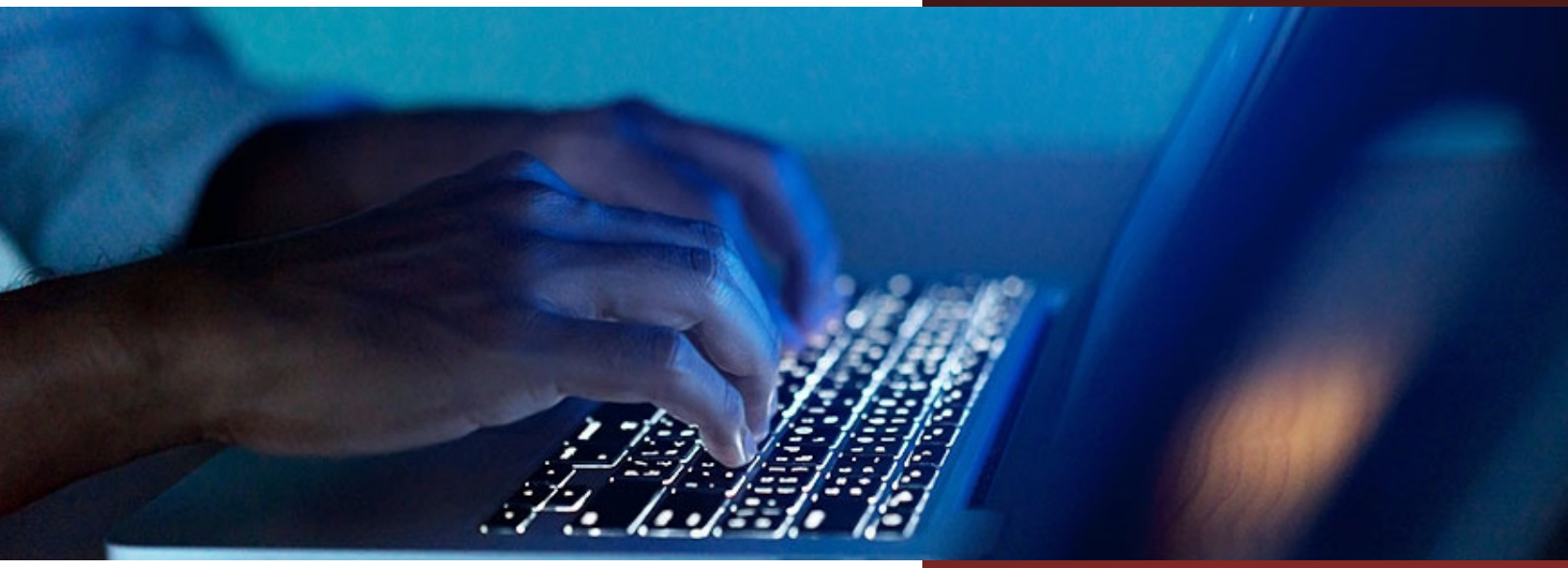
ALERTENTERPRISE



Addressing Insider Threats Requires A Cyber-Physical Blended Approach

While most security teams are focused on preventing malicious outsider attacks, recent data suggests that close to 30 percent of confirmed breaches today involve insiders.

Today's increasingly complex networks across physical, information technology (IT) and operational technology (OT) systems make it difficult for security teams to detect and prevent insider threats. This is compounded by the proliferation of data, devices, applications, and users accessing networked resources.

Rising Insider Malicious Attacks Threat

According to the 2017 U.S. State of Cybercrime Survey, 50 percent of organizations experience at least one malicious insider incident per year. And the Verizon 2018 Data Breach Report found that close to 30 percent of confirmed breaches today involve insiders. In August 2018, a tragic crash involving a Seattle airplane stolen by an employee raised awareness for the need for physical insider threat awareness (as well as more psychological screening before employment).

"As the threat landscape evolves rapidly, CISOs need to step up their game"

"Threats now originate not only in the physical space but also in cyber environments"

"Oftentimes we think the most harmful insider threats are intentional"

"Risk management leaders should start by developing a compelling vision"

As the threat landscape evolves rapidly, CISOs need to step up their game, says Aamir Ghaffar, Director of Solutions Engineering at AlertEnterprise. They should implement security controls that protect their company's people, physical assets, data, intellectual property, and reputation both inside and out. And they need to do it while simultaneously satisfying industry compliance requirements. In response to our questions, Aamir Ghaffar offered some additional insights on the timely topic of insider threats.

Q: We are hearing discussion about the emergence of cyber-physical security systems. What are they and how do they help organizations address insider threats?

Ghaffar: The concept of convergence has evolved in response to risk and the overall threat landscape. Threats now originate not only in the physical space but also in cyber environments – this is what is commonly referred to as blended risk. These blended risks require a converged approach and a converged view of security as a whole; connecting data, building new capabilities and gaining new insights to allow security teams to better defend against attacks.

Q: How are organizations responding?

Ghaffar: They are shifting towards centralization – from the security operations center all the way to the executive level, where one C-Suite executive manages all security across physical, IT and OT domains. According to Gartner by 2023, 75% of organizations will restructure risk and security governance to address new cyber-physical systems (CPS) and converged IT, OT, Internet of Things (IoT) and physical security needs, which is an increase from fewer than 15% today.

Q: How does the shift impact insider threats?

Ghaffar: Unifying cyber and physical unlocks powerful new capabilities. For example, cyber-physical teams faced with a threat such as an intrusive device planted within their network environment, can quickly connect the cyber footprint to a physical location – understanding where the threats originate and identify those responsible for bringing it in. Converging physical and cyber identity through platforms that connect physical access control, IT and OT systems is an example of how organizations can better prepare for blended security threats.

Q: Sometimes the threat is about human error.

Ghaffar: Oftentimes we think the most harmful insider threats are intentional; however, unintentional user behavior and negligence could have serious ramifications for an organization. Organizations should deploy technology that delivers automation and active policy enforcement to prevent employees from making inadvertent yet critical errors. Organizations should also do regular risk assessments – not one and done. Don't implement a process and think you're secure. Automated identity and access management technology can provide scheduled access reviews to help detect high-risk user profiles with accumulated or a toxic combination of access, as well as segregation of duties violations due to department change or job transfers.

Q: What are the biggest misconceptions about insider threats?

Ghaffar: First, that the biggest threats originate outside my company. Or that insider threats are a problem for government agencies and highly sensitive organizations, not "regular" companies like us. A company may also mistakenly think that they have limited assets that could be exposed, or that the assets are of little value; therefore, a large-scale breach is less likely to happen. And even if it does, it probably won't have a big impact.

Q: So, they think "it can't happen here."?

Ghaffar: Yes, and they think their employees are inherently trustworthy, and that with basic security measures in place, the risk is small. They think that insider threats are always intentional. Or they think "it's not my job."

Q: What next steps should security leaders take in addressing insider threats in their organization?

Ghaffar: Security and risk management leaders should start by developing a compelling vision and strategy that will resonate with key company stakeholders. They can expand the visibility they have into user activity beyond things that happen on the network. Go beyond a data-centric approach to a people-centric approach through identity behavior analysis. Improving visibility into user activity and taking a more preventive approach are the best ways to manage risk of an incident. Develop an inside-out approach to security. By converging physical, cyber and OT security you'll gain a holistic view of your enterprise-wide security landscape.

Author Profile

Larry Anderson

Editor, SecurityInformed.Com & SourceSecurity.Com

An experienced journalist and long-time presence in the US security industry, Larry is SecurityInformed.com's eyes and ears in the fast-changing security marketplace, attending industry and corporate events, interviewing security leaders and contributing original editorial content to the site. He leads SecurityInformed's team of dedicated editorial and content professionals, guiding the "editorial roadmap" to ensure the site provides the most relevant content for security professionals.

People Mentioned In This Article

Aamir Gaffar

AlertEnterprise