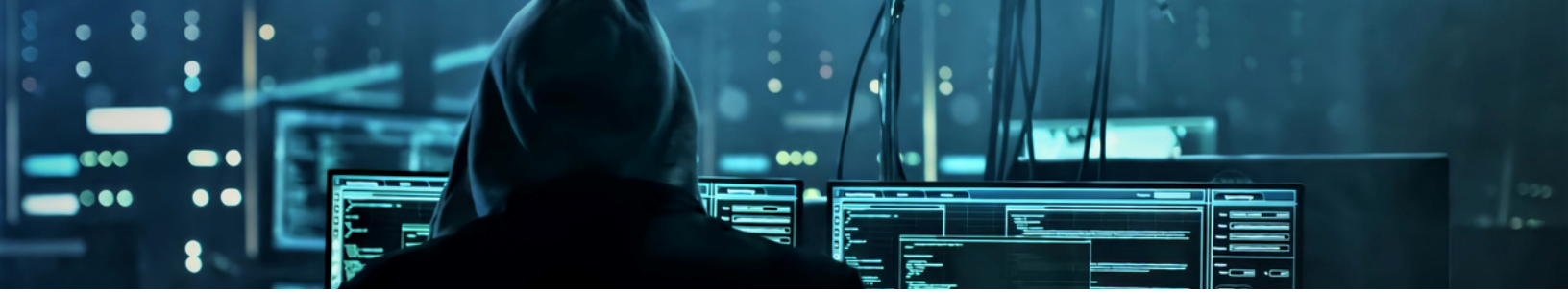


The Insider Threat

By: B. Stephanie Siegmann, Partner
Chair, Cybersecurity, Privacy & Data Protection
Chair, International Trade & Global Security

While serving as a national security prosecutor for more than 18 years at the U.S. Attorney's Office for the District of Massachusetts, I worked with law enforcement on numerous investigations involving employees who committed security and export violations, mishandled classified information, stole corporate IP and trade secrets (typically by emailing files or uploading data to an online platform or cloud storage), shared or disclosed valuable corporate data and IP electronic files with nonemployees or foreign persons, and altered or damaged network configurations or disabled system logs.

The insider threat constitutes one of the most serious national and economic security threats to our country.

Theft of intellectual property costs the United States between 1-3% of its $21 trillion annual GDP. Insider threats are increasing – insider threat incidents have increased over 44% the last two years and are costing businesses more than $15 million annually.

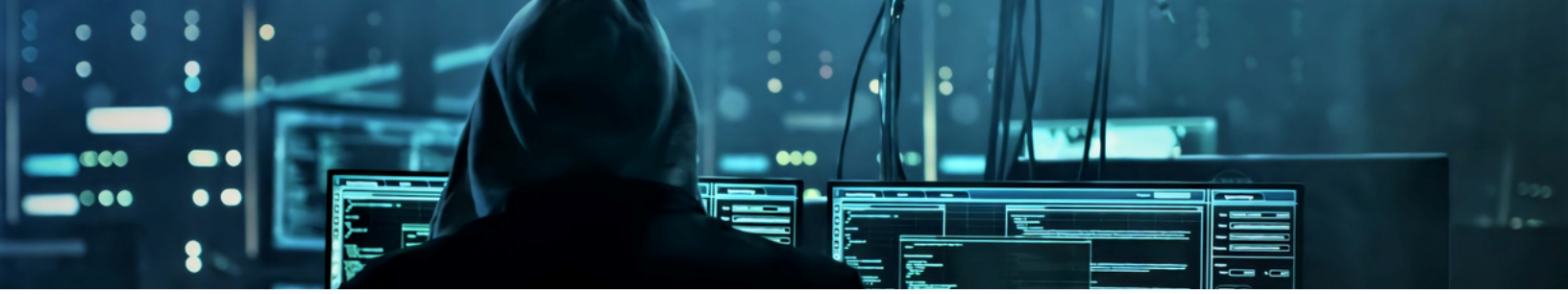
56% of organizations had insider data thefts resulting from employees leaving or joining new companies.

Negligent insiders are as concerning as malicious ones. Attacks that exploit human errors (i.e. phishing emails or business email compromise campaigns) far outnumber viruses, spyware and malware attacks.

Insider Threat Activities

- Fraud
- Data theft
- Damage and alterations to corporate network
  - Change critical configurations of corporate network
  - Prevent corporate systems from operating normally
  - Create backdoors for outside attackers
- Misuse of valuable corporate assets for personal gain

HINCKLEY ALLEN



Common Indicators/Red Flags

- Misuse of travel, time, and expenses
- Unexplained change in financial circumstances
- Behavioral changes such as decreased work performance, unexplained absenteeism, or conflicts with co-workers and supervisors
- Downloading/printing of large volumes of corporate data
- Engaging in security violations such as trying to bypass security measures or using unapproved storage devices (i.e., flash memory, USB sticks, etc.)
- Sending sensitive proprietary data or emails with large attachments to third parties
- Exhibiting a pattern of recent access to sensitive or proprietary records and systems, files, or accounts of other employees
- Showing interest in projects outside their area of responsibility and accessing sensitive files and data unrelated to their position
- Accessing office during non-working, odd hours
- Remotely accessing server during non-working hours, while on vacation, during a holiday, or from a foreign/unrecognized IP address

How can you protect your company from insider theft and industrial espionage/mitigate the risk?

- Carefully screen and review new hires and perform additional background checks prior to approving promotions or granting additional access.
- Monitor and record user/employee activities (including online activities such as websites visited, email exchange accessed/used, files and applications downloaded and uploaded, online searches conducted, manipulation of files or data, printing and USB drive connection activities).
- Audit and analyze user activity records and set alerts to respond to suspicious activities.
- Limit privileged access, especially to your organization's crown jewels and most valuable IP, and establish "need to know," role-based access controls on your network.
- Implement zero-trust model and adopt multi-factor authentication measures on your network.
- Manage electronic storage and USB devices across your network.
- Create/update cybersecurity policies and guidelines with focus being to build culture of IT security awareness.
- Develop Insider Threat Protection Program and provide training to employees, contractors, and vendors on common security mistakes and insider threat indicators.

Please email B. Stephanie Siegmann at ssiegmann@hinckleyallen.com if you have any questions or need assistance developing your organization's Insider Threat Program.

HINCKLEY ALLEN