VANDERBILT

News

ACRE & Cybersecurity: What You Need to Know

When you think of cybersecurity threats, you probably think of internet criminals going out of their way to harm you, right?

The people out in **cyberspace** that invade your privacy are usually the ones we prepare to protect ourselves from. Still, what if those people weren't the only threats we need to be wary of? According to a recent report from Forrester, this is the case more often than we think. Insider threats at security firms caused 59% of data security incidents over the last year, typically consisting of accounts being misused by internal employees or business associates, resulting in data leaks that would-be online criminals are looking to take advantage of.

With this in mind, why does it appear to be so common among cybersecurity firms? The most likely reason is that a staggering 70% of EMEA organizations have little to no risk strategies set in place to prevent insider data leaks.

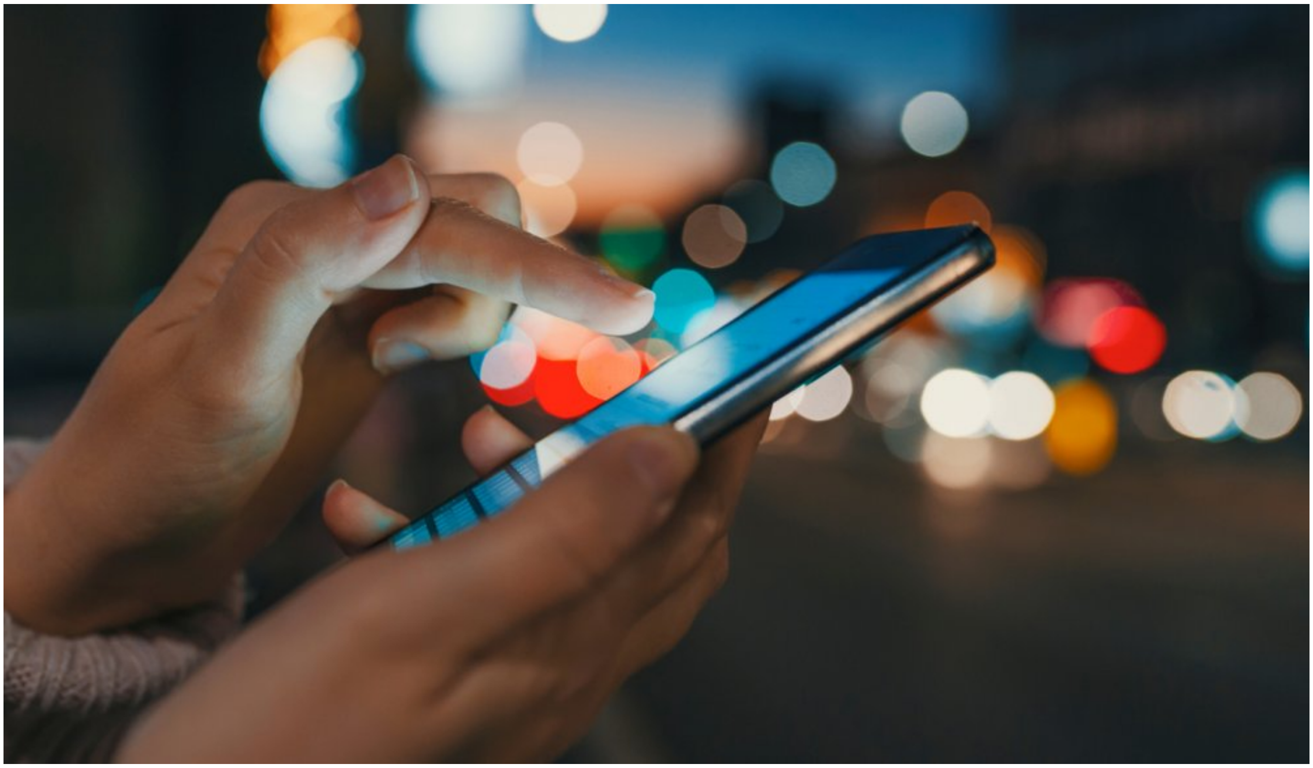
Suppose insider risk is such a prominent issue in the **cybersecurity** industry. Why are companies failing to take action against this problem? According to Forrester, around 39% of organizations experiencing trouble with insider data leaks cited a lack of budget, and 38% cited a lack of internal expertise as the reason behind insider risks 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 a risk strategy is as high.

So we've identified the problem: some organizations aren't taking the risk of insider data leaks as seriously as they probably should, but what can we do to fix this? According to a report from Forrester, 65% of respondents cited staff training as a solution, 50% cited manual monitoring of employee activity, and 47% cited improved encryption as a potential tactic to quell insider risk.

At ACRE, we understand the importance of education in the **cybersecurity** industry, 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 cybersecurity firms with insider risk strategies that exceed expectations.

Physical and Cybersecurity Convergence

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



User Awareness and Detection

Cybersecurity needs to be at the forefront to stop attacks like phishing or false authentication, and mitigate threats. Upwards of 90% of **cybersecurity** incidents are not as a result of IT infrastructure weaknesses, such as weak firewall policies, but actually as a result of a lack of employee cyber security awareness, resulting in people making ill-informed decisions in their day to day activities, and ultimately facilitating a security incident.

Best practices in an organization include encouraging employees to view cybersecurity as a necessity for themselves and the organization. Suppose the heads of the organization care deeply about these policies. In that case, it will lead to a better overall organizational culture, and utilizing cyber security solutions while promoting best practices will become the norm across the organization.

Multifactor Authentication

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 in age, and its importance is not spoken about enough. Even if it can cause a bit of a setback, the amount of security it provides is well worth the minor inconvenience of two or three logins.