White Paper

Cybersecurity in Modern Critical Infrastructure Environments

SECURE-ICS™

Be in Control Securing Industrial Automation & Control Systems®

This document is part of CGI’s SECURE-ICS™ family of cyber security methods, tools, materials, services, etc. to secure industrial automation and control system environments and critical infrastructures.
# Table of Contents

INTRODUCTION ......................................................................................................................... 3

CYBERSECURITY TRENDS, CHALLENGES & OPPORTUNITIES ............................................ 3

BUSINESS DRIVERS & CHALLENGES ...................................................................................... 4

  INCREASING SOPHISTICATION OF CYBERCRIME ............................................................... 5
  CLOUD COMPUTING .............................................................................................................. 6
  RISE OF MOBILE DEVICES & APPLICATIONS ................................................................. 7
  CRITICAL INFRASTRUCTURE ................................................................................................. 7
  LEAKAGE OF SENSITIVE DATA / INTELLECTUAL PROPERTY ........................................... 7
  INCREASING REGULATORY ENVIRONMENT ....................................................................... 7

TACKLING CYBERSECURITY IN THE ENTERPRISE ................................................................. 7

ESTABLISHING A CYBERSECURITY MANAGEMENT FRAMEWORK ........................................ 9

SUMMARY & RECOMMENDATIONS ......................................................................................... 12

ABOUT CGI ............................................................................................................................. 13

REFERENCES ........................................................................................................................ 14
**INTRODUCTION**

In today’s business environment, disruptive technologies such as cloud computing, social computing and next-generation mobile computing, as well as the interconnections between corporate networks and process control networks, are fundamentally changing how organizations use information technology for sharing information and conducting commerce online. This wave of technology innovation, often driven by information technology trends that are being rapidly adopted across the enterprise, has created unparalleled levels of access and connectivity across people, information, systems and assets worldwide and has transformed today’s network-delivered society.

In the cybersecurity arena, the increasing sophistication, frequency and scale of cybercrime as a result of this open and network-oriented society, coupled with an explosion in the use of “edge” devices and cloud applications as well as increasing regulatory requirements, has created an urgent need for organizations to rapidly advance their security countermeasures and re-think traditional approaches. On a more global level, due to the compelling and pressing nature of the issues involved, many countries have elevated cybersecurity to a top-tier priority within their national security strategies.

To keep pace and stay ahead of escalating risk levels while at the same time efficiently managing costs, business leaders need to rethink their cybersecurity postures in the context of a broader risk management strategy and adopt a new strategic framework that addresses these numerous disruptive trends across the IT landscape. By having a logical framework for understanding cybersecurity and the major domains it represents, enterprises can implement their cyber strategies and develop specific plans tailored for each domain and exposure area in a holistic manner.

Key focus areas should include the following:

- Governance
- Risk and compliance
- Users (identity assurance, regardless of location or device type)
- Data (sensitive data protection, no matter where it resides)
- Applications (application security modernization)
- Infrastructure (securing the “borderless” enterprise, including cloud computing)
- Production (industrial control systems/critical infrastructures)
- Assets (cyber supply chain)

The challenge is far broader than simply addressing one issue such as securing data, securing mobile devices or securing cloud computing environments. By ensuring a cybersecurity strategy addresses all of these interrelated issues, business leaders can be confident of a defense-in-depth approach.

For businesses and governments alike, getting the cybersecurity posture right across all key areas is vital for future growth, innovation and competitive advantage. It’s also vital for truly exploiting the business and economic opportunities provided by technologies such as cloud, mobile, and social computing, as well as smart computing, industrial automation and IT appliances. A cybersecurity-related misstep in any of these rapidly emerging areas can lead to lost productivity and serious damage to brand reputation.

There is no single answer for success. However, by working across public and private sector partnerships and by advancing security measures—particularly with regard to mission-critical systems, processes and applications that are connected in cyberspace—businesses will be able to work towards a future environment that is open, secure and prosperous.

**CYBERSECURITY TRENDS, CHALLENGES & OPPORTUNITIES**

While traditional information security has always included practice areas related to the security of information and systems, the cyber world that we live in today has become increasingly connected and increasingly mission critical due to our network-delivered society. The traditional enterprise boundaries that formed the basis for securing the perimeter from the outside world have, by necessity, become increasingly porous to support this new, routinely wireless and ubiquitous “always-on” connectivity.
The major challenge for organizations today is determining how to embrace disruptive technologies and trends such as “everything connected,” cloud, mobile, and social computing, while at the same time managing the inherent risks that conducting business in cyberspace creates.

Before studying the business drivers and challenges related to cybersecurity, it’s important to understand the general definition and scope of the term and how it relates within the broader context of security. A useful definition comes from the UK’s cybersecurity strategy:

“Cyber Security embraces the protection of both private and public sector interest in cyber space and their dependency on digital networks and also the protection of exploitation of opportunities—commercial or public policy—that cyberspace offers.”

While there are many definitions, the key point to note is that the scope of cybersecurity extends not only to the security of IT systems across the enterprise, but also to the broader digital networks upon which they rely, including cyberspace itself and critical infrastructures.

On a national level, many governments have deemed cybersecurity a tier one priority within their national security strategies, recognizing the likelihood and impact of potential attacks. Some figures clearly illustrate the magnitude of the problem. In less than 15 years, the number of global web users has exploded by more than a hundredfold, from 16 million in 1995 to more than 1.7 billion today. By 2015, there will be more interconnected devices on the planet than humans. As this “fourth utility” (after electricity, water and the telephone system) as it is sometimes called has grown, cybercrime has grown significantly as well. In fact, the cost of cybercrime has been estimated at more than $1 trillion per year globally.

One of the key implications of this definition of cybersecurity is that we now have a society dependent on network-delivered services. Protecting this new dependency is what we call cybersecurity. It spans both the logical world of IT, i.e., bits and bytes and computers, as well as the “real world” of utilities, productions and services in cyberspace. Everything we do is network-delivered, even crime. One of the imperatives for any cybersecurity strategy is therefore to take a more holistic approach to how we defend and protect our organizations, and even our society, and to help recover when things go wrong.

BUSINESS DRIVERS & CHALLENGES

Today, some of the major cybersecurity business drivers impacting the enterprise include the following:

- Increasing sophistication, frequency and scale of cybercrime
- Malicious and inadvertent leakage of sensitive data
- Loss of intellectual property
- Increasing regulatory environment
- Interconnections between corporate and process control networks
- Vulnerabilities introduced by the rise of cloud computing, mobile devices and Web 2.0 applications within the enterprise (see next figure)

Each of these business drivers creates unique challenges for CIOs and CISOs (chief information security officers) within both the public and private sectors (see next figure). While these are not the only drivers, they are of a magnitude that requires serious attention to compete in the cybersecurity “arms race” by managing risk and protecting assets.

We’ll now examine some of these drivers and challenges individually and their impact on businesses.
INCREASING SOPHISTICATION OF CYBERCRIME

The increasing sophistication, frequency and scale of cybercrime is requiring public and private sectors to scale up their levels of protection across their operations and become more “predictive” to avoid becoming the next headline. One such illustration of this increasing sophistication was the Stuxnet worm, which was discovered in June 2010, and infected computer systems around the world. This worm was thought to have more than 4,000 functions, comparable to some commercial software.

While Stuxnet may or may not have been government-sponsored, it’s an example of the complexity of some of these worms. Symantec has monitored more than 40,000 Stuxnet infected IP addresses in 155 countries. In terms of frequency, cyber attacks have become common occurrences with companies. A recent Cisco study shows that 4.5 billion e-mails and 80 million web requests are blocked every day and that 50,000 network intrusions are detected every day. A Ponemon study found that the average cost to the enterprise for a data breach was $3.4 million when factoring in detection and escalation, notification, response and lost business.

This study excluded catastrophic data breach incidents to avoid skewing overall findings. All of this points to the challenge of business leaders in raising protection levels against cybercrime while reducing or maintaining costs.
As organizations move towards cloud computing for the inherent agility and economic benefits this IT delivery model offers, they are increasingly moving towards hybrid enterprise environments that consist of a mix of cloud, non-cloud, internal and external IT service delivery models. This is due to the fact that not all application workloads, whether they are business-as-usual, mission-critical or highly innovative, are suited to cloud deployments and may need to remain within a more traditional model for reasons as varied as architecture, regulatory compliance and the location of stored data.

This hybrid enterprise environment is more than just a hybrid cloud model consisting of two or more cloud-based entities. It is a composition of cloud, non-cloud, internal and external IT service delivery models that remain unique entities, but are bound together by an integrated management environment and common technology, processes and policies. The cybersecurity challenge for cloud computing is therefore not only to protect data within public clouds and hosted private clouds, but to ensure governance, risk and compliance is addressed across this fully integrated environment where applications and data may be highly virtualized across the end-to-end infrastructure.
RISE OF MOBILE DEVICES & APPLICATIONS

The consumerization of IT, as noted by recent IDC research, exposes a broader array of end user or consumer devices in use within the enterprise, many of which are personally owned. There is also an ever increasing use of social computing technologies and platforms for internal and external collaboration. Research has revealed that information workers are using an average of four consumer devices and multiple third-party applications, such as social networking sites, in the course of their day. In addition, the number of connections via mobile devices is expected to reach nearly 9.7 billion by 2017, according to “The Mobile Economy 2013,” an A.T. Kearney report. The challenge for security practitioners is how to secure this increasingly porous and seemingly borderless enterprise, and manage the risks of lost or stolen devices, inadequate authentication of mobile workers, and unauthorized disclosure of confidential and sensitive data via social networks.

CRITICAL INFRASTRUCTURE

Organizations within critical infrastructure sectors provide the essentials of modern life and defend our national security. Their services impact national economic security, as well as national public health and safety. Many sector components influence or impact any combination of these critical national concerns.

Cybersecurity is an integral part of overall critical infrastructure sector security, and governments are addressing the risks as a sector-wide challenge to minimize the potential impact on both public safety and the economy.

Because these sectors touch so many aspects of how we live our lives and how business is conducted around the world, technology, connectivity and information exchange are three of the greatest challenges and essential aspects of company operations and processes within these sectors. However, the same technologies that make business operations and critical infrastructure processes more efficient can introduce new risks. As the world faces increased threats, critical infrastructure sectors need to increase their capability to manage cybersecurity risks and protect against the threat of unauthorized access to information for the purpose of causing a physical attack or disruption in the supply chain.

LEAKAGE OF SENSITIVE DATA / INTELLECTUAL PROPERTY

The leakage of sensitive data is another area that has been highly publicized. One of the most recent examples is the WikiLeaks saga related to the exposure of stolen classified U.S. diplomatic documents during which WikiLeaks shared these classified documents with newspapers such as The New York Times, Le Monde, Der Spiegel, and The Guardian. This highlights the increasingly complex issue of protecting intellectual capital and maintaining privacy. The U.S. alone has 50 states with a multitude of data breach laws and differing data protection practices. Sensitive data protection has to be addressed along with privacy while organizations move to the cloud, add more mobile devices and adopt social computing paradigms. Business leaders need to address how to secure and protect sensitive data no matter where it resides—including real-time detection and prevention of unauthorized disclosures—and how to strike the right balance between “need to know” and “need to share.”

INCREASING REGULATORY ENVIRONMENT

Organizations are also grappling with the expected impact of new security legislation and mandates applicable to the protection of critical infrastructures and key resources across all sectors. International committees have been wrestling with protecting the Internet without regulating it. There has been a significant amount of international discussion about what constitutes cyber war and what treaties need to be enacted. The dynamic has swung the pendulum from historically reactive monitoring to proactive, continuous monitoring for situational awareness. Another requirement is the migration to trust-based systems with built-in, end-to-end, security.

TACKLING CYBERSECURITY IN THE ENTERPRISE

Because cybersecurity and overall security, which includes “physical” or “real world” security, are so intricately linked, we believe it is important to have integrated strategies within the enterprise for both. An organization’s strategy for prevention, detection and reaction should take a more holistic approach and be built on the
concept of a common operating picture and situational awareness across all fronts—both cyber and non-cyber. This supports a defense-in-depth approach where each layer of security, whether physical or logical, helps to ensure the overall security posture of the organization—from society to sensor in critical infrastructure/process control networks where production environments are interconnected with corporate networks.

The cybersecurity framework you choose or may already have in place will likely depend upon your specific industry and the countries in which you conduct business. While these frameworks can range from simple to complex, the main goal is to categorize the cybersecurity areas that should be secured and integrated as part of your overall approach. This, of course, should be in addition to following standards and compliance-based approaches and requirements such as the ISO 27000 series and ISA99/IEC62344, which provide best

**ESTABLISHING A CYBERSECURITY MANAGEMENT FRAMEWORK**

In the context of this overall security strategy, it is important to understand the gaps and overlaps between cybersecurity and the other security domains. By having a logical cybersecurity management framework for understanding cybersecurity and the major domains it represents, enterprises can implement their cyber strategies and develop specific plans tailored for each domain. The challenge is far broader than simply addressing one issue such as securing mobile devices or securing cloud computing environments. By ensuring the cybersecurity strategy and logical framework addresses all of these interrelated issues, business leaders can be confident of a comprehensive approach. Additionally, a logical cybersecurity management framework and reference architecture for addressing cybersecurity can help an organization migrate from tactical, point solutions to a more coordinated set of tools and techniques, or systems approach, by seeing the “big picture.”

The mission of a critical infrastructure cybersecurity management framework is cybersecurity risk management and reduction to provide open, secure information and industrial and control systems that protect employees and communities and facilitate business operations.

Companies achieve the greatest number of benefits when a holistic system management approach is implemented. This guidance does not necessitate new stand-alone programs, but rather describes opportunities for reliance on and adaptation to other management frameworks. The fundamental objective is to use familiar management frameworks to enhance cybersecurity. Through an integrated approach, indirect benefits also can be anticipated. The enterprise, as well as the critical infrastructure domains, have unique industrial and control and information system characteristics. These characteristics combined with the value chain create a potential physical security impact.

In general, a cybersecurity management framework should cover the following:

- **Introduction:** Introduces the overall topic of cybersecurity for the critical infrastructure sector.
- **Statement of management practice:** Identifies the scope and objectives of the key framework elements.
- **Applicability of cybersecurity in the critical infrastructure sector:** Describes cybersecurity objectives for the critical infrastructure sector, focusing on applicability to traditional IT assets, manufacturing and control systems, and critical infrastructure sector value chain components.
- **General baseline practices:** Outline common options for critical infrastructure sector companies to consider for benchmarking and enhancing cybersecurity practices. Additional or alternative practices may be required based on a company’s individual circumstances.
- **How critical infrastructure companies are approaching cybersecurity:** Builds upon general baseline practices and describes some of the innovative approaches critical infrastructure sector companies are using to further enhance cybersecurity.
- **Resources used:** Lists sources for additional information as well as referenced documents.

The figure below represents CGI’s cybersecurity management framework for critical infrastructures based on international standards and industry best practices. This cybersecurity management framework is completely in line with the new USA NIST Cybersecurity Framework 2014 and even covers more elements than addressed in the NIST Cybersecurity Framework.
The following is a brief summary of 21 specific elements a cybersecurity management framework should address:

1. **Importance of cybersecurity in operations**: Describes the importance of having an awareness and understanding of the impact of cybersecurity on IT operations and risks. This extends to manufacturing and control systems, value chain operations, joint ventures, third parties, outsourcing partners, as well as business-related IT activities.

2. **Scope of cybersecurity management framework**: Notes that management must determine the scope of the framework. The scope can include all aspects of business information systems, manufacturing and control systems, and integration points with business partners, customers and suppliers. A management framework can be established to initiate and control the implementation and ongoing operations of cybersecurity within the company.

3. **Security policies**: Addresses the need for senior leadership commitment to continuous improvement through published policies. Providing policies to employees and reviewing them regularly is recommended.

4. **Cybersecurity reference architecture**: Addresses the principles, concepts and structures necessary for secure sites/plants. The main principle is defense-in-depth.
5. **Risk identification, classification and assessment:** Discusses the importance of identifying, prioritizing and analyzing potential security threats, vulnerabilities and consequences using accepted methodologies.

6. **Risk management and implementation:** Addresses the need to develop security measures that are commensurate with risks. The security measures may take into account inherently safer approaches to process design and engineering, as well as administrative, manual and procedural controls, and prevention and mitigation measures. The importance of risk mitigation is to convert all risk management plans into actions and have a program plan in place to monitor effectiveness.

7. **Statement of applicability (SoA):** Addresses the need to document the results of all security controls, as well as the elements of each security control. Documented results aid in the decision-making process, facilitate the communication of decisions, provide a basis for training and education, improve response time to incidents and threats, and provide a basis for subsequent self-assessment or auditing of the security control compliance.

8. **Business continuity plan:** Addresses the need for a course of action in responding to disasters, security failures and loss of services. Contingency plans should be developed, implemented and tested to help ensure that business processes are restored in a timely fashion.

9. **Organizational security:** Addresses the need to establish an organization, structure or network with responsibility for overall security, recognizing there are physical as well as cyber components involved. Organizational security requires accountability to be established to provide direction and oversight for a company's cybersecurity strategy. Cybersecurity in the broadest sense covers not only data but also systems (hardware and software) that generate or store this information and includes elements of physical security as well. Manufacturing and control systems specialists, value chain partners, third-party contractors, joint venture partners, outsourcing partners and physical security specialists can be considered by the organization as part of the overall security structure, and hence included in the scope of responsibility.

10. **Personnel security:** Describes security responsibilities at the recruitment phase and the inclusion of these responsibilities in all contracts and individual monitoring during employment. Recruits can be screened as part of the process, especially for sensitive jobs. Companies may consider having all employees and third-party users of information processing facilities sign a confidentiality or nondisclosure agreement.

11. **Physical and environmental security:** Addresses the protection of tangible or physical assets (e.g., locations, buildings, computers, networks, manufacturing processes equipment, etc.) from damage, loss, unauthorized access or misuse. Critical information or assets can be safeguarded by placing them in secure areas, protected by security perimeters and entry controls (security zones and conduits). These physical security controls work in conjunction with cybersecurity measures to protect information.

12. **Information and network/communication security:** Addresses the protection of information and network/communication security assets from damage, loss, unauthorized access or misuse. Critical information or assets can be safeguarded by placing them in secure IT areas, protected by security perimeters and access controls (security zones and conduits).

13. **Incident planning and response:** Addresses the need to be vigilant in efforts to deter and detect any cybersecurity incident. If an incident occurs, the company needs to promptly respond and involve management and government agencies as appropriate. After investigating the incident, the company may consider incorporating key lessons and, if appropriate, share those lessons with others in the industry, as well as government agencies, and implement corrective actions.

14. **Communications, operations and change management:** Addresses the development of processes and procedures to ensure the security of computer systems and information processing facilities. Clearly articulating the operational security aspects can enhance these overall management practices and procedures. The need for security is very strong for manufacturing and control systems that are used to operate facilities because security lapses have the potential to result in safety, health or environmental issues.
15. **Identity access management**: Addresses account administration, authorization and authentication. Account administration involves the development of rules to ensure that users’ access to systems and data is controlled. There are rules that are enforced administratively, and those that are enforced automatically through the use of technology. Both kinds of rules are generally addressed as part of the overall access control strategy. Authorization addresses the need for businesses to establish and employ a set of authentication practices commensurate with the risk of granting unauthorized users, hosts, applications, services and resources access to critical system resources. Authentication describes the process of positively identifying network users, hosts, applications, services and resources for some sort of computerized transaction using a combination of identification factors or credentials. Authentication is the prerequisite to allowing access to resources in a system.

16. **Information and document management**: Addresses processes for data classification and the safeguarding of information, as well as document management processes associated with a cybersecurity management system. Document management is generally a part of a company’s records retention and document management system.

17. **System development and maintenance**: Addresses the need for security to be built into the information system and sustained through normal maintenance tasks.

18. **Staff training and security awareness**: Describes how management commitment is critical to providing a stable computing environment for both information and manufacturing and control systems. Effective cybersecurity training and security awareness programs provide each employee with the information necessary to identify, review and remediate control exposures, and help ensure their own work practices are utilizing effective controls.

19. **Compliance and privacy**: Addresses scheduling and conducting audits, and compliance with legal, regulatory and contractual security requirements. A company should periodically assess its security programs and processes to ensure their adequacy and proper application. In appropriate circumstances, assessments should also be conducted with suppliers, logistics service providers, joint ventures or customers. In addition, to avoid breaches of criminal or civil law, as well as regulatory and contractual obligations, a compliance audit may be necessary.

20. **Cybersecurity framework monitoring and review**: Addresses the continuous monitoring and review of the cybersecurity management framework. Internal checking methods such as system audits, compliance audits and incident investigations help determine the effectiveness of the management framework and whether it is operating according to expectations. Finally, through a management review process, the company’s senior leaders should assess the performance of the framework and identify any deviations from the goals, targets and objectives established during the planning process. If there are deviations or non-conformance, revisiting the original assumptions and/or taking appropriate corrective actions may be necessary.

21. **Maintaining and implementing improvements**: Describes the importance of maintaining and implementing improvements to the cybersecurity management framework. Because security practices continually evolve, company security programs and measures must evolve, reflecting new knowledge and technology. Ongoing tracking, measuring and improvements are key to ensuring security.

**SUMMARY AND RECOMMENDATIONS**

Cybersecurity is clearly much more than simply another name for IT security. In fact, it has been elevated by many governments, such as those in the U.S., Canada and Europe, to the level of a top-tier priority for economic and national security. These governments also recognize that cyberspace is woven into the fabric of our societies. In the civilian world, it has been named the “fourth utility,” alongside telecommunications, electricity, and water, and, in the military world, it is a strategic asset to be protected alongside land, sea, air and space.

For businesses and governments alike, getting the cybersecurity posture right across all its elements is vital for future growth, innovation and competitive advantage. There is no single answer for success, but by working across public and private sector partnerships and by advancing security measures, particularly with
regard to mission-critical systems, processes and applications that are connected in cyberspace, businesses will be able to work towards a future environment that is open, secure and prosperous.

Following are recommendations for improving your cybersecurity posture:

- **Establish a logical cybersecurity management framework for enterprise and critical infrastructures:** The challenge is far broader than simply addressing one issue such as securing mobile devices or securing cloud computing environments. An effective cybersecurity management framework addresses all of these interrelated issues, and business leaders can be confident of a comprehensive approach from society to sensor.

- **Revisit plans related to governance, risk and compliance:** Conduct a security assessment and revisit business continuity plans at the corporate level and at the process control network level as a defense against cyber attacks and determine alternate security controls and measures for critical business / production operations.

- **Manage user/device identities and entitlements in a comprehensive, integrated approach:** Centralized identity and access management applications that integrate user system access with user device management are the key to protecting cyber assets in a mobile environment. Be aware that there are no interdependencies between the corporate and process control levels. Develop a strategy for trusted identities that includes identity enablement and strong authentication across multiple platforms that are interoperable and resilient. Take into account the specific requirements for identity, device and access management in process control networks.

- **Take a coordinated approach to sensitive data/intellectual property protection:** Your plan should encompass a broad array of scenarios, including secure document access and delivery, encryption of data at rest and data in motion, data masking, and digital rights management, as well as more recent areas such as cloud computing and the use of social networks where sensitive data can be particularly at risk.

- **Incorporate cybersecurity enhancements as an integral part of application modernization initiatives in critical infrastructure and plant/production designs:** As mission-critical business applications are modernized in areas such as web, cloud and mobile enablement, it is important to review and potentially upgrade their security levels as well. Accordingly, cybersecurity in process control networks should specify end-to-end protection aligned with the corporate initiatives, with respect to the specific security and safety requirements in this critical infrastructure.

- **Re-assess the integrity of your cyber supply value chain:** Build a trusted relationship with suppliers and contractors at all levels in the supply chain and adopt best practices across systems and processes to protect against counterfeits and ensure the integrity of your end-to-end cyber value chain operations. Outsourcing partners, suppliers and contractors must assure and prove (through audits or third-party reviews) that they are at least on the same cybersecurity level in the supply chain.

- **Take advantage of the built-in capabilities of today’s next generation devices to better secure mobile users, devices and applications:** In many cases, biometric techniques via voice, signature or even facial recognition can be used to provide strong, two-factor authentication as opposed to having to invest in expensive add-on hardware.

- **Be aware of the different types of wireless communication:** In computer networking, wireless communication such as WLAN has been used for many years. For close-range wireless communication, technologies such as RFID, Bluetooth or Zigbee are popular choices. Wireless technology is also entering the industrial automation market, with technologies for Wireless HART, Ethernet or PROFIBUS.

**About CGI**

A global business and IT leader, CGI has vast cybersecurity experience, managing cyber risks and attacks within our own data centers, as well as for the clients we serve. We provide end-to-end security services, including the following:

- **Enterprise security management:** Includes the governance, strategies, frameworks, plans and assessments necessary to develop and manage an effective enterprise-wide security program.

- **Security architecting and engineering:** Encompasses the architecture, design, development and deployment of cybersecurity solutions and services that secure your information assets and critical infrastructures.
• **Business continuity**: Ensures that contingency plans and enablers are in place to keep your business running when disaster hits.

• **Managed security services**: Provide reliable protection from viruses, hacker intrusions, internal misuse/abuse, spam and other unwanted Internet traffic to prevent downtime and other productivity losses.

• **Cloud security**: Protects client data in a cloud computing environment.

• **U.S. federal cybersecurity**: Solutions and services that help U.S. federal agencies protect themselves from ever-evolving cyber attacks, including advanced analytics, computer network defense and federal identity management solutions.

• **Industrial control systems cybersecurity**: SECURE-ICS is CGI’s approach and methodology for cybersecurity in industrial control system (ICS) environments. It is based on a risk assessment approach for industrial process automation and control system environments, as well a cybersecurity management framework. The framework is supported by cybersecurity reference guides, baseline standards and policies for plant managers and operators for ensuring proper implementation, monitoring and control.

**REFERENCES**

• United Kingdom, Cyber Security Strategy, 2009.

• *Information Week*, “Securing the Cyber Supply Chain,” 2009.


• Symantec, “Internet Security Threat Report,” 2013

• Ponemon Institute, “Costs of Data Breach Study: Global Analysis,” 2013

