SEC

SECURITY EXECUTIVE COUNCIL

A research and advisory firm

How Does Your Insider Threat Compare?

A short evaluation of your insider threat vulnerability

Bob Hayes and Kathleen Kotwica

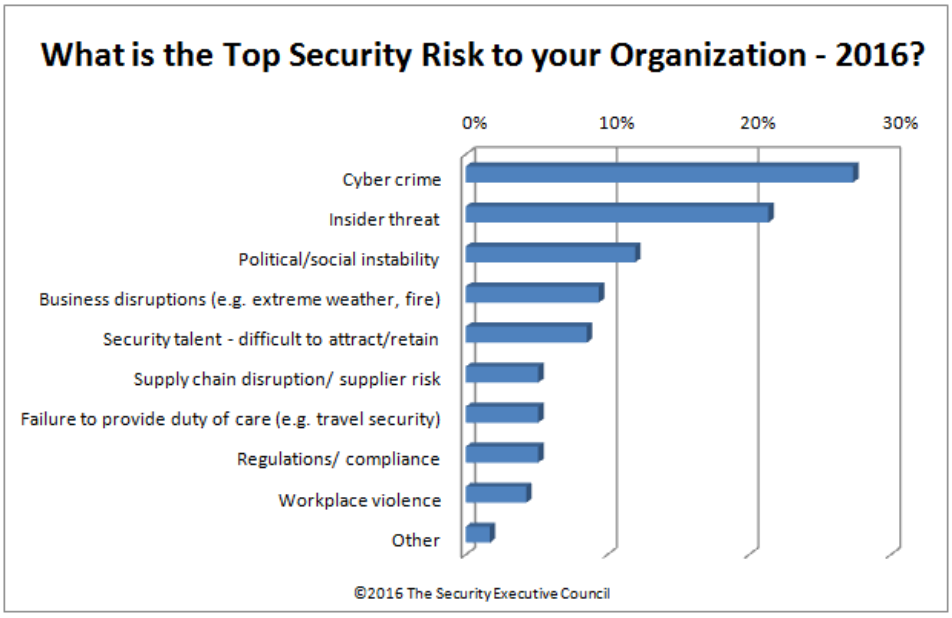
In May of 2016, the DOD published Change 2 to DoD 5220.22-M, "National Industrial Security Operating Manual (NISPOM)." This requires government contractors to establish and maintain an insider threat program to detect, deter and mitigate insider threats. While “contractor” means any industrial, educational, commercial, or other entity that has been granted a facility security clearance – the fact the US government is mandating an insider threat program has gotten the attention of private business leaders and Boards of Directors. Many companies are now building or enhancing their insider threat program – and beyond classified information security.

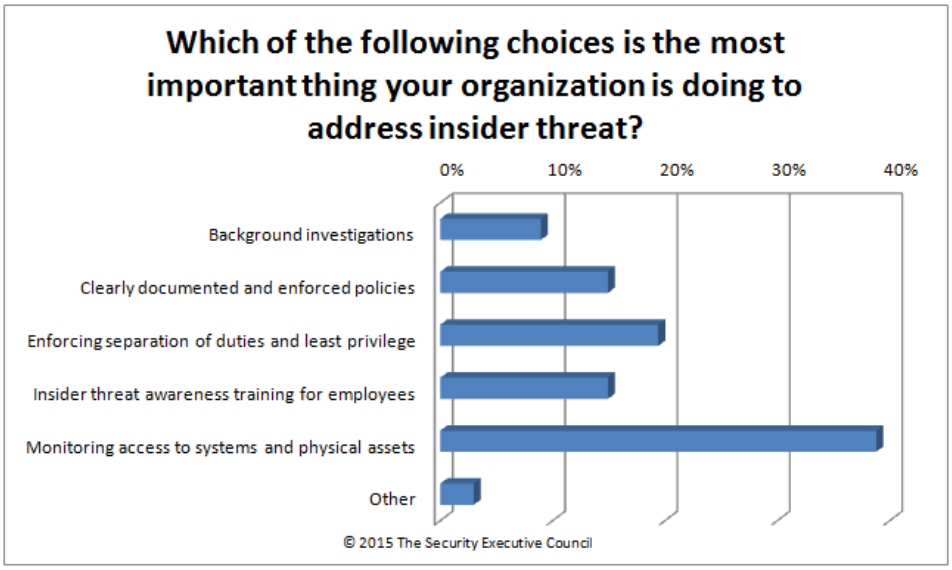
Based on numerous conversations with Fortune 500 corporate security practitioners the SEC has created the following definition of insider threat that covers the issues being identified within these businesses.

Insider threat:

Any risk posed by current or formerly trusted individual(s) with access or privileged knowledge used to damage, deprive, diminish, injure or interrupt organizational stakeholders, assets, critical processes, information, systems or brand reputation. Insider threats include any illegal, prohibited or unauthorized conduct (acts or omissions).

Is insider threat becoming a bigger issue to companies? When asked about top risks to organizations, an SEC practitioner poll showed that insider threat came up in second place (cybercrime was the top risk). However, in the same poll, only 46% of respondents had a formal insider threat program in place. When asked, what was the most important thing organizations were doing to address insider risk, monitoring access to systems and physical assets was the most often cited answer.





However, in recent discussions with security practitioners the SEC is finding some security leaders are looking for new tools and resources to proactively address insider threats. The most significant initiative we've seen recently is attempting to take all the sources of data and information from current initiatives (e.g., shown in the poll above) to address insider threat and combining it new and emerging sources of information that could proactively identify risks; and turn this combination of information into actionable strategy. Newer sources of early warning indicators can consist of: information from social media, "dark web" criminal activity monitoring, real time reporting of arrests and associated information and civil court final proceedings. This should be combined with internal corporate data including performance data and corrective actions taken. All this information has the potential to identify and communicate behaviors that could signal a troubled person or a troubling situation that could escalate to an insider threat action.

The biggest organizational hurdle to combat insider threat is made apparent by the diversity of functions that manage and oversee these varied sources of information. There will never be a 100% prefect process to identify all risks to people and organizations proactively – there are just too many variables. However, when a unified risk oversight model that promotes the inclusion of all corporate stakeholders and possible information sources is used, the likelihood of avoiding significant losses or incidents is greatly reduced.

How vulnerable is your company to insider threat? The SEC has put together a list of questions for the security leader to assess their organization's level of risk.

How Vulnerable is your Company to Malicious Insiders?

1. Do you know who is responsible for pre-employment screening in your enterprise?
2. Do you get regular reports on pre-employment screening results?
3. Do you know the screening criteria and whether they contain the elements that would most likely indicate an insider risk?
4. Do you have a program that identifies potential violence at its earliest stages?
5. Does your company have a behavior analytics reporting system on your key computer assets?
6. Do you track and investigate unusual access attempts to facilities, information and systems by employees and contractors?
7. Have you recently reviewed your separation of duties and responsibilities?
8. Have you asked all your key managers what insider threat events they're monitoring for?
9. Did they all answer appropriately, or are you confident they would if asked?
10. Have you asked all your direct reports what steps they've taken to reduce brand, people, property and product risk from insiders?
11. Is an assessment made of the access rights of every employee leaving the company, and appropriate actions taken to revoke those access rights?

Scoring:
If you answered yes to 5 or less: High Risk
You need to become more involved in your risk oversight process and learn what controls the organization has in place.

If you answered yes to 6-8: Moderate Risk
You are probably concerned and involved with risk management but should broaden your horizon to other areas of risk.

If you answered yes to 9 or more: Low Risk
You clearly have a good understanding of insider risk and the controls; or you've recently had insider security breaches.

About the Security Executive Council (SEC)

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com