To The Point
Information Security: Managing the Risk

What is Your Information Security Risk?

The answer most likely is greater and deeper than you may realize. Information is the life blood of today's business. Loss or damage to information assets such as confidential electronic databases, back-up tapes, computer operating systems, or data reliant software applications can significantly impact a business' reputation and performance. The direct and indirect costs can be far reaching as seen in recent, well-publicized industry and governmental security breaches.

Modern business models rely on "always on" broadband access to the global Internet. Additionally, modern companies engage in ever-expanding network boundaries that connect wirelessly and are integrated to business partners, vendors, and customers, creating a dependent and often virtualized, cloud-driven environment.

Risk management is often focused on more traditional issues such as property protection and worker safety. However, in today's technology driven world, information security is equally important. Security breaches are too easy to incur and may result in financial loss, damaged brand reputation, and regulatory actions.

The goal with information security is to protect your data assets from a wide range of threats in order to ensure business continuity, minimize business damage, and maximize return on investment and business opportunities. Information security has also become a legal requirement, mandated by federal and state legislation.

A Holistic Approach

When addressing information security, a holistic approach is needed. Safeguarding the lifeblood of your business requires adherence to the guiding principles of information security known as "CIA":

Confidentiality–Ensuring that information is accessible only to authorized users

Integrity–Safeguarding the accuracy and completeness of information and processing methods

Availability–Ensuring that authorized users have access to information and associated assets when required

Chubb Risk Consulting

To adequately address your information security exposure, identify your business information assets, understand the security threats and vulnerabilities posed by the assets from a CIA perspective, and then implement a risk management approach that balances countermeasures against your information security needs.

Brand Reputation

When assessing information security, look both internally and externally. How will the business community, your customers, and your shareholders react if you have an information security breach? If you were accused of a significant data breach, could you prove that you took "reasonable" measures to mitigate the breach from occurring, given your business risk profile? While all companies should employ basic controls such as firewalls, anti-virus software, and password protected access, there are other levels of risk management that need to be evaluated based on CIA.

What Can you Do?

To properly protect your information confidentiality, integrity, and availability, it is vital to adopt a structured and systematic approach. This includes understanding the avenues by which a "loss" could arise and the protections needed to safeguard your assets. As defined by ISO 27001, this methodology is termed an Information Security Management System (ISMS). Information security is not just about protecting networks. It also includes protection of data, wherever it resides (laptops, PDA, backup tapes, etc.), employee adherence to policies and procedures, and physical protection of the facility.

Implementing a structured ISMS embeds information security throughout the organization. The implementation of an ISMS must be appropriate to your company's size and business activities. For example, a company that deals with hosted patient medical records generally has a greater business risk and therefore would require a more comprehensive ISMS than a brick-and-mortar retailer with a small web-based sales portal. Ultimately, only you can decide what business assets, threats, and vulnerabilities constitute appropriate levels of control for your organization.

Elements of an ISMS require:

- Detailed assessment of information security threats including identifying the value of critical data and where it is located.
- Development and implementation of Information Security policy, procedures, and protections relative to the level of risk arising from the critical data identified.
- Vigilance in taking a holistic approach to Information Security rather than concentrating solely on technology. In addition to technology-specific countermeasures, an ISMS should also cover:
  - Confidentiality and privacy
  - Policy documentation and implementation
  - Human resources and premises security
  - Outsourcing (cloud, third party vendors, business partners, etc.)
- Development of objectives with achievable and measurable outcomes to facilitate benchmarking of the results to allow future comparisons to be undertaken.

Detailed guidance on the structure, content, and practical implementation of an ISMS can be found in the ISO27001:2005 ISMS – Requirements and 27002:2005 Code of Practice for Information Security Management, as well as other valid models.

Information Technology versus Information Security

Most information security strategies focus only IT resources on the information security issues. When this happens, the overall point may be missed. While technological controls play a crucial role, information security is more about understanding the overall business processes, such as "What is at risk for my organization, my partners and ultimately my customers?", "How is my company internally mitigating that risk at all levels of the organization?", and "How is my company mitigating the risk associated with customers and external business partners?"

Information Security Culture

Most security experts agree that promoting a culture of security across the organization is universal and paramount for an ISMS to be successful. While this can be challenging, given the diversity of your workforce, vendors, contractors, and partners, security culture must be understood and implemented by all.

An information security culture doesn't just begin and end with a policy statement. It takes training and education, as well as the commitment to invest in the appropriate level of technology. In addition, you need to ensure that your defenses are working by implementing the necessary patches and routinely addressing the vulnerabilities of network perimeter and cloud-based systems in order to protect confidential databases and other assets residing within your in-house and hosted networks.

Summary

Safeguarding the lifeblood of your business is absolutely essential for the success of your business. It is an ongoing process that requires continuous threat reassessment, proper hardware and software tools, and employees who understand the importance of information security. An ISMS program based on safeguarding CIA is the primary risk management tool available to minimize the chance of information security-related losses.

Resources

Information Security Management System
www.iso.org/isoiec-27001-information-security.html

Test your information security risk management. Answer these sample questions to find out if you may have a weakness in your information security efforts.

Information Security Checklist	Yes	No
Confidentiality and Privacy		
Is your organization operating in full compliance with current Payment Card Industry (PCI) standards for operations that collect and store sensitive credit card data?	□	□
Does your organization have a "sensitive data" policy in place with appropriate access/authentication ontrols, data backup, redundancy and encryption of sensitive information/personally identifiable information (PII)?	□	□
Has your organization identified and regularly updated its knowledge of all statutory, regulatory and contractual requirements applicable to their operations and activities?	□	□
Policy Documentation and Implementation		
Does your organization have in place a documented information security policy which is supported to by management, communicated to employees and regularly reviewed?	□	□
Have information/data-specific asset values been established along with associated inter-dependencies to establish overall business impact values?	□	□
Has there been a formal assessment of threats that includes both deliberate and accidental threats, insider attack and past incidents?	□	□
Does your organization have a documented and enforced "Acceptable Use Policy" for employees?	□	□
Human Resources and Premises Security		
Have individual roles and responsibilities for information security within your organization been clearly defined and documented?	□	□
Does staff undertake regular awareness training including: current threats, social engineering, phishing, posting blogs, clear screen/desk policies, hard passwords, "Peer to Peer" (P2P) sites, wireless, detachable drives and/or mistakes?	□	□
Does premises security include target hardening with layered security combining physical protections, active access control and intruder detection with appropriate alarm response?	□	□
Is premises security planned on the basis of collaboration between those responsible for facilities security and IS?	□	□
Is there operating redundancy including: uninterruptible power supplies where appropriate to allow smooth power transition or controlled shut down, back up generator and redundant HVAC providing operational IT continuity and/or redundant avenues of telecom connectivity (multiple carriers and cable feeds)?	□	□
Outsourcing		
Has the risk of unauthorized modification or misuse of data or damage to the IT system by third parties (either deliberately or accidentally) been assessed and documented prior to any activities commencing?	□	□
Has there been formal evaluation of vendor security controls including policy, procedures and technological countermeasures with particular attention being paid to privacy and confidentiality controls such as vendor staff training and web-based threats via hosted cloud vendor business models?	□	□
Is the scope of any product or service deliverables to be undertaken by third parties fully understood, agreed and documented in order to ensure only authorized activities are undertaken?	□	□
Has a formal exit strategy has been developed in respect of both normal and extraordinary termination of vendor contracts?	□	□
Have contingency plans been drawn up and documented that include vendor data controller agreements specifying information security responsibilities and the return or destruction of information, software and equipment?	□	□

Information Security Checklist	Yes	No
Technology		
Are data backup arrangements consistent across the enterprise and proactively tested?	□	□
Are a combination of technology solutions and procedural controls deployed in order to detect accidental or deliberate addition, deletion or alteration of critical data records?	□	□
Are passwords a minimum of eight alpha numeric characters and required to be changed every 60 days with no re-use permitted within 24 cycles?	□	□
Are firewalls and anti-virus detection installed on all mobile computing equipment (including endpoint security technologies)? Are these programs/applications regularly updated?	□	□
Is data on hard disks encrypted in order to prevent unauthorized access/disclosure?	□	□
Have your company's networks ever received a penetration "Pen" test? If so, do you know if the issues ere resolved? Are pen tests repeated on an ongoing basis (e.g. annually)?	□	□

Chubb is the marketing name used to refer to subsidiaries of Chubb Limited providing insurance and related services. For a list of these subsidiaries, please visit our website at www.chubb.com. Insurance provided by ACE American Insurance Company and its U.S. based Chubb underwriting company affiliates. All products may not be available in all states. Surplus lines insurance sold only through licensed surplus lines producers. The material presented herein is advisory in nature and is offered as a resource to be used together with your professional insurance advisors in maintaining a loss prevention program. It is not intended as a substitute for legal, insurance, or other professional advice, but rather is presented for general information only. You should consult knowledgeable legal counsel or other knowledgeable experts as to any legal or technical questions you may have. Chubb, 202 Hall's Mill Road, Whitehouse Station, NJ 08889-1600.