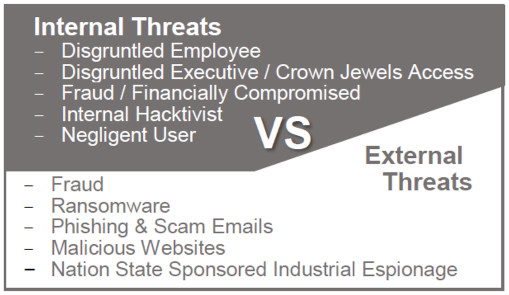
Insider Threat Program

Is your agency doing enough?

Many organizations think of cybersecurity threats as originating only from the outside. Yet, some of the most potentially damaging threats come from trusted insiders, whether intentionally or unintentionally. The challenge? Employees, contractors or partners have authorized access to many corporate and government crown jewels. Even worse, they know what and where those jewels are.

A PROACTIVE SOLUTION TO PROTECTING YOUR ASSETS

Agencies face sophisticated, ever-evolving cyber-attacks against critical infrastructure, systems and data, threats that are both intentional (e.g., hacktivists or disgruntled employees) and unintentional (e.g., victims of phishing or clicking on web popups introducing malware such as botnets and ransomware). CGI's robust federal cybersecurity solutions help agencies prevent, detect and respond to cyber-attacks, and ensure business continuity.



Internal Threats

- Disgruntled Employee
- Disgruntled Executive / Crown Jewels Access
- Fraud / Financially Compromised
- Internal Hacktivist
- Negligent User

VS

External Threats

- Fraud
- Ransomware
- Phishing & Scam Emails
- Malicious Websites
- Nation State Sponsored Industrial Espionage

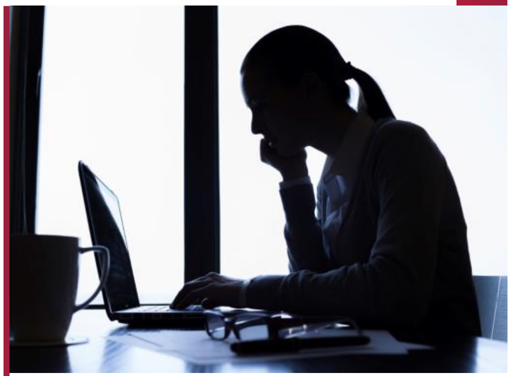
An active insider threat risk management program should be an integral part of security for every organization, and may be required for those working with the U.S. federal government. CGI's proactive approach focuses on protecting America's assets, emphasizing organizational cultural change and collaboration.

ORGANIZATIONAL CULTURAL CHANGE AND COLLABORATION

We focus on organizational cultural and behavioral change so executives and employees alike start to view activities with an insider threat "lens."

Consider this scenario: An employee requests permission to take a part-time job in a completely different industry. At first blush, there may seem to be no issue. Evaluating this matter through an insider threat lens, however, could suggest a need to investigate whether the employee is taking the job due to serious financial troubles and thus is vulnerable to compromising his or her access to information for financial gain.

Tools and technologies are only one part of our comprehensive program. Insider threats are human in nature and require human intervention. There must be collaboration and information sharing across traditionally "siloed" functions of human resources (HR), information technology, cybersecurity, industrial security, legal and communications. Involving these departments in all stages of the



CGI INSIDER THREAT PROGRAM KEY BENEFITS

ASSESS THE RISK

- Assess current vulnerabilities and weaknesses
- Identify impacts to the organization

PROTECT THE BUSINESS

- Prevent threats from damaging assets, technology and people, or causing reputational harm
- Establish effective documentation, policies and procedures
- Respond with speed and resiliency to all incidents
- Evaluate and mitigate damage while pre-empting additional or ongoing attacks

OPERATE WITH CONFIDENCE

- Ensure business continuity through precise, ongoing and consistently evaluated planning
- Measure program effectiveness by gathering concrete metrics on activities such as policy violations, data leakage events and even sabotage

For more information, email us at info@cgifederal.com.

cgi.com/us-federal

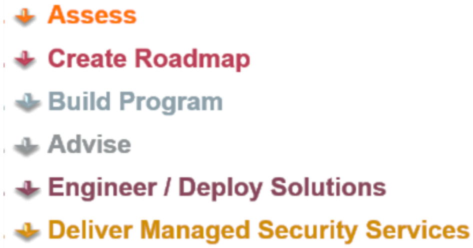
program helps organizations understand and prepare for the human element.
Key success factors include executive sponsorship for program monitoring, detailed compliance processes and plans and training workforces to recognize behaviors that are red flags for insider threats, then educating them on enterprise policies.

DATA CORRELATION AND ANALYTICS

Another key enabler to a more proactive posture is the use of data correlation and analytics to uncover potential risks and threats. Predictive analytics can take streams of data from network monitors, physical security devices and HR actions and use them to identify employees who are at highest risk for insider threat activities. For example, a combination of data about an employee's late office hours, Internet usage, and HR data (performance improvement plan) could trigger an alert.

CGI'S END-TO-END INSIDER THREAT PROGRAM

CGI offers a full spectrum of insider threat program services to assist clients in improving their program maturity. We can step in at any phase to help an organization implement an end-to-end program, starting with an assessment and roadmap, and providing program design, engineering, implementation and management, as needed.



Assess
Create Roadmap
Build Program
Advise
Engineer / Deploy Solutions
Deliver Managed Security Services

ASSESS

A critical part of our end-to-end program starts with a deep dive evaluation into existing systems, controls, services, tools, policies and processes to:

- Develop a business and threat profile for the organization
- Conduct an insider threat risk assessment using the SEI-CERT Insider Threat Joint Assessment Tool and perform other security assessments determined to be necessary (e.g., cyber vulnerability, penetration testing, application security, etc.)
- Capture threat and risk data through interview workshops
- Build a risk register of threat scenarios with likelihoods, impacts and abilities to mitigate
- Identify vulnerabilities, risks and gaps
- Evaluate existing capabilities against best practices

ROADMAP

A customized best practices-based roadmap centered on the assessment phase findings is created to:

- Address areas where response is significantly behind peer standards, or regulatory or reputational imperatives are a factor
- Outline necessary steps, expertise and investments for effective programs, such as creating an insider threat steering committee
- Identify desired tools, techniques and business process changes
- Provide benefit metrics to demonstrate business value of changes

BUILD PROGRAM

Collaboration with stakeholders is necessary to:

- Apply a best-practices framework (e.g., NIST, NERC, etc.) to build a holistic map of recognized threats and possible responses
- Develop a program plan outlining key objectives, tasks, projects, deliverables and schedules

ADVISE

We provide our customers with program execution support across several areas to:

- Create policy and incident support and training
- Develop an enhanced insider threat awareness campaign
- Establish and insider threat steering committee
- Facilitate open communications about insider threat

ENGINEER / DEPLOY SOLUTIONS

Assistance with technology engineering, integration and deployment services helps to:

- Architect and design solutions for identified gaps
- Evaluate and select a comprehensive security tool set
- Engineer, integrate and deploy the technical tools
- Develop and deploy insider threat training modules
- Test system readiness, conduct UAT and training and provide documentation

DELIVER MANAGED SECURITY SERVICES

CGI provides cost-effective managed security services and technology focused on insider threat protection, detection and response in an effort to:

- Implement insider Threat Program Office setup and 24/7 monitoring services from our global network of Security Operations Centers
- Deliver ongoing protection and monitoring services, real-time reporting and immediate action on suspicious insider activity such as data loss prevention, host intrusion detection, advance threat detection, log event monitoring, database access monitoring, user behavior analysis, file integrity monitoring, managed insider threat training, strong authentication and insurance fraud.

CGI-SEI/CERT PARTNERSHIP

SEI Partner Network
Carnegie Mellon University

CGI is one of the first companies that has partnered with the Carnegie Mellon University Software Engineering Institute (SEI) for Insider Threat and is licensed to provide official SEI services in Insider Threat Vulnerability appraisals.

Carnegie Mellon University works with the U.S. Computer Emergency Response Team (CERT) to analyze known insider threat cases in an effort to draw attention and understanding of motivation and opportunity and to help communicate important risk factors. This unique partnership allows CGI to provide a unique combination of services and solutions to our customers which includes the ability to:

- Assess an organization’s capabilities to prevent, detect and respond to insider threats
- Develop solutions to fill the gaps identified during the assessment
- Provide expertise to assist them in building a program to tie everything together

WHY CGI

CGI's expertise helps provide organizations with:

- Proven expertise, technology, continuous support and an established best practices program
- The ability to scale enterprise programs to meet changing insider threats
- End-to-end programs tailored to meet client requirements
- Insider threat program plans 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) which continuously identify and deploy the best solutions to maintain a state-of-the-art infrastructure
- State-of-the-art Cyber Threat Analysis Center (CTAC)
- One of the few providers worldwide with three accredited common criteria certification facilities—in the UK, Canada and the U.S.

CGI AND CYBERSECURITY

At CGI, security is a part of everything we do. Enterprises look to CGI's expertise to build security into every aspect of their operations from infrastructure and networks to mobile applications to employee education and business continuity. We partner with our clients to assess and analyze potential cybersecurity risks, continuously monitor for threats in real-time, put in place the necessary defenses and ensure continuity of operations, even during a cybersecurity incident.

Our global team of cybersecurity experts works with government and commercial clients to help ensure their business-critical systems and services are effectively secure.

PROTECTING AMERICA'S ASSETS

CYBERSECURITY OFFERING FRAMEWORK

ASSESS
Consulting
& Advisory Services

BUILD
Engineering
& Implementation Services

MANAGE
Security Operations / Managed
Security Services

The CGI Cybersecurity Offering Framework provides an end-to-end portfolio of enablement and transformation solutions that assist clients through the journey of becoming a highly secure organization.

ABOUT CGI

Founded in 1976, CGI is one of the largest IT and business consulting services firms in the world. Operating in hundreds of locations across the globe, CGI professionals help clients to achieve their goals, including becoming customer-centric digital organizations. We deliver an end-to-end portfolio of capabilities, from high-end IT and business consulting to systems integration, outsourcing services and intellectual property solutions that help accelerate clients' results. CGI works with clients around the world through a unique client proximity model complemented by a global delivery center of excellence network to help clients accelerate results, transform their organizations and drive competitive advantage.

For more information, email us at info@cgifederal.com.

cgi.com/us-federal