CGI

Experience the commitment®

We say this in confidence

Security health check

If it's about security, It matters

A virus alert on a PC registered with the organisation. An email read by someone who shouldn't have seen it in the first place. An unmanned desk with an email left open to view on the computer screen. Company equipment has been stolen. Normal service disrupted due to power failure or disasters such as fire or flood. Someone, not carrying a staff or visitor pass, in your office premises. Employees not following password security policies in the organisation. Any of these incidents constitutes a security breach and must be dealt with promptly. Before your customers begin to see them as a threat.

What's important for organisations is to recognise the risk associated with such a breach and prepare measures to prevent its happening again. To prevent what might seem a one-off incident from becoming a trend and to scale down the impact that it might otherwise have on the organisation.

Security risk assessments must not be delayed in favour of 'business critical' work. For, there is a real threat to an organisation in the form of

undiscovered security exposures. At CGI, we believe that recognising there is a breach or a potential threat is the first step to fixing it. And we're here to help.

What does security mean?

Security is about protecting the confidentiality, integrity and availability of assets (people, premises, property or information). It is protection against attack, theft, disclosure, corruption or non-availability – all potential threats that may be deliberate or accidental. Everyone needs security - across every part of the organisation, regardless of the size of operations.

To ensure the right Sec urity measures are in Place?

It's not just a matter of following rules and regulations. It is also about being aware of the issues, of realising people's responsibilities and applying common sense when protecting business assets.

Who is responsible?

Everyone. Keeping things secure should become part of everyone's job. Directors and managers must lead by example whilst all employees have a role in protecting the viability of the organisation. Every employee needs to know, understand and be responsible for their own security actions. They also need to know who to go for advice or more information.

Let's say security policy, standards, guidance and awareness initiatives are in place. How can directors and senior managers be sure business is robust? You may be working towards ISO 27001compliance or certification and need to know that you are making the right kind of progress. Or you may be looking for an informal review of the security measures and procedures without having to do a formal audit. In either case, security needs to be a frame of mind, a demonstrable behaviour across your organisation.

How can CGI help?

We have developed a 'security health check toolkit' to validate the level of security compliance in an organisation. It is based on the ISO 27000 series of standards. We have a team of security consultants who can be depended upon to manage such projects proficiently.

The toolkit has nine modules that cover security areas such as:

- management and policy
- identification and authentication
- technical auditing
- malicious software controls
- network access controls
- operational procedures
- incident investigation
- personnel procedures
- physical security.

A separate approach, not contained in this toolkit, has been designed for business continuity.

How long will it take?

Typically, it would take a week to ten man days with two specialist consultants. The toolkit has been refined over several years and aligned to the ISO 27000 series. We'll factor in additional scope or details if required.

What you receive is a comprehensive report that has:

- an executive summary
- security status graphics
- evidenced exposures
- a scale of threats
- a summary of recommended actions
- an evaluation of how these actions would mitigate exposures
- a presentation of findings to the Board
- a copy of raw data collected.

This report will enable you direct security spending in the most appropriate areas and can provide confidence to stakeholders that your security is being effectively managed.

The toolkit is both tangible and robust – that's how we've designed it to be. All output is based on a series of data collection and analysis modules ensuring complete and consistent evaluation. We've a track record that shows how well it works.

Why work with CGI?

We'll help you protect your people – whether it's the citizens you need to keep safe or staff and customers – along with your operations and reputation. We'll do so through solutions that build security into your organisation. Just as we have for governments globally and companies in every sector.

CGI

cgi.com

With 68,000 professionals operating in 400 offices in 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. As a demonstration of our commitment, our average client satisfaction score for the past 10 years has measured consistently higher than 9 out of 10.