Insider Threat Program

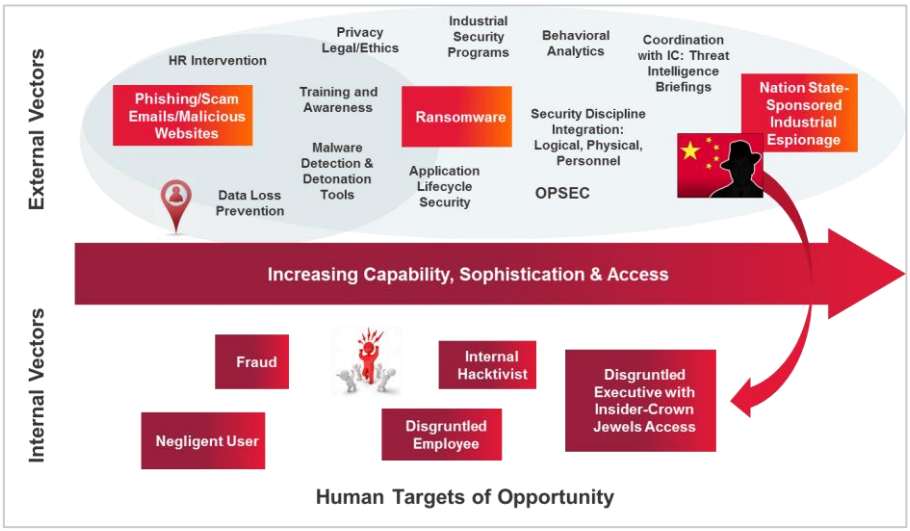
Proven best practices, end-to-end approach

Experience the commitment®

THE CHALLENGE

Many organizations think of cybersecurity threats as originating on the outside. Yet, some of the most potentially damaging threats come from trusted insiders, whether intentionally (e.g., hacktivists or disgruntled employees) or unintentionally (e.g., victims of phishing or clicking on web popups introducing malware such as botnets and ransomware). Employees, contractors or partners have authorized access to many corporate (or government) crown jewels, and what is worse, they know what and where those jewels are.

The Spectrum of Insider Threats



A PROACTIVE SOLUTION

An active insider threat risk management program should be an integral part of security for every organization, and may be required for organizations working with the U.S. federal government.

CGI helps clients prevent, detect and respond to both intentional and unintentional threats from within their organizations with a proactive approach emphasizing cultural change and collaboration.

Cultural change and collaboration

We focus on 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.

CGI INSIDER THREAT PROGRAM AT A GLANCE

- Risk and vulnerability assessment
- Gap analysis
- Roadmap
- Program design/build
- Ongoing advisory services
- Technology selection, engineering and deployment
- Management and monitoring

cgi.com/cyber

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.

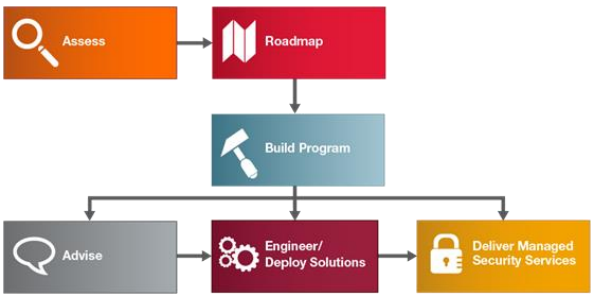
Tools and technologies are only one part of our comprehensive program. Insider threats are human in nature, and require human intervention. There must be collaboration and information sharing across traditionally "siloed" functions of human resources (HR), information technology, cybersecurity, industrial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

Involving these departments in all stages of the 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, and 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

In the assessment phase, we:

- Develop a business and threat profile for the organization
- Document existing controls, services, tools, policies and processes
- 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

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

- 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

Based on the assessment, we create a customized, best-practices based roadmap and recommendations 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
- Provides benefit metrics to demonstrate business value of changes

Build program plan

We then collaborate with stakeholders 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 program execution support across several areas, including:

- Policy and incident support and training
- Enhanced insider threat awareness campaign
- Establishment of insider threat steering committee
- Open communications about insider threat

Engineer/Deploy

We assist with technology engineering, integration and deployment services 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

Manage

We also offer cost-effective managed security services and technology focused on insider threat protection, detection and response, including:

- Insider Threat Program Office setup and 24/7 monitoring services from our global network of Security Operations Centers
- 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

CGI is one of the first companies to partner with the Carnegie Mellon University Software Engineering Institute (SEI) for Insider Threat and 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 enables CGI to provide a unique combination of services and solutions:

- An assessment of an organization's capabilities to prevent, detect and respond to insider threats
- Solutions to fill the gaps identified during the assessment
- Expertise to assist them in building a program to tie everything together

Why CGI

- Proven expertise, technology, continuous support and established, best practices program
- Ability to scale enterprise programs to meet changing insider threats
- End-to-end program tailored to meet client requirements
- Insider threat program plan assessed by Defense Security Services to be compliant with expected NISTPOM requirements
- One of SEI/CERT's three corporate partners for Insider Threat Vulnerability Assessment as of April 2016
- World-class cyber engineering capabilities and global network of Security Operations Centers (SOCs) which continuously identifies and deploys the best solutions to maintain a state-of-the-art infrastructure
- 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 ensure their business-critical systems and services are effective and secure.

ABOUT CGI

Founded in 1976, CGI is one of the largest IT and business process services providers in the world, delivering high-quality business consulting, systems integration and managed services. With a deep commitment to providing innovative services and solutions, CGI has an industry-leading track record of delivering 95% of projects on time and within budget, aligning our teams with clients' business strategies to achieve top-to-bottom line results.

For more information, contact info@cgi.com or visit www.cgi.com/cyber