Global Information Assurance Certification Paper

Information Security: A Risk Managed Approach for Microbusinesses

Richard Helliwell
June 2004

GSEC Practical Requirements Version 1.4b Option 1

Abstract

The risks to information systems are constantly changing, with new threats arising almost on a daily basis. Staying aware of and managing these risks can be a full time job in itself. However, not all businesses have the expertise or resources to protect themselves. Microbusinesses are one such category of business. Microbusiness are defined as having less than five employees, and are usually characterised by having very limited resouces such as time, money, and information security experise. For a microbusiness it is crucial that information security risks are managed methodically with resources allocated as effeciently as possible. Risk management is one way to achieve this goal.

This paper is intended to assist information security professionals providing advice to a microbusiness. It presents a typical profile for this type of business and outlines a systematic risk management process based upon the Australian and New Zealand Standard AS/NZS 4360:1999. In addition, a sample set of threats, risks and potential treatments are also discussed.

1 Introduction

A common definition for a microbusiness, also known as a very small business, is a business employing less than five people [1]. The importance of the microbusiness to the economy should not be underestimated. For example, in Australia, it is estimated that they account for 65% of all businesses [2].

This paper is intended to provide information security professionals with an understanding of the constraints and risks that a typical microbusiness will generally face. A set of high level threats, risks and potential treatments are also discussed in conjunction with a risk management framework based upon the Australian and New Zealand Standard AS/NZS 4360:1999. However, as each business has a different set of circumstances, not all aspects of this analysis may be relevant.

The Australian Bureau of Statistics [3] measured the proportion of Australian businesses using information technology on 30 June 2001 [2]. Figures for Internet access, and the percentage of businesses with a web presence are summarised in Table 1. From these statistics a profile of a typical microbusiness can be developed.

	Computers %	*Internet access* %	*Website* %
Microbusiness 0-4 employees	79	64	14

Table 1: Information Technology Use in Microbusinesses

2 A Sample Microbusiness Profile

Microbusinesses share a number of common characteristics, allowing a generic profile to be developed. It is important to note that an individual assessment is needed for each business to determine if and what requirements differ. In particular, an in-depth understanding of business environment is required to construct each profile. The following assumptions have been made:

Minimal Resources: By definition all businesses are constrained by limited resources, whether they be employees, money, hardware, etc. This is even more so in the case of a microbusiness, resulting in the business being unable to dedicate a large amount of time or money to developing or maintaining security. Any risk treatments will have to take this factor into account.

Lack of IT Security Expertise: It is often the case in a microbusiness, and even small businesses (5-20 employees), that IT administration and security duties will fall to the employee that exhibits an interest in information technology. Unless an employee, or the business owner has specific expertise in this area, it is assumed that employees lack an in-depth knowledge of IT security. Thus, any risk treatment strategies must require minimal expertise to implement and maintain.

Has Internet access: The majority (64%) of microbusinesses have Internet access (Table 1). It is assumed for this paper that the microbusiness has Internet access and that the principle Internet applications used are email and web browsing.

Does not host Internet services: The majority (86%), of microbusinesses do not have a web presence (Table 1). It is assumed for this paper that the microbusiness does not host a website or any other services such as a ftp or mail server. This does not preclude the business from using these services.

Computer use is restricted to business users only: Many microbusinesses are located in a home office, creating the possibility that the computer is also used by family members. To simplify the profile, it is assumed that computer use is restricted to business users only. However, the profile does allow for limited personal use of the computer systems by users, such as web browsing and email.

3 Risk Management

3.1 Overview

Risk Management is an iterative process that is used to determine and treat the risks that occur: during an activity or function; to a project, product or asset. It is a critical management process, providing a methodology to minimise losses and maximise opportunities [4].

From an information security perspective, it is important to undertake a risk managed approach in a systematic manner. Without following through this process it is possible for the wrong risks to be prioritised while leaving the greater risks untreated. For example, a risk exists that a burglar will attempt to gain access to a premises. A standard response to this risk, is to buy additional locks for the front door. This may decrease the likelihood of the locks being picked or broken, but have the alternative methods of entry such as being able to climb through an open window also been addressed? If not, then the overall risk of theft has not been reduced and the money might have been better spent elsewhere, perhaps in this case on window locks.

Focusing on the wrong threats is not restricted to physical security – it often occurs in information security. A good example includes email software encryption products. The focus on security usually rests on the type of encryption algorithm used and the corresponding key lengths. While these are important considerations, Bruce Schneier presented a vulnerability analysis of the public key encryption product, *Pretty Good Privacy (PGP)* [5] and showed that breaking the encryption is often not the most profitable type of attack. He suggested a number alternative attack methods that require far less effort and expertise to execute. Applying a risk management framework in a systematic manner assists in overcoming these failures. It helps to identify all the risks and their associated treatments whilst providing a methodology in which they can be prioritised.

The following sections are based upon the methodology described in the standard AS/NZS 4360:1999 [4]. They have been tailored to the needs of the microbusiness profile stated in Section 2.

3.2 Establish the Risk Management Context

The context in which the risk management applies must be firmly established. It provides the scope and boundary, while also identifying the overall objectives for the process. Another important aspect of this stage is to identify the roles and responsibilities of the relevant stakeholders.

For this paper, the scope of the risk management process is limited to threats posed to the information technology assets. This point should be checked with the business owner as they may wish to change the scope. By confining the scope to the information technology assets - the goals are easily defined. The accepted goals of information security [6] are:

1. Confidentiality.
2. Integrity.
3. Availability.

The assets of the business should also be defined at this stage. An asset is anything that the business wishes to protect. Assets can range from physical assets such as hardware to intangible assets such as intellectual property. These will vary from business to business, but some examples of information security related assets are discussed in the following sections.

3.2.1 Business Reputation

Reputation is an important business asset. It determines the level of trust that customers express in the business, and can affect the profitability of the business. It is difficult to quantify the amount of reputation that a business has with its customers and in the community. In turn, this makes it difficult to measure the effects of the loss

of reputation. Loss of reputation principally occurs through negative publicity where a risk impacts upon external parties, including customers.

3.2.2 Business data

Business data is defined broadly as any data that is stored electronically including customer data, stock price lists, proprietary business processes and email.

3.2..3 Information Technology Hardware

Information technology hardware is a broad asset category that covers the physical devices that a business may own. It may include: laptops; desktop computers; networking equipment; servers; printers and electronic media.

3.2..4 Software

Software is another broad asset category that includes operating systems and applications. Applications may include utilities and business applications such as word processors and spreadsheets. It is unlikely that a microbusiness of the profile described will have any custom built applications due to monetary costs involved in hiring external parties and expetise requirements for developing in-house.

Finally, all the stakeholders in the risk management process must be identified along with their roles and responsibilities. This is necessary so that responsibility for risk treatments can be assigned appropriately.

3.3 Identify threats

A threat contributes to a level of risk against an asset. A threat itself can be considered in two seperate components: the threat agent; and the attack. A threat agent is something or someone that will act to the detriment of an asset. Examples of threat agents include a hacker/cracker, malicious code, and nature. The attack is defined as the method in which a threat agent may act. The threats identification stage includes all threats, even if they are beyond the scope of control of the business to affect. It is not the purpose to undertake analysis at this time but to identify what and how something can happen.

There are a number of resources to assist in identifying threats to information systems. A classification scheme for information security threats [7] describes broad categories of threat agents, attacks, consequences and defences. It is comprehensive reference, and is useful in providing assurance that all threats have been considered. In addition to vendor websites, there are a plethora of websites and studies that provide information relating to the vulnerabilities of operating systems and applications [8] [9] [10].

3.4 Analyse Risks

Risk is a measurement of the likelihood and consequence of a threat occurring against an asset [4] [11]. Risk analysis prioritises risks by ranking the likelihood and consequences of threats occurring. There are two broad categories of analysis: qualitative and quantitative.

Qualitative analysis uses a descriptive scale to convey the likelihood and potential consequences. By its very nature this analysis is imprecise. However, this does not negate its usefulness; natural language can clearly convey the level of risk posed. It does present a problem when trying to make comparisons between different categories of risks. This problem can be reduced through the careful use of language, strict definitions, and consensus.

Quantitative analysis uses numerical scales to describe likelihood and potential consequences. These values are usually determined through statistical modelling. For example, in the manufacturing industry the measure used to model the likelihood that a component will fail is known as *mean time to failure*. The quality of this type of analysis is highly dependent upon the accuracy of models used [4]. It is unlikely that an accurate enough statistical model can be created to be of practical use for the majority of information security risks faced by a microbusiness.

As the name suggests, semi-quantitative analysis combines aspects of qualitative and quantitative analysis. Numerical values are used in conjunction with a descriptive scale in order to convey consequences and likelihoods. This is often achieved by attaching a monetary value to a consequence and a frequency to a likelihood. The risk management standard warns that care must be taken in the use of this analysis as the numerical scales chosen may not accurately differentiate between risks, particularly when the consequences or likelihood are extreme [4]. In some instances it can be difficult to quantify the monetary cost of a risk. For example, the damage from the loss of business reputation can be difficult to quantify. If the loss of reputation is severe then the business may cease operating; a dollar value may be assigned in this instance. However, where the damage is less, assigning a cost is problematic. Therefore, when an arbitrary value is allocated to a risk care must be taken that it is in proportion with the values chosen for other damages.

For each threat the consequence and likelihood should be assigned a value based upon experience and best practice. If there are any existing controls, such as business processes, in place that contribute to reducing these threats, they should be analysed for appropriateness and included in this assessment.

An example of a qualitative classification that may be used for a microbusiness is listed in Tables 2 and 3. These tables are a modified from the examples included in the risk management standard [4]. A semi-quantitative analysis may be created by adding financial descriptors to the consequence descriptions. As noted earlier, care must be taken that these figures are as realistic as possible.

Level	*Descriptor*	*Detail Description*
1	Insignificant	No financial loss. No reduction in productivity.
2	Minor	Low financial loss. Minor reduction in productivity.
3	Moderate	Low financial loss. Moderate reduction in productivity. Minor loss of business reputation.
4	Major	Medium financial loss. Productivity halted for a short period of time. Medium loss of business reputation.
5	Catastrophic	High financial loss. Business reputation destroyed. Business activities halted for an indeterminate period of time. May result in the cessation of business.

Table 2: An Example of Qualitative Measure of Consequence for a Microbusiness

Level	*Descriptor*	*Description*
A	Almost certain	Likely to occur at least once per month
B	Likely	Likely to occur at least once every six months
C	Possible	Likely to occur once per year
D	Unlikely	May occur once every five years
E	Rare	Occurs only in exceptional circumstances

Table 3: An Example of Qualitative Measures of Likelihood for a Microbusiness

As previously stated, the level of risk is the combination of the magnitude of the consequence and the likelihood of the threat occurring. Once the consequence and likelihood have been assigned values, the level of risk can be determined by examining the Table 4 [4]. The levels of risk are prioritised in order of magnitude from low to extreme.

It is important to note that even if the consequences of a threat are minimal, if it occurs on a regular basis it is classed as a high risk, due to the comparatively large amount of effort required to manage the risk. The levels of risk, as well as Tables 2, 3, and 4 should be modified to suit the particular microbusiness.

	Consequences				
	Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	1	2	3	4	5
A (Almost certain)	High	High	Extreme	Extreme	Extreme
B (Likely)	Moderate	High	High	Extreme	Extreme
C (Possible)	Low	Moderate	High	Extreme	Extreme
D (Unlikely)	Low	Low	Moderate	High	High
E (Rare)	Low	Low	Moderate	High	High

Table 4: Qualitative risk analysis matrix

3.5 Evaluate Risks

Risk evaluation is the part of the evaluation where the risks identified in Section 3.4 are prioritised. During the context phase, an idea of the risk profile that the business is willing to tolerate should have been determined. Risks that have been classified as low and are in the acceptable category can be accepted without further treatment. For completeness, these risks should be recorded. These risks should be audited on a regular basis, to check that the level of risk has not increased.

3.6 Risk Treatment Strategies

Risks that are not acquitted in Section 3.5 require further treatment. Treatment of risks is divided into five categories:

1. **Avoiding risk** is achieved by choosing not to undertake the activity that results in the risk. Business, by definition, entails a certain level of risk, however, there are circumstances where the level of risk that may be incurred can outweigh any potential benefit.
2. **Reducing the likelihood** of a threat can occur through a number of different controls such as: audit and compliance programs; education, preventative; and technical controls.
3. **Reducing the consequence** of a threat can be achieved by: undertaking contingency planning; business continuity planning; public relations; and minimising the level of exposure to the source of the risk.
4. **Transferring the risk** is accomplished by having another party incur the risk on the businesses behalf. The most notable example of this is paying an insurance company to underwrite a risk.
5. **Accepting the risk** occurs when the business owner is willing to undertake the risk. Self-insurance fits into this category, as does ignoring the risk and hoping that it will disappear.

In some risk management frameworks *reducing the likelihood* and *reducing the consequence* are considered as a single risk treatment, usually termed *mitigation.* However, it is useful to seperate them as it is possible in certain circumstances to reduce the likelihood of an event but not to effect the consequences and vice versa. The relevant treatments for each risk will in the end be the decision of the business owner.

3.7 Monitoring and Review

As previously stated, risk management is an iterative process. A treatment needs to be monitored to ensure that the control is effective. Likewise, threats are constantly changing - especially in the quickly evolving field of information technology. New vulnerabilities and associated threats are being discovered regularly. It is possible that a control may not remain effective against new risks.

Periodic audits are an effective method for monitoring. These can be performed internally or by an external party. Contracting an external party with the appropriate technical skills to perform an audit may be a cost effective method for reducing risk by ensuring that controls remain effective.

Finally, the risk management plan itself must be reviewed and updated regularly. The plan is an important record of the risks faced by the business and the controls in place to deal with this risk. It also demonstrates due diligence and provides an audit trail.

4 Risk Analysis of a Microbusiness

The following section describes a partial risk analysis of the microbusiness described in Sections 2 and 3.2. Section 4.1 discusses the broad category of threat agents and attacks that may be faced. Further details, including the risk level, can only be determined in a specific set circumstances.

Section 4.2 describes a set of treatments aimed to reduce the level of risk posed by these threats, mainly through technical controls. Each treatment suggested is evaluated to comply with the profile and goals listed in Sections 2 and 3.2. That is, they have been judged against the following criteria:

1. Level of IT expertise and resources to maintain.
2. Ease to install or configure.
3. Cost.
4. Level of automation.

4.1 Threats

4.1.1 Threat Agents

A sample of threat agents that may be relevant to a microbusiness include:

Employees: Employees are a threat to assets as they often have a high level of access. As the number of employees in a microbusiness is minimal, it is more likely that an employee will pose a threat through an accidental act rather than intentional. Temporary staff and contractors also fit into this category, but may pose a greater malicious threat.

Competitors: Other businesses that are in direct competition may gain a competitive advantage if the businesses assets are damaged.

Hackers: Hackers are individuals who are interested in information technology, while generally not malicious their actions may indirectly pose a threat to the business. For example, a hacker may publish a new software vulnerability that is later exploited by others.

Crackers: Crackers are individuals who deliberately cause harm to information technology systems, either directly or indirectly.

Thieves: Thieves are people who steal, usually physical objects, for a living. Professional thieves are well organised and can possess a high attack capability.

Vandals: Vandals are people who damage property for the sake of it.
Nature: Natural phenomenon can have a detrimental effect on assets, such as, hardware failing through wear and tear.

4.1.2 Attacks

A sample of attacks that may be used by the threat agents include:
Power failure: An interruption to a power supply will cause a loss availability for information technology systems. It may also cause hardware failure and data loss.
Fire: A fire can cause physical damage to assets, and will usually require an emergency response.
Flood: A flood can cause physical damage to assets, and will usually require an emergency response.
Malicious Code: Malicious code, including viruses and trojan horses, are computer programs that can cause loss of confidentiality, integrity and availability of data. They can also cause denial of service attacks, and hardware failure.
Breaking Password: Passords can be gained through guessing, dictionary and brute force attacks.
Hardware theft: Hardware may be stolen for its value or the information that it contains.
Backup theft: Backups are not usually as well protected as hardware and may be easily targetted for theft.
Hardware failure: Hardware has a limited life and will eventually fail through wear and tear. Failure may cause loss of integrity and availability of data.
Backup failure: Restoration from backups may fail for various reasons including the presence of malicious code, media failure, and failure to backup data correctly.
Software Vulnerability Exploitation: The greater the complexity of a piece of software the greater the chance that it will contain vulnerabilities. These may be exploited to cause a loss of confidenitality, integrity and/or availability of data.
Denial of Service: A denial of service attack is usually against an internet service and may be targetted against individual companies. While it is not likely that the business will be a target, it may be used to mount a distributed attack against another target.

4.2 Risk Treatment Strategies

Although the information security threats in Section 4.1 are only described in general terms, it is obvious that a number of risks share a common basis. This section considers possible treatments for these risks.

4.2.1 Physical Security

Physical security is generally well understood. It is likely that the business will already have a secured premises, and perhaps an alarm system. Possible avenues for improvement include:

- Locks for desktop computers and laptops.
- Removable hard drives that can be locked in a safe after business hours.
- Backups kept in a fireproof safe and/or offsite
- Encrypting all sensitive data.

4.2.2 System Hardening

System hardening is likely to be beyond the scope of the abilities of the business and its employees. However, it is possible to secure an operating system, so that minimal ongoing IT expertise is required. Options include:

- Separate user accounts for employees requiring computer access.
- User accounts only possess the level of authority required to perform day to day to functions.
- Strong passwords are to be used. A good guide is provided by the reference, *Choosing good passwords* [12].
- Unnecessary services should be disabled. This will need to be conducted in conjunction with the computer users to determine what services are required.
- Well known vulnerabilities, such as *The SANS Top 20 Internet Security Vulnerabilities* [13] should be addressed.
- Automatic patching for the operating system and applications should be enabled where possible. Although accepting patches without question poses a risk, it outweighs the risk that this aspect of security will be neglected [9].

4.2.3 Firewall

Firewalls are a front-line defence against external attackers. Personal software firewalls are inexpensive, and some ADSL routers come with an inbuilt firewall. Commercial firewalls usually come with sets of preconfigured policies. Examples include *ZoneAlarm* [14], and *Norton Personal Firewall* [15].

4.2.4 Malicious Code

Malicious code is increasingly becoming a problem for businesses, with 88% of attacks involving viruses, worms or Trojans [9] [16]. As with a firewall, virus scanning software is essential. Automatic updates and regular virus scans should be scheduled. There are numerous commercial anti-virus software packages, such as *Norton Anti-virus* [15] and *McAfee VirusScan* [17]. *Protecting your computer from malicious code* [18] provides a good introduction to this subject.

The threat of spyware to privacy is increasing. Spyware is also known as tracking software which is installed without the users knowledge. Some of these programs have the potential to hijack a web-browser session and record keystrokes [19]. Utilities such as Lavasoft's *Adaware* [20] and *Spybot - Search and Destroy*[21], can detect and remove spyware.

4.2.5 Regular backups

Regular data backups are essential in ensuring business continuity in instances where data has been lost or corrupted. This is often overlooked by small businesses. A regular backup schedule, including testing and rotating backups on a periodic basis, should be instigated if it is not already being performed. In addition, a set of backup should be stored securely off site.

4.2.6 User Education and Policies

In any security system, the human element is usually the weakest link. There are two ways in which to guard against this: through user education; and policies concerning the use of information technology. Both can be time consuming to implement.

Policies can serve two purposes: provide a standardised approach to security issues, and assist in educating users. A number of policy templates are located at the

SANS Security Policy Project [22]. These can be easily modified to suit the needs of the business. Note however, policies can not be developed in isolation. Employees should be consulted to ensure that an acceptable balance is found between functionality and security. It is also a good opportunity to educate users in the basics of information security.

Education can be partially achieved through policies. However, policies alone are not sufficient. There are security guides published on the Internet that cater for small businesses. A good example of this is *Trusting the Internet* [23]. Another guide concerned with the small home business is *Home Network Security* [24], however it is orientated towards a more technical audience.

4.2.7 Monitoring and Audit

Ongoing monitoring and regular audits are important aspects of risk management. It assists in ensuring that risk levels remain at tolerable levels. Audits may be outsourced to an external party, however, the cost of this may be too prohibitive.

Another function of monitoring and audit is to discover malicious insiders. An advantage of the small size of these businesses is that it is a difficult environment for a user intent on damaging the organisation to operate without being quickly discovered.

5 Conclusion

Information security is difficult. The risks faced to information technology systems are constantly changing as new vulnerabilities are discovered daily, and older vulnerabilities are exploited in new ways.

Information security is particularly difficult for the microbusiness. These businesses are characterised by having low resources, time, people, and money. Furthermore, they often do not have sufficient IT expertise to maintain a suitable level of security.

This paper outlined a risk management approach, advocated in the Australian and New Zealand Risk Management Standard (AS/NZS 4360:1999), that has been tailored to meet the needs of the microbusiness. A sample set of risks and treatments for the microbusiness was also discussed.

With this information, an IT security professional should be able to construct a realistic risk management plan for a microbusiness with an understanding of the special needs and restrictions of this group of businesses.

References

[1] Australian Bureau of Statistics. "1321.0 Small Business in Australia". 23/10/2002. URL: http://www.abs.gov.au/ausstats (10/06/2004).

[2] Australian Bureau of Statistics. "Year Book Australia 2003, Communications and Information Technology, Business use of information technology". 26/05/2004. URL: http://www.abs.gov.au/ausstats (10/06/2004)

[3] Australian Bureau of Statistics. URL: http://www.abs.gov.au (10/06/2004)

[4] Standards Australia and Standards New Zealand. Risk management. AS/NZS 4360:1999

[5] Schneier, Bruce. "Modelling security threats". December 1999. URL: http://www.schneier.com/paper-attacktrees-ddj-ft.html (10/06/2004)

[6] Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security Essentials with CISSP CBK. Version 2.1. Volume 1. SANS Press. April 2003. 259

[7] Cohen, Fred. Phillips, Cynthia. Swiler, Laura Painton. Gaylor, Timothy. Leary, Patricia. Rupley, Fran. Isler, Richard. Dart, Eli. "A Preliminary Classification Scheme for Information System Threats, Attacks, and Defenses; A Cause and Effect Model; and Some Analysis Based on That Model". September 1998. URL: http://all.net/journal/ntb/cause-and-effect.html (10/06/2004)

[8] AusCERT. URL: http://www.auscert.org.au

[9] "2004 Australian Computer Crime and Security Survey". 24 May 2004. URL: http://www.auscert.org.au/crimesurvey (10/06/2004)

[10] BugTraq. URL: http://www.securityfocus.com (10/06/2004)

[11] Bauer, Mick. "Practical Threat Analysis and Risk Management". 1 January 2002. URL: http://www.linuxjournal.com/article.php? sid=5567 (10/06/2004)

[12] "Choosing good passwords". 1 February 2001. URL: http://www.auscert.org.au/render.html? it=2260&cid=1920 (10/06/2004)

[13] "The SANS Top 20 Internet Security Vulnerabilities". 8 October 2003. URL: http://www.sans.org/top20/ (10/06/2004)

[14] ZoneLabs. URL: http://www.zonelabs.com (10/06/2004)

[15] Symantec. URL: http://www.symantec.com/index.htm (10/06/2004)

[16] Dearne, Karen. "Security reels under virus load". 25 May 2004. URL: http://www.australianit.news.com.au/articles/0,7204,9653586%5E15317%5E%5Enbv%5E15306,00.html (10/06/2004)

[17] McAfee Virus Scan. URL: http://us.mcafee.com (10/06/2004)

[18] "Protecting your computer from malicious code". 18 August 2003. URL: http://www.auscert.org.au/render.html? it=3352&cid=1920 (10/06/2004)

[19] "Spyware threat grows". 7 May 2004. URL: http://australianit.news.com.au/articles/0,7204,9493783%5E15841%5E%5Enbv%5E,00.html (10/06/2004)

[20] Lavasoft. URL: http://www.lavasoftusa.com/software/adaware/ (10/06/2004)

[21] Spybot - Search and Destroy. URL: http://www.safer-networking.org/index.php?lang=pl (10/06/2004)

[22] "The SANS Security Policy Project". URL: http://www.sans.org/resources/policies/ (10/06/2004)

[23] Department of Communications, Information Technology and the Arts. "Trusting the Internet - Small Business Guide to E-Security". July 2002. URL: http://www2.dcita.gov.au/__data/assets/file/21407/trusting_the_internet.pdf (10/06/2004)

[24] "Home Network Security". URL: http://www.staysafeonline.info/appendix_a.adp (10/06/2004)

[25] "Beginner's Guide to Computer Security". URL: http://www.staysafeonline.info/appendix_c.adp (10/06/2004)

Recommended Reading

Herbert, Jeff. "Introducing Security to the Small Business Enterprise". 28 April 2003. URL: http://www.sans.org/rr/papers/48/1066.pdf (10/06/2004)

Pierce II, Elton L. "The Value of Risk Assessment - A Case Study". 31 March 2003. URL: http://www.sans.org/rr/papers/9/1035.pdf (10/06/2004)

Straub, Kenneth R. "Information Security Managing Risk with Defense in Depth". 12 August 2003. URL: http://www.sans.org/rr/papers/22/1224.pdf (10/06/2004)

Pholi, Leon. "Security in Practice - Reducing the Effort". April 2003. URL: http://www.sans.org/rr/papers/8/1106.pdf (10/06/2004)

Browne, Doug. "Case Study: A Risk Audit of a Very Small Business". 11 September 2003. URL: http://www.sans.org/rr/papers/9/1243.pdf (10/06/2004)

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS