Publication

Alvin K. Brown, LL.M., J.D.
Security Expert Witness for Negligent Security, Premises Liability, Use of Force, Workplace Violence Prevention, Insider Threat, and Executive Protection Matters

https://www.linkedin.com/posts/akbrownlaw_in-todays-security-landscape-headlines-activity-7364347976497917953-qs0P?utm_source=share&utm_medium=member_desktop&rcm=ACoAAAbCL8oBV1XRNZLhS2LMb_wIyPk9741sc00

In today's security landscape, headlines are dominated by cyberattacks, rapid advances in artificial intelligence, and the promise of autonomous systems. Organizations are investing heavily in technological defenses, yet an essential truth is often overlooked: technology alone cannot secure the enterprise. The greatest vulnerabilities—and opportunities for defense—still reside in the human element.

While sophisticated malware and zero-day exploits attract attention, the majority of successful attacks begin with a simple act of deception. Social engineering—tricking individuals into revealing credentials or granting access—remains the preferred entry point for malicious actors. Privileged access, often entrusted to a select group within an organization, is frequently exploited through human manipulation rather than technical compromise.

Consider the rise of business email compromise schemes, where attackers impersonate senior executives or trusted partners to convince employees to authorize fraudulent wire transfers. In these cases, technology is merely the delivery vehicle; the real attack occurs in the minds and behaviors of individuals. Decision-makers are prime targets, as their actions can have far-reaching financial and reputational consequences for the organization.

Against this backdrop, the private sector must urgently rebalance its security investments. Human intelligence—proactively understanding adversary tactics and employee vulnerabilities—enables organizations to anticipate and prevent attacks before they materialize. Counterintelligence efforts can identify and neutralize attempts by competitors or nation-state actors to infiltrate or manipulate the workforce. Insider threat programs, when implemented effectively, detect and mitigate risks posed by trusted employees before they become incidents.

To lead this shift, organizations require Chief Security Officers (CSOs) with expertise not only in technology, but also in intelligence, fraud investigations, counterintelligence, and insider threat management. These leaders bring a holistic approach, integrating human-centric security disciplines into corporate strategy. Making such skilled CSOs standard across the private sector

is no longer optional—it is essential to safeguard assets, reputation, and competitive advantage.

As threats evolve, so too must our defenses. The private sector cannot afford to treat human intelligence, counterintelligence, and insider threat as afterthoughts. Now is the time for corporate leaders to invest in the people, programs, and expertise that address the human side of security. By doing so, organizations will build resilience not only against today's threats, but also those yet to emerge.

1001 3rd Avenue West, Suite 375, Bradenton, FL 34205
Tel: (941) 953-2825 ~ alvin@sotersolutionsllc.com
www.sotersolutionsllc.com