VANDERBILT

News

4 Ways To Ensure Cyber Protection with Physical Security Solutions

In a world where ever-evolving technology produces incredible innovations, it raises threats and concerns for global organizations more than ever before. In response to this increasing threat, the security industry must commit to being as proactive as possible by educating, training, and staying updated on cybersecurity practices.

The issues surrounding cybersecurity are increasing yearly as technology advances and cyber risks become more prevalent. According to BITM “As the digital landscape continues to evolve, cyber security remains a top priority for organizations of all sizes”. Many organizations seeking to implement integrated security solutions must ask what risks their security system can create.

In this article we will be exploring some of the key ways global organizations can ensure cyber protection with physical security solutions:

1. User Awareness and Detection

Security knowledge should be focused on awareness for all by training employees with key roles, and educating cybersecurity specialists. Insider threats caused 59% of data security incidents throughout 2021. These incidents typically consisted of accounts being misused by internal employees or business associates resulting in data leaks that potential online criminals are looking to take advantage of.

According to Forrester, around “39% of organizations experiencing trouble with insider data leaks cited a lack of budget, and 38% cited a lack of internal expertise as the reason behind insider leaks in their organizations”. In addition to this, 29% claimed that they do not see employees of the company as a significant threat to their company’s data, making it a bit easier to speculate why the number of organizations without risk of strategy is as high.

At ACRE, we understand the importance of education with regards to cybersecurity, not only for customers looking to protect themselves online but also for employees in the industry. By adequately educating our employees and training them to manage accounts accordingly, we can ensure that we remain among the global firms with insider risk strategies that exceed expectations.

Cybersecurity awareness needs to be at the forefront to stop attacks like phishing or false authentication. Upwards of 90% of cybersecurity incidents are not as a result of weak firewall policies, but, a result of a lack of cyber security awareness training for employees. This commonly results in people making ill-informed decisions in their day-to-day activities, and ultimately facilitating a security incident.

2. Physical and Cybersecurity Convergence

Security convergence refers to the merging of physical security systems with cybersecurity measures. According to the 2023 Security Megatrends report by the Security Industry Association, “convergence has been challenging on vendors, integrators and practitioners as their scope of work and duties have expanded greatly”. Through vast digital integrations, facilities can approach security as a whole rather than separately. Unified workplace solutions will therefore greatly reduce security risks that may arise.

The idea of physical and cybersecurity convergence is not new and has been a discussion amongst industry leaders for many years. It has been proven that organizations with combined physical and cybersecurity operations are better prepared and more robust enabling them to easily define risks, and prevent, mitigate, and respond to threats plaguing the organization. Convergence also allows data sharing and unified growth of security best practices across security departments.

Best practices within an organization merging physical and cybersecurity measures include the encouragement provided for employees to view cybersecurity as a necessity for themselves and the organization. A holistic approach must be defined and expanded to cover applications and workloads during runtime wherever they may reside to protect our enterprise systems better. This is the only way to ensure that the correct code and processes can execute and nothing else, regardless of the threat environment.

3. Multifactor Authentication and Encryption

Individuals simply assigning or attempting to create passwords with letters, numbers or characters is no longer a sustainable security option for most devices. Those seeking harm will try to crack passwords with highly sophisticated programs and have been known to use all types of brute-force attacks to get what they want. Multifactor authentication is vital in this day and age. The amount of security it provides facilities is well worth the minor inconvenience of two or three logins.

Regarding our security solutions, ACRE strives to balance our security strategy. Adhering to cyber security best practices, we actively train our specialists to be conscious of security and data protection in every step of the product lifecycle from initial concept through retirement. With multi-layered security solutions, encryption is standard across the entire system, aiding compliance and privacy protection to safeguard personal information and ensure maximum system security, from system login to trusted field devices.

Any organization that believes it is doing enough or becomes too negligent in security strategies could be heading down a dangerous path. Organizations must stay engaged and vigilant and remain dedicated to keeping their employees, suppliers, and customers informed. After all, security is and will always be a team effort.

4. Developing Site Access Control Measures

Access control has seen a significant transition over recent years and the introduction of the cloud has significantly impacted organizations in almost every area including business function, data storage, shared workspaces, and general workplace security. The implementation of access control technology revolutionized how facilities monitor and control who can enter your property and when. Furthermore, cloud-based technology has further simplified the process of simply managing and streamlining your access control system for the future.

A lack of access control solutions can be devastating if the wrong person gets in and gains access to your data. Developing enhanced measures that merge your access control solutions with cybersecurity best practices is the best way to advance your facility, safely. Fortunately, innovative solutions, cybersecurity measures and tools will help you to optimize your access control.

In conclusion, preparing your organization with the best tools for preventing cyber risk will help to future-proof and enhance daily operations, safely and securely. Creating awareness around the subject of cyber protection for your facility is key to protecting your organization's people, property, and assets. 2023 is the year to make significant improvements to help streamline services and prepare your industry for longevity beyond the basic cyber security measures that are constantly evolving.