Appendix D

Protection Checklist for Individuals and Organizations Template

---

Introduction

This appendix has three parts:

Part I: Protection checklist – what individuals can do to protect themselves from cyberthreats and to avoid falling victim to cybercrimes.
Part II: Various types of incident handling checklists and charts for organizations.
Part III: Computer incident reporting – formats and templates for organizations.

Use this appendix with reference to Chapters 1–7, 9 and 11 (Chapter 11 in CD).

Part I: Protection Checklist for Individuals (Cyberthreats and Cybercrimes)

The Internet is a great medium and has transformed over the years into a "cyberspace" where we work, play games, learn, socialize and communicate; we can even attend "virtual" classes. While all this sounds so wonderful, we should remember that the cyberspace and the Internet has also become a harbor for those who use it to lure unsuspecting "netizens" into unlawful behavior and to disseminate inappropriate or illegal material. The term "netizen" is introduced in Section 1.10 of Chapter 1. "Netizen" is someone who spends considerable time online and also has a considerable presence online through websites about the person, through his/her active blog contribution and/or also his/her participation in the online chat rooms. In this section (Part I), security tips are provided to help individuals to protect themselves from becoming a victim of cybercrime.

Cybercrimes are on the rise each year (refer to Chapter 1). Cybercriminals steal good amount of money from victims to plague netizens through various methods and techniques as explained in Chapters 2–5. As explained in Chapter 9, organizations also have considerable threats in the cyberspace. In addition to the security measures explained in Chapters 2–5, the security tips mentioned below explain preventive measures that will help individuals to take care while surfing and/or entering over the Internet.

D.1 Protect Computer Systems

These are a few basic tips to protect personal computer systems, that is, desktops as well as laptops. (Refer to Section 3.12 of Chapter 3 on security measures for laptops.)

Enable "System Boot" Password and "OS Login" Password

The password is the first key to get an entry into the computer system. Enabling these passwords is very essential, especially for laptops while you are traveling, which can act as a first line of defense. Along with these passwords, screen-saver passwords are also required to be enabled and needless to say, the passwords should follow all the norms as explained in Section 4.4.3 of Chapter 4.

Keep the Operating System Up-to-Date

Operating systems (OS) should be updated periodically to fix the vulnerabilities and to stay in tune with technology requirements. This is done by installing OS patches.

Installing OS Patches

There are many OS vulnerabilities. When you install an antivirus program and a firewall, it helps you to make your PC secure. However, hackers can still sneak their way into your PC to exploit vulnerabilities. Vulnerabilities are "holes" that develop in your computer's OS. Vendors/developers of OS react to each vulnerability discovered in their OS by releasing special software updates known as security patches. Such fixes for known software bugs work by replacing a piece of code with a new one that is "repaired" and no longer contains vulnerability. OS patch installation can be handled in an auto (automatic) manner or manually. For example, in the Windows world, the best way to update security patches is to get your computer configured to automatically connect with the latest security patch updates. When new updates are released, your OS will automatically notify you and install the updates. Alternatively, you can go for "manual" update option. Within that you have two choices: (a) express or (b) custom. Make an appropriate choice by consulting technical persons that support your computer.

Install and Always Keep Firewall Turned ON

As mentioned previously, firewall helps to protect the computer system from attackers who might try to gain access to conduct malicious activities such as delete information, crash the computer system or steal passwords and/or other sensitive information. The firewall is prepackaged with some operating systems or should be purchased for personal computers. Firewall software must be updated with patches released by the vendor, to plug the vulnerabilities which may arise due to new techniques developed by the attackers. (Refer to B.1.IX in Appendix B for list of personal firewalls; also see Ref. #1, Books, Further Reading).

Install and/or Update Antivirus Software

Antivirus software is designed to detect and prevent Malicious Code, like a virus or a worm, from embedding on the computer system and/or to disarm or remove it. Antivirus software must be updated with patches released by the vendor to avoid infection by latest Malicious Code released by the attackers. (Refer to Tables B.1.IV and V of Appendix B.)

Install and/or Update Anti-Spyware Software

In Section 4.5.4 of Chapter 4, Spywares and threats from Spywares are mentioned. The attackers install Spyware software without user's knowledge on the computer system to collect sensitive information and/or record the activities on computer such as visited websites, user IDs and passwords. Be wary of the advertisement posted on the websites and/or pop-up while surfing on the Internet about any anti-Spyware, as in some cases such products may be bogus and may actually contain Spyware and/or other Malicious Code. (Refer to Table B.1.VI of Appendix B.)

Be Careful While Downloading Any Artificats from the Internet

Never open an attachment received in an E-Mail from someone you do not know and/or attachments received into "forwards" from people you know. Downloading such E-Mail attachments can circumvent the antivirus and/or anti-Spyware tools by unwittingly advanced Malicious Code. (Refer to Box 9.9 in Chapter 9.) Be especially careful about free music downloads and free movie downloads; chances are there may be viruses/malware/Trojans sitting inside them!

Turn OFF Internet Connection and/or Webcam

With the growth of the Internet, many opt to have high-speed Internet connections at home and leave their computer systems ON and ready for action. In spite of protection aids such as firewall, antivirus and anti-Spyware installed on the computer system, leaving the system always ON with the Internet connection attract the attacker to use the system as a zombie to launch the attacks on the target or else your machine can be targeted to conduct malicious activities.

Internet and E-Mail Systems Safety

Internet and E-Mail systems are the communication medium in this E-World. Appendix C mentions KRESV test for E-Mails with attachments. Following are few basic security measures to be considered with the precaution mentioned in Appendix C.

1. Maintain separate E-Mail accounts for personal and business use.
2. Change the passwords at regular intervals.
3. Do not open E-Mails which have been received from unknown sources.
4. Do not install/download attachments received from unknown sources.
5. Always scan the attachments to check virus/malware before downloading on your system.
6. While storing personal information on your E-Mail account (e.g., biodata, scanned copies of passport, educational certificates) provide file-level password.
7. Always logout from the website before closing the browser window.
8. Ensure the authenticity of website before entering any personal information and provide minimum personal information (i.e., provide only required personal information usually denoted with asterisk as "*" in front of a text box) while registering on any website.
9. Avoid committing any financial transactions from the Internet provided at public places such as cybercafes and holiday resorts, and in case you have to do so due to some emergency, use the virtual keyboard and change the password of transacted accounts as soon as possible from the secured computer system.
10. While installing any freeware/software utilities, ensure the authenticity of the source and the software utility.
11. Always disconnect the Internet connection when not in use and/or not required to be used.

Social Networking Safety

Chapter 7 discusses about security aspects of social networking (see Section 7.14). Social networking sites such as Facebook, Orkut, Myspace, etc. have become inevitable nowadays. Netizens use social networking sites to connect with new friends, to keep in touch with current friends, reconnect with old friends or create real-life friendships through similar interests or groups. Besides establishing important social relationships, social networking members can share their interests with other like-minded members by joining groups and forums. (The readers may want to visit http://social-networking-websites-review.toptenreviews.com/ to know 2011 social networking websites review comparisons.) Following are a few tips on security measures while one is using social networking sites:

1. Date and place of birth: These place you at massive risk of identity theft. They are the most commonly used security questions on password resetting sites.
2. Mother's maiden name: A lot of websites use mother's maiden name to authenticate who you are.
3. Name of your school/college: A lot of websites also use the school or the college you went to as a security question.
4. Address: It again puts you at risk not only from identity fraud, but also from burglars and stalkers.
5. Phone number: You may be bombarded with unsolicited phone calls and/or text messages from people trying to sell you something.
6. Short trips/holidays: There can be a risk of burglary and stalking. If you post the message on Facebook saying: "Can't wait till next week-end – two weeks at hill station at Matheran near Mumbai yeh!" … you are basically saying: "Come and rob me."
7. Photos: There is again again risk of identity theft and photos of your tours, which are uploaded while you are on tour, can be a risk of burglary. (Refer to Box 5.16 of Chapter 5 on Geotagging.)
8. Confessionals: Posting about your personal and/or professional life grievances to your friends/colleagues always provides an opportunity to get the required information by social engineering.
9. Children's names: These can be used for identity theft and moreover present risk from pedophiles. It is much easier to steal a child's identity. (Refer to Section 5.3.2 of Chapter 5 on types of identity theft.)
10. Be cautious while clicking on the URLs that you receive in messages from your friends/relatives on your social website.
11. While choosing your social networking site, evaluate the terms and conditions, especially the privacy policy. It is very important to understand how your personal information will be used and whether the site monitors content that people post.

12. Be careful about installing third-party utilities on your site. Many social networking sites provide the facility of downloading third-party utilities that let you do more with your personal page. Attackers sometimes use these applications to steal your personal information.
13. Be aware that everything you put on a social networking site is permanent. Even if you delete your account, anyone on the Internet, who has already downloaded your information, printed the photos or saved the images and videos on his/her system, already has the details.

Personal privacy is important, therefore, never ever reveal your personal details as mentioned above on social networking sites, which are used for identity theft. To know more on personally identifiable information, refer to Section 5.3.1 of Chapter 5.

Mobile Phones and Portable Gadgets Safety

The concept of mobile phones security is as good as that of protecting computer systems. Internet connectivity and mobile banking is now available on the individual's fingertips through mobile phones. These features are useful and convenient for an individual as a fastest medium of communication; attackers try to exploit these features. (Refer to Section 3.8 of Chapter 3 about attacks on mobile/cell phones.) As a result, an attacker may be able to accomplish the following:

1. Gain access to account information.
2. Utilize your cell phone or available features/services in an attack.
3. Lure an individual to a malicious website.
4. Abuse mobile services.

Chapter 3 explains various attacks on mobile phones, such as Mishing (Mobile + Phishing), mobile theft, mobile viruses and Bluetooth exploitation as well as explains the countermeasures toward these attacks. In addition to it, following are some of the common security measures to be implemented on mobile devices:

1. Install and maintain antivirus software (refer to Table B.1.XIII in Appendix B on mobile security software).
2. Install antitheft software on your mobile (refer to Box 3.6 of Chapter 3 on tips to secure your cell/mobile phone from being stolen/lost).
3. Store important data in a secure place.
4. Encrypt files which contain important and personal data.
5. Back up important data from mobile phones/laptop on CDs/DVDs/pen drives.
6. Ensure periodically that backed-up media is not damaged and the data can be recovered whenever it is required.

Investment Plans and Lottery Schemes Safety

Fraudsters send mail(s) to lure netizens to respond and if he gets the response, it becomes the first positive step for him to fetch the target into his net. Chapter 5 explains such attacks known as Phishing and the discussion details about numerous methods and techniques of Phishing attacks along with countermeasures. Here are a few fundamental security tips to avoid being duped, besides the important fact of ensuring the legitimacy of the E-Mail and/or website before taking any action on it.

1. Be leery when responding to investment offers received through unsolicited E-Mail.
2. If the opportunity (i.e., Investment Plan/Lottery Scheme) appears too good to be true, it probably is not:
   - Beware of promises to make fast profits.
   - Be wary of investments that offer high returns at little or no risk.
   - Be cautious when dealing with individuals outside of your own country.
3. Do not assume that an organization is legitimate on the basis of the "appearance" of the E-Mail and/or website.
4. Do not invest in anything unless you have understood the terms and conditions and/or the complete plan/scheme.
5. Research the parties involved and the nature of the investment.

6. Be cautious if you do not remember entering into any lottery scheme or contest and receive E-Mail/telephone call/SMS stating you are the winner in a lottery.
7. Beware of lotteries that demand to send any amount toward tax/fees prior to delivery of your prize and/or being eligible for future winnings.

Plastic Money Safety

Refer to Chapter 11 (Section 11.4.1) for illustrations about financial crimes. Credit cards and debit cards make purchases of goods and services easy as well as convenient. The Internet and plastic money further enable an individual to shop from anywhere and at anytime. This facility has opened another playground for fraudsters. Chapter 3 explains credit card frauds in mobile and wireless computing era in Section 3.4 along with tips to prevent credit card frauds in Box 3.2. In addition to it, following are a few common security measures to avoid online financial frauds.

1. Ensure who you are doing business with – conduct research.
2. Obtain the name, address and telephone number of the individual or organization.
3. Conduct your research to ensure authenticity of an individual or organization. (Ask for names of other customers of the individual or company and contact them.)
4. Ensure legitimacy of the website before providing your credit card details online.
5. Ensure the secured communication channel, that is, HTTPS in the URL. (Do not trust a website just because it claims to be secure.)
6. While purchasing merchandise, ensure it is from a reputable and legitimate source.
7. Make habit to reconcile credit card statements at frequent time intervals (i.e., fortnightly/monthly) to avoid unauthorized charges.
8. Beware of providing credit card information when requested through unsolicited E-Mails and/or text messages received on mobile phones.
9. Be cautious when dealing with individuals outside of your own country.
10. Ensure that you understand all terms and conditions of any agreement.
11. Be skeptical about the businesses that operate from P.O. boxes or mail drops.
12. When the deal sounds too good to be true, it probably is not.

Parental Guidelines: Child Safety

Chapter 1 explains Children's Online Privacy Protection Act (COPPA). The advancement of technology and immediate availability of electronic gadgets requires the "grooming" of youngsters, especially children (below 15 years), about cybersecurity, which is very essential in this century. Chapter 2 explains cyberbullying – a common threat to innocent people like children. Threats, harassment and psychological torment via E-Mail or in a virtual chat room or through SMS can have a devastating effect on a child. Here are a few guidelines for parents for their child safety while the children are surfing over the Internet.

1. Spend some time with your kid every day to understand about the websites visited and E-Mail that has been exchanged.
2. Create awareness among children that they should disclose personal information as minimum as possible while on the Internet.
3. While opening an E-Mail account, User ID and password should be shared with the parents. Parents can monitor during initial days and
   - Get an understanding from whom they are receiving the mails and what is the nature of these mails.
   - Ensure that the kids are not doing anything which they are not supposed to do.
   - User ID and password are the keys to login to the E-Mail accounts, websites; hence should NOT be shared (other than parents) with anyone.
4. Parents should insist to their kids about taking their permission before visiting any blog or before joining a social networking site (such as MySpace, Orkut or Facebook).
5. The kids should always consult their parents before logging into new blogs/websites/chat rooms.
6. The kids should always consult with their parents before downloading any pictures, audio/video clippings, games, utilities available at "free of cost."

7. Parent may install "Parent Control Software" (Refer to Table B.1.XII of Appendix B) on the computer system, which provides the facility to block the access to certain types of websites or to log the child's Internet activity.
8. Check and verify the history of websites regularly visited by your kid. If the history has been deleted, question your child.

It is important to note few websites (mentioned below), which publish cybersecurity guidelines. Netizens should make a habit to visit these websites frequently to get updates about new threats and security measures to be followed to avoid being a victim of cybercrime.

1. www.b4usurf.org
2. www.getsafeonline.org
3. www.staysafeonline.org
4. www.lookstoogoodtobetrue.com
5. www.online-tech-tips.com
6. www.onguardonline.gov
7. www.surfnetparents.com
8. www.safefamilies.org
9. www.lovingyourchild.com

Part II: Incident Handling Checklist and Templates for Organizations

Importance of "Incident Response Management" and "Incident Handling" are explained in Chapter 9 from organization's perspective. Refer to Section 9.9.8 (Checklists) of Chapter 9; a number of checklists are mentioned there. In this section of the appendix, those checklists are provided. While using them you may need to do some tailoring depending on the specific usage context in your organization. While going through each of the checklists presented below, keep in mind the discussion in Section 9.9.1 and Fig. 9.11. Table 9.4 in Chapter 9 should also be kept in mind while using the following checklists.

Checklists/tables presented in this section are listed below for a glance:

1. Table D.II.1: Checklist for initial handling of incident.
2. Table D.II.2: Generic checklist for incident handling.
3. Table D.II.3: Checklist for handling DoS incident.
4. Table D.II.4: DoS troubleshooting chart (precursors and indicators).
5. Table D.II.5: Chart of Malicious Code indications.
6. Table D.II.6: Unauthorized access troubleshooting chart (precursors and indicators).
7. Table D.II.7: Preventing unauthorized access incidents – actions to be taken.
8. Table D.II.8: Checklist for handling unauthorized access.
9. Table D.II.9: Checklist for handling Malicious Code incident.
10. Table D.II.10: Chart of inappropriate usage indications.
11. Table D.II.11: Checklist for handling inappropriate usage incident.
12. Table D.II.12: Checklist for handling multiple component incidents.
13. Table D.II.13: Checklist for critical review of log.

The first checklist presented in Table D.II.1 is about initial handling of an incident and the one after that in Table D.II.2 is a generic one. The remaining checklists/charts are presented one after the other.

Table D.II.1 Checklist for initial handling of incident

Action	*Completed (yes/no)*
Detection and Analysis	
1. Determine whether an incident has occurred: • Analyze the precursors and indications. • Look for corroborating information. • Carry out research. • As soon as it is believed that an incident has occurred, begin documenting the investigation and start gathering evidence.	
2. Classify the incident using a suitable incident classification scheme (e.g., denial of service, Malicious Code, unauthorized access, inappropriate usage, multiple component). *Note:* You can refer to the incident classification scheme presented in Section 9.9.1 in Chapter 9.	
3. Follow the appropriate incident category checklist – if the incident does not fit into any of the categories, follow the generic checklist.	

Table D.II.2 Generic checklist for incident handling

Action	*Completed (yes/no)*
Detection and Analysis	
1. Prioritize handling the incident based on the business impact: • Identify which resources have been affected and forecast which resources will be affected. • Estimate the current and potential technical effect of the incident. • Find the appropriate cell(s) in the prioritization matrix based on the technical effect and affected resources. *Note:* Refer to the guidance provided in Section 9.9.1 in Chapter 9 (generally accepted scheme used in industry for priority levels for risks arising from incidents).	
2. Report the incident to the appropriate internal personnel and external organizations. *Note:* For example, see Table 9.5 in Chapter 9.	
Containment, Eradication and Recovery	
3. Acquire, preserve, secure and document evidence. *Note:* Remember the chain of custody concept explained in Chapter 7.	
4. Contain the incident. *Note:* Recall Table 9.4 and Fig. 9.16 in Chapter 9.	
5. Eradicate the incident. • Identify and mitigate all vulnerabilities that were exploited.	

- Remove Malicious Code, inappropriate materials and other components.

6. Recover from the incident

- Return affected systems to an operationally ready state.
- Confirm that the affected systems are functioning normally.
- If necessary, implement additional monitoring to look for future-related activity.

Post-Incident Activity

7. Prepare a follow-up report.

8. Hold a "lessons learned" meeting.

Denial-of-service (DoS) attack and Distributed-Denial-of-service attack (DDoS) both are mentioned in Chapter 2 and explained in Chapter 4. The checklist in Table D.II.3 is to be used with reference to incidents regarding these attacks.

Table D.II.3 Checklist for handling DoS incident

Action	*Completed (yes/no)*
Detection and Analysis	
1. Prioritize handling the incident based on the business impact. *Note:* Refer to the guidance provided in Section 9.9.1 in Chapter 9 (generally accepted scheme used in industry for priority levels for risks arising from incidents). **1.1** Identify which resources have been affected and forecast which resources will be affected. **1.2** Estimate the current and potential technical effect of the incident. **1.3** Find the appropriate cell(s) in the prioritization matrix based on the technical effect and affected resources. *Note:* For example, see Table 9.5 Diagnostic matrix example in Chapter 9.	
2. Report the incident to the appropriate internal personnel and external organizations.	
Containment, Eradication and Recovery	
3. Acquire, preserve, secure and document evidence. *Note:* Remember the chain of custody concept explained in Chapter 7.	
4. Contain the incident – halt the DoS if it has not already stopped. *Note:* Recall Table 9.4 and Fig. 9.16 in Chapter 9. **4.1** Identify and mitigate all vulnerabilities that were used. **4.2** If not yet contained, implement filtering based on the characteristics of the attack, if feasible.	

4.3 If not yet contained, contact the ISP for assistance in filtering the attack.
4.4 If not yet contained, relocate the target.

5. Eradicate the incident; if Step 4.1 was not performed, identify and mitigate all vulnerabilities that were used.

6. Recover from the incident.

6.1 Return affected systems to an operationally ready state.
6.2 Confirm that the affected systems are functioning normally.
6.3 If necessary and feasible, implement additional monitoring to look for future-related activity.

Post-Incident Activity

7. Prepare a follow-up report.

8. Hold a "lessons learned" meeting.

The small chart presented in Table D.II.4 explains how troubleshooting is useful in case of DoS attacks explained in Chapters 2 (Section 2.2.1) and 4 – keep that discussion in mind while using the chart. For technical background and greater discussion, readers should refer to Ref. #7, Books, Further Reading.

Table D.II.4 DoS troubleshooting chart (precursors and indicators)

Precursor to DoS Attack	***Possible Response***
DoS attacks are often preceded by *reconnaissance activity* – generally, a low volume of the traffic that will be used in the actual attack to determine which attacks may be effective. Examine new tool and, if possible, modify security controls so that the tool should not be successful against the organization.	If handlers detect unusual activity that appears to be preparation for a DoS attack, the organization may be able to block the attack by quickly changing its security stance, for example, changing firewall rules to block a particular protocol from being used or protect a vulnerable host.
Security Threat	***Possible Indications***
Network-based DoS against a network.	• Unavailability of system and network is reported by users. • Network connection losses that cannot be explained. • Network intrusion detection alerts. • Increased network bandwidth utilization. • Asymmetric network traffic pattern (large amount of traffic entering the network, little traffic leaving the network). • Firewall and router log entries. • Packets with unusual source addresses. • Packets with non-existent destination addresses.
DoS against the operating system of a particular host.	• Unavailability of system and application reported by users. • Network and host intrusion detection alerts. • Operating system log entries. • Packets with unusual source addresses.
DoS against an application on a particular host.	• Application unavailability reported by users.

	• Network and host intrusion detection alerts. • Application log entries. • Packets with unusual source addresses.

The topic of "Malicious Code" is mentioned in Chapters 1 and 2. The checklists and charts presented in Table D.II.5 are in that context.

Table D.II.5 Chart of Malicious Code indications

Malicious Action Noted	***Possible Indications***
An E-Mail-based virus infects a host.	• Antivirus software alerts of infected files. • Unexpected increase in the number of E-Mails being sent and received. • Changes to templates for word processing documents, spreadsheets, etc. • Deleted, corrupted or inaccessible files. • Strange items on the screen, such as odd messages and graphics. • Programs start slowly, run slowly or do not run at all. • System instability and crashes. *Note:* If the virus achieves root-level access, see the indications for "root compromise of a host" presented in Table D.II.6.
A worm that spreads through a vulnerable service infects a host.	• Antivirus software alerts of infected files. • Port scans and failed connection targeted attempts at the vulnerable service (e.g., open Windows shares, HTTP). • Increased network usage. • Programs start slowly, run slowly or do not run at all. • System instability and crashes. *Note:* If the worm achieves root-level access, see the indications for "root compromise of a host" presented in Table D.II.6.
A Trojan Horse is installed and running on a host.	• Antivirus software alerts of Trojan Horse versions of files. • Network intrusion detection alerts of Trojan Horse client–server communications. • Firewall and router log entries for Trojan Horse client–server communications. • Network connections between the host and unknown remote systems. • Unusual and unexpected ports open. • Unknown processes running. • High amounts of network traffic generated by the host, particularly if directed at external host(s). • Programs start slowly, run slowly or do not run at all. • System instability and crashes.

	Note: If the Trojan Horse achieves root-level access, see the indications for "root compromise of a host" presented in Table D.II.6.
Malicious mobile code on a website is used to infect a host with a virus, worm or Trojan Horse.	• Indications listed above for the pertinent type of Malicious Code. • Unexpected dialog boxes requesting permission to do something. • Unusual graphics such as overlapping or overlaid message boxes.
Malicious mobile code on a website exploits vulnerabilities on a host.	• Unexpected dialog boxes requesting permission to do something. • Unusual graphics such as overlapping or overlaid message boxes. • Sudden increase in the number of E-Mails being sent and received. • Network connections between the host and unknown remote systems. *Note:* If the mobile code achieves root-level access, see the indications for "root compromise of a host" presented in Table D.II.6.
A user receives a virus hoax message.	• Original source of the message is not an authoritative computer security group, but a government agency or an important official person. • No links to outside sources. • Tone and terminology attempt to invoke panic or a sense of urgency. • Urges recipients to delete certain files and forward the message to others.

The causes of most of the indications mentioned in Table D.II.5 could be other than malware. For example, a web server could crash because of a non-malware attack, an OS fault or a power disruption among other reasons. These complications exemplify the challenges involved in detecting and validating a malware incident, and the need to have well-trained, technically knowledgeable incident handlers who can carry out analysis quickly to determine what has happened.

It is explained in Chapter 1 that unauthorized access is a cybercrime. Chapters 2 and 4 also have discussions about unauthorized access. The charts in Tables D.II.6 and D.II.7 are to be used in the context of unauthorized access.

Table D.II.6 Unauthorized access troubleshooting chart (precursors and indicators)

Precursor to Unauthorized Access	***Possible Response***
Unauthorized access incidents are frequently preceded by reconnaissance activity to map hosts and services and to identify vulnerabilities. Activity may include port scans, host scans, vulnerability scans, pings, traceroutes, DNS zone transfers, OS fingerprinting and banner grabbing. Such activity is detected primarily through IDPS software, secondarily through log analysis.	Incident handlers should look for discrete changes in reconnaissance patterns – for example, an unexpected interest in a particular port number or host. If this activity points out a vulnerability that could be exploited, the organization may have time to block future attacks by mitigating the vulnerability (e.g., patching a host, disabling an unused service and modifying firewall rules).

Note: Readers can refer to Table 35.2 (Vulnerability scanning tools) in Ref. #7, Books, Further Reading.	
A new exploit for gaining unauthorized access is released publicly, and it poses a significant threat to the organization.	The organization should look into the new exploit and, if possible, change security controls to decrease the potential impact of the exploit for the organization.
Users report possible *social engineering* attempts – attackers trying to trap them into revealing sensitive information, such as passwords, or encouraging them to download or run programs and file attachments. *Note:* Recall the discussion in Chapters 2 (Section 2.3), 4 and 5 about "social engineering."	The incident response team should send a bulletin to users with advice on handling the social engineering attempts. The team should determine what resources the attacker was interested in and look for corresponding log-based precursors because it is likely that the social engineering is only part of the reconnaissance.
A person or system may study a failed physical access attempt (e.g., outsider attempting to open a locked wiring closet door or unidentified person using a cancelled ID badge).	When feasible, security should control the person. The intention of the activity should be established, and it should be confirmed that the physical and computer security controls are adequately strong to block the noticeable threat. (An attacker who cannot gain physical access may perform distant computing-based attacks instead.) Physical and computer security controls should be fortified if necessary.

Malicious Action	***Possible Indications***
Root compromise of a host	• Existence of unauthorized security-related tools or exploits. • Unusual traffic to and from the host (e.g., attacker may use the host to attack other systems). • Changes in system configuration including: **a.** Process/service modifications or additions. **b.** Unexpected open ports. **c.** System status changes (restarts and shutdowns). **d.** Changes to log and audit policies and data. **e.** Network interface card set to promiscuous mode (packet sniffing). **f.** New administrative-level user account or group. • Modifications of critical files, timestamps and privileges, including executable programs, OS kernels, system libraries, and configuration and data files. • Unexplained account usage (e.g., idle account in use, account in use from multiple locations at once, unexpected commands from a particular user, large number of locked-out accounts).

	• Significant changes in expected resource usage (e.g., CPU, network activity, full logs or file systems). • User reports of system unavailability. • Network and host intrusion detection alerts. • New files or directories with unusual names (e.g., binary characters, leading spaces, leading dots). • Highly unusual operating system and application log messages. • Attacker contacts the organization to say that he/she has compromised a host.
Unauthorized data modification (e.g., web server defacement, FTP warez server). *Note:* A "warez server" is a file server that is used to distribute illegal content. Originally, *warez* referred to pirated software, but the term now also includes other illegal content such as copies of copyrighted songs and movies. Attackers often exploit vulnerabilities in FTP servers to gain unauthorized access so that they can use the server to distribute their warez files.	• Network and host intrusion detection alerts. • Increased resource utilization. • User reports of the data modification (e.g., defaced website). • Modifications to critical files (e.g., webpages). • New files or directories with unusual names (e.g., binary characters, leading spaces, leading dots). • Significant changes in expected resource usage (e.g., CPU, network activity, full logs or file systems).
Unauthorized usage of standard user account.	• Access attempts to critical files (e.g., password files). • Unexplained account usage (e.g., idle account in use, account in use from multiple locations at once, commands that are unexpected from a particular user, large number of locked-out accounts). • Web proxy log entries showing the download of attacker tools.
Physical intruder	• User reports of network or system unavailability. • System status changes (restarts and shutdowns). • Hardware is completely or partially missing (i.e., a system was opened and a particular component removed). · Unauthorized new hardware (e.g., attacker connects a packet sniffing laptop to a network or a modem to a host).
Unauthorized data access (e.g., database of customer information and password files).	• Intrusion detection alerts of attempts to gain access to the data through FTP, HTTP and other protocols. • Host-recorded access attempts to critical files.

Table D.II.7 Preventing unauthorized access incidents – actions to take

Incident Category	*Actions Recommended*
Network security	• Configure the network perimeter to reject all incoming traffic that is not expressly permitted. • Properly secure all remote access methods, including modems and VPNs (virtual private networks). An unsecured modem can easily provide attainable unauthorized access to internal systems and networks. War dialing is the most efficient technique for identifying improperly secured modems. When securing remote access, carefully consider the trustworthiness of the clients; if they are outside the organization's control, they should be given as little access to resources as possible, and their actions should be closely monitored. *Note: War dialing* is the process of dialing blocks of phone numbers to identify modems that are listening, then attempting to gain access to the host to which the modem is connected. Although the prevalence of modems has greatly decreased from its peak, many organizations still use modems for certain functions. • Put all publicly accessible services on secured demilitarized zone (DMZ) network segments. The network perimeter can then be configured so that external hosts can establish connections only to hosts on the DMZ and not to internal network segments. • Use private IP addresses for all hosts on internal networks. This will restrict the ability of attackers to establish direct connections to internal hosts.
Host security	• Perform regular vulnerability assessments to identify serious risks and mitigate the risks to an acceptable level. • Disable all unwanted services on hosts. Separate critical services so that they run on different hosts. If an attacker then compromises a host, immediate access should be gained only to a single service. • Run services with the least privileges possible to reduce the immediate impact of successful exploits. • Use host-based/personal firewall software to limit individual hosts' exposure to attacks. • Limit unauthorized physical access to logged-in systems by requiring hosts to lock idle screens automatically and asking users to log off before leaving the office.

	• Regularly verify the permission settings for critical resources, including password files, sensitive databases and public webpages. This process can be easily automated to report changes in permissions on a regular basis.
Authentication and authorization	• Create a password policy that requires the use of complex, difficult-to-guess passwords, forbids password sharing and directs users to use different passwords on different systems, especially external hosts and applications. • Implement sufficiently strong authentication, particularly for accessing critical resources. • Create authentication and authorization standards for employees and contractors to follow when evaluating or developing software. For example, passwords should be strongly encrypted. • Establish procedures for enabling and disabling user accounts. These should include an approval process for new account requests and a process for periodically disabling or deleting accounts that are no longer needed.
Physical Security	• Implement physical security measures that restrict access to critical resources. *Note:* For a detailed discussion on the topic of "Physical Security" readers should refer to Refs. #3 and #4 in Books, Further Reading.

While using the checklist presented in Table D.II.8, keep in mind Tables D.II.6 and D.II.7.

Table D.II.8 Checklist for handling unauthorized access

Action	***Completed (yes/no)***
Detection and Analysis	
1. Prioritize handling the incident based on the business impact. • Identify which resources have been affected and forecast which resources will be affected. • Estimate the current and potential technical effect of the incident. • Find the appropriate cell(s) in the prioritization matrix based on the technical effect and affected resources.	

Note: Refer to the guidance provided in Section 9.9.1 in Chapter 9 (generally accepted scheme used in industry for priority levels for risks arising from incidents).

2. Report the incident to the appropriate internal personnel and external organizations.
Note: For example, see Table 9.5 Diagnostic matrix example in Chapter 9.

Containment, Eradication and Recovery

3. Perform an initial containment of the incident.

4. Acquire, preserve, secure and document evidence.

Note: Remember the chain of custody concept explained in Chapter 7.

5. Confirm the containment of the incident.

- Further analyze the incident and determine if containment was sufficient (including checking other systems for signs of intrusion).
- Implement additional containment measures if necessary.

Note: Recall Table 9.4 and Fig. 9.16 in Chapter 9.

6. Eradicate the incident.

- Identify and mitigate all vulnerabilities that were exploited.
- Remove components of the incident from systems.

7. Recover from the incident

- Return affected systems to an operationally ready state.
- Confirm that the affected systems are functioning normally.
- If necessary and feasible, implement additional monitoring to look for future-related activity.

Post-Incident Activity

8. Prepare a follow-up report.

9. Hold a "lessons learned" meeting.

Table D.II.9 presents a checklist for handling a security incident related to Malicious Code. The topic of "Malicious Code" is mentioned in Chapters 1 and 2.

Table D.II.9 Checklist for handling Malicious Code incident

	Action	*Completed (yes/no)*
	Detection and Analysis	
1.	Prioritize handling the incident based on the business impact. • Identify which resources have been affected and forecast which resources will be affected. • Estimate the current and potential technical effect of the incident. • Find the appropriate cell(s) in the prioritization matrix based on the technical effect and affected resources. *Note:* Refer to the guidance provided in Section 9.9.1 in Chapter 9 (generally accepted scheme used in industry for priority levels for risks arising from incidents).	
2.	Report the incident to the appropriate internal personnel and external organizations. *Note:* For example, refer to diagnostic matrix example in Table 9.5 in Chapter 9.	
	Containment, Eradication and Recovery	
3.	Contain the incident. • Identify infected systems. • Disconnect infected systems from the network. • Mitigate vulnerabilities that were exploited by the Malicious Code. If necessary, block the transmission mechanisms for the Malicious Code.	
4.	Eradicate the incident. • Disinfect, quarantine, delete and replace infected files. • Mitigate the exploited vulnerabilities for other hosts within the organization.	
5.	Recover from the incident. • Confirm that the affected systems are functioning normally. • If necessary, implement additional monitoring to look for future-related activity.	
	Post-Incident Activity	
6.	Prepare a follow-up report.	
7.	Hold a "lessons learned" meeting.	

Recall the discussion in Chapter 9 Internet usage and safe computing guidelines, computer usage policy (Section 9.8). The chart presented in Table D.II.10 is with that reference. Also keep in mind the discussion about "Spam" in the chapters of this book.

Table D.II.10 Chart of inappropriate usage indications

Inappropriate Action	*Possible Indications*
Unauthorized service usage (e.g., web server, file sharing and music sharing). *Note:* Recall the discussion in Chapter 3 regarding use of mobile devices for music.	• Network intrusion detection and network behavior analysis software alerts. *Note:* Readers can refer to Ref. #5, Books, Further Reading. • Unusual traffic to and from the host. • New process/software installed and running on a host. • New files or directories with unusual names (e.g., "warez" server style names). *Note:* A "warez server" is a file server that is used to distribute illegal content. Originally, "warez" referred to pirated software, but the term now also includes other illegal content such as copies of copyrighted songs and movies. Attackers often exploit vulnerabilities in FTP servers to gain unauthorized access so that they can use the server to distribute their warez files. • Increased resource utilization (e.g., CPU, file storage, network activity). • User reports. • Application log entries (e.g., web proxies, FTP servers and E-Mail servers).
Access to inappropriate materials (e.g., downloading pornography and sending Spam). *Note:* Recall the discussion about COPPA in Chapters 1 and 6. Attack against external party.	• Network intrusion detection alerts. • User reports. • Application log entries (e.g., web proxies, FTP servers and E-Mail servers). • Inappropriate files on workstations, servers or removable media. • Network intrusion detection alerts. • Outside party reports. • Network, host and application log entries. *Note:* Examples of indications include E-Mail server log entries of bounced E-Mails with forged source addresses and firewall log entries of TCP RST packets that do not have a corresponding SYN (i.e., backscatter from spoofed packets).

In Chapter 9 we discussed cybersecurity threats to organizations. It was mentioned there that one of the threats comes from inappropriate usage of computing resources (refer to Tables 9.2 and 9.5 in Chapter 9). The checklist presented in Table D.II.11 is to be used in that context. Note that this checklist is referred to as one of the listed items in Section 9.9.8 (Checklists) in Chapter 9.

Table D.II.11 Checklist for handling inappropriate usage incident

	Action	*Completed (yes/no)*
	Detection and Analysis	
1.	Prioritize handling the incident based on the business impact. • Determine whether the activity seems criminal in nature. • Forecast how severely the organization's reputation may be damaged. • Find the appropriate cell(s) in the prioritization matrix based on the technical effect and affected resources. *Note:* Refer to the guidance provided in Section 9.9.1 in Chapter 9 (generally accepted scheme used in industry for priority levels for risks arising from incidents).	
2.	Report the incident to the appropriate internal personnel and external organizations. *Note:* For example, refer to diagnostic matrix example in Table 9.5 in Chapter 9.	
	Containment, Eradication and Recovery	
3.	Acquire, preserve, secure and document evidence. *Note:* Remember the chain of custody concept explained in Chapter 7.	
4.	If necessary, contain and eradicate the incident (e.g., remove inappropriate materials).	
	Post-Incident Activity	
5.	Prepare a follow-up report**.**	
6.	Hold a "lessons learned" meeting.	

A *multiple component incident* is a single incident that encompasses two or more incidents. Figure D.1 illustrates an example of the steps that could comprise a multiple component incident:

1. Malicious Code spread through E-Mail compromises an internal workstation. Remember that it was mentioned in Chapter 2 that E-Mail attachments are used to send Malicious Code to a victim's system, which will automatically get executed.
2. An attacker (who may or may not be the one who sent the Malicious Code) uses the infected workstation to compromise additional workstations and servers.
3. An attacker (who may or may not have been involved in Steps 1 or 2 shown in Fig. D.1) uses one of the compromised hosts to launch a DDoS attack against another organization.

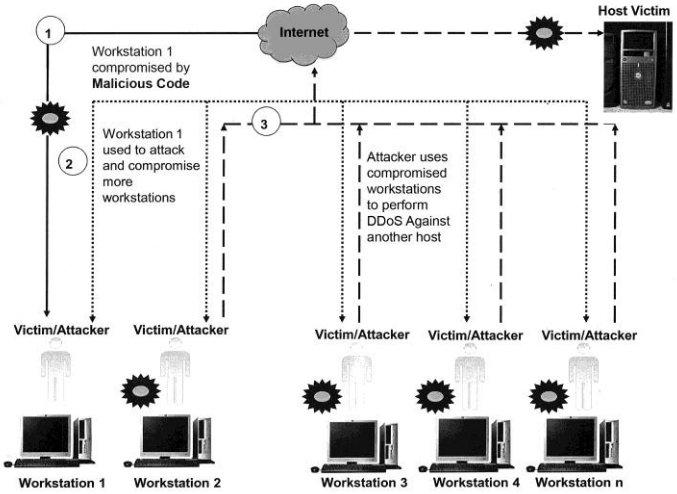

Figure D.1 Multiple component incidents (an example).

The checklist presented in Table D.II.12 is one of listed items in Section 9.9.8 (Checklists) in Chapter 9.

Table D.II.12 Checklist for handling multiple component incidents

Action	*Completed (yes/no)*
Detection and Analysis	
1. Prioritize handling of the incident based on the business impact. • Decide the risk level applicable for each incident category. • Determine the proper course of action for each incident component. *Note:* Refer to the guidance provided in Section 9.9.1 in Chapter 9 (generally accepted scheme used in industry for priority levels for risks arising from incidents).	
2. Report the incident to the appropriate internal personnel and external organizations.	
Containment, Eradication and Recovery	
3. Follow the containment, eradication and recovery steps for each component based on the results of risk analysis.	
Post-Incident Activity	
4. Prepare a follow-up report. **5.** Hold a "lessons learned" meeting.	

The list provided in Table D.II.13 can be used as a critical log review checklist for security incidents.

Table D.II.13 Checklist for critical review of log

Areas of Critical Inspection	*What to Focus on (Examples)*
General approach to prepare for the review is as follows: **1.** Identify which log sources and automated tools you can use during the analysis. **2.** Copy log records to a single location where you will be able to review them. **3.** Minimize "noise" by removing routine and repetitive log entries from view after confirming that they are benign. **4.** Establish whether you can rely on logs' timestamps, consider time zone differences. **5.** Focus on recent changes, failures, errors, status changes, access and administration events, and other events unusual for your environment. **6.** Retrospect in time from now to reconstruct actions after and before the incident. **7.** Correlate activities across different logs to get a comprehensive picture. **8.** Develop hypotheses about what has gone wrong; explore logs to confirm or disprove those hypotheses.	NA
Looking for potential sources of security log **1.** Server and workstation operating system logs. **2.** Application logs (e.g., web server and database server). **3.** Security tool logs (e.g., antivirus, change detection, intrusion detection/prevention system). **4.** Outbound proxy logs and end-user application logs. **5.** Also consider other, non-log sources for security events.	NA
Looking for typical sources of logs **1.** Server and workstation operating system logs. **2.** Application logs (e.g., web server, database server). **3.** Security tool logs (e.g., antivirus, change detection, intrusion detection/prevention system. **4.** Outbound proxy logs and end-user application logs. **5.** Also consider other, non-log sources for security events.	
Looking for typical locations of the logs **1.** Linux OS and core applications: /var/log	

2. Windows OS and core applications: Windows
3. Event Log (Security, System and Application)
4. Network devices: usually logged via Syslog; some use proprietary locations and formats

Linux – What to look for?

1.	Successful user login.	• Accepted password • Accepted public key • Session opened
2.	Failed user login.	• Authentication failure • Failed password
3.	User log-off.	• Session closed
4.	User account change or deletion.	• Password changed • New user • Delete user
5.	Sudo actions.	"sudo: … COMMAND=…" "FAILED su"
6.	Service failure.	"failed" or "failure"

Windows – What to look for?

Event IDs are listed below for Windows 2000/XP. For Vista/7 security event ID, add 4096 to the event ID.

Most of the events below are in the security log; many are only logged on the domain controller.

1.	User logon/logoff events.	Successful logon 528, 540; failed logon 529-537, 539; logoff 538, 551, etc.
2.	User account changes.	Created 624; enabled 626; changed 642; disabled 629; deleted 630
3.	Password changes.	To self: 628; to others: 627
4.	Service started or stopped.	7035, 7036, etc.
5.	Object access denied (if auditing enabled).	560, 567, etc.

Network devices – What to look for?

1. Look at both inbound and outbound activities.

Examples below show log excerpts from Cisco ASA logs; other devices have similar functionality.

1.	Traffic allowed on firewall.	"Built … connection," "access-list … permitted"

2.	Traffic blocked on firewall	"access-list … denied," "deny inbound"; "Deny … by"
3.	Bytes transferred (large files?).	"Teardown TCP connection … duration … bytes … "
4.	Bandwidth and protocol usage.	"limit … exceeded," "CPU utilization,"
5.	Detected attack activity.	"attack from"
6.	User account changes	"user added," "user deleted," "User priv level changed"
7.	Administrator access	"AAA user …," "User … locked out," "login failed"

Web servers – what to look for?

1.	Excessive access attempts to non-existent files.	
2.	Code (SQL, HTML) seen as part of the URL.	
3.	Access to extensions you have not implemented.	
4.	Web service stopped/started/failed messages.	
5.	Access to "risky" pages that accept user input.	
6.	Review logs on all servers in the load balancer pool.	
7.	Error code 200 on files that are not yours.	
8.	Failed user authentication.	Error code 401, 403
9.	Invalid request.	Error code 400
10.	Internal server error.	Error code 500

Other resources to consider

1. Windows event ID lookup: www.eventid.net
2. A listing of many Windows Security Log events: ultimatewindowssecurity.com/.../Default.aspx
3. Log analysis references: www.loganalysis.org
4. A list of open-source log analysis tools: securitywarriorconsulting.com/logtools.
5. Log management blogs published on the Web.
6. Security incident response-related cheat sheets.

Part III: Computer Incident Reporting – Formats and Templates for Organizations

Presented below are the last artifacts of this appendix. Table D.III.1 is a suggested form for reporting a security incident. There are two possible definitions for an incident such as:

1. The act of violating an explicit or implied security policy.
2. An adverse event in an information system, and/or network, or the threat of the occurrence of such an event.

The format presented below is only indicative – you can modify it to suit your needs based on your context. Recall the incident classification mentioned in Section 9.9 in Chapter 9 while using the form from Tables D.III.1 and D.III.2 (which is an alternate for the form below).

Table D.III.1 Form for reporting computer security incident

Computer Incident Reporting Form

Use this form for reporting security incidents to Security Officer
Status (tick what is applicable)
Attack on website □ Past incident □
Repeated incidents □ Unresolved □

_____

Contract information
Name of Organization/Business Unit/Department/ Function name

_____

Name
First _____ Last _____ Middle _____

Title/Designation _____

E-Mail ID _____ Phone _____

Location(s)/Site(s) _____

_____

Type of Incident
DoS □ Unauthorized access (i.e., intrusion/hack) □
Website defacement □
Malicious Code (e.g., virus/worm or Trojan) □
Threat/Harassment via electronic medium □
Misuse of system(s) □
Others, please specify □

_____

Date/Time of Incident Recovery

Date _____ Time _____

Duration of Incident _____ (Days/Hrs/Min)

How did you detect the Incident _____

Has the incident been resolved? Yes □ No □
Brief narration/explanation of resolution

_____

_____

Who have been notified about the Incident (check as applicable)
Systems Administrator □

Department/Business Unit Director	□
HR function	□
Central security function of the organization	□
Law enforcement agency (depending on the level)	□
Other (please specify)	□

_____

Impact of Incident

Loss/compromise of data	□
System downtime	□
System damage (internal systems)	□
Damage of external organization's system(s)	□
Damage to integrity of information systems	□

Incident severity (including financial loss and/or infrastructure damage)

High (defaced websites)	□
Medium (Trojan detected)	□
Low (small virus outbreak)	□
Unknown	□

Privacy impact (depending on level of data sensitivity)

High	□	Medium	□
Low	□	Unknown	□

Computer OS and any other software involved

_____

Actions taken to respond to Incident (check all applicable)

No action taken; system disconnected from network	□
Restored data from backup	□
Updated virus definitions and scanned hard drives	□
Log files examined	□
Physically secured the system	□
Others	□

The template presented in Table D.III.2 is an alternate one to that presented in Table D.III.1. Recall the incident classification mentioned in Section 9.9 of Chapter 9 while using the form below and the next which is an alternate for the form below.

Table D.III.2 Incidence report template

Incident Reporting Template

Use this template for internal reporting within organization

Incident Number (to be linked to Incident Tracker) _____

Brief description of the incident

_____

Location/building impacted (brief description)

_____

Status (tick what is applicable)

Denial of service	□	Malicious Code/virus	□
Information Leakage	□	Data theft	□

Theft of physical asset □ Any other (please specify)
_____
_____

Vulnerability (describe in brief)
_____
_____

Attacker's motive (if known)
_____

Incident impact (preliminary assessment – tick as applicable)
A. Internal impact
Financial □
HR □
B. External impact effect on customer □
Effect on brand image □

_____

Incident Reporting Details
Date when incident occurred (dd/mm/yyyy) _____
Date when incident reported (dd/mm/yyyy) _____
Incident reported by (person name, designation, contact numbers)
_____
Incident reported to (person name, designation, contact numbers)
_____
Other entities contacted
_____
Organization's internal entities involved
_____

_____

Investigation related
A. Tools used for investigation
1. _____ 2. _____
3. _____ 4. _____
B. Investigation Team
Team lead name _____
Team member names _____
Time spent on the investigation (Hrs/Days/Months) _____
_____

Additional information on the incident
Is this a repeat incident? Yes □ No □
Is Media involved? Yes □ No □
Is there a possibility of occurrence in other locations?
Yes □ No □
Does the incident involved contractual violation impacting work with client?
Yes □ No □
_____
Details of personnel interviewed in connection with the incident
Name: Last _____ Middle _____ First _____
Position/Title _____
Employee ID _____
Reporting to _____
_____

Summary
Action taken (brief description)
_____
_____
Recommendation(s) _____

_____

Incident Summary (What, When, Where, Who, How, etc.)

Investigation Summary (for briefing to management)

_____

Remember that incident reporting is very important from analysis and prevention perspective. Readers can revisit Chapter 9 if not already perused before visiting this appendix.

Further Reading

Additional Useful Web References

1. To understand about operating system updates and patches for computer safety, visit the link at: http://www.cumc.columbia.edu/it/getting_started/os.html (2 February 2011).
2. To understand about updating your operating system with security patches, visit: link http://www.spamlaws.com/updating-security-patches.html (2 February 2011).
3. Patch management FAQs can be visited at: http://www.tcnj.edu/~it/security/patchmanagement.html (2 February 2011).

Books

1. Godbole, N. (2009) Chapter 15 (Firewalls for Network Protection), *Information Systems Security: Security anagement, Metrics, Frameworks and Best Practices*, Wiley India, New Delhi.
2. ibid, Chapter 3 (Security Considerations in Mobile and Wireless Computing).
3. ibid, Chapters 7(Overview of Physical Security for Information System).
4. ibid, Chapter 8 (Perimeter Security for Physical Protection).
5. ibid, Chapter 14 (Intrusion Detection for Securing the Networks).
6. ibid, Chapter 21 (Security of Operating Systems).
7. ibid, Chapter 35 (Auditing for Security) Section 35.9 (Technology-based Audits: Vulnerability Scanning and Penetration Testing).