CGI

Experience the commitment®

IT Security Governance

A holistic approach

Understanding IT security governance

Why do we need it? Won’t technology be enough?

INTRODUCTION

The threat to technology-based information assets is higher now than it has been in the past. As technology has advanced, so too have the tools and methods employed by those who seek to gain unauthorized access to data, or disrupt business processes.

Attacks on any organization are inevitable. But the sophistication and persistence of those attacks depend on the attractiveness of that organization as a target—primarily its role and assets. Today, threats originating from misguided individuals have been replaced by highly skilled international organized crime groups or foreign nation-states that have the skills, personnel and tools to conduct sophisticated covert cyberespionage attacks.

Those attacks are not strictly focused on government entities; instead, there have been numerous incidents in recent years where large corporations have also been penetrated, and their data covertly accessed over a period of years without their knowledge.

In fact, enhanced cybersecurity emerged as a top IT priority across industries during the annual, in-person, in-depth client interviews that CGI conducted in 2015*. So while businesses in certain industries, such as aerospace and strategic resources, may be prime targets for nation-state cyberespionage, others dealing with largescale financial and credit card assets are equally attractive to international criminal groups.

Today’s threat actors do not rely solely on defeating technical safeguards. Instead, they probe and exploit a range of weaknesses found in the target environment. In our experience, these weaknesses are not due to technology alone, but also due to failures in procedural safeguards or gaps in vulnerability management practices. The best technology in the world, when poorly applied or misemployed, does not provide a substantive defense against such threats.

*In 2015, CGI held 965 in-person client interviews across 10 industries and 17 countries as part of its Voice of Our Clients program.

> “Companies spend millions of dollars on firewalls, encryption and secure access devices, and it’s money wasted, because none of these measures address the weakest link in the security chain.” [people]
>
> – *Kevin Mitnick*
>
> Convicted in the USA for hacking major corporations, and now a world recognized security advisor.

RELIANCE ON SECURITY TECHNOLOGY ALONE

We live in a world driven by technology. It is not uncommon for companies to first turn to technical security solutions without addressing how those solutions are going to be implemented, maintained and managed on a day-to-day basis.

Too often we see organizations implement technical security safeguards, such as firewalls or intrusion detection, but fail to implement proper **security policies or procedures**. As a result **weak practices persist that undermine security and expose assets to significant risk**.

The following are just a few examples of such practices:

- **Non-existent security policies** or procedures
- **Outdated and/or ignored security policies**, where they do exist
- **Poor awareness of security practices** at all levels
- **Lack of effective network zoning**, or compliance thereof
- **Inadequate hardening** and patching
- **Poor access control practices** such as uncontrolled group passwords, shared accounts, proliferated "god" privileges, shared root access, absence of an authorization process (except at a low operational level)
- **Lack of security compliance audits** and reviews
- **Absence of an authority figure for decisions** affecting the security and integrity of infrastructure and information assets

The end result is an enterprise that feels secure because it has invested in security solutions, but has so many inherent vulnerabilities that little meaningful security protection is achieved. In this case, a **dangerous sense of false confidence** exists, but the organization remains extremely vulnerable to attack, with intruders exploiting those weak practices to circumvent technical security solutions and gain control of systems. This is not theoretical—**it is a common scenario** that has been observed as a root cause in many well publicized and successful attacks on major corporations and government agencies

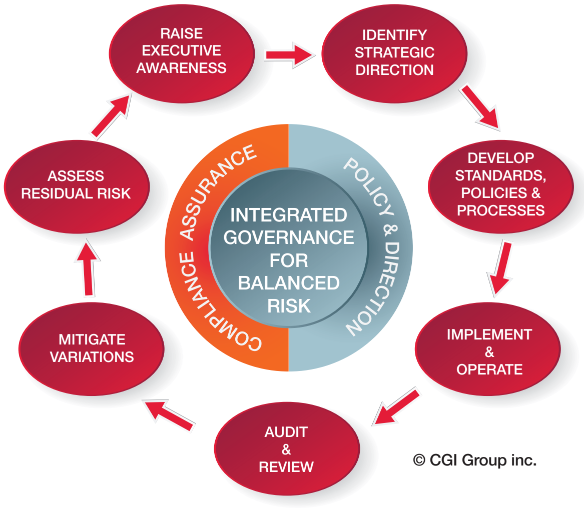
THE ROLE OF IT SECURITY GOVERNANCE

Security governance is the glue that binds together all the core elements of cyber defense and effective risk management. Without it, dangers persist and the resulting compromise of assets is inevitable. Moreover, senior leadership is unaware of their organization's risk exposure, for which they will ultimately be held accountable.

Security cannot exist in a vacuum and must be part of a larger risk management strategy, driven by the organization's business goals, objectives and values. Organizations must be aware of their risk tolerance threshold, or "level of acceptable risk." This threshold may vary by asset grouping. For example, an organization may tolerate a certain amount of risk when the impact is considered low, but may be very risk averse regarding anything that might adversely impact its reputation.

Governance is the mechanism by which those risk-related values are reflected in direction and judgment that shape business plans, information architecture, security policies and procedures, as well as operational practices. However, providing direction without having any means to ensure that it is followed is meaningless.

Thus, **compliance is the critical feedback loop in security governance**. It ensures that everyone is working according to plan, as a team, to deliver business activities and ensure the protection of assets within the context of risk management and security strategy and direction. Where that is not possible, it ensures that variances that result in risk exposures are made known at the leadership level, so that they can either decide to accept these risks, or provide mitigating direction and the resources necessary to address them.


RAISE EXECUTIVE AWARENESS
IDENTIFY STRATEGIC DIRECTION
DEVELOP STANDARDS, POLICIES & PROCESSES
IMPLEMENT & OPERATE
AUDIT & REVIEW
MITIGATE VARIATIONS
ASSESS RESIDUAL RISK
COMPLIANCE ASSURANCE
POLICY & DIRECTION
INTEGRATED GOVERNANCE FOR BALANCED RISK

© CGI Group inc.

> “If you think technology [alone] can solve your security problems, then you don’t understand the problems and you don’t understand the technology.”
>
> – *Bruce Schneier*
>
> Industry recognized cryptographer, computer security and privacy specialist, Fellow at the Berkman Center for Internet & Society at Harvard Law School, Program Fellow at the New America Foundation’s Open Technology Institute and the CTO of Resilient Systems.

EXECUTIVE RESPONSIBILITY FOR IT SECURITY GOVERNANCE

In the past, security was often left to managers and administrators at the technical and operational levels. However, as both technology and the nature of threats have increased in scale and complexity, **the ultimate responsibility for protecting an organization’s mission and assets is now being been laid at the doorstep of senior management**.

A key example is the massive security breach in 2013 of a major multi-national corporation that was estimated to involve the compromise of tens of millions of credit card accounts and customers’ personal data, which led to the resignation of the Chief Information Officer and, ultimately, the Chief Executive Officer. According to industry sources, over US$60 million was spent in mitigation measures in the aftermath of that breach. Based on the hard lessons and massive loss experienced in that incident, subsequent mitigation actions were put in place and this company now has what many analysts feel is a model security program that includes accountability and visibility at all levels.

It is interesting to note a potential divide in the perspectives of CEOs and line managers. From CGI’s Voice of Our Clients interviews in 2015, as compared to line managers who were interviewed, CEOs said the impact of data protection was less, the completeness of their cyber programs was greater and the spend on cybersecurity was lower.

While we have seen senior management in organizations insist on the creation of security policies and procedures in response to the industry recognition of increased threat and the importance of security best practices, we have also seen instances where adequate policies and procedures exist, but have not been implemented consistently (or at all) at the operational level.

The end result is that senior leaders are confident that their responsibility for diligence has been satisfied and that risks are being managed effectively. Yet the reverse is often true, and **they are unaware that their organization remains extremely vulnerable through endemic failures in the governance process**. Ultimately, critical risks persist—where senior management may have been uninformed, but is still held accountable. This false sense of security is extremely dangerous for an organization and results in an uncontrolled state of risk and liability.

THE ANSWER — VISIBILITY, ACCOUNTABILITY AND COMPLIANCE MANAGEMENT

To meet modern security challenges, organizations must consistently **apply effective risk management practices at all levels**. Risks must be made visible to senior management. These executives must play a key role in either accepting those risks or directing activities and enabling resources to mitigate them to acceptable levels from a business, legal, legislative and regulatory standpoint. To do that, **senior management must have visibility regarding responsibility and accountability in each instance**.

Accountability and responsibility must be assigned to all persons involved in risk management and the delivery and operation of an information environment that is resilient, aware and provides adequate confidentiality, integrity and availability. To that end, an overarching corporate security strategy or policy should include an RACI table[1], which does exactly that. This RACI table should be a key part of compliance audits and reviews.

COMPLIANCE AUDIT & REVIEW — YOUR SAFETY NET

Compliance audits and reviews are “the secret ingredients” that ensure that security policies and processes are being consistently followed, according to a corporate risk management or security strategy. It is also an integral element of all operational management schemes, including ISO 27001, COBIT, Sarbanes Oxley and ITIL®. **Without a compliance assurance process, it is impossible to ensure that risks are being managed as planned,** or identify and correct any problems when this is not the case.

Compliance assurance audits and reviews provide a barometer on the functioning of security governance, and give senior management visibility into areas where risk exposure exists and adjustments need to be made. Moreover, unless there is an understanding that actions, decisions and results will be audited according to established controls and standards, there is little incentive to ensure compliance, resulting in “compliance drift.” Over a period of time, variance will grow, as will any resulting risks.

Although operational managers often see audits and reviews as being intrusive and even punitive, this view should not be allowed to prevail. Audits and reviews are the manager’s opportunity to highlight areas where controls and standards are not being met for a variety of reasons beyond their control, such as a lack of resources, technology, prioritization, or funding. **Audits and reviews are the essential mechanisms by which challenges at the operational level can be made known to senior management** so that they can be resolved.

Typically, there are three types of compliance assurance activities:

- **Internal compliance reviews**: These are conducted at the operational management level as a means of identifying problems early and implementing corrective measures that are within the scope of operational level resources. Evaluations such as vulnerability analysis and penetration testing should be included in compliance reviews on a regular basis. Testing and accreditation services should also be considered. In the same way that compliance with ISO 9000 standards was used as an external kick start for quality governance, we believe that this should be the approach for security governance as well.

[1] **Responsible, Accountable, Consulted, Informed**. A matrix approach to mapping roles and responsibilities. Consistent with ITIL v3 and ISO 27001-2013

- **Internal audits**: Performed by independent internal personnel, internal audits are designed to provide a compliance status check to senior management, prepare for external audits, or to apply focus on areas where persistent problems are believed to exist. Internal audits should not be performed by the same group that is responsible for achieving compliance.
- **External audits**: These are conducted for certification purposes, or when there is a particularly critical problem area that requires an independent "outside" view. As a part of this activity, it is important to work closely with international security associations and standards bodies.

> Critical and persistent problems identified in internal reviews should be made known to an Executive Risk Review Board (ERRB), consisting of key senior stakeholders (e.g., C-suite officers), so that they are aware of any associated risks and can also consider the allocation of mitigating resources.
>
> Reports from both internal and external audits should always be presented to the ERRB for the same reasons.
>
> In all cases, the ERRB should require that a risk mitigation plan be provided and resources allocated accordingly.

10 MEASURES FOR GOOD IT SECURITY GOVERNANCE

Create governance

1. Governance must be top down from the board level, through the C suite.
2. Develop and implement a risk management approach and an overarching corporate security policy that is aligned to business requirements and processes.
3. Establish, or incorporate into the current risk structure, an IT Security Executive Risk Review Board (ERRB) as defined in your overall risk management strategy.
4. Appoint a corporate IT security authority, preferably with a different reporting chain than those responsible for IT operations. Clearly identify roles and responsibilities.
5. Establish an internal audit and review authority with direct lines of communication to the ERRB.
6. Establish and implement an audit and review compliance framework, ensuring that its goals and objectives are known throughout the organization.

Deliver governance

7. In conjunction with the lines of business, identify the assets and critical information and the threat and associated risk.
8. Develop and implement a series of security controls and associated procedures, with responsibility and accountability as defined in the RACI model for risk management.
9. Create, deploy and ensure participation in a mandatory security awareness program, so that personnel understand their responsibilities, and what the risk management and security controls are intended to achieve, and why.

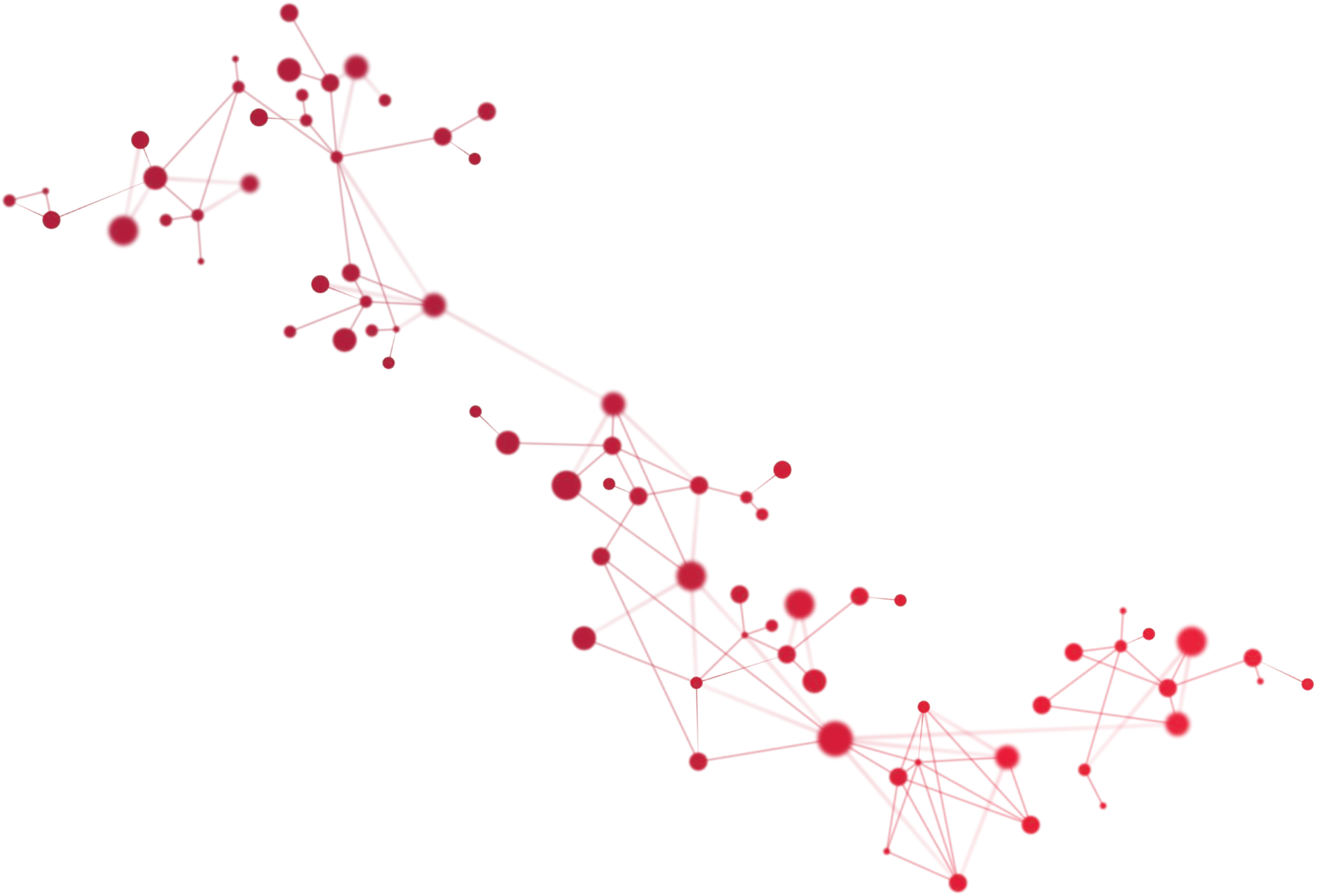
Review on an ongoing basis

10. Review all elements of the program on a regular basis to make adjustments as necessary to ensure that risks are being effectively managed in a balanced manner that accommodates business needs.

CONCLUSION

Adequate security and governance of information assets can no longer be achieved on an ad hoc basis in large modern organizations, nor can it be achieved by deploying technical solutions alone. Instead, organizations need a more holistic approach, applying **effective risk management and good governance throughout the organization, with the key values of visibility, accountability and responsibility** exercised at all levels. However, not every organization can make this transition without any assistance, and CGI has worked with several businesses to help them evolve an adequate IT security governance process.

Senior management has a critical part to play in making risk-based decisions, issuing direction and ensuring that adequate resources are available to execute that direction. This is only possible if **senior management is engaged and informed through a robust compliance and reporting process**—with external support where required. If the measures outlined in this paper are undertaken, an organization will be better prepared to manage risks as they arise and achieve the security resilience required to meet today's threats.



Founded in 1976, CGI is one of the largest IT and business process services providers in the world. We combine innovative services and solutions with a disciplined delivery approach that has resulted in an industry-leading track record of delivering 95% of projects on time and within budget. Our global reach, combined with our proximity model of serving clients from 400 locations worldwide, provides the scale and immediacy required to rapidly respond to client needs. Our business consulting, systems integration and managed services help clients leverage current investments while adopting technology and business strategies that achieve top and bottom line results. As a demonstration of our commitment, our client satisfaction score consistently measures 9 out of 10.

Visit cgi.com for more information