

Uniting Cybersecurity & Physical Security: A Modern Government Strategy



Table of Contents

3 Foreword

PART 1

4 Understanding the need for physical security and cybersecurity convergence

PART 2

7 Better together: restructuring security teams for better outcomes

PART 3

11 The value of physical security and cybersecurity convergence

PART 4

13 A new approach: why proactive strategies are the future of security

PART 5

16 Why the cloud is key to successful convergence

18 Thinking holistically

Foreword

In this e-book, we will outline the key components of a modern government security strategy and share best practices to strengthen security posturing, protect constituent data, and future-proof your organization with cloud-based technologies.

Today, very few agencies are running without cybersecurity and physical security systems in place. However, as IoT technology for organizations evolves and more systems move into the cloud, agencies should continuously reevaluate their security strategies to identify potential risks.

While no organization plans to be the victim of a breach, being proactive with physical and IT security convergence can help protect your employees, constituents, and even your yearly budgets.

The cost of a data breach averages \$3.86 million globally

In order to improve the value of physical security and cybersecurity for your agency, new strategies need to be developed and implemented that address the emerging threats of a new security landscape.

[IBM – COST OF A DATA BREACH REPORT 2021 →](#)

PART 1

Understanding the need for physical security and cybersecurity convergence

“In digital transformation, strategy must come before technology.”

DON ERICKSON

CEO, Security Industry Association



The security industry fulfills a crucial role in cybersecurity and national security by providing systems that manage credentials for government workers and contractors and control access to facilities and computer networks.

Competing priorities and the lack of available resources, however, have limited the ability of many agencies to modernize their physical security systems with equipment and software that include security protections that meet federal standards. In many cases, low-assurance authentication mechanisms are in use, leaving significant physical security and cybersecurity risks unaddressed. Though cybercrime is often the leading concern and media-covered issue for governments, when it comes to security, these incidents are frequently linked to oversights in physical security practices.


Think about your building's access control system: it likely contains personally identifiable information and a log of access activity throughout your property, and it controls which doors are locked or open. Moreover, governments control the access to critical

infrastructure and buildings, such as utilities. Now imagine if the wrong person gained access to those controls, compromising not only the security of sensitive data but the safety of your employees and constituents. It's not an implausible event. In fact, a strong cybersecurity strategy is essential to safeguard the sensitive data that physical systems retain.

Similar to how physical security protects cybersecurity by limiting who has access to spaces where data is stored, the reverse is also true. Physical security components connected to the internet, such as RFID key card door locks, video surveillance cameras, and smartphones are all common targets for hackers.

By taking a **holistic approach** to physical security and cybersecurity, agencies have the opportunity to improve security across the board and prevent costly breaches before they occur.

Understanding the relationship between physical security and cybersecurity components



	Physical security	Cybersecurity
Detecting threats	Video alerts, alarms, access alerts	Network monitoring
Preventing intrusions	Doors, gates, turnstiles	Firewalls and encryption
Limiting access	Door locks	Passwords, MFA, IP restrictions
Vulnerability fixes	Hardware and software upgrades	Patch management
Incident response	Reporting and hardware audits	System audit logs
People and culture	Security awareness training	Cybersecurity training

PART 2

Better together: restructuring security teams for better outcomes

In addition to bringing systems together, successful physical and IT security convergence must also bring together the people who manage, monitor, and make business decisions for these functions. Knowing which roles should have a seat at the table is imperative. In this case, physical security and IT leaders should work as a unified team to ensure the right technology is deployed and that there are best-practice programs and processes in place to maximize security within and across government agencies. Some of the key players in a converged security strategy include the chief security officer (CSO), chief information security officer (CISO), and IT director, along with the emergency planning director, police chief, operations director, facilities director, and additional physical security titles within your jurisdiction.



“A unified team is also quicker to adopt and evolve best practices across both physical and IT functions, resulting in a more efficient team structure and better productivity.”

By merging physical and IT security teams, convergence creates better communication across previously siloed departments. Creating an avenue for formal collaboration gives teams a better way to share information from their prospective systems and apply those learnings holistically to improve both cybersecurity and physical security. Establishing open lines of communication between these roles—and leveraging data compiled from integrated systems—gives government leaders a more complete picture of security posturing across their organizations and communities. Physical and IT security convergence also aligns risk and threat assessment under one holistic view, which is key for identifying potential vulnerabilities in the system for a faster, more accurate incident response.

Creating shared goals and KPIs, eliminating redundancies, and clearly defining which roles are responsible for specific tasks helps establish a unified team. It's also quicker to adopt and evolve best practices across both physical and IT functions, resulting in a more efficient governing structure and better productivity.

Cybersecurity and physical security convergence implementation checklist

How prepared is your organization?
Use this checklist to assess your readiness.

Audit your current security systems for vulnerabilities, oversights, and gaps

Do they have automatic updating for patches and firmware?

Identify redundancies between cybersecurity and physical security teams

Unify IT and physical security teams

Formalize new teams and roles

Enable open information sharing and communication across departments

Set common goals and KPIs to align strategies

Install controls to limit access to specific areas (including virtual spaces)

Survey your site for camera coverage

Secure IT and server rooms with physical access control and video surveillance

Integrate security systems and data to provide a more complete picture of what's happening in the space at any given moment

Migrate to cloud-based solutions to centralize security operations

Conduct a risk assessment to determine which systems are most vulnerable

Determine hardware and software requirements

Select systems that can easily integrate with existing security infrastructure

Train personnel on new systems and platforms

Build out new processes and strategies for risk management and incident response

PART 3

The value of physical security and cybersecurity convergence

When IT and OT converge, some amazing results can materialize, both planned and unplanned.

Security systems are an important investment for any government, yet it can be difficult to make the value case for a new system until after a costly breach or incident. Merging physical security and cybersecurity adds **significant value** to your agency, providing scalability and flexibility for the future via improved team efficiency, streamlined processes, and reduced costs.

Converged security that employs full-system automation can also have a measurable impact. Automation is an area of focus for many governments and is very relevant as a security trend as IoT devices continue to expand. The possibilities of fully integrated building systems, with data from every

corner of every building ingested into AI-powered business intelligence tools, means agencies are able to analyze and apply learnings quickly, with increasing accuracy. Automation helps streamline tasks and inform governing decisions, freeing up valuable time and IT resources while strengthening security posturing, sustainability efforts, and building positive employee and constituent experiences at the same time.

PART 4

A new approach: why proactive strategies are the future of security

“A successful cyber or physical attack on connected industrial control systems (ICS) and networks can disrupt operations or even deny critical services to society.”

**CYBERSECURITY & INFRASTRUCTURE
SECURITY AGENCY →**

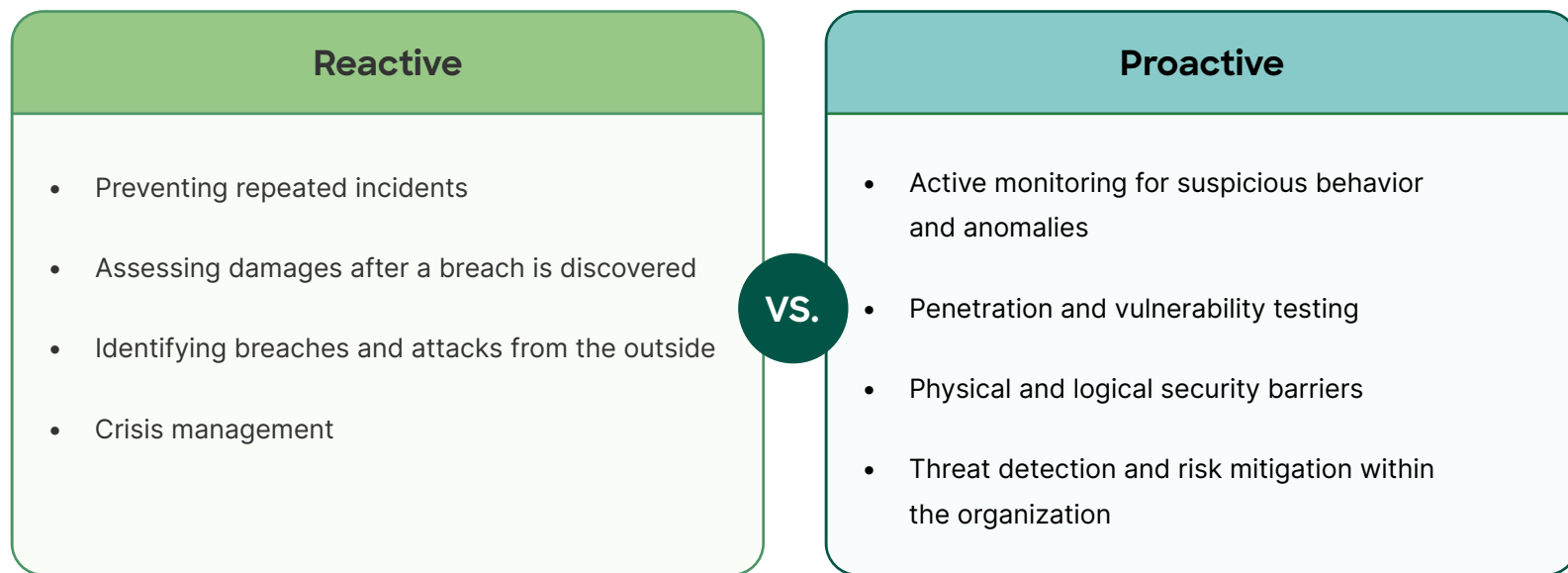
In a government agency that employs reactive security strategies, nothing happens until after a breach, attack, or incident. Proactive security, on the other hand, works to prevent an incident before it occurs. Both strategies have value, however, many organizations forego proactive strategies because they think it is too expensive, time consuming, or difficult to manage. With the right systems and tools in place, proactive security is less costly in the long run. By taking advantage of cloud-based infrastructure, remote management, automated system processes, and triggered alerts, teams can proactively monitor security with less investment.

While proactive security is necessary to prevent the costly damages of a breach, reactive security is still important. Even with the most advanced security technology, agencies cannot anticipate every possible threat. If something does get through your security measures, reactive strategies need to be used to understand why it happened and identify methods to prevent a repeat event.

“Organizations with proactive security strategies experience 53% fewer cyberattacks and breaches.”

**THE ECONOMIST INTELLIGENCE
UNIT REPORT**

Reactive vs. proactive security



PART 5

Why the cloud is key to successful convergence

The prevalence of cloud-based solutions can be hugely beneficial to governments that want to be more scalable and flexible. However, not all systems are designed to “play nice” with the cloud. Many traditional on-premises systems are unable to fully integrate with newer cloud-based solutions and are limited in their functionality, even if they can integrate. When it comes to security technology, operating on an outdated system is like leaving your front door wide open for potential threats. Hackers are already familiar with the technology, and it’s more likely to be the target of new vulnerabilities and threats. Cybersecurity and physical security systems that are completely cloud-based and interoperable not only give you the best protection against security threats, they also have surprising ROI implications.

For instance, one of the key benefits of a cloud-managed security platform is that important software updates can be deployed over the air (OTA), minimizing the disruption to operations and eliminating the cost of in-person maintenance. OTA updates also mean your systems are always running the latest version of the software, giving you better protection from emerging security threats as soon as they are identified. In a world where hackers and cybercrime are a constant threat, having peace of mind that your physical access control, video surveillance, and identity management systems are secure is invaluable.

Another benefit of the cloud is the ability to seamlessly integrate and automate processes across your organization. The value of physical security and cybersecurity systems depends on an agency’s ability to apply convergence strategies across the technology. The pandemic has taught governments that IT modernization is possible and successful, but they must continue with this growth. More and more, outdated on-premises technology can limit distributed teams and multi-location departments from sharing important security information automatically—and it can be more difficult to scale security practices to other buildings and sites. Because physical and IT security convergence is dependent on collaboration and communication between both people and systems, **modernizing to cloud-based security technology** is an important step to successfully improve security posturing.



Thinking holistically



Creating a holistic approach to physical security and cybersecurity comes down to three main components: strategy, roles, and technology. Outlining a strategy that merges physical security and cybersecurity practices across teams and systems helps governments identify current security vulnerabilities and defines the goals and objectives for the entire organization moving forward.

The pandemic showed that governments could change quickly, but it also demonstrated that the future of physical security combined with IT will be drastically different from what we know today. With IT and IoT united, teams will be able to predict and mitigate threats before they occur, freeing up resources to focus on strategic governing, enhanced planning, and positive constituent experiences. Every step forward in transformation is a step closer to realizing this vision. After all, this IT/IoT convergence is not a destination, it's a journey.



Visit [our website](#) to learn more

Take a proactive approach to your organization's
security today with an [instant demo](#).