cisco Meraki

A Guide to Converged Cybersecurity and Physical Security

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 Wrap up

Foreword

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

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

While no company plans to be the victim of a breach, being proactive with physical and IT security convergence can help protect your business—and your bottom line.

The cost of a data breach averages $3.86 million globally

IBM – COST OF A DATA BREACH REPORT 2021

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

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

Though cybercrime is often what companies are most concerned with 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 employee identity information and a log of access activity throughout your property, and controls which doors are locked or open. 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 customers. 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. A strong cybersecurity strategy is essential to safeguard the sensitive data that physical systems retain.

By taking a holistic approach to physical security and cybersecurity, businesses 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. 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 across the entire organization. Some of the key players in a converged security strategy include the chief security officer (CSO) and chief information security officer (CISO), IT director, physical security employees, and facility managers.

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.

“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. ”

Establishing open lines of communication between these roles and leveraging data compiled from integrated systems gives leadership a more complete picture of security posturing across the organization. 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.

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. Additionally, creating shared goals and KPIs, eliminating redundancies, and clearly defining which roles are responsible for specific tasks helps establish a unified team.

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 areas containing sensitive information
- [ ] 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 business, yet it's often 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 business providing scalability and flexibility for the future. This is realized via improved team efficiency, streamlined processes, and reduced costs.

Converged security that employs full system automation can also have a measurable impact. Automation is a security trend that's gaining traction as IoT devices continue to flood the market. The possibilities of fully integrated building systems, with data from every corner of every building ingested into AI-powered business intelligence tools, means businesses are able to analyze and apply learnings quickly, and with increasing accuracy. Automation helps streamline tasks and inform business decisions, freeing up valuable time and IT resources, while strengthening security posturing, sustainability efforts, and building experiences at the same time.

PART 4

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

"We're just scratching the surface. The holy grail is being able to predict incidents before they occur and prevent them."

MICHAEL GIPS
Chief Global Knowledge and Learning Officer, ASIS

In an organization that employs reactive security strategies, nothing happens until *after* a breach, attack, or incident. On the contrary, proactive security 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 and/or 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, businesses 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

Reactive		Proactive
• Preventing repeated incidents • Assessing damages after a breach is discovered • Identifying breaches and attacks from the outside • Crisis management	VS.	• Active monitoring for suspicious behavior and anomalies • Penetration and vulnerability testing • Physical and logical security barriers • Threat detection and risk mitigation within the organization

PART 5

Why the cloud is key to successful convergence

The prevalence of cloud-based solutions is hugely beneficial to businesses 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. 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.

One of the key benefits of a cloud-managed security platform over legacy on-premises solutions 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 your teams' ability to apply convergence strategies across the technology. Outdated on-premises technology will greatly limit distributed teams and multi-location enterprises from sharing important security information automatically, and make it 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.

Wrap up

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 businesses identify current security vulnerabilities and defines the goals and objectives for the entire organization moving forward.

The future of physical security combined with IT will be drastically different from what we know today. Teams will be able to predict and mitigate threats before they occur, freeing up resources to focus on strategic action and decisions. Every step forward in transformation is a step closer to realizing this vision.

This convergence is not a destination—it's a journey. Every transformation should start with a clear vision that is communicated by leadership. This vision should also prepare team members to expect disruption as part of the process; incremental growth will take too long and preserve too many legacy systems. A team that understands this reality and meets every challenge with a solution-oriented mindset will succeed.

Meraki

To learn more, visit Meraki.com

Ready to take a proactive approach to your organization's security? Email our IoT sales team to discuss further: merakiiot@cisco.com.