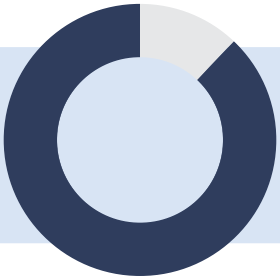
5 Hidden Costs of a Physical Security Breach

As the C-suite continues to prioritize “doing more, with less,” often physical security teams are placed in the crosshairs, tasked with ensuring the safety and security of the organization with the resources they already have. But tying their abilities to protect from and mitigate risks to the financial impact to the company can go a long way in justifying additional investment in tools and technology that address physical security concerns.

Security leaders – 88% to be exact – say they’ve experienced a dramatic increase in physical threat activity since early 2021, according to the 2022 State of Protective Intelligence Report from Ontic.



And 84% say they feel less prepared to handle those threats now compared to last year.

The same report found that the majority of companies are ignoring the risks to their organizations, resulting in more reactive measures (rather than proactive security), a lack of workplace violence training, policies and procedures that are inconsistent, and a lack of cross-functional communication with multiple departments.

> The result? Around 83% of respondents said:
> **“Unmanaged physical security threats are increasing corporate risk, are having a financially crippling effect, and are negatively affecting business continuity at my company.”**

WHAT IS A PHYSICAL SECURITY BREACH?

Physical security breaches involve a loss of property or information due to a space (such as an office or building) becoming compromised.

WHAT IS THE COST OF A BREACH?

While it’s typically difficult to quantify the effect of a physical security breach, since the impact of a breach will vary based on numerous factors, there are some hidden costs associated with such breaches that many businesses might not consider, including:

Brand Reputation

In the event of a large-scale physical security breach that directly impacts the health and well-being of employees, many companies experience a loss of trust in the organization. This can result in a loss of clientele, customers, and trust. Addressing the brand’s reputation and managing the crisis is costly – especially if you don’t have an internal crisis management team to jump in.

According to a report from The Economist that looked at the top eight scandals from 2010 to 2018, it found that while all of the companies survived, they were worth, on average, **30% less today than they would have been based on their peers.** In the event of a breach, costs can go up exponentially if you’re not prepared.

Employee Well-being

There’s a direct link between employee wellbeing and the feeling of safety. The latest focus for maintaining a profitable business enterprise has moved beyond just workplace safety to include overall employee health and wellness. Physical security breaches can have a negative impact on the mental health and wellbeing of employees, resulting in decreased productivity and turnover.

High turnover results in the constant onboarding and offboarding of employees, which **can cost a company 1.5 to 2 times the employee’s salary**, according to Deloitte.

Intellectual Property Loss

Deloitte reports that intellectual property (IP) can constitute **more than 80% of a single company's value today**, making loss of IP especially damaging to brands.

IP theft can mean lost revenue, higher costs of IP protection, damage to brand, and a lack of incentive for teams to innovate because of potential theft. Taken together, this can be especially damaging for an organization in the long-term.

Insurance Claims

Breaches and theft of IP or damage to infrastructure can cause insurance rates to climb, not to mention the amount spent on deductibles. Oftentimes, having technology in place to protect assets can offset these costs, resulting in lower insurance payments and better protection for the business.

Revenue Loss

Ultimately, a physical security breach – no matter how serious – can result in a loss of business continuity, which directly impacts productivity and the ability for an organization to generate revenue. This can have a direct impact on the organization’s bottom line, affecting all levels of a company long-term.

While this isn’t a comprehensive list, the overall cost of a physical security breach can’t be determined by industry averages. The size of the company, scope of the incident, and subsequent fallout can vary. But there are ways to minimize the risk to an organization.

HOW DO YOU ADDRESS PHYSICAL SECURITY RISK?

There are three tools that organizations can use to address the risks associated with physical security breaches centered around identifying, assessing, and mitigating risk.

Governance

Put simply, governance is the documentation through which security organizations apply structure and direction to their operations in a formal way. Governance suites include policies, frameworks, standards, procedures, and templates that define and enable the operating requirements for running a security function. Beyond streamlining security operations, a governance suite is critical to ensure security functions have key risk controls in place to meet legal and regulatory obligations.

Culture

The security culture of an organization is defined as the ideas, customs, and social behaviors of a group that influence its security. This encompasses everything from the internal campaigns they run to the willingness of various departments to engage with security teams cross functionally. Focusing on security culture and building knowledge around best practices for physical (and cyber) security is a critical piece of the program effectiveness measurement. And employees are often at the center of this initiative; they can either be easy prey, or they can become an effective human layer of defense.

Technology

Finally, the organization must prioritize the ability to measure the effectiveness and progress of the security program using technology. A powerful place to start is identifying software technology that addresses the three tenants of risk management. Features like proactive threat intelligence (identify), mass communication and emergency response communication tools (mitigate), and false alarm management/built-in standard operating procedures (assess) go a long way in helping security leaders who are responsible for the risk management lifecycle.

Ultimately, risk to the physical security of an organization is a risk to the company's bottom line, creating a ripple effect across departments and affecting revenue. The best way to address risk and protect people, assets, and the brand, is to make strategic investments in innovative technology that balances business goals with protection.

HiveWatch