Experience the commitment®

SOLUTION BRIEF

The Insider Threat Problem

Is your organization doing enough to protect against insider threats?

With several highly publicized insider threat incidents resulting in harmful data breaches for both government and industry, preventing and detecting such threats are a high priority for our clients. Regulations governing access to classified information have established baseline requirements for insider threat programs. Industry studies confirm that risks are increasing, but not enough is being done to combat those risks.

Is your organization doing enough?

DEFINING THE INSIDER THREAT

An insider threat is an individual with access to an organization's systems and data, who, through either malicious or inadvertent actions, can cause irreparable damage to the organization itself, other industries, government and even citizens. Malicious activities can include theft, espionage, sabotage and insider trading. Non-malicious activities can include falling victim to phishing, malware and ransomware attacks from malicious outsiders.

The growing challenge of insider threats is recognized by our clients as a major risk. CGI's 2016 Global 1000 is an outlook on trends and priorities based on 1,000+ in-person conversations with business and IT executives conducted by CGI leaders. Among hundreds of U.S. executives participating in these conversations:

- 93% felt vulnerable to insider threats
- 53% saw privileged users as the biggest threat
- 44% had a breach or failed a compliance audit

Recent industry studies also indicate that:

- Remediating a successful insider attack costs $445,000 per incident
- Consequences of an insider attack cost $15 million in annual company losses
- Only 40% of IT budgets include funding for insider threats
- Nearly a third of all U.S. organizations surveyed by SANS in 2015 had no capability to prevent or deter an insider incident or attack[1]

WHAT IS YOUR ORGANIZATION DOING TO PROTECT AGAINST INSIDER THREATS?

Is your organization just doing enough to meet baseline regulatory requirements until there is an insider threat incident? If you've already had an incident, are you doing enough to make sure it does not happen again and repair the reputational damage? Or, like most organizations, are you always trying to catch up?

The continued increase in data breaches from insider threats gives organizations across sectors no choice but to place greater emphasis on this problem. While the market continues to focus on individual tools and capabilities to fill gaps in protection, organizations that approach insider threats from a holistic, enterprise view will be better positioned to prevent, detect and respond. There is no single means to prevent an insider threat, so the concept of defense in depth applies here as it does to all areas of security.

"The world is a different place than it used to be. Insider Threat is occurring and it is increasing at a rapid pace. Organizations that do not understand it or are not willing to get on the bandwagon are going to suffer damage and loss. Organizations that are going to survive have to realize the threat is real and take action immediately, because most likely the damage has already begun beneath the surface."[2]

Dr. Eric Cole and Sandra Ring, *Insider Threat: Protecting the Enterprise from Sabotage, Spying and Theft*

---

[1] Insider Threats and the Need for Fast and Directed Response, A SANS Survey Written by Dr. Eric Cole, April 2015, accessed December 8, 2016: http://www.veriato.com/docs/default-source/whitepapers/insider-threats-fast-and-directed-response.pdf?sfvrsn=14

2 Insider Threat: Protecting the Enterprise from Sabotage, Spying and Theft, Dr. Eric Cole and Sandra Ring, Syngress; 1 edition (March 15, 2006)

BEST PRACTICES IN DEFINING INSIDER THREAT PROGRAMS

Federal government guidance

Given the lack of industry-specific guidance for developing insider threat programs, CGI recommends that all organizations look to existing federal guidelines and requirements to define an insider threat program, including:

- Executive Order 13575 (October 2011) requiring federal government executive agencies to establish insider threat programs
- DoD 5220.22-M National Industrial Security Operating Manual (NISPOM) Conforming Change 2 (May 2016) requiring cleared contractors to establish insider threat programs
- The NISPOM Industrial Security Letter (ISL) 2016-2 (2016) providing guidance to cleared contractors on insider threat program implementation
- The NIST 800-171 guidance on "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (August 2015) covering requirements for unclassified computer systems and networks and requiring insider threat program training for organizations. This requirement is effective December 31, 2017.

SEI-CERT Framework

The Carnegie Mellon University Software Engineering Institute (SEI) CERT Division has established a robust *Insider Threat Program Framework*. It defines essential program elements in an *Insider Threat Program Roadmap* that follow four defined phases: Initiation, Planning, Operations and Reporting.

According to SEI CERT, key program components that organizations should incorporate include:

- Integration with enterprise risk management
- Insider threat practices related to trusted business partners
- Prevention, detection and response infrastructure
- Insider threat training and awareness
- Data collection and analysis tools, techniques and practices
- Policies, procedures, and practices to support the insider threat program
- Protection of employee civil liberties and privacy rights
- Communication of insider threat events
- Insider threat response plan
- Confidential reporting procedures and mechanisms
- Oversight of program compliance and effectiveness
- Organization-wide participation
- Formalized and defined program

CGI is proud to be a partner of SEI in delivering best-practice insider threat program solutions.

"Organizations must understand that security is an ongoing task that must constantly be done and readjusted. Security goes way beyond technology and is never complete. There is no such thing as 100% percent security. Which means you will never get it right but you have to keep trying to get it close enough. In order to properly implement security you must understand the organization's structure, mission, and politics so security can be seamlessly integrated. Security is a means to and end but it is not an end state."[3]

Dr. Eric Cole and
Sandra Ring

DELIVERING AN INSIDER THREAT PROGRAM

While organizations can refer to the federal guidance and SEI CERT best practices, they often lack the skills and expertise to operationalize an insider threat program. With extensive experience delivering cybersecurity programs and expertise across government and commercial sectors, CGI stands as a trusted partner to organizations looking to implement robust and effective insider threat programs.

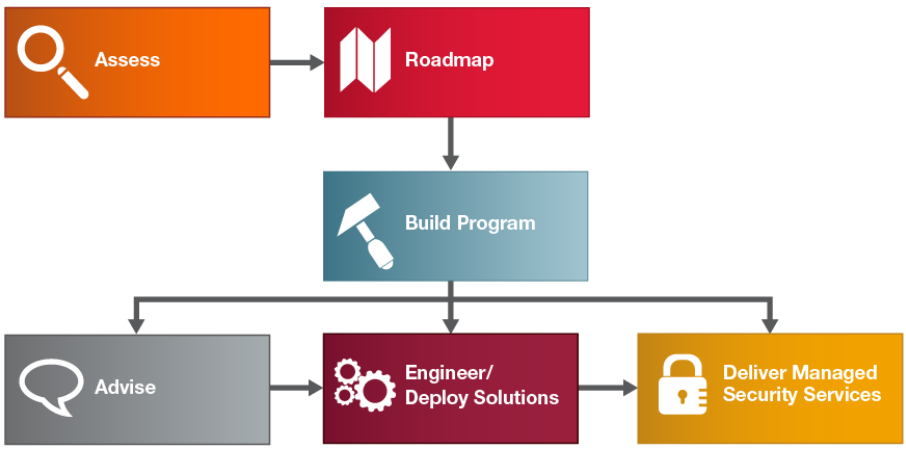
We offer strategic advisory and implementation services to help government and commercial clients address cybersecurity threats and risks come from trusted insiders. Our services are designed to help organizations:

- Focus on cultural and behavioral change to view seemingly normal, everyday actions of employees through an insider threat “lens”
- Ensure collaboration and information sharing across human resources, information technology, cybersecurity, industrial security, legal and communications
- Analyze and correlate disparate data sources to uncover potential risks and threats, thereby becoming more proactive at mitigating insider risks
- Establish standard procedures to comply with insider threat program requirements included in NISPOM Change 2

CGI is uniquely positioned across not only the defense industrial base but multiple market sectors, giving us the expertise to create a custom approach to defining your program. We are one of only a few global firms with the talent, scale and end-to-end services and solutions necessary to help find protection gaps and protect your assets.

Our comprehensive approach leverages SEI CERT best practices and certified professionals to assess vulnerabilities, develop roadmaps, build programs, advise on priorities, engineer/ deploy solutions, and deliver managed security services to protect clients from insider threats.

CGI’S END-TO-END INSIDER THREAT PROGRAM APPROACH



SEI CERT INSIDER THREAT ASSESSMENT

CGI is certified to deliver SEI CERT Insider Threat vulnerability assessments. These assessments look at an organization's capabilities across seven key areas that have been exploited in prior insider threat incidents. An assessment engagement looks at how well an organization is positioned to prevent, detect and respond to insider threats. Results of the assessment enable focused efforts to close exploitable gaps, thus providing the roadmap for program expansion.

STRATEGY ROADMAP

Following an assessment, CGI can customize a roadmap for a client's unique vulnerabilities and gaps. The roadmap is all about making a series of unique decisions aligned to your organizations mission and future. It is also used to obtain the management team's buy in on the strategic options for what can be developed in the subsequent program. The roadmap provides a strategic plan for establishing protections against insider threats. Deconstructing the roadmap into specific activities will assist in building your insider threat program.

BUILDING THE PROGRAM

The assessment and roadmap enable the organization to build a framework to protect against insider threats. CGI will identify the most effective solution to meet your strategic goals and objectives. Not only will the program take into consideration your current state, but it also will identify and document the ongoing activities to address your future growth and organizational changes. CGI will work with you to define the best platform to meet your strategic needs through advisory services, engineering and integration services and managed security services. Together we will build the program to meet your organization's unique requirements.

ADVISORY SERVICES

In response to the assessment and the increasing risk posed by insiders, CGI security experts will work closely with CGI yours to help you prioritize your insider threat initiatives and align them with your business. CGI management and technical advisory services address all aspects of a successful Insider threat program.

ENGINEERING & INTEGRATION SERVICES

CGI will help design, develop and integrate systems and applications to reduce the risk of an Insider Threat. We have deep expertise in all facets of our clients' business and technology environments, enabling us to not only advise but to implement and manage solutions. Our best-fit global delivery approach offers a powerful combination of value and expertise for delivering your insider threat program.

MANAGED SECURITY SERVICES

CGI is recognized as a leader in managed security services. We have a successful history of providing managed security services to government clients as well as corporate clients. With two U.S. Security Operations Centers (SOCs) providing around-the-clock coverage, and with eight SOCs globally, our advanced platforms and insider threat continuous monitoring enable our clients stay abreast of the latest insider threats to security, along with the latest technologies and processes to help address them.

WHY CGI?

- Proven expertise, technology and continuous support
- Established, best practices program
- Ability to scale enterprise programs to meet changing insider threats
- Insider threat program plan assessed by Defense Security Services to be compliant with expected NISPOM requirements
- One of the first SEI CERT corporate partners for Insider Threat Vulnerability Assessment World-class cyber engineering capabilities and global network of Security Operations Centers (SOCs)

ABOUT CGI

CGI helps clients understand cyber threats, build strong security business cases, strengthen their resilience and determine the ROI of security investments. We also help them share, use and store information securely while safeguarding their intellectual property, data, networks and data centers. Our proven cybersecurity services and solutions help clients securely obtain and share information for accurate decision-making, find and remediate vulnerabilities within applications, and prevent unauthorized access to systems and buildings. Our full life-cycle services help ensure only the right people can access the right information at the right time. We give clients the peace of mind to focus on what's most important to them: protecting the business and operating with confidence.

Founded in 1976, CGI is one of the largest IT and business process services providers in the world. We combine innovative services and solutions with a disciplined delivery approach that has resulted in an industry-leading track record of delivering 95% of projects on time and within budget. Our global reach, combined with our proximity model of serving clients from hundreds of locations worldwide, provides the scale and immediacy required to rapidly respond to client needs. Our business consulting, systems integration and managed services help clients leverage current investments while adopting technology and business strategies that achieve top and bottom line results. As a demonstration of our commitment, our client satisfaction score consistently measures 9 out of 10.

SEI Partner Network
Carnegie Mellon University

cgi.com