noggin

Security

An Introduction to Operational Security Management: The operational security management controls and systems you need to protect people and assets

Why we're talking about operational security management now

With physical security increasingly compromised, operational security management matters more than ever.

Physical security management, if you didn't know, is all about protecting personnel, information and physical assets from the physical threats that can cause harm, damage, and/or disruption to your business operations. Those threats not only include intentional acts of destruction, such as theft, vandalism, and arson. But they also comprise natural events or other environmental conditions that might have an impact on the physical security environment.

So, where does operational security management fit in? Well, operational security management gauges the effectiveness of the technical controls (e.g., access controls, authentication, and security technologies) your company has put in place to secure its premises and safeguard the confidentiality, integrity, and/or availability of its systems and data.

Why we're talking about it now is that compelling evidence suggests that existing operational security controls have been inadequate. For instance, 20 percent of enterprises acknowledge experiencing an increase in physical security incidents since the start of the COVID-19 crisis. What's more, a third of organisations think that they will see an increase in physical security incidents in 2021. What's going on?

20% of enterprises acknowledge experiencing an increase in physical security incidents since the start of the **COVID-19** crisis

Challenges to deploying effective operational security management controls

A big issue we're seeing with operational security management in the era of COVID-19 is security guards aren't able to stop physical security incidents.

However, if you look back to the pre-pandemic data, many of the same operational security management challenges existed. Specifically, security professionals noted an increase in workplace risk, while also decrying high levels of unpreparedness to deal with specific physical security threats like workplace violence, environmental incidents, and active shooter events.

In addition, there was particular concern with the increasingly mobile nature of the physical security threat. After all, the workforce is more mobile and mobile-reliant than ever. The information assets those mobile workers store on their corporate-liable mobile devices, however, still exist in physical environments that must be secured and protected.

If that isn't enough, maintaining security poses an important operational risk to the organisation. Physical security incidents themselves have massive spill-over to all segments of the business. Yet, the physical security capability doesn't always treat every aspect of security, including risks and hazards. We can tell, because the operational security tools procured often only provide for data capture and analysis as well as other incident reporting capabilities.

Sure, those features are important. But limited operational security management system functionality impedes physical security incident response, as teams respond without a clear understanding of the underlying risk. Similarly, upper management makes less informed security policy decisions with limited situational awareness of the company's physical security risk profile.

Operational security management controls to better safeguard the confidentiality, integrity, and/or availability of systems and data

What then are some possible operational security management controls that organisations can put in place to better protect physical and environmental security? For starters, when approaching operational security management, organisations should live by the risk-based mantra that the higher the value and the risk, the higher the level of protection.

Organisations can also break down operational security management into two manageable categories: securing areas and securing equipment. More ambiguous than equipment, secure areas are sites where organisations handle sensitive information or keep business-critical IT equipment and personnel. Operational security management provisions would deal with protecting the physical environment in which those assets are housed, e.g., buildings, offices, data centres, etc.

To this end, organisations should be looking at the specific risks of physical access to those assets. Organisations must then deploy operational security management controls, where appropriate, to manage (limit or simply control) physical access.

Operational security management protocols for equipment security should follow a similar logic. Organisations should consider where their equipment is housed and whether that equipment is housed appropriately. Practically, that puts the onus on security managers to ask risk-based questions like:

Is important IT equipment vulnerable to water damage or other form of compromise?

Where are cables running?

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

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

What are some specific operational security management controls organisations can put in place? Well, international security management standard, ISO 27001, recommends the following measures for securing areas and equipment:

Operational security management controls for securing areas and equipment

Secure areas	
Type	**Control**
Physical security perimeter	Security perimeters (barriers such as walls, card-controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.
Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
Securing offices, rooms, and facilities	Physical security for offices, rooms, and facilities shall be designed and applied.
Protecting against external and environmental threats	Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied.
Working in secure areas	Physical protection and guidelines for working in secure areas shall be designed and applied.
Public access, delivery, and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
Equipment security	
Type	**Control**
Equipment sitting and protection	Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.
Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.
Removal of assets	Equipment, information, or software shall not be taken off-site without prior authorization
Security or equipment off-premises	Security shall be applied to off-site equipment taking into account the different risks of working outside the organization's premises.
Secure disposal or re-use of equipment	All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.
Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection
Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

Building a best-practice operational security management practice

The operational security management controls detailed above all serve as a means of preventing unauthorised access, damage, and interference. There exists the danger, though, that those controls will be implemented piecemeal.

To be effective, operational security management
controls have to be in keeping with a broader physical security strategy. Here, companies should think holistically about how the part (operational security management) fits into the whole (physical security management). Steps might include:

- Integrating the allocation of physical security resources into the organisation's overall mission, objectives, and goals
- Consolidating operational security management controls and other physical security functions into an internal security office that reports directly into the C-suite
- Naming a director of Security who would be responsible for managing and allocating physical resources based on risk assessments and using pre-defined metrics measures to justify the allocation of security resources
- Periodically reassessing that resource allocation

Operational security management technology to achieve your physical security objectives

Another thing: the physical security capability itself can't exist in a silo – not from IT or from the other safety-promoting programs in the organisation. In fact, we'd go so far as to say that the physical security program should involve active collaboration of the C-suite and Security Management with the facilities management, work safety, emergency management, crisis management, and business continuity programs.

Nor should that collaboration be in name only. Safety and security protecting software systems should all be integrated, as well. That's because in a given organisation, the relevant information relating to physical security risks will oftentimes exists in multiple software platforms. That information becomes especially pertinent during a security incident.

How to ensure that information is available to security personnel when it matters most? These operational security management software capabilities are critical:

Make your security guards your data centres. By nature of the game, security guards will be field-focused. But that doesn't mean they can't be valuable sources of actionable data, both before an incident occurs as well as in the middle of incident response. However, most operational security management platforms don't do a great job of empowering guards to do the kind of data gathering and transmission work that actually reduces physical security risk and improves the efficiency of operational security management controls.

To better leverage guards' data-gathering potential, security teams need mobile physical security software that gives field personnel the ability to easily capture rich logs for patrols, shift-changes, parking infringements, lost and found property, security escorts, and other activities.

An added bonus: incident reports delivered via mobile also give security managers more context into the security event itself than manual reports, generated hours or days after the fact.

Add geospatial functionality to a mobile solution. Geographically dispersed asset systems are quickly becoming the norm, especially in the era of COVID-19. An unintended consequence: components in the field often lack appropriate physical security.

Overcoming that particular challenge takes operational security management software that gives teams real-time spatial information, via fully integrated mapping features. That way guards and the rest of the security team can better visualise the locations of risks, incidents, people, and other assets.

What specific mapping capabilities are required? Foremost, locations should be automatically geo-referenced, so that teams can create maps of events, assets, risks, etc. Once created, those maps should be publishable on system dashboards, in reports, or as feeds. Operational security management software should also enable security teams to design their own maps, by selecting and filtering layers of information, as well as visualising spatial data.

Enhance information flow, enable multi-channel communication. Another limitation of traditional, command- and control-based physical security operations is that their underlying paper-based processes severely restrict the way information flows. In many cases, the business units who help manage risk and response have little to no access to relevant physical security data.

Operational security management apps can help, though, enabling teams to communicate, share information, and follow-up across a variety of channels, *all within the mobile app itself*, including dedicated, event-specific chat rooms, email, SMS, and app notifications.

Additional, advanced features to improve collaboration in a mobile setting include workspace dashboards for security managers, supervisors, dispatchers, and patrol officers.

Meet duty of care obligations. Physical security threats exacerbated by increasing mobilisation often compromise legally-mandated work safety protections. Since mobile operational security management apps enable security personnel to capture information faster, they bring much-needed speed and efficiency to incident response, especially when integrated with safety management software that handles the health aspect of business continuity management.

Other features to consider include best practice safety forms for the most common health and security-compromising incident types: fire, explosion, bomb threat, hazardous materials, industrial action, vehicle incident, etc.

From business-as-usual to crisis and back again. As mentioned, operational security management has important overlaps with crisis and emergency management. Security incidents can spiral into larger, critical events, which usually necessitate coordinated, cross-functional interventions. It's possible, however, to respond to those types of incidents within the same, integrated solution.

Of course, security teams do more than tackle critical incidents. There're also a number of routine business-as-usual operations they engage in on a daily basis, e.g., patrols, checks, inspections, and business-as-usual logging and reporting. The right operational security management solution should bring demonstrable efficiencies to those operations, as well: in essence, scaling up to meet extraordinary incidents and back down for routine operations.

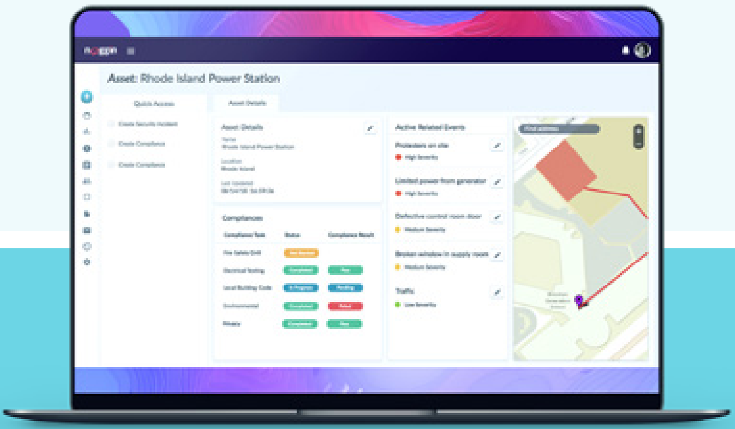
Finally, the COVID-19 crisis has exposed many of the weaknesses in operational security management controls. Integrated security management software for physical operations can bring much-need efficiencies, even when staff is geographically distributed. Looking to build your business case for a software solution that scales with the pace of physical security crises? Download our buyer's guide to operational security management software.

Like what you read? Follow Noggin on social media

@teamnoggin

facebook.com/teamnoggin

linkedin.com/company/noggin-it



noggin
for Security

Meet the next-generation tool for corporate crisis and business continuity management teams to collaborate, plan, track their response, and share information. Built on the Noggin Core platform, Noggin Security gives response teams and decision makers the tools to know what's happening, collaborate quickly and effectively, make better decisions, and enact the right plans to take action when it counts the most.

The Noggin Security solution pack is backed by the Noggin Library with hundreds of plans and best-practice workflows, out of the box, and installed in minutes.

To learn more,
visit: **www.noggin.io**
or contact: **sales@noggin.io**