Keeping *it online*

Building risk mitigation and business continuity into SOCs, by Ryan Schonfeld, Co-Founder & CEO of HiveWatch

At the end of October, thousands of AWS-supported sites were affected by an outage that disrupted operations and computer processes for customers around the globe. Popular apps like Snapchat and Reddit, along with Venmo and Zoom, were affected, creating headaches and keeping companies from conducting normal everyday tasks.

This outage – and others like it – highlighted how vulnerable the world's interconnected technologies are – all from a single cluster of data centers. It also highlights the importance of redundancy and ongoing focus on business continuity across multiple verticals – especially when security technology is involved.

When there's no redundancy

When your security operations center (SOC) goes down without a backup system, you and your team are essentially "flying blind."

"The purpose of your SOC isn't just about stopping threats; it's also about making sure you can recover quickly and communicate effectively when the worst happens."

Think about it: your access control systems stop working, surveillance cameras go dark, alarms no longer come in and suddenly your security team has no visibility into what's happening across your facilities. Guards can't verify identities, you can't track who's coming and going, and if there's an actual emergency unfolding, you might not even know about it until someone physically tells you.

In a world where security threats can escalate in minutes, losing your operational capability isn't just inconvenient; it's genuinely dangerous for both your people and your assets.

The ripple effects of an outage like this can be long-lasting. Without functioning security systems, you might not be able to lock down facilities or switch to manual processes that your team probably hasn't practiced in years (but should). Employees get stuck outside buildings they need to access for their jobs. Deliveries pile up because no one can verify and process them properly. Critical areas that require constant monitoring, such as data centers, warehouses full of valuable inventory or facilities with hazardous materials, are suddenly operating without security protocols. If you're in an industry with compliance requirements, every minute your systems are down potentially creates regulatory headaches.

Here's what really keeps security leaders up at night: when your systems go down, the bad guys know it – or may have caused it. Whether it's internal theft, external break-ins or worse, criminals understand that the window when your defenses are down is their best opportunity to strike.

Financial ramifications

The financial hit from a SOC outage isn't just about the cost of getting systems back online. You're looking at potential losses from theft or damage that occurred while you were unable to oversee facilities, overtime costs for security personnel trying to cover gaps manually, lost productivity across the entire organization and possible fines if you're in a regulated industry.

Some companies have had to literally shut down operations entirely until their security systems were restored because the liability of operating without proper safeguards was just too high. And if something actually goes wrong during an outage – such as an injury, a theft, a security breach – it can mean trouble for security leaders when speaking to leadership, insurers or lawyers about why they didn't have redundancy built into such a critical system.

> **"In your SOC, consider adding a secondary internet connection and a tertiary internet connection."**

Where to start in mitigating risk

There's a lot of talk about risk within organizations as security leadership discuss building redundancies to protect from outages or disruptions to operations. However, the actual methods to build resiliency into security operations is very difficult when different business units don't talk to each other, when systems are completely siloed and when security isn't at the table to learn about the goals of the business.

Running an effective SOC means having a clear game plan for identifying, analyzing and addressing threats before they become major problems.

Document everything: The first thing your SOC needs to do is get everything documented: What are you actually worried about? Workplace violence incidents, natural disasters, equipment theft – whatever keeps you up at night. Once you've got all these threats written down and organized, you can actually show leadership what you're up against. Here's the thing: your security team can't protect the business from threats they don't even know exist, so getting everyone on the same page about what risks you're facing is absolutely critical. Once you have your threats documented, run tabletop exercises to test your team's response to these scenarios. These simulation exercises will quickly reveal gaps in ▸

your documentation, expose unclear procedures and give your team valuable practice before they're facing a real incident.

> **"Running an effective SOC means having a clear game plan for identifying, analyzing and addressing threats."**

How likely are these incidents: Once you know what threats are out there, you need to figure out which ones are actually likely to happen and how bad things would get if they did. This is where your SOC team digs into the data with both hard numbers and gut-check insights to understand what might cause problems and what the fallout would look like. You're basically asking yourself: "What are the odds this actually happens? Do we have safeguards in place? And if those safeguards fail, how screwed are we?" Getting honest answers to these questions helps you focus your energy and budget on the risks that really matter.

Identify the resources: When it comes to actually dealing with threats, security leaders work with what's called the four T's: Tolerate it, Transfer it, Treat it, or Terminate it. Your toolkit for handling risks should be pretty diverse: employee hotlines, threat monitoring software, social media tracking, training sessions for HR, solid relationships with local law enforcement, you name it. The goal is to act fast and bring that risk down to a level everyone can live with. You're never going to have just one magic solution that fixes everything, so you need multiple layers of defense that fit your organization's specific situation.

How to create SOC redundancy

You can't prevent every bad thing from happening, but you can try to imagine the worst case scenario and prepare for how you need to deal with it. It's why I have a job. It's why crisis management and business continuity planning are so important for your SOC.

In your SOC, consider adding a secondary internet connection and a tertiary internet connection ("backup to the backup") in case of an outage. Revert to site snapshots that don't live in the cloud that have important numbers and information for contacts so that you're able to communicate effectively. Have a plan in place to move cloud operations to another location. Create a plan for how to communicate manually if you aren't able to mobilize your teams online.

The bottom line is: you need incident response plans that your team actually practices regularly, not just dusty documents sitting in a drawer somewhere. When something does go sideways, having those plans tested and ready means your team can jump into action, keep the damage contained and help the business keep running. The purpose of your SOC isn't just about stopping threats; it's also about making sure you can recover quickly and communicate effectively when the worst happens. The SOC shouldn't just be about responding to alarms and managing guards – it should be the backbone of the enterprise during a crisis.

You can't wait to build resiliency

The AWS outage showed us that even tech giants with seemingly unlimited resources aren't immune to catastrophic failures. For physical security operations, the stakes are even higher because you're not just protecting data or ensuring people can post on social media; you're directly responsible for keeping human beings safe and securing physical assets worth millions or billions of dollars.

A redundant system might seem like an expensive insurance policy you hope to never use, but the real question isn't whether you can afford redundancy; it's whether you can afford to operate without it when everything goes sideways. ■