Cyber Security – An Issue Of National Importance

Protect your business from cybercrime and data breaches

Cyber Security and US legislation

> "Cyber threat is one of the most serious economic and national security challenges we face as a nation... America's economic prosperity in the 21st century will depend on cybersecurity."
>
> President Obama's speech on Cyber Security, 29 May 2009

In today's information economy, the protection of information assets (information security) is a key element in the long-term competitiveness and survival of commercial organizations. In an environment where the survival of individual organizations is at least partially dependent on the security of critical national infrastructure, all organizations must contribute to improved cyber security. With the Internet becoming a ubiquitous communication and application platform, the greatest risk to your business is likely to be cyber crime.

In May 2011, the US Government has proposed a legislative package focused on improving cyber security for the American people, the Nation's critical infrastructure, and the Federal Government's own networks and computers.

This document recognizes that the cyber security vulnerabilities in the US Government and critical infrastructure are a risk to national security, public safety, and economic prosperity.

A fact sheet on the legislative package states that more transparency will be required from critical-infrastructure operators and they will be accountable for their cyber security. Moreover, the cyber security risk mitigation plans of each critical-infrastructure operator will be assessed by a third-party, commercial auditor.

The legislation will help consumers protect themselves against identity theft, whilst also motivating businesses to adopt better cyber security measures. Consumers who are affected by a data breach will have to be informed about the leak by the company that suffered the intrusion. In the view of the US government, the proposed changes will "(1) improve our resilience to cyber incidents and (2) reduce the cyber threat".

If accepted, the legislative package will create the need for many organizations to review their cyber security strategy (if they have one in place), or they will have to start implementing one.

Refer to the 5 essential steps for implementing an effective security strategy.

Document Control
Version: 1.0

Data Breaches and Data Protection

> "The many recent and troubling data breaches in the private sector and in our government are clear evidence that developing a comprehensive national strategy to protect data privacy and security is one of the most challenging and important issues facing our country"
>
> From a Statement Of Senator Patrick Leahy, 07 June 2011

In June 2011 the Senate introduced a federal Bill known as the Personal Data Privacy and Security Act. The Bill if enacted (and, sooner or later, something like it will be), will impose strict data security measures. US-based companies would be required to report data breaches that threaten consumer privacy and could face stiff penalties for concealing them. Companies should familiarize themselves with the relevant state breach laws and take immediate action to protect themselves from cyber attacks.

The number of cyber attacks in 2011 increased drastically in the US:

- In June, the **US Senate** website was hacked. The Senate had become a victim of a high profile cyber attack by the hacker group called Lulz Security, which was allegedly behind the attack on Sony Pictures. Internal data of the website was taken and published on the attacker's website.

- Also in June, **Sony Pictures** website was attacked - more than one million passwords, email addresses and other information of Sony users were compromised.

- Around 200,000 account holders in North America had their names, account numbers and email addresses stolen by hackers who broke into **Citi bank's** online account site in June.

- **The International Monetary Fund (IMF)** was also a victim of the high profile hacking attempts on major corporations and institutions in June.

- In June, hackers breached the **Nintendo** US server's in a cyber attack.

- In May, **Lockheed Martin**, USA's largest defense contractor, admitted it has been attacked. Hackers reportedly exploited Lockheed's VPN access system, which allows employees to log in remotely by using their RSA SecurID hardware tokens. Attackers are likely to have possessed the factory-encoded random keys used by some of Lockheed's SecurID hardware fobs, as well as serial numbers and the underlying algorithm used to secure the devices.

- In April, the **Sony Playstation** network was hacked. The attackers managed to access users' personal details including passwords and credit card numbers. It is reported that account holder's profile data, including purchase history and billing address, and their PlayStation Network password security answers may have also been obtained."

Document Control
Version: 1.0

Cyber Security – An Issue Of National Importance

Protect your business from cybercrime and data breaches

Class Action Lawsuits - The Stakes Are High

[How to Survive a Data Breach](#) This handy pocket guide tells you what you need to do to prepare for a data breach. It explains the key measures you need to take to handle the situation and to minimise the damage. The information is drawn from various regulatory publications and interviews with security experts, lawyers and software suppliers.

Customers whose data has been exposed can bring class action lawsuits in Federal Court for negligence against an organization that has been hacked. Although costs are usually covered by insurance, lawsuits are still very expensive and time consuming. Moreover, the brand damage is irreparable, and the process consumes huge amounts of time for executive management.

It took just nine days for a class action lawsuit to be filed against Sony by users of the Playstation® Network, whose sensitive information Sony failed to protect when its network was hacked in April 2011.

"The failure of a major company to implement security controls and a later breach seem to lead directly to a class action case. The lesson learned here is that it is better to implement the security remediation before the breach, rather than paying remediation costs – and incident response costs and fees and costs to defend the inevitable expensive class action suit—after a breach.", comments Stephen Wu, Partner at Cooke Kobrick & Wu LLP, in his post on [RSA Conference website](#) .

Class action lawsuits can affect company employees directly, as they can be raised against the officers of the company. Bob Uda explains the risks in his post on the [ICTTF website](#).

"One of the major legal risks arising from cyber security breaches is the possibility of derivative suits against corporate officers and directors alleging that they have breached their duty of care by failing adequately to protect against security breaches. Directors and officers have a fiduciary obligation to use reasonable care in overseeing the business operations of the company, under the doctrine of corporate duty of care. See, e.g., In re Logue Mechanical Contracting Corp., 106 B.R. 436, 439 (Bankr. W.D. Pa. 1989). Traditionally, directors and officers could defend against a duty of care claim by showing that they acted with reasonable care by relying on information reasonably available to them. In the past few years, however, courts have expanded this reasonable care standard to create a duty of oversight requiring directors and officers to act affirmatively to assure that adequate information and compliance systems are in place (Matus, Polak, Mancini, & Nonna, 2002)."

Many things can go wrong also for companies that fail to comply with the payment card industry's data security standards (PCI) when accepting and processing credit card data. [This document](#) provides a few scenarios which every organisation should try to avoid. In summary, organisations are liable if they:

- allow customers' data to be stolen as a result of a cyber attack;
- an employee sends inadvertently an email containing customer's personal information;
- fail to timely notify their client(s) of the loss of their data.

Document Control
Version: 1.0

Cyber Security – An Issue Of National Importance

Protect your business from cybercrime and data breaches

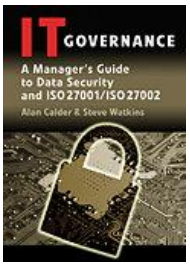
ISO27001 – The International Cyber Security Standard

Cyber security standards are an important element in building a strong, resilient information and communications infrastructure.

ISO/IEC 27001 is the world's only internationally-recognized cyber security management system standard against which an entity's information security management system (ISMS) can be independently audited and certified. Compliance to ISO27001 is the basis for meeting all other information security-related regulatory compliance requirements, such as:

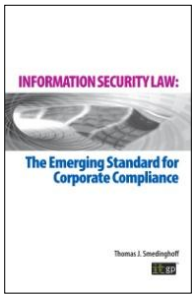
- FISMA,
- GLBA,
- HIPAA,
- PIPEDA, etc.

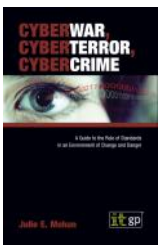
ISO27001 is also closely allied with the Code of Practice ISO/IEC 27002 (formerly ISO/IEC17799). Implementing ISO/IEC 27001 and creating an effective information security management system for the first time can be challenging.



The IT Governance: A Manager's Guide to Data Security and ISO 27001/ISO 27002, Fourth Edition covers all aspects of data protection and information security are covered including viruses, hackers, online fraud, privacy regulations, computer misuse, investigatory powers, etc. This manual - which is also the (UK's) Open University's post-graduate information security textbook - provides clear, unique guidance for both technical and non-technical managers. It details how to design, implement and deliver an ISMS that complies with ISO27001.

Information Security Law: The Emerging Standard for Corporate Compliance is a book that takes a high level view of the multitude of security laws and regulations, and summarizes the global legal framework for information security that emerges from them. It is written for companies struggling to comply with several information security laws in multiple jurisdictions, as well as for companies that want to better understand their obligations under a single law. It explains the common approach of most security laws, and seeks to help businesses understand the issues that they need to address to become generally legally compliant.





Another book, CyberWar, CyberTerror, CyberCrime, gives a stark and timely analysis of the hostile online landscape that today's corporate systems inhabit, providing CIOs and IT professionals with a practical introduction to the defensive strategies that they can employ in response. This is a straightforward and no-nonsense guide to using best practices and standards, such as ISO 27001, to instil a culture of information security awareness within an organization.

Document Control
Version: 1.0

ISO27001 Certification – The Benefits

Standalone ISO27001 ISMS Documentation Toolkit will save you months of work, help you avoid costly trial-and-error dead-ends, and ensure everything is covered to the current ISO/IEC27001 Standard.

Accredited Certification to ISO27001 gives an organisation internationally recognised and accepted proof that its system for managing information security - its ISMS or cyber security readiness - is of an acceptable, independently audited and verified standard. Accredited certification enables an organization in the US to demonstrate to a potential client elsewhere in the US, or anywhere else in the world that its approach to selecting information security controls and its overall information security procedures are in line with internationally recognised best-practice.

Cyber Resilience – Standards

The idea of resilience - that an organization's systems and processes should be resilient against outside attack or natural disaster - is a key principle underpinning ISO27001. Business continuity planning is fundamental to an effective ISMS.

There are three core standards for business resilience – two of them are American and one British. The three standards which have been adopted by the US Department of Homeland Security, for the Voluntary Private Sector Preparedness Accreditation and Certification Program (PS-Prep), are:

- ASIS SPC.1-2009 Organizational Resilience: Security Preparedness, and Continuity Management Systems – available from the American Society for Industrial Security
- National Fire Protection Association 1600:2007 Standard on Disaster/Emergency Management and Business Continuity Programs – available from the National Fire Protection Association
- British Standard 25999-2:2007 Business Continuity Management – available from our online store. BS25999 provides a set of best practice for business continuity management. It details how to go about designing, implementing and maintaining business continuity management system (BCMS).

Five-Step Cyber Security Strategy

There are five key actions that should form part of an effective cyber security strategy for any organization:

1. Secure the cyber perimeter: test all your internet-facing applications and network connections to ensure that they all known vulnerabilities are identified and patched. This should include testing all wireless networks. Once this exercise – penetration testing, remediation and confirmation re-testing – has been completed, schedule regular network tests. Depending on the level of risk, these should take place either quarterly or, at least, every six months. Perimeter security also includes ensuring that security in the inward and outward bound communications channels – email, instant messaging, Live Chat and so on – are also secure, with appropriate arrangements for data archiving and an appropriate balance between protecting confidentiality, integrity and availability.

2. Secure mobile devices beyond the perimeter: encrypt and secure access to all portable and mobile devices – laptops, mobile phones, Blackberries, USB sticks etc – to ensure that the increasingly elastic network perimeter remains secure and that data taken beyond the perimeter remains secure.

3. Secure the internal network: identify risks and control against intrusions from rogue wireless access points, from unauthorised USB sticks and from mobile data storage devices – including mobile phones, iPods and so on.

4. Train staff: attackers understand that employees are the weakest link in the security chain and take advantage of natural human weaknesses through a style of attack known as social engineering. Staff must therefore be trained to recognize and respond appropriately to social engineering attacks that range from tailgating through to phishing and pharming. Also ensure that you have a well-thought through social media strategy that minimises information loss through social media websites such as Facebook, LinkedIn and Twitter.

5. Adopt ISO/IEC 27001 and BS25999 as standards for developing and implementing comprehensive cyber security and business resilience management systems.

Document Control
Version: 1.0

Cyber Security – An Issue Of National Importance

Protect your business from cybercrime and data breaches

Effective Cyber Security Tips

Be aware what you share.

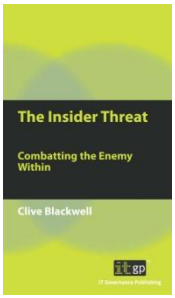
Many social media attacks and email spam campaigns are successful because they create the illusion that the target knows and should trust the attacker. Dealing effectively with social media requires a joined-up approach that is aligned with the objectives and risk appetite of the business - a governance approach.

The Solution: Social Media Governance Toolkit

The ITG Social Media Governance Toolkit contains a comprehensive suite of documents and templates that will help you develop, implement, monitor and improve social media activities across your organization.

Understand the threat from insiders.

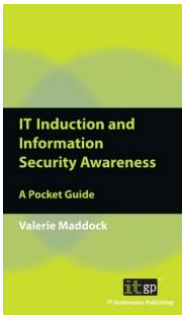
Ensure that your IT systems cannot be manipulated for purposes of insider fraud. With the right strategy in place, you can restrict the opportunities open to disgruntled employees to disrupt your business operations through your IT system**.**



The Solution: The Insider Treat: A Pocket Guide.

This new pocket guide intends to shed light on the key security issues facing organizations from insiders to get them up to speed quickly.

Develop an IT induction programme for your staff that can help safeguard your business information .



If you want to tackle the problem of information security, you cannot rely on the help of technology alone. Information security breaches tend to occur as a result of human, as well as technological, failings. However, the human factor usually receives far less attention.

The Solution: IT Induction and Information Security Awareness.

This pocket guide teaches you how to strike the right balance in your approach to staff training, thereby enabling you to provide your employees with an IT Induction that is at once informative and accessible.

Document Control
Version: 1.0

Cyber Security – An Issue Of National Importance

Protect your business from cybercrime and data breaches

Train your staff.

Whether you are implementing an ISMS or need to deal with payment card risk, you can't do this effectively without the support of your staff. E-learning is a proven technique in educating staff in fundamental information security principles.

The Solution: Information Security Awareness e-Learning Course

This online e-learning program (developed, produced and hosted by the IT Governance e-Learning team) helps organizations impart basic training on information security, and create awareness in the organization around email, internet and related policies. The course covers all the fundamentals of information security.

Assess the confidentiality, integrity and availability of your organization's information assets

Risk assessment is the core competence of information security management. Every control ('control' = 'risk countermeasure') decision you make must be proportionate to the actual risk your organization faces. You must therefore assess risks on a structured asset-by-asset basis - and experience proves you need to save time and money with a risk assessment tool that automates and simplifies this process.

The Solution: vsRisk - ISO 27001: 2005 Compliant Information Security Risk Assessment Tool

vsRisk™ has been designed with the user in mind and for the first time empowers the user to comply with the requirements of ISO 27001:2005 and to effectively identify, analyse and control their actual information risks in line with their business objectives.

Contact IT Governance:

By phone (toll free): +1 877 317 3454
By email: servicecenter@itgovernanceusa.com

www.itgovernanceusa.com

Document Control
Version: 1.0