CGI

Experience the commitment®

Response to Request for Information

State of Florida

Department of Management Services

Cyber-Security Assessment, Remediation, and Identity Protection, Monitoring, and Restoration Services

September 3, 2015

© 2015 CGI Technologies and Solutions Inc. All rights reserved.

DISCLAIMER

This document is being submitted for your review and consideration. Any offer of services is subject to ongoing due diligence and customary business investigations by CGI with respect to the requisite business arrangements necessary to carry out its obligations. The results of such a review may impact upon the terms and conditions of this document, including in respect of business structure, business terms and financial arrangements.

The information in this proposal is submitted on September 3, 2015 on behalf of CGI by the following authorized representative:

Keith Pigue

Vice President

CGI Technologies and Solutions Inc.

Keith.Pigue@cgi.com

205 919 2918 mobile

© 2015 CGI GROUP INC

Table of Contents

© 2015 CGI GROUP INC

Introduction

CGI is pleased to respond to State of Florida Department of Management Services Division of State Purchasing Request for Information (RFI) to perform cyber-security assessment and remediation, as well as identity protection, monitoring and restoration services under the General Services Administration (GSA) Schedule 70. CGI does not currently provide public relations, legal call center, identity restoration or credit monitoring services; however, CGI does have the ability to establish relationships in these areas should State of Florida agencies prefer a turnkey capability.

CGI Cyber Security Highlights

- DHS recently awarded CGI a prime position on the $6B Continuous Diagnostics and Mitigation (CDM) Blanket Purchase Agreement (BPA).
- The Pentagon trusts CGI to manage the first line of defense for attacks on the Pentagon's networks: *200 events each second or 15+ million each day*.
- The Defense Information Systems Agency (DISA) trusts CGI to provide computer network defense services at the most highly attacked network entry points within the Department of Defense (DoD): *analyzing/correlating an average of two billion events per day.*

CGI understands there is a high degree of versatility in the breach response services in support of cyber insurance. We support many organizations across the world and each has a particular nuance in such things as how a breach is detected, processes of client screening and coverage validation, who notifies of breach, breadth of applicable coverage, payment terms etc. The information provided below is a representation of CGI capability in this area and can be adjusted to align more directly with the State's defined process.

Purpose

CGI understands that the State seeks to implement a comprehensive Breach Response program to include pre-incident and post-incident services to support a detailed, deliberate response in the event that the State experiences a breach of data or systems.

Program Creation

Prior to launch of cyber-security assessment and remediation services, as well as identity protection, monitoring and protection services program, CGI works with the State to facilitate mutual information sharing and understanding on the overarching program, other stakeholders and providers, processes, contact lists, and other preparations. This information assists in identifying where processes, programs, or procedures need to be enhanced to improve Incident Response readiness.

Actions and tasks include, but are not limited to:

- Orientation kickoff meeting
- Documentation collection
- Scope and other party interactions
- Creation of procedures and processes
- Client review and approvals
- Implementation

With knowledge of the State's preferred processes and procedures in place, CGI is able to assist with and lead incidents in a prompt and effective manner.

© 2015 CGI GROUP INC

Incident Response Service

CGI Security Policy and Standards Expertise

CGI has experience providing federal civilian and DoD customers with years of security policy and standards services. Some of our customers include: Pentagon, Department of Agriculture, Department of State, CMS, EPA, DISA, and US Cyber Command.

CGI's Incident Response (IR) services involve both Pre-Incident and Post-Incident services as requested in the RFI. CGI works to provide Incident Response Agreements, Assessments, Preparation, Cyber-Security Incident Response Plans, and Training. We work to deliver operations services including call centers that can service the Breach Services Toll-free Hotline, Investigation/Clean-up, Incident response, and Mitigation Plans. Our partner network would provide Identity Monitoring, Protection, and Restoration services.

CGI's Incident Response services involve the receipt, triage, and response to digital-related incidents where a breach or incident, either internal or external, is believed to have occurred. CGI identifies the scope of the incident, the extent of the damage caused, and the available response strategies and workarounds.

This service may include vulnerability and/or artifact analysis in order to correlate the events associated with the incident and develop a response strategy. Forensic evidence collection is commonly a part of incident response and includes the collection, preservation, and documentation of evidence from compromised or otherwise suspect computer systems. Forensic analysis of this evidence is used to determine changes to the systems and to reconstruct the chain of events leading to the incident and its discovery.

Typical activities involved in incident response may include:

- Determination of intruder activity on specific devices or network segments
- Filtering of network traffic
- Executing actions to protect systems and/or network segments
- Providing mitigation recommendations and strategies
- Providing mitigation solutions and strategies
- Forensic evidence collection
- Digital analysis of involved systems

Service Activities

CGI's Digital Forensics Team offers full scope digital forensics and incident response capabilities to CGI clients. Our highly trained digital forensics team possesses years of experience in a wide range of situations. Should an client require courtroom testimony to support litigation as a result of a digital forensic investigation or other matter, CGI forensic examiners are available to provide testimony as a the case investigator on a specific case or to act as expert witness in information security and digital forensics.

Method of Engagement

CGI works to understand the State's existing processes and investments to further define the engagement process and the method of delivery. The CGI SOC team will be integrated into the process for incident take over and response. A notional process is detailed below.

© 2015 CGI GROUP INC

Methodology

Pre-Incident Services:

- **Incident Response Agreements** – Terms and conditions in place ahead of time to allow for quicker response in the event of a cyber-security incident:

  Like most organizations, the State must be prepared to respond to an incident before an incident occurs; this is one of the most critical facets of an incident response (IR) management function. This advance preparation avoids disorganized response to incidents. This preparation also limits the potential for damage by familiarizing all staff with response plans, thus making coordination easier. In support of this **Planning** phase (**IR Phase 1**), our approach validates the proper development and documentation of Terms and Conditions (Ts&Cs), Service Level Agreements (SLAs), as well as Standard Operating Procedures (SOPs) for management of the phases of the State Incident Response process. This includes coordination with other State and Local Security Operations Center (SOC) teams, the State's IT Operations and Management teams, State contractors, DHS organizations, and other pertinent organizations supporting the resolution of security incidents. These SOPs contain escalation matrices and workflows and dictate the prioritization of Security Incidents based on the criticality of the threat and the risk tolerance levels assessed by the State. Our approach also validates that trained Incident Response personnel (with proper skills and appropriate physical and logical access) are on-site and capable of performing the required job and supporting monitoring personnel 24x7.

- **Assessments** – Evaluate a State Agency's current state of information security and cyber-security incident response capability:

  In order to effectively respond to an incident, it's important to establish a clear, phased approach to include the steps required to respond to an incident. The following section summarizes Phases 2 through 5 (Phase 1, Planning is detailed above) to which the State will be assessed.

  IR Phase 2: Identification and Declaration. CGI's assessment includes the State's approach to identification of an incident, the preliminary analysis, identification, and categorizing of incidents, and begins with the process of performing initial analysis of the data associated with an event of interest (EOI) escalated by the SOC Monitoring and Notification Service (Case Escalation) to determine if it is a reportable event or incident. As part of the incident response process, the State must associate each event or incident with a category according to DHS and United States Computer Emergency Readiness Team (US-CERT) policies. Based on our Pentagon and Defense Information Systems Agency (DISA) experience, CGI recommends the State use a standardized benchmark for defining a reportable event or incident and place a high emphasis on validating performance of a proper preliminary analysis to prevent incidents from going unidentified or unreported. Once a determination is made on whether or not an event of interest (EOI) is a reportable event or incident, CGI recommends the State's IR analyst continue the coordination and notification process through technical and operational reporting channels with the appropriate organizations according to the State's Incident Management SOPs and following DHS and US-CERT reporting guidance. The IR analyst should update the case within the SIEM tool (Case Creation) and the Security Portal, and then move into the containment phase of the IR process.

© 2015 CGI GROUP INC

IR Phase 3: Containment. The State's approach to containment should include preliminary response actions comprised of the coordinated and initial actions taken to protect the State's networks and systems from any further malicious activity and to acquire the initial data required for further analysis. The primary objectives of this phase are to contain the incident, acquire and preserve data, and continue documentation and coordination. CGI works with the State to assess whether or not the incident contains any potential threat and works to protect the affected system or network and prevent any further contamination, intrusion, or malicious activity. Depending on the attack vector and the security technologies in use by the State, the preliminary response actions vary but typically include:

1) Disconnecting the victim system and/or implementing switch port blocks;
2) Blocking hostile external IP's via Firewall rules and router ACLS;
3) Blocking hostile external domains via a URL filtering device and/or DNS Black-holing hostile external domains;
4) Filtering email via Email Protection Software rules (source, content, attachments, subject etc.);
5) stripping hostile software, documents etc. from entering the network with IPS and Gateway Firewall rules; and
6) Shutting down or disabling a system, server, account, or service to help limit damage or prevent further access to the system.

IR Phases 4 & 5: Eradication and Recovery. Our approach to assessing the State's response to an Incident includes IR Phases 4 & 5, the Eradication and Recovery phases. CGI brings lessons learned experience to develop and continually improve the mutually agreed upon detailed response steps that prevent further damage through eradication of malware, restoring the integrity of affected systems, and implementing follow-up strategies to prevent the incident from happening again. These phases are presented together as they often occur at the same time. Eradication and recovery requires a combination of technical, management, and/or Law Enforcement (LE) actions. Technical actions include changes in the network and system infrastructure to remove the risk or threat. Management steps include administrative, human resources, public relations, or policy creation and management activities. LE actions include further investigation or criminal prosecution. Specific eradication and recovery actions depend on the nature of the incident. However, some common actions taken by IR analysts should include remediating or mitigating the vulnerability, modifying network and system access controls, and rebuilding systems, beyond the removal of malware. The removal of malware actions can include quarantining or deleting the malware, or replacing or restoring the integrity of infected files. In most cases, this will require rebuilding the system from trusted media. This can also involve updating antivirus signatures. Under most conditions, once a system is compromised, the integrity of that system cannot be verified until it has been restored from trusted media. If a system contains malware, keeping it in operation is not recommended unless the complete integrity of that system can be once again verified, or the system is left running and monitored closely as part of an ongoing LE case. To prevent similar incidents from occurring, IR analysts should make recommendations to the local technical staff regarding baseline configurations, tightening network perimeter security, updating anti-virus and scanning tools signature files, rebuilding the system from trusted media, conducting user training, or implementing countermeasures that mitigate the risk.

IR Phase 6: Follow up. Learning and improving is one of the most important parts of incident response, but it is also the most often omitted. CGI performs a hotwash to capture the immediate

© 2015 CGI GROUP INC

"after-action" discussions and evaluations of performance following an exercise, training session, or major incident to include follow up, a post-mortem analysis, additional cyber threat analysis, correlation and fusion, incident reporting, retention and distribution, and continued coordination and notification. CGI brings experience providing post-mortem analysis for the Pentagon and DISA to review with the State the incident, including the detection, analysis, and response to the incident. Data captured in the post-mortem analysis includes lessons learned, initial root cause, problems with executing response actions, missing policies and procedures, and inadequate infrastructure defenses. Post-mortem results make improvements to the incident management process and methodology and to the security posture and defenses of the State's networks. It's important to note that not all individual incidents require a post-mortem. Usually, an incident that is large in scope, handled poorly, involves LE, or cause severe damage requires a post-mortem.

- **Preparation** – Provide guidance on requirements and best practices

  CGI has vast experience providing IR services, especially for the gov't sector.

  The following regulatory policies and guidance documents are a sampling of the requirements and best practices CGI commonly applied to customer environments. CGI works to tailor the program to meet the State's policies and regulatory guidance when developing recommendations for the Incident Response Policy.

  - *Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, et seq.),* requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency.
  - *NIST 800-61 revision 2, Computer Security Incident Handling Guide*, provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident.
  - *NIST SP 800-53 revision 3, Recommended Security Controls for Federal Information Systems*, provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. The guidelines apply to all components of an information system that process, store or transmit federal information.
  - *NIST SP 800-82, Guide to Malware Incident Prevention and Handling,* provides guidelines for understanding real-world threats posed by malware and to mitigate the risks associated with malware incidents.

- **Developing Cyber-Security Incident Response Plans** – Develop or assist in development of written State Agency plans for incident response in the event of a cyber-security incident

  CGI develops the Incident Response Plan (IRP) to provide guidance and assign responsibilities for establishing and testing the incident response functions. CGI brings extensive lessons learned developing the IRP numerous agencies to provide a foundation for timely and effective detection, notification, reaction, investigation, response, and recovery from security incidents occurring within the environment. The purpose of the IRP plan is to provide guidance on implementing policy for incident response.

  In response to security incidents, the goals of the IRP are:

© 2015 CGI GROUP INC

- Protect personnel and network assets
- Validate the integrity of critical systems and data
- Contain the incident to avoid escalation
- Recover critical services and data
- Restore normal operations
- Determine the cause of the incident
- Document lessons learned in order to update policies and procedures
- Provide assistance in prosecuting violators

- **Training** – Provide training for State Agency staff from basic user awareness to technical education

Security awareness and training is crucial and is required for all State users of information technology assets. This is the first line of defense in protecting the IT infrastructure and information and is pivotal in determining the success of an information technology security program. This awareness program validates that users understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources provided to them through exercises and assessments. Before users are provided access to State's IT resources, they must understand and comply with security policies and procedures and be appropriately trained. They must be aware that the actions they take could have an adverse effect on the State's security posture as a whole. These actions include, but are not limited to, proper passwords, data backups, antivirus protections, knowing how to spot and accurately report suspected incidents and/or violations of security policies, and following rules established to avoid social engineering and phishing attacks.

User Awareness Delivery Methods
▪ Annual user IA Awareness training via CBTs
▪ Security tips and messages: emails, post-it notes, pens
▪ Games
▪ Award Programs
▪ Screen Savers
▪ Posters

Throughout the awareness campaign, we use several delivery methods to provide materials in addition to traditional classroom training. We identify and customize these methods for each respective environment including, but not limited to, those shown in **Figure 2.**

Awareness topics delivered during this program provides a measurable understanding of industry best practices in information security. These topics include but are not limited to:

- Password complexity, changes and safeguarding
- Internet usage
- Incidents and violation reporting
- Antivirus programs
- Social engineering
- Screen locking and account safeguarding
- Email (Phishing, social engineering, spam, attachments, virus, etc)

© 2015 CGI GROUP INC

- Software patching
- Operational security (OPSEC)
- Mobile device vulnerabilities
- Security policy

Post-Incident Services:

- **Breach Services Toll-free Hotline** – Provide a scalable, resilient call center for incident response information to State Agencies

CGI's extensive network of delivery centers is the foundation of our global delivery model. CGI operates 24 global delivery centers including 4 in the United States. CGI Call Centers Business Practice provides Operator Services and Call Centers improve the bottom line. Key Industries include Financial Services, Government, Health, Manufacturing, Retail and Consumer Services.

MSS and Remote Delivery Excellence

- CGI provides 150+ federal and commercial customers with a range of MSS capabilities.
- CGI delivery center resources perform remote IT support services for the following federal agencies: Environmental Protection Agency (EPA), Centers for Medicare and Medicaid Services (CMS), Department of State, the General Services Administration (GSA) and the US Army.

CGI works with the State to implement the Breach Services Toll-free Hotline such that users report suspicious or questionable network traffic or activity within the environment to the call center for incident response. We support this with ongoing awareness and training activities. The call center creates an IT service management (ITSM) incident ticket. The ITSM system escalates the completed ticket to the proper category triggering an email of incident notification to the State and CGI. The ITSM call center documents, tracks, and administers security incident tickets through a centralized database tool.

From serving as an extension of clients' internal teams to developing and managing solutions on clients' behalf, CGI has the call center knowledge, expertise, software, tools, and operations to implement solutions that quickly and effectively solve incident response business problems. DISA trusts CGI to provide computer network defense services at the most highly attacked network entry points within the Department of Defense (DoD): *analyzing/correlating an average of two billion events per day.*

- **Investigation/Clean-up** – Conduct rapid evaluation of incidents, lead investigations, and provide remediation services to restore State Agency operations to pre-incident levels

CGI effectively defends the network and manages vulnerabilities monitoring near real-time "threat level" status, providing management with the ability to snapshot enterprise status and map progress toward security milestones. CGI conducts vulnerability analysis of the State's network-attached devices to determine compliance status, identify potential threats, and categorize the risk associated with identified vulnerabilities. We perform these scans during non-peak periods so that each device is scanned at least once a month without interfering with user activities. Security analysts evaluate the scan results, prioritize the vulnerabilities, and recommend remediation actions based on risk. This remediation plan mitigates weaknesses, deficiencies, and known vulnerabilities. We provide a detailed record of vulnerabilities that were determined to be acceptable for the Senate and independent auditors by logging exceptions for review and approval. These system architecture compensating controls mitigate risk.

© 2015 CGI GROUP INC

CGI has experience using a variety of network monitoring and security tools to monitor device availability and security. At the EPA, we configure tools to provide automatic alerting to our support staff when detecting a potential problem. We use these tools for regular reporting regarding bandwidth usage statistics and trends, interface errors, uptime/downtime, and other related artifacts.

- **Incident response** – Provide guidance or technical staff to assist State Agencies in response to an incident

  CGI works with the State to provide Incident response planning during the Planning & Requirements Definition Phase and carried out during the Operations & Maintenance Phase of the system development life cycle to verify the most cost effective and appropriate measures.

  The containment, eradication, and recovery phases cover steps taken by the CGI incident response team for remediation of the incident. CGI develops a strategy for containment, eradication, and recovery with the State prior taking action. The strategy is dependent upon the incident category.

  CGI's Digital Forensics Team offers full scope digital forensics and incident response capabilities to CGI clients. Our highly trained digital forensics team possesses years of experience in a wide range of situations.

  In general, execution of our services is triggered by a system event or client request, such as the report of a compromised host, malware infection or intrusion detection either by human or automated resources and is thus, reactive and/or investigative in nature. The following list describes a generalized list of digital forensics services available. When CGI's Incident Response service is initiated, one or more of the following activities may be carried out:

  - **Computer Investigations** - CGI provides a rapid and legally defensible strategy for combating computer crimes such as unauthorized access, embezzlement, data theft and use of inappropriate content. The Incident Response Consulting Team can investigate user activities, create timelines of events and recover evidence. The team uses proven and forensically sound tools and procedures to collect, document and analyze electronic artifacts that provide evidence of a computer crime or employee misconduct. This includes common system and user artifacts such as email, web mail, chat/instant messaging, browser URL history, browser search history, event log analysis, software installation, recovery of deleted files, application use and removal, wireless access point history (for laptops) and analysis of live system memory.
  - **Network Examinations** - Network traffic is captured and a technical examination of the activity is performed looking for evidence of user misuse or indicators of compromise such as intruder activity and malware communications.
  - **Malware Analysis** - Analysis of workstations, network traffic, and files will be performed to identify the presence of malicious software, especially custom crafted targeted malware that cannot be detected by antivirus. An examination of recovered malicious code is executed in an effort to understand its behavior and intended actions, as well as to discover, when possible, its origin and those involved in its creation.

    Malware analysis involves static and/or dynamic analysis of the suspect code. Static analysis involves the deconstruction and examination of the physical components of the malicious software without execution of the code. Code disassemblers, de-compilers, and source code analyzers; as well as, other forensic and system utilities; are commonly used during static analysis. Dynamic analysis of malware involves the actual execution of the malicious code in a controlled environment to determine its effects on the surrounding environment. Debuggers, function call tracers, machine emulators, logic analyzers, and network sniffers are commonly used in this process.

© 2015 CGI GROUP INC

- **Expert Witness Testimony** - Should the State require courtroom testimony to support litigation as a result of a digital forensic investigation or other matter, CGI forensic examiners are available to provide testimony as a the case investigator on a specific case or to act as expert witness in information security and digital forensics.

- **Mitigation Plans** – Assist State Agency staff in development of mitigation plans based on investigation and incident response. Assist State Agency staff with incident mitigation activities

  CGI works to limit the spread of the incident prior to the incident overwhelming information technology resources or causing additional damages. Once an incident has been contained, eradication steps may be necessary to eliminate components of the incidents such as deleting malicious code or disabling breached user accounts. Following eradication activities, CGI initiates recovery efforts to restore the impacted system to normal operations and if applicable, harden systems to prevent future similar incidents. Examples of recovery strategies include restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security.

  Our security analysts provide State staff with a vulnerability report that includes system owner and point of contact information, initial cost estimates (should the remediation represent significant effort), risk analysis, and a Plan of Action and Milestones (POAM). We track the remediation activities and independently assess the results for compliance, upon completion of work by the system owner. On occasion, the system owner may demonstrate that other aspects of their configuration mitigate the risk, in which case we log this exception for future reference by our analysts and independent auditors.

  CGI brings extensive experience dealing with potentially threatening situations and established proactive, consistent policies and procedures to eliminate the risk of ad-hoc responses to security issues. CGI's Digital Forensics Team is the escalation point for the SOC when a breach or incident is suspected. The team provides full scope computer forensic, data recovery and incident response capabilities, as well as a variety of other digital media-based forensic and investigative services to CGI clients. Our highly trained Digital Forensics team possesses years of experience in a wide range of situations. Our Network Security & Incident Handling and Security Engineering team members will be engaged by the Digital Forensics Lead where necessary. These teams are ready to stop any ongoing security intrusion by implementing proven technical mitigation strategies and will assist investigations, when needed, to determine depth and breadth of an incident.

- **Identity Monitoring, Protection, and Restoration** – Provide identity monitoring, protection, and restoration services to any individuals potentially affected by a cyber-security incident

  Our partner network provides Identity Monitoring, Protection, and Restoration service as CGI does not currently provide direct public relations, legal call center, identity restoration or credit monitoring services. CGI does have the ability to establish relationships in these areas should State of Florida agencies wish a turnkey capability.

© 2015 CGI GROUP INC

Assumptions, Limitations and Constraints

The proposed approach is based on the following assumptions:

- The State will be available as required to support completion of any required deliverables
- Any relevant system and application information will be made available to complete the assessment
- Estimates regarding the level of effort will be provided to the State prior to any project commencement.

© 2015 CGI GROUP INC

Appendix A – CGI at a Glance

With 68,000 professionals operating in 400 offices and 40 countries, CGI fosters local accountability for client success while bringing global delivery capabilities to clients' front doors. Founded in 1976, CGI applies a disciplined delivery approach that has achieved an industry-leading track record of on-time, on-budget projects. Our high-quality business consulting, systems integration and outsourcing services help clients leverage current investments while adopting new technology and business strategies that achieve top and bottom line results.

At CGI, we are in the business of satisfying clients by helping them succeed. Since our founding in 1976, we have operated upon the principles of sharing in clients' challenges and delivering quality services to address them. With a satisfaction ranking 9.1 out of 10 from 2,400 signed client assessments, CGI is committed to helping clients achieve superior performance and gain competitive advantage.

OUR SERVICES

From providing consulting and systems integration services to managing IT and business functions on behalf of our clients, CGI provides an all-encompassing offering that includes the planning, design, development, implementation and management of highly effective business and IT environments. Our global delivery capabilities include onsite, home-shore, near-shore and offshore options, giving our clients the flexibility to choose the model that best meet their needs.

CGI has a comprehensive portfolio of services that enable us to serve as clients' full- service provider in improving all facets of their operations. Key service areas include:

- **High-end business and IT consulting**—a wide array of services including business and IT strategy, enterprise architecture, process redesign, change management and performance measurement
- **Systems integration**—system architecture, system development and implementation of business and technology solutions
- **Application development and management**—design, development, implementation and day-to-day maintenance and improvement of clients' business applications Infrastructure services—comprehensive infrastructure management capabilities that adapt to clients' unique business requirements and service priorities
- **Business process services**—management of back-office business processes to streamline operations
- **Proprietary solutions**—deep portfolio of 100+ mission-critical solutions that reduce costs and create competitive advantage for our clients

OUR CAPABILITIES

We provide clients with a partner that is not only expert in IT, but also expert in their industries. This combination of business knowledge and technology expertise allows us to help our clients adapt as their industries change. Key capabilities include:

- **Consulting, Development and Systems integration** - CGI acts as a trusted advisor, providing a full range of IT and management consulting and implementation services that cover the full scope of today's enterprise IT environment.
- **Technology Management** - CGI has full IT infrastructure management capabilities, allowing clients to delegate entire or partial responsibility for their IT functions.

© 2015 CGI GROUP INC

- **Application Management** - We provide day-to-day maintenance and improvement for clients' business applications, helping reduce costs and ensure faster delivery of new initiatives.
- **Systems Integration and Development** - CGI acts as a trusted advisor, providing a full range of IT and management consulting and implementation services that cover the full scope of today's enterprise IT environment.
- **Business Process Management** - We manage back-office business processes and transactions on behalf of our clients, allowing them to concentrate on their core business, strengthen their competitiveness and improve their bottom line.
- **Proprietary security solutions** - CGI possesses a deep portfolio of 100+ mission critical solutions that reduce costs and increase our client's competitive advantage.

OUR APPROACH

CGI developed an innovative, flexible, and personal approach to providing services. We structure each relationship to meet our client's unique business goals and build in flexibility to meet current and future needs. CGI provides end-to-end IT and business process services that include consulting, systems integration and the management of business and IT functions as well as industry specific solutions. CGI employs a compelling and unique global delivery model, a flexible, scalable, and cost-effective solution to meet our client's business and IT needs. Clients choose from a palette of offerings to create the onsite, offsite, nearshore, offshore combination that gives them the savings, efficiencies, and control that they want. Our delivery model is supported by our strong corporate governance policies, which prescribe our beliefs and practices and balance the needs of our three key stakeholders: clients, members, and shareholders.

To each relationship, we bring:

Quality and delivery track record – Quality processes have always been at the forefront of CGI's operations. Our track record of on-time, on-budget delivery is rooted in the CGI Management Foundation, which encompasses our ISO-9001 certified client, member (employee) and shareholder management frameworks. Our delivery approach differentiates CGI from many competitors. We adapt to the client's way of conducting business, which is the least disruptive to them and maintains their control of strategic functions. We listen closely to thoroughly understand client needs and carefully adapt our solutions and processes accordingly.

Flexible and accountable partnerships – Leaders in many industries have made CGI their partner of choice. We have achieved this status by listening to our clients and by nurturing an internal business concept that provides the right degree of empowerment and accountability at all levels. Through our client proximity-operating model, CGI ensures that clients have local contacts that live and work in their communities, fully understanding their business needs and being accountable for project success. This translates into rapid decision-making, agile delivery and ability to adapt to challenging situations.

Industry depth and expertise - CGI has long and focused practices in all its core industries, providing clients with a partner that is not only expert in IT, but also expert in their industries. Our knowledge and experience with each industry's business environment and practices enables us to design solutions that address industry-specific issues. This combination of business knowledge and technology expertise allows us to help our clients adapt as their industries change.

© 2015 CGI GROUP INC

Our mission

The mission of CGI is to help its clients with professional services of outstanding quality, competence and objectivity, delivering the best solutions to fully satisfy client objectives in information technology, business processes and management. In all we do, we foster a culture of partnership, intrapreneurship, teamwork and integrity, building a world class IT and business process services company.

Our values

Sharing the same values allows us to enjoy considerable autonomy and swiftness of action without compromising our cohesiveness. It also allows us to mobilize teams more rapidly and bring together the most experienced individuals from across the company, who are able to quickly work as one to address a given challenge. And, of course, these values guide our decisions and actions.

Our team

CGI Excellence in Security Support

CGI is a 4-time winner of the James S. Cogswell Outstanding Industrial Security Achievement Award.

CGI comprises designers, practitioners, and managers known for their competence, professional standing and energy. They have been recruited based on the quality and breadth of their experience, as well as on their sense of initiative, service, innovation, and team spirit. We call our employees “members” because all who join our ranks take full ownership in building a world-class company. CGI members have strong industry backgrounds - many having worked in their client's industries for years - and have expertise in both the business and technology sides of the business. Ninety percent of our professionals are active shareholders of CGI, reinforcing our commitment to client success.

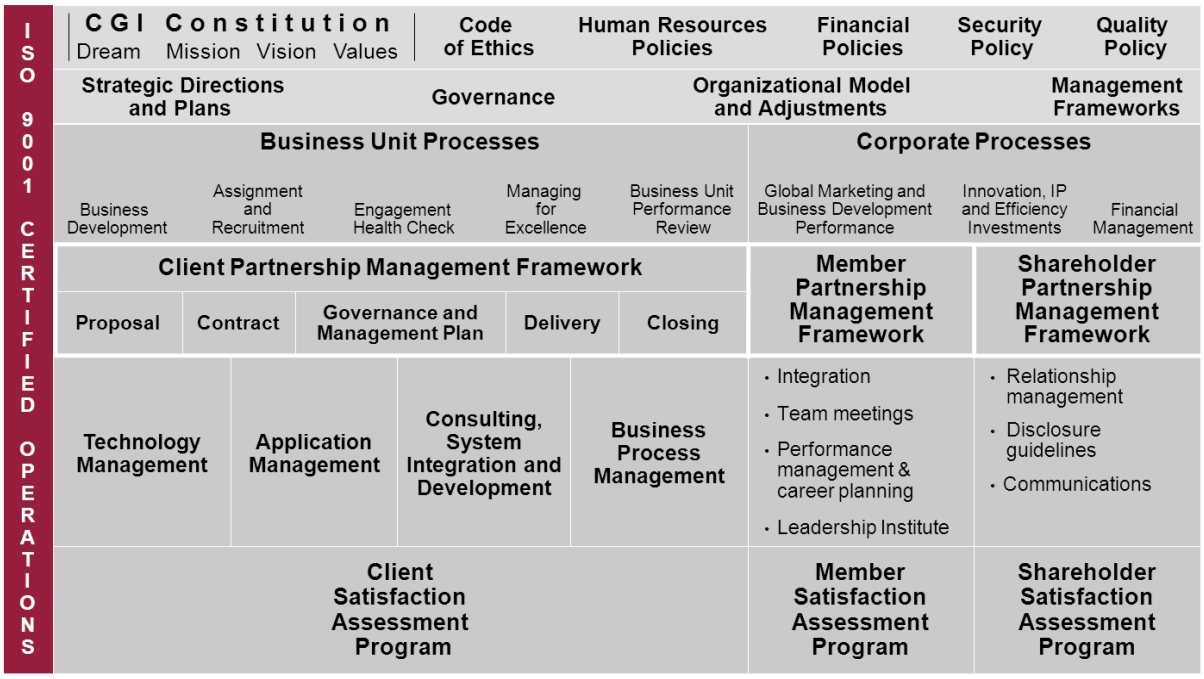
To keep pace with the most recent developments in technology and management, CGI ensures the on-going training and professional development of its members. This assures the client the best business solution.

CGI's growth as a company is attributable, among others, to the commitment of all of CGI's members and to the company's fundamental values, which the management has always embraced.

CUSTOMER SATISFACTION

In all of our client engagements CGI uses its Management Foundation. This is shown below and encapsulates how we deal with all of the stakeholders in a project.

© 2015 CGI GROUP INC



© 2012 CGI Group Inc.

CGI's Client Partnership Management Framework (CPMF) is the critical client-facing management framework that governs the success of all engagements. The Client Satisfaction Assessment Program (CSAP) is a critical element of the CPMF, providing feedback from clients to fuel our continuous improvement efforts. During CSAP review, CGI measures ten (10) areas of client satisfaction including CGI's understanding of business requirements, customer focus, and quality of service delivered. The client rates these areas, one (1 - lowest) to ten (10 - highest), on an Assessment Questionnaire signed by both a Client and CGI representative upon completion.

CSAP reviews are planned for each six-month period of continuous service delivery. All completed CSAP forms are sent to the Quality Systems Coordinator to be entered into a CGI database and the CGI Process Management system for tracking and reference. If the CSAP has at least one score of less than or equal to five (5), the QSC must initiate CGI's non-conformity process. The non-conformity process determines root cause and implements corrective action, which is revisited to measure resolution to the client's satisfaction.

WHY CHOOSE A MANAGED SECURITY SERVICE PROVIDER?

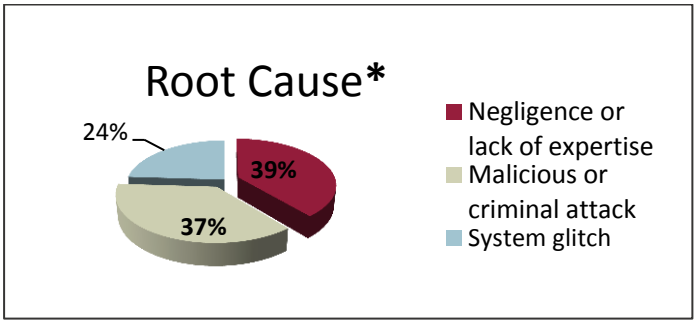
Several factors contribute to an increasing demand for Managed Security Service (MSS) Providers.

- **Staffing and budget constraints**: Corporations face the need to reduce operational costs and capital expenditures, and avoid staffing increases, while maintaining a sufficient security posture and meeting compliance mandates. Delivering security services incurs a personnel and expense overhead for each and every security appliance that the organization identifies it needs. This low-level appliance focus takes internal staff away from the more useful organizational issues.
- **Evolving compliance requirements**: Compliance reporting requirements continue to contribute in almost every MSS engagement. This is a result of compliance requirements and governance policies evolution driving stronger requirements for incident monitoring, identification and response among business partners and suppliers. As formal compliance regimes evolve or audit/enforcement activity increases, organizations consider external providers to reduce the costs of meeting compliance

requirements. A primary driver continues to be PCI DSS, however many other regulations see continuous monitoring requirements as an increasing factor for government agencies, commercial firms that sell to the government, and organizations funded by government grants, such as universities.

- **Expansion of Internet connection points**: Enterprises continue to enable local Internet connectivity for remote offices. This increasing complexity drives MSS demand for firewalls and Unified Threat Management (UTM) devices, as well as for network-based firewall, Intrusion Prevention Services (IPS) and security gateways as service offerings.
- **Contextual security**: Organizations that conduct their own security only have the context of their own security issues and the incidents they are currently dealing with, on their own. By engaging a multi-national MSS provider, an organization can get advance warning of threats that 'follow the sun' and incidents that have effected similar organizations. This allows for pre-emptive defensive measures and for the organization to draw on the security expertise of the MSS.

The 2011 Cost of Data Breach Study, published by the Ponemon Institute LLC in March 2012, interviewed 49 U.S. companies in 14 different industry sectors. The chart below indicates that employee or contractor negligence and/or lack of expertise represents approximately two-fifths of all reported IT system breeches while malicious/targeted attacks account for 37 per cent. Malicious and targeted attacks are the most costly to an organization with an estimated cost of $222 per incident.



*2011 Cost of Data Breach Study, Ponemon Institute LLC

The Ponemon Institute study indicates that malicious attacks come from a variety of areas, each representing a unique attack vector within an organization (incidents can involve blended attack types).

DELIVERING GLOBAL SECURE OUTCOMES

CGI is one of the most comprehensive and leading providers of end-to-end security services. With professional security specialists in each geographic region and business unit, CGI has had a formal Security Center of Expertise (COE) for over 15 years. Under the guidance of the global cyber security leads, CGI has over 1400 security services and consulting professionals providing services to 100s of clients across world.

CGI has developed a breadth of security service offerings to meet the varying requirements of its clients across multiple verticals as well as small, medium and enterprise markets. Each service line consists of a base service offering with flexible delivery models, and flexible asset ownership as well as vendor independence. CGI's Security Service offerings are managed using standard product management methodologies ensuring CGI is continually evaluating its services, the technologies deployed, and the business and regulatory requirements driving the future demands of our clients.

CGI Cyber Resilience was recently formed to further draw together these key areas of expertise into a powerful, industry-leading capability. Leveraging centers of expertise across the globe, it provides CGI clients not only with MSSP offerings, but also with security expertise and solutions in all disciplines, including security governance, security testing, and certification, vulnerability analysis, penetration testing and forensic

© 2015 CGI GROUP INC

investigation. The result is a comprehensive, end-to-end offering of integrated security services and solutions designed to provide government and industry clients with the type of in-depth asset protection and assurance required in today's high threat environment.

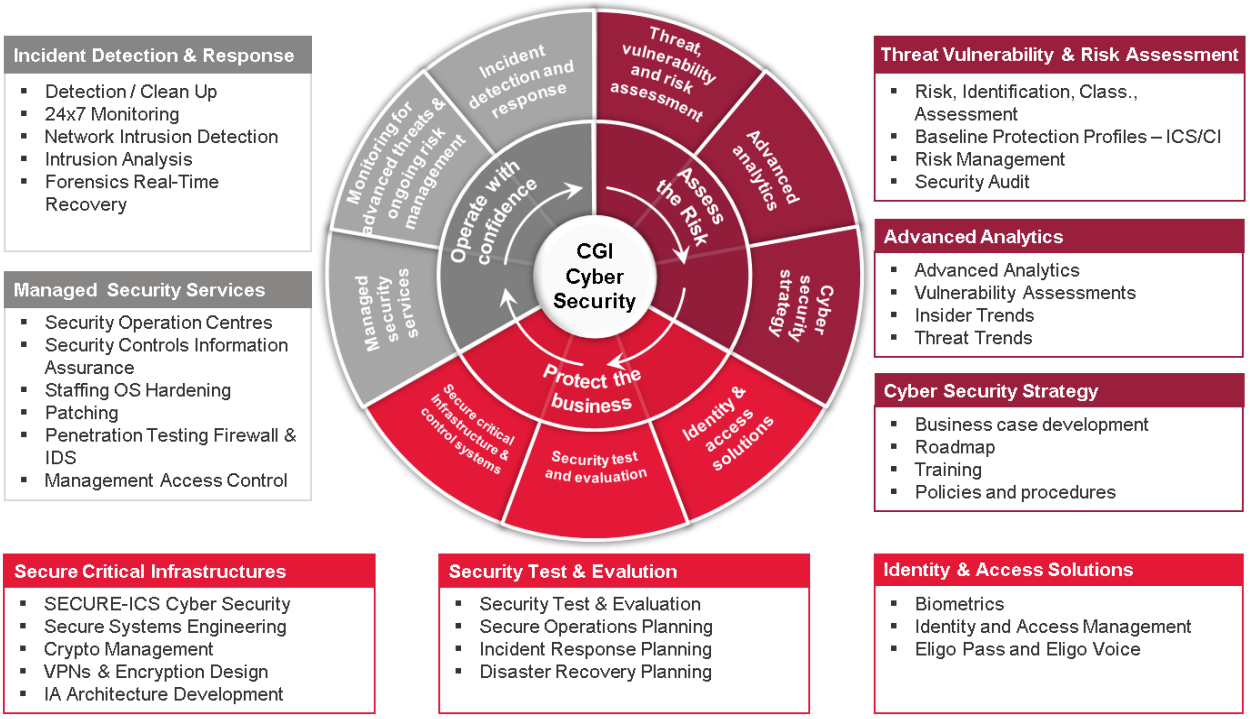


Figure 1: CGI delivers security solutions that assess the Risk, Protect the Business, and promote Operating with Confidence

MANAGED SECURITY SERVICES

CGI was ranked as the leading provider of Managed Security Services (MSS) in a study released by the analyst firm IDC Canada. The MSS group delivers the same enterprise security services and solutions to the internal CGI infrastructure and business units as it does to client's environments and businesses. This ensures our very strong internal security standards are met, and that clients have less risk to the environments that CGI manages.

MSS services are delivered using ISO 9001-certified quality processes grounded in proven industry best practices. With over 200 certified security professionals holding certifications from SANS, ISO, GIAC, ISC2, NIST, CC and ISACA supported by a 24x7 state-of-the-art Security Operation Center (SOC), CGI has the depth of knowledge and support coverage organizations need to meet the increasing demand for security compliance and vigilance.

SECURITY CONSULTING

CGI's security team has completed over 1000 security projects for private industry and government departments and agencies. CGI Globally has over 300 former Government Intelligence officers with various specialties that can provide a truly holistic security perspective. This tied with CGI's in-house e-learning capability provides a robust training knowledge base and capacity. Our professional security consultants include more than 1400 security professionals. Additionally, we employ Certified Information System Auditors (CISA), ISO-27001 Lead Auditors, Project Management Professionals (PMP), Professional Engineers

© 2015 CGI GROUP INC

(P.Eng.), personnel with advanced degrees (e.g. PhD's) in Computer Engineering and Computer Sciences, SANS Global Information Assurance Certified (GIAC) certified Forensic Investigators, Certified Business Continuity Planners (conferred by the Disaster Recovery Institute), and GIAC certified Incident Analysts.

KEY DIFFERENTIATORS

Unlike many companies, CGI does not require third parties to be involved in delivering our managed security services; including Security Event and Information Management (SEIM). CGI does not 'white label' other companies services for security thus avoiding the inherent security risk that would incur.

- Our 24x7x365 Security Operations Center is staffed by CGI employees
- We are vendor neutral and will only use security products that are a best fit for the client
- We are an IT company, not an ISP, telco, product vendor or audit company
- We provide our services; they are not white-labeled, sub-contracted or virtualized
- We have the flexibility to provide emergency security support to our clients and work with them to define and then deliver services based on their specific requirements

SECURITY OPERATIONS CENTER

People

CGI's corporate recruiting policy validates that all members are properly screened to the appropriate level specified by local laws, regulations, and contract requirements prior to authorizing their employment on projects involving access to sensitive information or assets within the limit of applicable laws. Before being granted access to sensitive IT systems, information, or assets, each CGI member is provided with security awareness training and records management training by Human Resource. Additional training is recommended per employee and is available online through CGI's Skills portal. CGI members are required to read the CGI security policies, sign as having read and understood them, and comply with them. All CGI members must adhere to a non-disclosure agreement as part of their employment contract by signing the Member Commitment to the CGI Code of Ethics and Business Conduct, which is filed in Human Resources. All CGI members must sign this document every year as part of the annual evaluation process.

As dictated by CGI Enterprise Security Policies and Standards, the following presents an overview of the elements that fall under the three levels of member security:

Level 1 - Minimum Standard (All members)

- Personal Data Check (Identity)
- Education/ Professional Qualifications
- Employment History and References

Level 2 - Conventional Standard (Members with access to CGI/client financials or by client requirement)

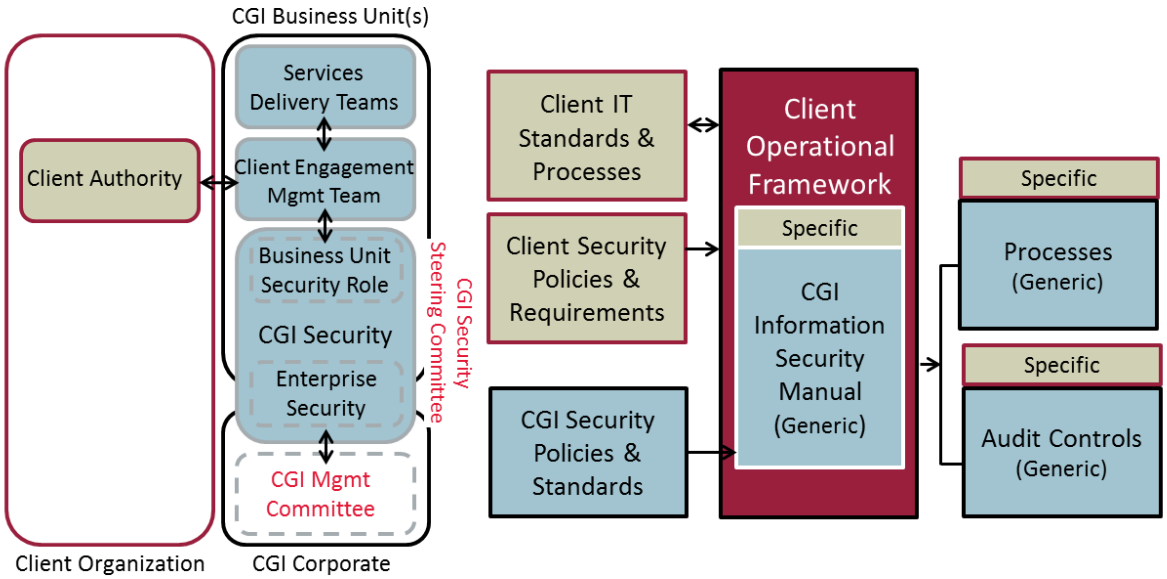
- Credit Check
- Criminal Record Check

Level 3 - Government Level Security Clearance (SOC Members & CoE Consultants)

© 2015 CGI GROUP INC

Process

CGI has implemented an information security management program which aligns with its ISO certified Client Partnership Membership Framework© (CPMF). This program provides consistent management direction and support for information security risk management, and defines broad guidance for all key controls. This mandates compliance to CGI security policies, standards and guidelines, which map CGI practices to the legal and regulatory requirements to which CGI and its clients are subjected. Policies within the program are approved by the Chief Executive Officer of CGI, maintained by CGI Enterprise Security, implemented by CGI Business Unit security officers, and followed by CGI service delivery teams. Policy exceptions, incidents and remedial activities are communicated to the designated Client Authority by Client Engagement Management teams on a continuous basis as part of CGI's Operations Framework.



CGI Information security management program governance structure and alignment to processes and procedures

To validate compliance with different laws and regulations, CGI has developed its own compliance framework of internal controls based on governance, risk assessment and compliance requirements. The CGI portfolio of key controls has been developed over years of continuous improvement iteration, and is mapped to COSO and CoBIT with the associated processes based on ITIL v3 best practices. Standards implementation guidance is cross-referenced to ISO/IEC 27002:2005. As a public company, our processes are also subject to compliance to Sarbanes-Oxley S.404.

CGI's data center operations and hosting are audited under, and in compliance with, SAS 70 and CICA 5025 reporting standards for many CGI clients. These reporting standards are appropriate for financial solutions and systems managing financial information.

CGI is also ISO 9001 certified. CGI will utilize its ISO 9001 certified CPMF to manage the delivery and support of the proposed solution. By design, all Managed Security Services are delivered using ISO 9001-

© 2015 CGI GROUP INC

certified, 27001-aligned quality processes grounded in proven industry best practices such as ITIL. CGI has adopted the SANS methodology as the basis for its security incident handling procedures.

Technology

CGI uses state-of-the-art tools to provide comprehensive health and availability monitoring 24x7x365 on our client's environment for both technical infrastructure incidents and to identify security events that need investigating. Our Security Engineering team members continuously seek and deploy the latest and best solutions, which maintains CGI state-of-the-art security infrastructure. At the core of our Managed Security Services, is our Security Event and Information Management (SEIM) solution. Our SEIM solution provides our clients with an industry-leading single, enterprise-wide, target repository for security logs, and provides the separation of duties of system administration vs. security analysis sought by many organizations.

© 2015 CGI GROUP INC

cgi.com

© 2015 CGI GROUP INC