized, decentralized or somewhere in-between—it should be complemented by a network of passive and active monitoring mechanisms. Security leaders can then easily identify and maintain visibility of known and emerging risks.

To do so effectively, many leaders rely on real-time information tools like Dataminr Pulse, which uses a powerful and innovative AI platform to detect the earliest signals of high-impact events, emerging risks, cyber threats and other business-critical information.

A Look Ahead: NextGen Risks and The Way Forward

The World Economic Forum (WEF) predicts that the top risks of the next 10 years are climate action failure, extreme weather, cybersecurity failure, infectious diseases and debt crises. With the world now more attuned to risk, a question all security leaders need to ask themselves is: What can I do to evolve my risk mitigation strategy beyond 2022?

It's not enough to plan for only one or two years ahead. We know for a fact that emerging risks and high-impact events are occurring with unprecedented frequency and unpredictability. As such, organizations must closely examine how they can strengthen and maintain their business resilience and agility with a five to ten-year plan.

An approach that takes into account what will be needed today and tomorrow should address three key factors:

1. Designing a culture that can maintain and strengthen business resilience and agility
2. Protecting a more dispersed workforce given the recent shift to remote and hybrid work models
3. Integrating the right technology and tools, such as real-time information solutions, into your security operations and workflow

Foster a culture of resilience and agility

An organization's resiliency and agility are inextricably tied to its workforce, making it more important than ever that businesses foster a culture that includes both. When they do, they eliminate the rigidity of pre-pandemic processes—created in the name of efficiency and growth—that hinder their ability to respond to crises and disruptions quickly and effectively. The need is not new. We've long known what happens when one or both are missing, or when resiliency and agility aren't as strong or embedded in the culture as once thought.

"It took getting hit in the face with a door hard, especially with COVID-19, [for many organizations] to wake up [to that idea]," said Matt McCracken, ServiceNow Risk and Resilience Practice Leader.

As a result, many organizations are prioritizing resilience and agility and taking deliberate actions to clearly demonstrate how vital they are to workplace culture. For example, more organizations are investing in business continuity, risk and resilience positions at the leadership level. This is evidenced by the increase in such job postings on recruiting platforms like LinkedIn and Indeed.

Other businesses are investing in technologies and tools that enable more responsive and flexible ways of working for employees across the enterprise. The result is a more efficient and flexible resiliency model that can sustain and streamline operations during a crisis or major disruption.

Resiliency reminders

Resilient 'parts' do not equal enterprise resilience. When only parts of an organization are resilient, they become more rigid. This makes it difficult for the enterprise to maintain critical agility when a crisis hits. The entire enterprise—not just specific functions or lines of business—must be resilient.

Democratize information. COVID-19 showed us the speed at which disruption can spread. Ensuring that real-time information and insights gleaned from it are accessible as fast as possible across the organization is a vital part of a resilience strategy.

Protect a dispersed workforce

Now that remote and hybrid work have become commonplace, companies have to reassess their security standards and practices in both the physical and digital domain and consider them as a whole rather than siloed operations.

Physical spaces

Conduct a thorough examination of your duty of care obligations, and whether the processes of protecting your company's workforce extends to wherever your employees are working. Ask yourself:

- Should we constantly monitor and inform our employees of issues that affect their physical location during work hours?
- Why would this be any different from the normal situational awareness provided in our traditional office settings?
- Do we have the suitable people, processes and technology to deliver on this?

Today, organizations of all kinds use Dataminr's real-time alerts to keep their employees informed of potential threats and high-impact events in as close proximity to the event occurrence as possible. In the near future, security leaders might provide employees with direct access to such real-time information, especially as many workforces span multiple cities in various regions throughout the world.

The digital domain

Companies' attack surface is no longer contained to their office network. Remote and hybrid work has made it much wider—and the opportunity for compromising it much more apparent. Protect both employee and company data by assessing how that data is accessed, stored and moved. Ask yourself:

- Do I know where my data is?
- How is my data being accessed? What controls do I have in place?
- Do I have enough resources and readiness to discover risks, so that appropriate remediation can occur quickly and effectively?
- Have I created a suitable culture across the organization whereby security is everyone's business? Is my intellectual property secure?

Real-time information

It's an imperative that security leaders and teams have the right technologies and tools in place to safeguard their organizations in this new and ever-evolving threat landscape. Those tools, including real-time alerting solutions, should work in lockstep with decision makers in identifying and mitigating both unexpected and long-term risk factors.

Organizations that view real-time information as a competitive advantage—not just a function—are able to extract its full value and a high return on investment (ROI). And, as we learned from the pandemic, acting quickly on information can actually save businesses and lives.

For example, in August 2021, when the Taliban regained control of Afghanistan, the lives of many were suddenly at risk. This included the lives of the Afghan girls robotics team, their family members, and more than 150 female students from Asian University for Women. In partnership with Dataminr NGO partner Direct Relief, Dataminr's real-time alerting solution helped to get the women to the Kabul airport and airlifted to safety. Not one woman in the group was left behind.

Pro tip: ensuring buy-in for critical technology

Shift from talking about risk in terms of "red, yellow and green" to talking about how it affects the organization's bottom line—including the ability remain operational, manage reputational risks and meet customer demands.

Recognizing the threat landscape's evolving and expansive nature, many forward-thinking businesses have already begun to broaden their strategy beyond traditional security to include more risk scenarios. For example, the remit of many security teams has evolved to include monitoring for brand and reputation and supply chain risks.

Others are looking at adopting a converged security model to ensure there's an appropriate exchange of relevant information and understanding of the wider security and business implications of an emerging risk.

But nearly all teams had a pandemic playbook that had to get dusted off come 2020. This is why it's crucial to have strategic plans to address long-term challenges as well as expected, frictionless pivots required for short-term crises.

The world was caught off guard once with the COVID-19 pandemic. If we take heed, we can prepare now for what's to come—from economic and geopolitical shifts to increased connectivity for businesses and communities. Key to that preparation is understanding how the vast information landscape is changing, as well as having access to the data in real time that organizations need to strengthen business resiliency in 2022 and far beyond.

Learn More

Learn how organizations like yours use Dataminr's real-time alerting solution, Dataminr Pulse, to effectively navigate the new and unexpected challenges of today and tomorrow.