

## Security Incident Handling Service

Security incidents often generate significant negative impact to the Government's brand and reputation, create legal or contractual liabilities, put intellectual property at risk, and expose financial assets to fraud. In order to control the potential risks of security incidents, the CGI Security Operations Center (SOC) reports and centrally manages all security incidents, vulnerabilities and weaknesses on behalf of the client.

Reporting all security incidents, vulnerabilities and weaknesses will ensure that:

- Security incidents, vulnerabilities and weaknesses are reported and managed using a proven procedure, and are executed by experienced resources
- Proactive mitigation measures will be applied on problematic areas
- Statistical data gathering will enable initiatives to monitor and improve the client's security posture

## What is a security incident?

Any event able to jeopardize the confidentiality, integrity or availability of your information is a security incident:

- Unauthorized access, use, disclosure, interference, modification or destruction of data,
- Loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, misrouting of mail, virus outbreak, denial of service, phishing, spam, etc.
- A violation of an explicit or implied information security policy, acceptable use policies, or standard information security practices.

The capabilities of the CGI SOC increase the ability to determine incident impacts and handle the containment, eradication and recovery accordingly. This service expands the capabilities and effectiveness of intrusion detection and log management to quickly identify, respond and prevent future security incidents. CGI does not necessarily have to provide all of the security services for the government entity. For example, an independent feed from IDS/IPS systems and system logs managed by other providers can help CGI become the trusted security advisor and prime security incident manager of many providers in a multi-sourced environment.

## Features

- Centrally managed
- Provides positive central control of security incidents
- Integration with client incident, problem, and change management processes can facilitate better workflow

## Benefits

- Industry standard SANS Institute methodology for security incident handling
- Central statistics regarding security incidents
- Security incident reporting and monthly summaries
- Guaranteed and measured service availability
- Minimal management
- Access to skilled security incident handlers with senior analyst support
- Prime integration point for several security providers in a multi-source environment
- 24x7 coverage through the MSS SOC