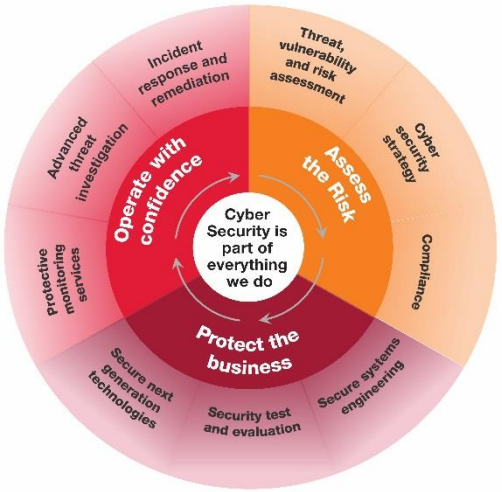
Cyber Security – Organisational Culture Change

Experience the commitment®



Developing a security-positive organisational culture is one of the most cost-effective ways to reduce the risks most likely to impact negatively on information dependent operations.

The culture change process successfully embeds lasting, game-changing, security-positive behaviours into the organisation's DNA. The concept can be used to react positively to security incidents or to fundamental change, such as new regulations, services or contract obligations. It increases the effectiveness of security programmes and reduces the cost of managing risks.

THE CHALLENGE

Organisational culture develops over many years. It is more than the formal structure - many of its most powerful characteristics are informal and undocumented. The behaviours seen within an organisation are the result of multiple drivers. Some are plainly visible and formal, such as process manuals. Others are less visible and are informal, yet still form a huge part of the culture.

The culture change concept seeks to change organisational culture to improve security, not impose a security culture. It can help ensure that security itself is not the problem. For decades, CGI has helped clients embed cyber security into their business operations and facilitate change.

OUR CYBER SECURITY CULTURE CHANGE SERVICE

CGI's culture change service uses a range of tools to find the root causes of security incidents, risks and problems, especially if they are not immediately apparent. Events that can trigger a culture change programme include unexpected or unexplained incidents, ongoing compliance failure, or significant regulatory and legal change. The service can take input from many sources, but, most importantly, it engages directly with the people who are involved.

The process is extremely flexible and can range from a relatively short-term engagement of just a few days, to a wider and deeper analysis. It uses a range of techniques that include root cause analysis, social network analysis and related approaches.

The process delivers a report that provides a description of the current security culture and the various threats and risks associated with it. This is followed by a description of the culture change needed and the prioritised remedial actions which will deliver it.

ORGANISATIONAL CULTURE

"Culture eats strategy for breakfast"

Peter Drucker (November 19, 1909 – November 11, 2005), an Austrian-born American management consultant, educator, and author. He has often been labelled "the founder of modern management".

Culture is "a complex pattern of beliefs, expectations, ideas, values, attitudes and behaviors in an organisation that binds members together and influences what they think about themselves and what they do."

Hellreigle D, Slocum, J., & Woodman, R, "Organizational Behavior" (1998)

It's widely accepted that changing what people do is the most permanent, powerful way of effecting security-positive change and that to achieve this, you need to change the organisational culture. CGI has the approach, skills and expertise to help.

These actions will typically include short-term initiatives to meet immediate high-impact risks and long term actions to evolve cultural maturity. The main recommendations will, however, focus on the measures required to more permanently change the current culture to the target culture, in line with the organisation's overall expectations.

Changing a culture to one that is security-positive means changing perceptions. It is a multi-level, multi-partite, multi-skilled activity that provides a fresh approach, and provides benefits across the organisation.

BENEFITS

The security-positive target culture materially reduces risk. Built-in behavioural change will continue to reduce risk long after it's been embedded. Benefits include:

- **Improved organisational performance.** An effective security-positive culture will have spin-offs such as improved team working, increased employee satisfaction, and higher levels of commitment to the organisation.
- **Increased engagement.** Employees will take real responsibility for security when it is seen and perceived as being taken seriously.
- **Reduced risk and vulnerability.** Improved protection to mitigate the frequency and impact of security breaches and incidents.
- **Reduction in loss or theft of information.** Employees will be more likely to report suspicious activity, personal errors and 'near-misses'.
- **Reduced risk of reputational and subsequent financial damage.** The chances of damage to the reputation of the organisation will be reduced.
- **Low-cost interventions.** Security culture change is relatively low-cost.
- **Reduced cyber security skills gap.** Co-opting the skills and capability of the organisation's people can help reduce over-dependency on scarce, expensive, cyber security specialists and technology.

WHY CGI?

For over 40 years, CGI has helped secure government and commercial clients and delivered some of the most complex technology projects and services. We have received many accolades for our work and have supported our clients to achieve a 100% success rate when undertaking ISO 27001 accreditation, which is reliant upon the right culture being in place.

The security culture change service builds on this solid background - amplifying and enhancing our technology and security management solutions. We have dedicated UK cyber security consultants advising a wide range of clients across UK public and private sectors – part of a nearly 2,000 consultant-strong global cyber security team who bring shared expertise, research, knowledge, capabilities and solutions to our client projects.

ABOUT CGI

With over 68,000 professionals 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.

CGI has a global team of cyber security experts, who work with governments and commercial clients, ensuring their business critical systems and services are effective and secure.

CGI is one of the few providers worldwide with accredited security certification facilities - located in the UK, Canada and the U.S. Our Security Operations Centres continuously identify and deploy the best solutions to maintain a state-of the-art infrastructure, handling over 74 million cyber events a day.

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.

For more information about CGI, visit: www.cgi-group.co.uk/cyber or email us at cyber@cgi.com.

For more information about CGI, visit www.cgi.com

or email us at info@cgi.com.