Interested in learning more about security?

SANS Institute InfoSec Reading Room

Information Risks & Risk Management

This brief will cover the various exposures that companies now face as they increasingly rely on twenty-first century technology. It will cover information in all forms and the new perils that put this information at risk. Classification of data into categories will determine the type and degree of risk. The types of processes and controls that firms can implement to minimize these risks will be examined. Within each section, targeted references and tips are provided for further insight. Finally, the paper will address...

INFORMATION RISKS & RISK MANAGEMENT

by John Wurzler

Information Risks & Risk Management

GIAC (GLEG) Gold Certification

Author: John Wurzler, john.wurzler@gmail.com
Advisor: Rick Wanner

Accepted: April 23, 2013

Abstract

This brief will cover the various exposures that companies now face as they increasingly rely on twenty-first century technology. It will cover information in all forms and the new perils that put this information at risk. Classification of data into categories will determine the type and degree of risk. The types of processes and controls that firms can implement to minimize these risks will be examined. Within each section, targeted references and tips are provided for further insight. Finally, the paper will address the steps needed to react, respond, and remediate in the event of an untoward event. As a postscript, the paper will also cover the forms of insurance available to help alleviate the financial pain often associated with these types of events.

1. Introduction

In a relatively short period of time, data in the business world has moved from paper files, carbon copies, and filing cabinets to electronic files stored on very powerful computers. We have gone from securing paper files in a file room within an office, to securing data on computers accessed on networks and via the Internet—a massive paradigm shift.

Managing records in electronic form has created a whole new industry, which, in turn, has created a seemingly quenchless thirst for smaller, faster, and more powerful technology. The result is a need for tools to manage and secure this electronic information efficiently and effectively. One could go on, but you get the point.

We have grown accustomed to experiencing change far more quickly than most of us could ever have imagined. It is, in fact, this twenty-first century business paradigm that has given rise to Information Risks. Information Risk is the probability that non-public or confidential electronically stored information could be accessed and/or exploited by unauthorized parties. It probably does not require much concentration to name a few companies who have been profiled in the news, not for their products or services, but for their alleged failure to protect non-public or private information in their care, custody, and control. Security incidents on computer networks and the ramifications of someone, or something, gaining unauthorized access to sensitive data are the key elements of Information Risk, a growing problem for businesses in every sector that utilizes technology.

Information risk, when uttered out loud in a conference room full of risk managers, can cause the room to go very quiet. Risk Managers express varying degrees of confidence when asked how safe their electronic information is from prying eyes, but they are often unclear as to how much protection is required or how to measure the effectiveness of their solutions.

Not so long ago, a company could deploy a security solution for the entire enterprise that might have remained effective for a couple of years. Today, IT professionals provide the tools required to conduct significant aspects of business today, as more and more companies become dependent on computer networks, digital information, remote cloud-based storage, electronic commerce, social media, electronic

mail, instant messaging, and Internet use in general. In this environment, a solution deployed to protect electronic assets or information has a relatively short half-life. The ever-changing dynamic of electronic information will dictate how long any security solution actually may be effective.

The paper will address the issues of determining what these risks are and how to manage and minimize them.

2. Information Risks & Risk Management

2.1. Identification of Major Exposures

IT Security professionals deal regularly with real and perceived threats to the very infrastructure that they deploy and protect. Sometimes it is difficult to sort out the real threats from the perceived ones raised by the numerous well-intentioned vendors providing alerts, all of which consume your very valuable time. You know the ones, like the "Advanced Threat Report" arriving in your email box every morning.

The theft of electronically stored information continues to increase annually as it has since the Computer Security Institute (CSI) started collecting this information in 1999 (CSI, 2012). The threats are real and are internal as well as external. Symantec placed the cost of Intellectual Property (IP) theft to U.S. companies at $250 billion a year and global cyber crime at $114 billion annually (Symantec, 2012). Further, FBI reports confirm that insiders are a major source of competitors' efforts to steal proprietary data. In this report, the common traits of an insider turned thief are outlined in general terms as being (Symantec, 2012):

- **Insider IP thieves are often in technical positions.** The majority of IP theft is committed by male employees, averaging 37 years of age, who are typically engineers, scientists, managers, and programmers. A large percentage of these thieves signed IP agreements. This indicates that policy alone—without employee comprehension and effective enforcement—is ineffective.
- **Typically, insider IP thieves already have a new job.** About 65% of employees who commit insider IP theft have already accepted positions

with a competing company or have started their own company at the time of the theft. About 20% were recruited by an outsider who targeted the data, and 25% gave the stolen IP to a foreign company or country. In addition, more than half steal data within a month of leaving.

- **Malicious insiders generally steal information they are authorized to access.** Subjects take the data they know, work with, and often feel entitled to in some way. In fact, 75% of insiders stole material they were authorized to access.
- **Trade secrets are the most common IP type stolen by insiders.** In fact, trade secrets were stolen in 52% of cases. Business information such as billing information, price lists, and other administrative data was stolen in 30%, followed by source code (20%), proprietary software (14%), customer information (12%), and business plans (6%).
- **Insiders use technical means to steal IP, but most theft is discovered by non-technical employees.** The majority of subjects (54%) used a network—email, a remote network access channel, or network file transfer—to remove their stolen data.
- **Key insider patterns precede departure and theft.** Common problems occur before insider thefts and probably contribute to insiders' motivation. These precipitants of IP theft support the role of personal psychological predispositions, stressful events, and concerning behaviors as indicators of insider risk.
- **Professional setbacks can fast-track insiders considering stealing IP.** Acceleration on the pathway to insider theft occurs when the employee gets tired of "thinking about it" and decides to take action or is solicited by others to do so. This move often occurs on the heels of a perceived professional setback or unmet expectations.[3]

The report cited goes on to describe some pragmatic steps, which taken in tandem with additional checks and balances and the involvement of an Internal Audit, can lead to a substantial reduction in insider theft.

[3] IBID

So far on the exposure front we have identified:

1. Unauthorized access — generally, and for this purpose, an external threat.
2. Theft of non-public or private information.
3. Insider theft — to which the subject often has authorized access.

2.2. Dollars and Sense

Serious money is spent annually to repair, reprogram, patch, re-enter, and restore information and/or systems that have been affected by external (and sometimes by disgruntled employees) threats or attacks. In the Ponemon statistical database, it suggests that firms incur, against these threats, an average of $8.9 million per incident (Ponemon, 2012). And realistically, how many IT managers have a budget line item for this expense? Additionally, it reportedly now takes 24 days to fully recover from such an attack, up from 18 days in 2011(Ponemon, 2012). That is a 42% increase in lost productivity, lost or hampered sales, and general downtime.

Companies victimized by an external threat may experience a loss of business income. For example, the company may be unable to conduct business because systems were unavailable for the transaction of business. This might occur if an e-commerce platform was offline or an in-store system was successfully hacked, compromised, and forced offline. This is a rare occurrence, but it is very real and extremely costly when it does happen.

A further exposure has been created by federal regulations, forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands, which now require that some action be taken when there has been unauthorized access to your systems. This is known as Security Breach Notification. Remedies vary by statute. The law firm of Perkins Coie in Washington State maintains a very useful Internet-based tool for use as a cheat sheet when encountering an incident in a state or territory for which you are not yet familiar (Perkins Coie, 2013).

There is a very real cost to the security breach notification process. In 2008, while working for a Chicago-based company, one of our clients in Maryland had an issue when the

personal details of individuals were inadvertently disclosed on a public-facing website. The cost to investigate and notify those impacted was more than $1.2 million.

There are two final major exposures. The first is damage to reputation. Reputational injury can take months to accurately measure. The damage often translates into millions of dollars; yet when the incident is properly handled, it is negligible. Lastly, for publicly traded companies, there is the potential impact on stock price. There is statistical evidence provided by the New York Stock Exchange that suggests firms that are the victims of a successful attack suffer losses in market capitalization of 1% to 5% (Zhou, 2003). This translates into shareholder losses of $50 million to $200 million, and could result in a shareholder lawsuit against the directors and officers of the affected company.

Estimates of the costs of these exposures come from a variety of sources. There are almost certainly inherent costs due to these exposures. The exact amount is most likely only quantifiable post-loss. The numbers shown here, while from reputable sources, are mostly speculative. Having the ability to recover quickly is important, and it stands to reason that such action will reduce costs.

To summarize, the major exposures are:

1. Unauthorized access — generally, and for this purpose, an external threat.
2. Theft of non-public or private information.
3. Insider theft — to which the subject often has authorized access.
4. IT costs to remediate systems.
5. Business income loss.
6. Regulatory — Security Breach Notification.
7. Reputational injury.
8. Stock price impact.
9. Legal – shareholder lawsuits.

Not every possible scenario has been covered above; there are certain others that are emerging.

2.3. 17 Critical Security Controls To Consider

Every company has unique features. As an example, Company A, who is involved in medical record management, has a daunting list of requirements to follow just to be

compliant with HIPAA regulations. Or, Company B, a service provider to financial services industry that has to comply with the Information Security Rules and individual Statutory Laws. When considering appropriate controls, the nature of the business, the sensitivity of the information stored, and the method used to access the information all need to be considered. This section lists security protocols a business can contemplate as security policy, and practices are reviewed and updated.

2.3.1. Have you established an information security policy that is understood and followed by all employees, contractors, or any other person with access to your private, non-public personal data?

What is an information security policy?

An information security policy is a written statement built around protecting an organization's information assets against accidental or malicious disclosure, modification, or destruction (Wurzler, 2004). Information security management enables data to be shared, while ensuring protection of that information. The policy statement's objectives should be to preserve the confidentiality, integrity, and availability of the organization's information assets. The policy should address network access by employees, contractors, or any other person with access to the company's network.

Why is an information security policy important?

- To help prevent security incidents
- To define responsibilities and expectations regarding:
    - Requirements for the protection of the company's technology and information assets
    - User awareness
    - Acceptable use for regular and privileged users
- To provide guidance for handling incidents if they occur including:
    - How to handle incidents more efficiently and effectively
    - Reducing the impact of incidents

Key characteristics of an information security policy (Douglas, Wurzler, Carr, 2008):

- Realistic and enforceable — fits the organization structure and is easily communicated and monitored.
- Long-term focus — aims to provide a cornerstone to the company foundation and culture so that it becomes embedded and routine.
- Clear and concise — establishes clear expectations.
- Role-based: identifying areas of responsibility and authority — tiered capabilities based upon the role of the individuals needs.
- Dynamically maintained for effectiveness — has to be flexible and easily modified to address current and future needs.
- Include social engineering — reminders that sensitive information should never be given out. Warnings about phone calls from "auditors" looking for help with passwords, phishing schemes in email looking for help. Not just protecting the company, but also the individuals.
- Include non-electronic data — explaining the need to put sensitive information in locked safe places when not in use is a necessary reminder. Some firms have adopted "clean desk" policies at the end of the workday.
- Communicated to all personnel — make all of this clearly available to all personnel. Many companies put this all in to a presentation and have it available annually on line for them to review and to also answer questions at the end of a section or the very end. Some companies even require 100% accuracy in answers before the viewer can sign off.

Key elements:

Acceptable Use Policy for All Users:

- Intended and/or appropriate use
- Password management
- Guidelines for accessing unprotected programs or files

- Signed annual acceptance by all users
- Disciplinary actions for unauthorized and/or unacceptable behaviors, such as:
    - Breaking into accounts
    - Cracking passwords
    - Disrupting service
    - Selecting weak passwords

Policy statement for Privileged (Administrative) Users — Guidelines should be more robust for these users, covering additional areas, such as:

- Authority and conditions for monitoring user activity (e.g., email, network traffic, other actions)
- Causing service disruptions
- Using vulnerability testing tools
- Accessing protected programs or files
- Disciplinary actions for unauthorized and/or unacceptable behaviors, such as
    - ✓ Sharing/creating accounts
    - ✓ Cracking passwords

How to implement an Information Security Policy

Determine your risks:

1. Identify and assign value to hardware and digital assets
    a. Include Data Classification
2. Determine vulnerability to threats and damage potential
3. Select cost-effective safeguards

2.3.2. Anti Virus – Spyware – Spam protection – Malicious code detection: anti-virus installed on all systems.

What is a virus and malicious code control program?

A Computer Virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. This virus can replicate itself and spread, and can often make unknown and unauthorized changes to the infected computer or network. It spreads in a variety of ingenious methods such as attaching to a photo image, an email, a Word document, or a spreadsheet macro, to name a few.

Malicious Code is any program created to modify, destroy, or steal information, use up resources on a computer network, or allow unauthorized access to your computer or network.

Spyware refers to a category of software that, once installed on a computer, collects personal information about a user without their informed consent. Keystroke logging is an example of spyware. Spyware can lead to financial loss, as in identity theft and credit card fraud, and it can also reduce consumers' confidence in online safety and lessen their willingness to participate in modern electronic commerce.

Anti-Virus software packages look for patterns in files or memory that indicate the possible presence of a known virus. Anti-virus packages know what to look for through the use of virus profiles or "signatures" provided by the vendor. Since new viruses are discovered every day, it is important to have the latest virus profiles installed.

Controls on shared drives and folders are locations on a network that allow multiple users to access a common space to store shared files. Unprotected Windows or Apple networking shares can and have been exploited.

Threat Notification tools not related to a vendor:

- **CERT National Cyber Alert System** — The United States Computer Emergency Readiness Team (US-CERT) is a partnership between the Department of Homeland Security and the public and private sectors. One of the responsibilities of US-CERT is the dissemination of cyber threat warning information. (CERT, 2012)

- **SANS Institute @RISK: The Consensus Security Alert** — The SANS (SysAdmin, Audit, Network, Security) Institute is a cooperative research and education organization that operates the Internet Storm Center and provides weekly vulnerability alerts (SANS, 2012).

Why is an anti-virus and malicious code detection/control program important?

Anti-virus: Simply stated, without this protection, viruses are free to infect your systems. Viruses may cause a variety of problems such as loss or damage to information residing on your network, network interruption, and network unavailability for your customers. What's more, liability may be incurred if your weak security measures allow a third party's systems to be infected.

Controls on shared drives and folders. Unprotected Windows networking shares can be exploited by intruders in an automated way to place tools on large numbers of Windows-based computers attached to the Internet (Wurzler, 2000). Unprotected shares can allow Distributed Denial of Service attacks to occur and are also leveraged to propagate viruses and worms. There is great potential for the emergence of other intruder tools that leverage unprotected Windows networking shares on a widespread basis.

CERT threat notification. It is important to utilize a **vendor-neutral** source of vulnerability and threat information in addition to other information that may be received. This assures that timely, nonbiased threat information is available for the coordination of appropriate defense.

Removal of spyware. There are significant privacy implications due to information that is viewed by unauthorized sources. The links in the Resources section provide additional anti-virus resources.

Controls on shared drives and folders. If sharing directories and files over your network is not essential, file sharing should be disabled. An alternative would be to create a dedicated directory for file sharing, and move or copy files to that directory for

future sharing. All network shares should be password protected (Douglas, Wurzler, Carr, 2006).

2.3.3. Do you enforce a software update process that includes at least weekly monitoring of vendors or automatic receiving of notices from them for availability of security patches and upgrades, and testing and installing critical security patches and upgrades as soon as possible, but no later than 30 days after availability (Johnson, 2006)?

What is a software update process?

Security patch management includes updates or patches regularly provided by software vendors to fix problems within their products.

Why is a software update process important?

Many of these patches fix vulnerabilities that could be exploited by hackers. Installing critical patches as soon as possible is highlighted by an experiment conducted by the San Diego Supercomputer Center. The purpose of this experiment was to determine the life expectancy of an unpatched popular commercial operating system when attached to the public Internet. Within eight hours of installation, the system was probed for vulnerabilities by hackers. After 21 days, 20 exploits had been attempted. After 30 days, vulnerability had been exploited, some system logs wiped, and attack tools installed.

Subscribe to patch notification services from the vendors providing all software utilized by your business to include ongoing reviews and weekly evaluations. Where possible, enable automatic update capabilities. Test and install critical security patches and upgrades as soon as possible, but no later than 30 days after availability. Test the system environment while offline to ensure changes are working properly. **Do not go live unless tested offline first**.

2.3.4. Do you have any mobile devices, unauthorized devices, or software in use? Inventory and management of such assets is important.

Without proper controls in place to detect, monitor, deactivate, and remove devices and software that are unauthorized, company systems are vulnerable to detection and exploitation by unauthorized parties from remote locations. Successfully gaining access may permit remote control of systems and stored information. Also, conduct an inventory of all mobile devices — authorized and unauthorized — at least annually.

The emergence of new technologies and cool applications has many employees bringing such devices to the office or downloading seemingly harmless new applications to their workstations. Unfortunately, cool has its risks. These new technologies make the company potentially vulnerable to attack and system breach. If hackers are successful, they can launch attacks on the system from within your network.

The solution is to utilize tools to monitor and maintain an inventory of the devices and software on the enterprise network, and use that information to properly secure and manage situations as necessary to maintain the integrity of the systems security.

2.3.5. Are your firewalls, information systems, and security mechanisms securely configured?

What are firewalls?

Network firewalls are devices or systems which, when properly configured, control the flow of traffic between networks with different levels of trust. In other words, the firewall enforces an access control policy between two networks. A typical application provides separation between a company's internal network and the Internet. Firewalls can also be used to restrict connectivity to and from portions of a company's internal networks that service more critical functions, such as accounting or human resources.

Why are firewalls important?

Without a properly configured firewall, there is nothing to control the information exchange between your systems and other networks. Appropriately configured firewalls can protect your systems from worms and viruses, filter content of

network traffic, and used to enforce acceptable use policies through the review of activity and event logs.

Further information on firewall configuration and policy can be found in the National Institute of Standards and Technology's Guidelines on Firewalls and Firewall Policy (see Resources section).

2.3.6. Do you test your security at least yearly to ensure the effectiveness of your technical controls, as well as your procedures for responding to security incidents (e.g., hacking, viruses, and denial of service attacks)?

What is testing of technical controls?

Testing encompasses a comprehensive assessment of the management, operational, and technical security controls in an information system to determine if the controls are implemented correctly, operating as intended, and producing the desired outcome for meeting the system's security requirements. The results are used to assess the risks and update the system security strategy and policies.

Why is testing of technical controls important?

Tests and assessments of an organization's information security procedures and technical controls provide much of the data needed to keep polices and controls up to date and to verify that the risks have been identified for a given system.

How to implement:

Test information security procedures and technical controls annually at minimum. Independent testing and certification is critical to the checks and balances to ensure integrity of ISO-27002 or better — not SAS 70. Utilize a reputable outside vendor.

2.3.7. Can you recover from data loss or corruption or a network failure within 24 hours for the critical network operations upon which you or your customers depend?

Bandwidth Management and Automatic Load Balancing.

Your ability to communicate continually in a robust manner is critical to your ongoing business operations. Constant attention, testing, and adjustment to the bandwidth available to conduct your business is vital. Improper bandwidth has collapsed numerous online events and caused brand degradation and embarrassment to many companies. Avoid this potential trap. Make provisions with your carriers for adjustable bandwidth on-demand and automatic load balancing. Make use of automatic failover switching to a backup bandwidth provider in the event that a catastrophe takes your primary bandwidth provider offline.

Do you have a backup site?

Maintaining your systems, websites, and ability to conduct business is critical. Do you have a backup site for your company? Is it a hot site, warm site, or a cold site? Do you have a redundant website(s) in the event of a disaster? If these are important to your company, make provisions before disaster strikes.

What is Emergency response/disaster recovery?

Emergency Response/Disaster Recovery, Business Continuity, Information Technology Continuity, and Computer Security Incident Response Plans. These plans work together to provide documented processes for recovery from disruptions related to risks that may be natural, technological, or human in nature. These plans and procedures are inherently interrelated, but depending on the size of the organization and complexity of operations, plans may range from modular components within a comprehensive plan to fully developed standalone documents. The exposures of concern here are primarily addressed by Information Technology Continuity and Computer Security Incident Response Plans. An **Information Technology Continuity Plan** is the backup method and procedure for implementing data recovery and reconstitution and the preventative controls that mitigate outage impacts. An organization's **Computer**

Security Incident Response Plan provides the capability to detect information security incidents rapidly, minimize loss and destruction, identify weaknesses, and restore information technology operations rapidly.

Why is it important?

Information Technology Continuity Plan. Without proper procedures for implementing data recovery and reconstitution and the controls to prevent outages of critical infrastructure, significant interruptions to an organization's operations can occur.

Without a Computer Security Incident Response Plan:

- The duration of a network or system compromise may be unknown.
- Exactly what information has been accessed or modified by intruders may be unclear.
- The methods that the perpetrator(s) used to gain access to systems or what steps can be taken to stop the intrusion activity may not be understood.
- Possible adverse effects that steps taken in response to an incident may have on the company's business operations may not be adequately identified.
- Knowing whom to contact in the organization to report an incident may be unclear. It also may be unclear who has the authority to make decisions related to containing the activity, contacting legal department/law enforcement, etc.
- There may be delays in identifying and contacting appropriate parties to inform them about the activity.

Key steps in developing an Information Technology Continuity Plan:

Conduct a Business Impact Analysis to identify:

- Critical IT resources
- Outage impacts and allowable outage times
- Protocols to provide uninterrupted power by using UPS devices, power

generators, and alternative energy

- Preventive controls such as backup power, fire suppression, redundant air conditioning, and thermal alarms.
- Backup network data and configuration files daily
    - ✓ Store backup data in a secure and protected offsite location.
    - ✓ Develop recovery strategies that allow critical IT resources to be recovered within 24 hours.
    - ✓ Document the recovery strategy.
    - ✓ Periodically test and maintain the plan and devices.

Computer Security Incident Response Plan. Implement a plan that addresses both direct (e.g., hacking) and indirect (e.g., virus) attacks. The major phases in the incident response process are:

- **Preparation.** Response policy, reporting, and communication procedures
- **Detection and Analysis.** Procedures for accurately detecting and assessing possible incidents, detecting when an incident has occurred, and determining the type, extent, and magnitude of the problem.
- **Containment, Eradication, and Recovery**
    - **Containment.** Predetermined strategies for containing specific types of incidents: shut down the system, disconnect from the network, disable certain system functions, etc.
    - **Eradication.** May be necessary to eliminate components of the incident such as deleting malicious code and disabling breached user accounts.
    - Recovery
- **Post Incident Activities** – Review effectiveness of incident handling and identify improvements to existing security controls and practices.

2.3.8. Is all remote access to your network authenticated, encrypted, and from systems that are at least as secure as your own?

What is authentication and encryption?

Authentication. Identification and authentication are fundamental to network access control. Identification is the means by which a user provides a claimed identity to the system. Authentication is the means of establishing the validity of this claim. Typically this information takes the form of a user ID and password.

Password policies need to be created. Require password lengths to be at least eight characters long, consisting of lowercase and uppercase letters, numbers, and at least one special character. Prohibit the use of words. Block reuse of old or previously used passwords for two years or more, and require passwords to be changed every 90 days. Make no exceptions for senior management.

Encryption is the conversion of data into a form that cannot be easily understood by unauthorized individuals. To provide secure transmission of data over a public network such as the Internet, encryption is necessary to assure the data is not understandable except by the authorized recipient.

Why are authentication and encryption important?

Remote user systems often present the weakest link in otherwise secure networks. Not only is data vulnerable during transport over public networks through eavesdropping by unauthorized individuals, but third-party systems such as vendors or contractors, and employee home computers may be less secure that the company network they are accessing. For example, a couple of years ago a medical transcriptionist was working form home on a personal system that was connected to the hospital for whom she worked. The connection was not encrypted and a third party was eavesdropping, later releasing sensitive data to the public in an extortion attempt.

2.8.9. Do you manage access privileges, restrict these on a "need to know" basis, and revoke privileges in a timely manner when no longer warranted, but no later than 24 hours after any change in access privileges?

What is managing access privileges?

Managing system user access privileges or **Access Control** is the means of controlling what information users can utilize, the programs they can run, and the modifications they are permitted to make. Access Control may be built into the operating system, incorporated into applications, or implemented through add-on security packages.

Why managing access privileges is important?

Access controls help protect:

- Operating systems and other system software from unauthorized modification or manipulation
- The integrity and availability of information by restricting the number of users and processes with access
- Confidential information from being disclosed to unauthorized individuals
    - Employee terminates—access cut immediately.

2.3.10. Do you have trained staff responsible for information security or have you outsourced your information security management to a qualified firm specializing in security?

What is a trained information security professional?

A designated individual or individuals with security training and experience is necessary to tie all of the individual activities together into a working security protection mechanism for your organization.

Why is training information security staff important?

Due to the potential severity of privacy injury, network damage, and business interruption caused by security breaches, information security cannot be learned on the job by trial and error. Furthermore, security is not static and must be reassessed

frequently to identify when changes within the organization and new threats require an adjustment to managerial, operational, or technical controls.

- Training is critical. Hiring technical expertise is only as good as the ongoing education they receive. Make certain your employees continually receive training to be able to address the unending stream of new threats, new technologies, and devices that they will encounter daily.
- This team should be prepared to push out training awareness to the rest of the company with alerts, reminders, and helpful assistance.

How to implement:

Appoint an IT Security Officer within the organization. This position must report to senior management and remain independent. The person should never report to IT. Designate trained staff to coordinate the organization's information security effort or outsource to a qualified vendor. Consider individuals with Information Security certifications such as CISSP (Certified Information Systems Security Professional) or CISA (Certified Information System Auditor) for this function.

2.3.11. If you need to circumvent or disable your security controls (e.g., for emergencies or necessary testing of controls), do you always require more than one person's approval and re-enable all such disabled controls as soon practical?

What is dual approval?

Separation of duties is the process of dividing roles and responsibilities so that a single individual cannot subvert a critical process. This process is commonly found in financial settings, for instance, no single individual should normally be given authority to issue checks. Typically, one person initiates a request for a payment and another authorizes that same payment.

Why is dual approval important?

Circumvention of security controls can potentially leave all of an organization's information technology processes at risk, therefore a high degree of oversight is needed. In 2008 a large insurance company on the East Coast took down security to make some changes and enhancements. The person forgot to turn it back on. There was no dual

control. For 48 hours all the company confidential information was publicly exposed. The cost to remedy the situation was in the millions. Had there been dual control this situation may have been eliminated.

How to implement:

Checks and balances need to be designed for the process, as well as for the specific personnel who will implement the process. Management should ensure that duties are well defined to allow clear separation of those duties.

2.3.12. Do you require all third parties to whom you entrust sensitive or nonpublic personal information to contractually agree to protect such information using safeguards at least equivalent to your own and to audit their compliance?

What is Sensitive or Nonpublic Personal Information?

Sensitive or nonpublic personal information includes data such as social security numbers, credit card numbers, medical records, or any other information of a sensitive or confidential nature retained by your organization or by third parties contracted by your organization.

Why is safeguarding sensitive or nonpublic personal information important?

Your organization can be liable for damages or privacy injury related to information entrusted to service providers or any third party allowed to access your networks.

How to implement secure oversight of nonpublic information:

Require the following of any third party to whom sensitive or nonpublic personal information is entrusted:

- A signed agreement regarding access to and appropriate use of your information and networks.
- Contractual compliance with your organization's information security standards.

Compliance with contract requirements should be audited on a regular basis. Verify that these written contracts adequately define the parties' responsibilities in regard to insurance and indemnity, such that appropriate levels of protection are present

for the information risks involved. The expertise of attorneys conversant with the legal issues relating to the subject matter should be utilized when drafting these agreements. Legal review of web-based privacy and acceptable use policies should occur at regular intervals to keep them compliant.

2.3.13. Do you implement processes that allow you to track and record the persons/entities who have access to or custody of nonpublic personal information and the time of such access or custody (e.g., "chain of custody")?

What is tracking and recording access?

Audit Trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. These controls are designed to prevent the loss of confidentiality, integrity, or availability of information, including data or software, wherever stored within organization's information systems.

Why is tracking access or custody important?

Audit trails provide the individual accountability, event reconstruction capability, and means of intrusion detection that are necessary to protect nonpublic personal information from unauthorized access. Likewise the "chain of custody" documentation of access to information is necessary to provide accountability for information stored on all types of media.

2.3.14. Do you retain nonpublic personal information and others' sensitive information only for as long as needed; and when it is no longer needed, is it irreversibly erased or destroyed using a technique that leaves no residual information?

What is Sanitization?

Sensitive and nonpublic information must be disposed of properly and retained only as long as needed. **Sanitization** is the process of removing information from media in a way that leaves no residual traces.

Why is it important?

Due to the risk of improper disclosure, sensitive or nonpublic personal information should be disposed of in a timely fashion and through an appropriate sanitization process. It is commonly believed that erasing a file makes the data irretrievable. In many cases, erasing a file simply removes the pointer to that file.

How to implement?

- Develop and implement specific information retention guidelines for the data handled, stored, or transmitted by your organization.
- Use appropriate sanitization methods to remove information from media:
  - **Overwriting** is an effective method for clearing data from magnetic media. This method uses a program to write (1s, 0s, or a combination) onto the media. Overwriting should not be confused with merely deleting the pointer to a file.
  - **Degaussing** is a method that utilizes strong permanent magnets or electronic degausses to magnetically erase data from magnetic media.
  - **Destruction** of the media is typically accomplished by shredding or burning.

It should be noted that appropriate sanitization techniques should also be utilized when equipment or media is being disposed because it has reached the disposal phase of its life cycle, or has been replaced by upgraded equipment (Sagalow, Wurzler, 2008). The final disposition of sanitized, discarded equipment also needs full documentation and a chain of custody log.

2.3.15. Do you employ physical security controls to prevent unauthorized access to your company's computers, networks, and data?

What is physical security?

Physical Security, or physical access controls, should be provided for the areas containing system hardware, locations of wiring used to connect elements of the system, the electrical power service, telephone and data lines, backup media and source documents, and any other elements required for the system's operation.

Why is physical security important?

Physical access to information system components is one of the easiest ways for intruders to circumvent system protective measures. Social engineering techniques such as posing as a contractor have been used by intruders to gain access to areas that were otherwise considered secure.

How to implement:

- Utilize physical access controls that restrict the entry and exit of personnel from areas that might be used to gain access to your system. Ensure that all building areas that house system elements are identified. Typical controls include:
  - Physical barriers that isolate sensitive areas with controlled entry points. Barriers should be of substantial construction, and barrier walls should be of true floor-to-ceiling construction.
  - Types of entry point controls include locks, guards, badges, electronic access controls, etc.
- Unescorted access to your facilities by visitors should not be allowed other than by your authorized contractors and consultants. The identity of all visitors should be verified and recorded.
  - Staff members who work in a restricted area should be trained to challenge people they do not recognize.
  - All desktop and other personal computing devices are equipped with a timeout feature that locks the device and requires user log-on and password entry after a period of inactivity.

2.3.16. Do you control and track all changes to your network to ensure that it remains secure?

What is configuration management?

Configuration management (CM) is the process for evaluating and keeping track of changes to hardware, software, and network configurations to ensure that changes to the system do not unintentionally or unknowingly diminish security.

Why is Configuration Management important?

Seemingly insignificant changes to information systems can have significant impact on their security. Systems are constantly being scanned and probed by potential intruders for exploitable weaknesses that may be introduced by these changes. Locking down system configuration makes it much more difficult for unauthorized, executable files or malicious code to be surreptitiously installed.

A Configuration Management process should be implemented that addresses the following key elements:

- **Configuration Management Policy and Procedures.** Addresses purpose, scope, roles, responsibilities and compliance, and documented procedures to facilitate the implementation of the CM policy and associated CM controls.
- **Documentation of Baseline Configuration.** Documented baseline configuration of the information system and an inventory of the system's constituent components.
- **Configuration Change Control.** Documentation and control of changes to the information system. Appropriate company officials should approve information system changes in accordance with organizational policies and procedures that should include separation of duties such that no individual can subvert this process.
- **Monitoring Configuration Changes.** Security impact analyses to determine the effects of the changes.

2.3.17. General Counsel review and involvement for regulatory compliance such as SOX, Red Flags rule, HIPAA, GLBA, State notification for CA and MA. Note: this is NOT an IT issue; it is an enterprise issue. Senior management involvement and responsibility is required.

- Contracts with all IT vendors should be reviewed for indemnification clauses, hold harmless provisions, and service level guarantees.
- Require all vendors to carry adequate limits of Errors & Omissions insurance and Information Risk (previously known as Cyber, Hacker, unauthorized access, theft, loss of use, or destruction of data coverage).

4. Summary: Planning Makes Perfect

IT Professionals are responsible for the prevention of a multitude of security tools and for safeguarding operating systems and data warehouse operations, patch management, implementation of user requested changes, and the development and implementation of new systems. As such, it is important to have an independent IT Security function, but fully communicating and involved in daily IT operations. This permits a singular focus — trying to keep bad things from happening. Unfortunately, this constant challenge sometimes comes up short. Unless you happen to be an IT security person with a crystal ball and can foretell the next security breach, bad things will sometimes happen. However, because of your diligence and commitment to security, you've planned for this in your recovery and continuity process. So test that plan, drill that plan, rehearse that plan until you dream about it. An airline pilot's job is probably at best dull on a routine flight, but when something breaks, they don't panic because they train endlessly on emergency and recovery procedures. They are cool, calm, and collected. They react and correct the problems 99% of the time. So will you.

Despite unprecedented spending on security in the past five years, attacks are actually more successful than ever. They are easier to create and carry out, and they produce ever-more devastating results. Most of these threats are not through disablement, but rather through corruption: tricking a system into executing the wrong tasks while it supposes it's working normally. An attack may irreversibly damage vital data, transmit to the attacker a database of customers details including social security numbers or secret military documents. As an IT professional, have you ever asked the questions: How do we pay for this damage? What are my options?

4.1. Investing in Protecting Security

Clearly, understanding the things that can go wrong and your company's risk of exposure is step one. Step two is developing and committing to a management plan to control this risk, often referred to as the risk management plan. The 17 controls outlined above are a part of this plan. The final step is determining how you will to pay for the unexpected costs.

When we have a car accident, we rely on our insurance policy to help pay for the unexpected costs. In our homes, we follow the same practice and often install risk management devices to reduce the exposures (e.g., smoke detectors, radon detectors, CO2 detectors, burglar and fire alarms.) Important tools such as these have become more and more sophisticated over the years, too. These tools, like the tools we implement at work, make our insurance less costly.

At work, we can utilize insurance solutions to help reduce or eliminate a great deal of the issues a company faces when an attack is successful. But what you don't know about conventional insurance for businesses can prove problematic.

4.1.1. Gaps in First-Party Insurance—this coverage pays to the company.

The coverage trigger is the physical loss or damage to tangible property. (The Internet is virtual and intangible, however.)

Generally confined to named physical perils. (Internet perils are viruses and hackers, not fire and rain.)

Electronic Data Processing. Data and media subject to damage from a wide range of perils such as dust, water, temperature, theft, or tampering. (Computer virus attacks are excluded, and copying of data is not covered.)

Crime & Fidelity Coverage. Covers loss because of fraud or theft of money, securities, or other physical property. Also covers theft by employees or fraud by employees of money, securities, or physical property. (Neither covers things stolen via the Internet.)

4.1.2. Gaps in Third-Party Coverage: General Liability. This coverage pays to a third party when the company does something negligent or causes damages to others.

A purely economic loss is not covered. The covered territory is strictly North America. (The Internet is worldwide.)

Intellectual Property infringement is only covered with regard to an insured company's own advertising activity. (The company website is not advertising activity or is it? Courts are conflicted.)

Advertising and Personal Injury may be excluded. (If you have a company website and you are sued, this exclusion may prevent coverage. Defamation, libel, and slander are probably excluded.)

With regard to privacy, the collection of information via cookies is now often excluded, as is the theft of electronically stored information. (Breach of Privacy)

Solutions are available:

- Obtain insurance coverage tailored to respond to wrongful acts in connection with "Internet media" in the conduct of the insured's business
- Elect coverage for any form of defamation (e.g., libel and/or slander)
- Coverage for infringement of intellectual property (e.g., copyright and/or trademark infringement)
- Coverage for invasion, infringement, or interference with rights of privacy or publicity, including false light, public disclosure of private facts, intrusion, and commercial appropriation of name, persona, or likeness.

Look for…

Internet media coverage, to specifically address any content on your website, including advertising. This adds back the coverage to provide protection for liability created by another entity's banner ad or hyperlink and covers the insured advertising activities on the web.

Advertising is defined to include publicity, promotion, including branding, co-branding, sponsorships, and/or endorsement on **your** own behalf or for others on your

website. (This is a broad definition that captures the fact that much of the advertising on a website may have nothing to do with that particular website.)

Assumed under contract liability assumed by **you** in the form of hold harmless or indemnity agreements executed with any party, but only with respect to material provided or disseminated by **you**. (This gives you coverage back for the creation and sharing of material on the Internet.)

Content-based liability arising from a third party acting upon **your Internet Content**. (A clarification of coverage that allows for claims where the material on your website caused a person to do or not to do something to their detriment.)

Breach of Security Liability or Cyber Liability or Computer Attack Liability. Look for coverage that permits intentional, unintentional, authorized access and unauthorized access, malicious or accidental, fraudulent or innocent, targeted or generally distributed, and regardless of motive. Make sure Identity Theft coverage and resolution services are included.

Failure of Security includes coverage for the information contained on hardware or devices that are stolen.

Location of the Data/Information your information stored on any media by you or when in the care, custody, and control of a contractual third party (e.g., cloud computing, data storage, hosting services).

Business Interruption provides coverage to you for online and offline revenue loss due to a covered computer attack.

Investigation & Computer Forensics Expenses. Make certain this is included and has a reasonable amount of funds available to you.

Trade Secrets & Copyright. Make certain both of these are included in the coverage.

Data loss expenses. Whether incurred by your company or on your behalf, in order to respond and remediate an **information risk incident.** This reimburses you for expenses incurred to make things right again (e.g., the costs to replace, reproduce, recreate, and recollect data if lost).

Privacy administrative award. Liability coverage for you in the event of a violation of a **privacy regulation.** (Remember those 46 states and territories? Each has a different requirement and it takes time and money to respond.)

Cyber Extortion. Coverage that will reimburse you for funds you may pay out to recover stolen data.

A Checklist for Reviewing Insurance Coverage

- ❑ **DO look for all broad coverage grants, free assessments, and post-incident support.**
- ❑ **Do look for definition of claim to include both monetary and nonmonetary relief.**
- ❑ **DO look for *express* cyber-terrorism coverage.**
- ❑ **AVOID restrictions on coverage based on intent or motive of cyber-attacker, including the use of the word "negligent" in the definition of a wrongful act.**
- ❑ **AVOID coverage triggers that are expressly limited to "negligence."**
- ❑ **AVOID theft of customer info or credit card exclusions.**
- ❑ **AVOID absolute inside attacker exclusion.**
- ❑ **AVOID low sub-limits for business income interruption coverage.**

5. Closing Comments

Information Security is a paramount risk management concern. Today, more than at any time in history, information security, risk management, and insurance are heavily intertwined. The incredibly large costs associated with a security breach or successful attack on an enterprise is appalling. Companies choose how much to spend on information security, risk management, and insurance, often while trying to carefully manage precious budget dollars. As IT professionals, you have to do your best with the share you are allotted. Keep doing your best. Keep asking for the tools to do your jobs. It would not hurt to gently let senior management know that they can add insurance coverage for these exposures.

When considering financial justification, remember that this is an overall enterprise issue and solution. It is not an IT problem. Despite the best efforts to minimize the exposure, you cannot totally eliminate it. There is no 100%, ironclad solution. Despite a company's best efforts there is always a gap exposure to security breach, information abuse, or business loss. Insurance then becomes a viable solution to make up that gap. Like the law of diminishing returns, once the minimum standards are met, more resources are required for incremental increases in security. In addition, knowledgeable insurers can provide valuable pre- and post-incident expertise to either enhance your security measures upfront or to coordinate an effective response and recovery once an incident occurs.

Network security in an economy that is highly data dependent is a critical investment. Ensuring that your organization is equipped to manage this ever-pressing challenge requires awareness of the exposures, a commitment to the resources and protocols required to mitigate and ably handle the risks, and financial protection to mitigate the impact of an event.

6. References

Canton, James, PhD. 2000. *Technofutures: How Leading-Edge Technology Will Transform Business in the 21st Century.* Hay House.

CERT Reading Room for Computer Viruses

(www.us-cert.gov/publications/virus-basics)

Clarke et al. 2004. e-Coverage, National Underwriter.

Douglas, Wurzler, Carr. 2008. Information Risk Critical Security Controls, a Primer, found currently at www.cna.com/riskcontrol.

Garfinkel, Simson and Gene Spafford. 2002. *Web Security & Commerce.* 2nd. Ed. O'Reilly & Associates.

Johnson, Charlie. 2006. Security Controls and the Security Life Cycle, Norfolk Chamber of Commerce, Norfolk VA.

Lange et al. 2000. *E-risk: Liabilities in a Wired World,* National Underwriter, 2000.

Perkins Coie: www.perkinscoie.com/statebreachchart

PriceWaterHouseCoopers. 2001. CyberRisk Handbook.

Rice, David. 2008. *Geekonomics: The Real Cost of Insecure Software.* Addison-Wesley.

Sagalow, Wurzler et al. 2008. The Financial Impact of Cyber Risk, American National Standards Institute.

SANS Security Policy Project. 2012.

Symantec. 2012. Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property, www.symantec.com.

Whiteley, Sandy, Ed. 1994. *Guide to Information Access.* Random House.

Wurzler John S. et al. 2009. Cyber Liability and Insurance, National Underwriter.

Wurzler, John S. 1999. "Website & E-Commerce Surface New Risks Which Require Effective Risk Management," VarBusiness.

Wurzler, John S. et al. 2010. The Financial Management of Cyber Risk, Internet Security Alliance & American National Standards Institute, ©2010.

Zhou, Lei et al. 2003. "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market," *Journal of Computer Security*, vol. 11, issue 3, pp. 431–448.

7. Resources

CERT/CC Overview

Further information on creating an information security policy:

SANS Security Policy Project

United States Computer Emergency Readiness Team (www.us-cert.gov)

CERT National Cyber Alert System – sign up here

(www.us-cert.gov/mailing-lists-and-feeds) Scroll to the bottom of this page.

ICSA Labs – on Spyware – an excellent paper

(www.us-cert.gov/sites/default/files/publications/spywarehome_0905.pdf)

IDC Research, available at www.nua.ie.surveys.

Windows Patch Management (www.windowsecurity.com)

How To Implement, Automate And Measure The Effectiveness Of Controls

(www.sans.org/critical-security-controls/control.php?id=1)

National Institute of Standards and Technology's *Guidelines on Firewalls and Firewall Policy* (csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf).

Information Security Handbook: A Guide for Managers, National Institute for Standards and Technology (csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf)

Contingency Planning Guide for Information Technology Systems, National Institute of Standards and Technology (www.itl.nist.gov/lab/bulletns/bltnjun02.htm)

Computer Security Incident Handling Guide, National Institute of Standards and Technology (csrc.nist.gov/publications/drafts/800-61-rev2/draft-sp800-61rev2.pdf)

Avoiding the Trail by Fire Approach to Security Incidents, CERT Frequently Asked Questions (www.cert.org/csirts/csirt_faq.html)

Security for Telecommuting and Broadband Communications, National Institute of Standards and Technology (www.itl.nist.gov/lab/bulletns/bltnnov02.htm)

An Introduction to Computer Security: The NIST Handbook Chapters 10 and 17, National Institute of Standards and Technology (csrc.nist.gov/publications/nistpubs/800-12/800-12-html/index.html)

Isalliance Common Sense Guides, Internet Security Alliance (www.isalliance.org)

Database of information security professionals certified by (ISC) https://www.isc2.org/sscp/Default.aspx

Information Systems Audit and Control Association (www.isaca.org)

An Introduction to Computer Security: The NIST Handbook Chapters 10 and 16, National Institute of Standards and Technology as circumvention is no longer necessary.

An Introduction to Computer Security: The NIST Handbook Chapters 14 and 18, National Institute of Standards and Technology (csrc.nist.gov/publications/nistpubs/800-12/800-12-html/index.html)

Guidelines for Media Sanitization, National Institute of Standards and Technology (www.nist.org/nist_plugins/content/content.php?content.52)

An Introduction to Computer Security: The NIST Handbook Chapter 14, National Institute of Standards and Technology (csrc.nist.gov/publications/nistpubs/800-12/800-12-html/index.html)

An Introduction to Computer Security: The NIST Handbook Chapter 14, National Institute of Standards and Technology

Last Updated: October 24th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
GridEx IV 2017	Online,	Nov 15, 2017 - Nov 16, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CAUS	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, GB	Nov 27, 2017 - Dec 02, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZUS	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Khobar 2017	Khobar, SA	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TXUS	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, DE	Dec 04, 2017 - Dec 09, 2017	Live Event
European Security Awareness Summit & Training 2017	London, GB	Dec 04, 2017 - Dec 07, 2017	Live Event
SANS Bangalore 2017	Bangalore, IN	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, DE	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS San Diego 2017	OnlineCAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced