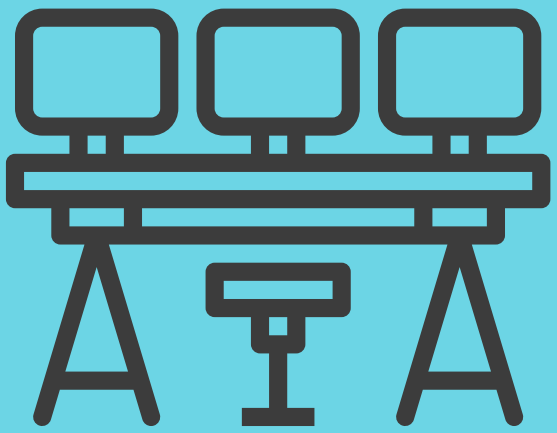
noggin

Security

Guide to Operating a Security Operations Center (SOC)



The operational security picture across industry today

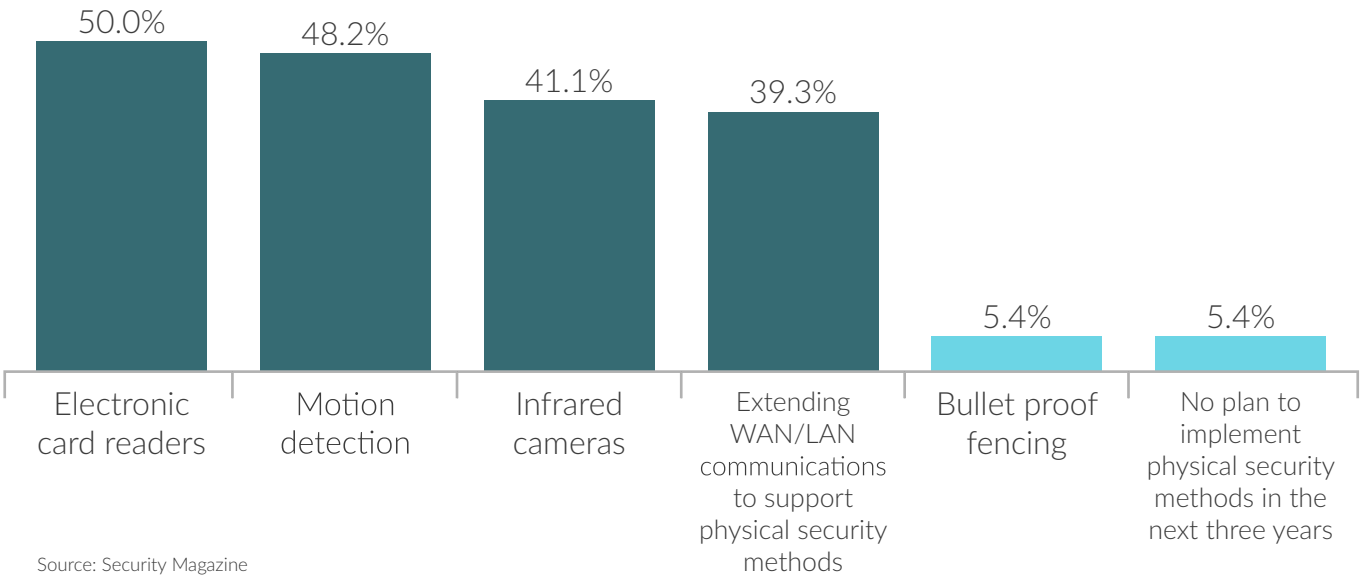
The September 11, 2001 terror attacks occasioned a wide-ranging reevaluation of operational security in most industries, especially in the critical infrastructure sector – not just asset operators, either, but ecosystem partners all along the supply chain. That trend of bolstering operational security of vulnerable physical assets continues to this day. Physical security is still vulnerable to common industrial security risks, e.g. workplace threats, violence, theft, counterfeiting, sabotage, trespassing, activist disruption, vandalism, contamination, and, of course, terrorist attacks.

The statistics bear this out. Security threats do, in fact, cause staggering material damage. In the construction industry, for instance, anywhere between $300 million and $1 billion a year is lost due to the theft of equipment and other high-value materials, according to the National Insurance Crime Bureau in the U.S[i].

In the construction industry anywhere between $300m and $1b a year is lost due to the theft of equipment and other high-value materials.

These numbers are hardly surprising. Buildings, sites, plants and equipment, materials, and other physical assets remain some of the easiest targets for malicious actors. Accordingly, 42 percent of security professionals are concerned with their organization's inability to secure those physical spaces, as reports the Ponemon Institute. For starters, those assets tend to be largescale, creating a larger physical environment to secure. Some of the equipment they house is old and obsolete, surely not designed with modern security concerns in mind. Also, physical security staff on the ground is overwhelmed, because lacking the support needed to protect people and prevent damage, theft, and unlawful entry.

Fig 1. Physical security organizations plan on implement in the next three years



Source: Security Magazine

The role of the Security Operations Center in managing operational risk

What's, then, to be done? Well, if organizations find it difficult to protect physical assets and people as well as coordinate speedy responses, the answer is clear: companies need to build robust Security Operations Centers (SOCs) to improve their operational security posture.

So what's an SOC, exactly? Definitions vary. But broadly speaking, an SOC provides a platform for detecting and reacting to security incidents[ii]. The actual SOC is a facility that houses an organized and highly-skilled security team, which relies on sophisticated technology and well-honed processes to achieve topline, security objectives for the organization[iii].

The security team responsible for carrying out the SOC's core mission usually includes the SOC manager who heads up operations, engineers, and security analysts – the team also works closely with the organization's Crisis, Emergency Management, and Business Continuity teams to coordinate responses to physical security incidents that become critical events. And the primary duties the team discharges consist of regularly monitoring and analyzing the organization's security posture. More specifically, the SOC team detects, investigates, responds to, and reports on security incidents – remember, the SOC is an operational unit; it's not responsible for developing security strategy. In essence, the SOC has to work to continuously manage known and existing risks and threats. Of course, those responsibilities don't cease when the traditional office closes down. Far from it: and that's why most SOCs are open around the clock.

The benefits of this particular, centralized security arrangement are pretty clear, though. It's widely understood that advanced equipment and technology alone aren't enough to achieve organizational security goals; if they were, there'd be far fewer physical security incidents, as security procurement went up. Instead, mitigating risks and improving incident preparedness and response call for a security apparatus *specifically* dedicated to preventing damage, theft, and intrusions, as well as protecting people.

And that's what SOCs do so well: consolidate security expertise and reporting into one centralized location. SOCs receive physical security data from the field to furnish a real-time picture of security threats and vulnerabilities. This centralizing approach cuts down on some of the security siloing characteristic of security incident management in most large enterprises. SOCs, instead, deliver gains in visibility and increases in security incident situational awareness. Also, when it comes to security incidents, SOCs help communicate to and interface with other parties in the business who need to be on high alert if a breach does occur, e.g. Legal and PR.

Finally, in recent times, lawmakers and national regulators have moved in aggressively to mandate baseline security measures, especially in the critical infrastructure sector. Robust EOCs and related practices go a long way toward ensuring compliance with those mandates, as well as attenuating the reputational damage of physical security incidents that do occur, by demonstrating an organization's longer-standing dedication to the most stringent security incident prevention measures.

Overcoming the challenges of setting up a Security Operations Center

Despite the clear benefits, SOC adoption isn't universal. In fact, 48 percent of companies still don't have an SOC, according to EY's Global Information Security Survey, 2017-2018[iv]. What's going on, here? Well, for starters, upfront capital costs for furnishing an SOC can be considerable; though, on balance, the financial investment that goes into building the SOC more than pays for itself in the lower incidence of security mishaps down the line. There's also the complexity of conforming with multiple, oft-overlapping regulations (external as well as internal), as organizations do build out their SOC infrastructure. Finally, qualified security analysts can be hard to come by.

Building and staffing an SOC don't necessarily guarantee success in the ever-evolving security realm, either. Once SOCs are fully operational, staff still encounter thorny challenges. For one, teams will need to get up to speed on a number of different security solutions, as many as 20 different technology combinations in some SOCs; of note: operational security management technology offers a consolidated feature set (see below)[v].

Operational Security Management: A concise buyer's guide

SOC operators must manage multiple technology sets at once. But there are means of easing the burden. Cloud-based, operational security management software not only keeps operations secure but SOCs humming along. Just look for the following features when procuring:

- Manage all operational security incidents and major events in a single system
- Perform security investigations
- Centralize, track, and manage security information, checklists, and actions
- Task and dispatch security staff to respond to any event
- Manage lost and found property
- Schedule security escorts
- Fully integrated mapping to visualize locations of incidents, hazards, people, and assets
- Perform hazard and risk assessments
- Automatically generate security statistics on dashboards and security reports
- Easily capture rich logs for patrols, shift-changes, parking infringements, and other security activities
- Integrated communication templates: email, SMS, voice, and more
- Conduct alarm tests and inspections
- Monitor persons of interest
- Manage security staff and contractors
- Built-in dashboard analytics, structures, and ad-hoc reporting
- Automate and follow business procedures with fully-configurable workflows
- Collect intelligence from the field via mobile apps

Best practices for planning and managing physical security resources

- Physical security programs should be holistic and the allocation of resources should be integrated into the agency's mission, objectives, goals, and budget process.
- Physical security functions should be consolidated within an internal security office, led by a Director of Security (i.e., CSO), who reports to a high ranking senior executive official who has ready access to the agency head, as needed.
- Director of Security (i.e., CSO) should be responsible for managing and allocating physical resources based on risk assessments and using performance measures to justify security resources across the agency's portfolio of facilities.
- Development and implementation of the physical security program should involve collaboration among top agency management, security, facilities management, emergency preparedness, budget, health and safety specialists, and other stakeholders.
- Physical security programs should be aligned with the agency's mission, strategic goals and multi-year budget cycle.
- Physical security programs should meet the cost-effective expectations of the agency leadership in terms of totally integrated security support and safety services rendered.
- Physical security programs and countermeasures should be balanced with other operational needs and competing interests.
- Physical security resource allocation should be periodically assessed, including historical spending records, which may be useful in future resource allocation considerations.

Source: Department of Homeland Security

Sure, those challenges aren't a walk in the park, but they are surmountable with the right practices. As mentioned, SOCs themselves are not responsible for developing security strategy. However, their aims must be consonant with the organization's overall, physical security strategy, which prescribes levels and ranges of risk tolerance.

In other words, SOCs, to be successful, must address specific, clearly-defined company (and customer) needs and scale to an organization's footprint. It helps, in this respect, to have C-suite sponsorship for your SOC. And that's because the SOC is by default a cross-functional operation; only senior executives can ensure that business-specific goals from various departments (as well as the participation of various business lines) are incorporated into the SOC's mission and the SOC, in turn, gets the necessary visibility across a defendable perimeter: if you're tasked with ensuring physical security, for instance, perimeters refer simply to doors, walls, and other physical barriers.

Context-aware threat intelligence is important, here. An SOC that undertakes a detailed site vulnerability assessment is far more likely to be successful than one that doesn't. The vulnerability assessment will help staff discover security gaps in need of greater focus (and protection). In terms of physical security, in particular, the vulnerability assessment gives organizations granular knowledge into layout and how employees act within their physical environment. The assessment also games out the impact of potential security incidents and their possible effects on security personnel and process operators, all of which helps determine physical security requirements. Examples include:

Identify and control individuals who enter and exit the facility

Track movements of building occupants and assets

Control access to restricted areas

Track and locate equipment, products, and other resources

Track the location of personnel on site in the event of an incident

Integrate control and security systems for greater speed and efficiency

Protecting process automation networks and systems from potential intrusion

Respond quickly to alarms and events[vi]

These requirements are part of the organization's, larger incident response framework, in which the SOC plays a key role. Indeed, the genesis of the SOC might have been to sure up security incident response, by giving the organization a centralized facility to consistently and continuously triage detected threats. Further, the most effective SOCs are governed by established, rigorous processes. Their staffs are engaged in continuous training that keeps pace with the persistent development of new threats[vii].

Putting it all together

International standards on the market mandate baselines for securing valuable assets, both digital and physical; compliance with those standards should be incorporated into your SOC strategy. The ISO 27000 family of standards, for instance, focuses on information assets. As mentioned, though, information assets exist in physical space, which leaves them vulnerable, despite robust cyber security measures.

For that reason, the information security management systems standard, ISO 27001 includes physical and environment security clauses. Often, security officials responsible for implementing ISO 27001 are reluctant to broach this later clause, because they don't have a background in physical security services. However, the practices outlined in the physical and environmental security clauses actually follow the same logic and framework as those that deal with digital information: defining context, assessing risks, and implementing appropriate controls. Remember, the higher the value and the risk, the higher the protection level.

More specifically, requirements in this section fall into two broad categories: secure areas and equipment security. Secure areas provisions – secure areas being sites where organizations handle sensitive information or shelter valuable IT equipment and personnel to achieve business objectives – deal with protecting the physical environment in which assets are housed, e.g. building, offices, etc. There, the standard asks organizations to look at risks relating to physical access to those assets and, where appropriate, put in controls to manage (limit or simply control) physical access to those assets.

Protocols for equipment security are similar. Essentially, the clause asks organizations to consider where equipment is housed and whether it's housed appropriately: for example, is important IT equipment near a water pipe? Other questions managers should ask:

Where are cables running?

Is equipment being maintained according to protocol?

Who's responsible for maintaining equipment? Are they qualified?

What provisions are in place for equipment that leaves the premises?

Building and staffing an SOC won't bring immediate changes to your security posture – if only things were that easy. But they're certainly important steps to take, that must be reinforced by provable best practices, like constant training, developing rigorous processes, implementing standards, procuring consolidated risk and operational security technology, etc. Finally, the benefits of creating a robust culture of curiosity centered around your SOC are clear, though: not only mitigating security risks, improving incident response, cutting down security cost, but also staying on the right side of stringent new regulations and public opinion that hold organizations foremost responsible for any security lapses.

Citations

i. *Scott Dicus, Nathan Ives, David Price, and David Mayers, Security Magazine: Protecting Physical Assets from Cyber Threats Grows in Priority. Available at https://www.securitymagazine.com/articles/88694-protecting-physical-assets-from-cyber-threats-grows-in-priority.*

ii. *Renaud Bidou: Security Operation Center Concepts & Implementation. Available at https://pdfs.semanticscholar.org/1ffa/f58ab9379b1d3ef11d18091fc08df777481b.pdf.*

iii. *Pierluigi Paganini, Security Affairs: What is a SOC (Security Operations Center)? Available at http://securityaffairs.co/wordpress/47631/breaking-news/soc-security-operations-center.html.*

iv. *EY: Cybersecurity regained: preparing to face cyber attacks: 20th Global Information Security Survey 2017-18. Available at https://www.ey.com/Publication/vwLUAssets/GISS_report_2017/%24FILE/REPORT%20-%20EY%20GISS%20Survey%202017-18.pdf.*

v. *Julie Tillyard, DFLabs: The Top 5 Challenges Faced by Security Operations Centers. Available at https://www.dflabs.com/blog/the-top-5-challenges-faced-by-security-operations-centers/.*

vi. *Honeywell, International Society of Automation: Physical security for industrial assets: Growing threats demand an integrated strategy. Available at https://www.honeywellprocess.com/library/marketing/article-reprints/Industrial_Security_Article_Reprint.pdf.*

vii. *Pierluigi Paganini, Security Affairs: What is a SOC? What is its mission? Which are the Security tools and technology components of a SOC? Here come all the answers. Available at http://securityaffairs.co/wordpress/47631/breaking-news/soc-security-operations-center.html.*

Like what you read? Follow Noggin on social media

@teamnoggin facebook.com/teamnoggin linkedin.com/company/noggin-it