# Module Guide

| | | | |
|---|---|---|---|
| **Faculty** | Information Technology | | |
| **Module Code** | ITSC311 | **Module Name** | Social Practices and Security |
| **NQF Level** | 7 | **Credit Value** | 15 |
| **Semester** | 1/2020 | **Year Level** | 3 |
| **Module Leader** | Dr Timothy Adeliyi | **Copy Editor** | Mr Kevin Levy |
| **Lecturing Hours** | 56 (04 hours a week) | **Tutorial Hours** | N/A |
| **Notional Hours** | 150 | **Pre-Requisites** | ITNT211 |

The module guide must be read in conjunction with the prescribed textbook. This document will be the first port of call to understanding what will be assessed and which assessments form part of the module.

The purpose of the module guide is to highlight:

- The learning outcomes and assessment criteria that need to be met to pass the module
- The assessment required to be completed for the module
- The additional resources required for the module
- The topics that will be focused on for the module

## Module Aim

Technical issues are central to any computing curriculum. However, they do not, by themselves, constitute a complete educational programme. Students must, therefore, develop an understanding of the social and professional contexts in which computing is executed.

This module will aim to prepare students to take managerial and technical decisions with regard to information security. Students will also examine strategies to manage and mitigate security risk.

## Module Description

The implementation of information security in an organisation takes a number of factors into consideration, including laws, regulations and the codes of conduct of professional organisations. Students will, further, understand that security is about business needs and, thereafter, information technology (IT). Students will also explore how risk analysis is conducted, and how risks are identified, assessed and controlled. They will identify the different methods available to hackers by which they gain access to and examine a system. This is required by the students in order to design/modify these methods so that hackers cannot gain access. Finally, students will gain an understanding of cryptographic techniques in the field of digital forensics.

## Learning Outcomes

By the end of this module, you will be able to:

| Learning Outcomes | Assessment Criteria |
|---|---|
| 1. Prove that security is primarily about business needs, rather than IT | 1.1 Describe key information security concepts<br>1.2 Describe the security system development life cycle (SecSDLC) methodology |
| | Blended learning activity:<br>• Ethical Decision Making |
| 2. Summarise principles of security | 2.1 Describe the categories of threats<br>2.2 Describe the sources of attacks |
| | Blended learning activity:<br>• Ethical Decision Making |
| 3. Evaluate legal and ethical issues | 3.1 Describe the law and ethics<br>3.2 Identify laws relevant to information security<br>3.3 Identify ethical concepts in IT |
| | Blended learning activity:<br>• Ethical Decision Making |
| 4. Apply, describe, discuss and explain the three steps involved in risk management | 4.1 Describe risk management<br>4.2 Describe risk identification<br>4.3 Describe risk control |

| | |
|---|---|
| | Blended learning activity:<br>• Ethical Decision Making |
| 5. Apply the three steps involved in risk management to a case study | 5.1 Identify resources and their vulnerabilities<br>5.2 Apply risk control strategies to mitigate risks |
| | Blended learning activity:<br>• Ethical Decision Making |
| 6. Design a blueprint for a case study and include continuity in the design | 6.1 Identify the considerations to be taken into account when creating a security blueprint<br>6.2 Identify the components of a blueprint<br>6.3 Describe business continuity strategies<br>6.4 Explain different ways of recovering from a disaster<br>6.5 Explain the use of digital forensics in identifying how attacks on assets occur |
| | Blended learning activity:<br>• GNS3 Software installation and VM integration |
| 7. Critique security technology that is available on the market today | 7.1 Explain how users are authenticated to gain access to systems<br>7.2 Describe access control policies (mandatory access control [MAC], discretionary access control [DAC] and non-DAC)<br>7.3 Describe the functions of firewalls |
| | Blended learning activity:<br>• GNS3 Software installation, VM integration and configuration |
| 8. Assess new technologies | 8.1 Explain the Kerberos Protocol<br>8.2 Describe virtual private network (VPN) technologies<br>8.3 Explain the functions of intrusion detection and prevention systems (IDPSs) |
| | Blended learning activity:<br>• Virtualisation |
| 9. Evaluate cryptography and justify the use for it today | 9.1 Explain how cryptography is used in access control |

| | |
|---|---|
| | 9.2 Describe asymmetric, symmetric and hybrid cryptographic methods<br>9.3 Apply cryptographic methods to secure information |
| | Blended learning activity:<br>• Hacking basics |
| 10. Compare and discuss different methods that hackers use to gain access to, and examine, a system in order to design/modify such so that they cannot gain access | 10.1 Describe common attack methods used by hackers<br>10.2 Identify measures to deny access to hackers |
| | Blended learning activity:<br>• Hacking basics |

## Prescribed Resource(s)

**Textbook(s)**

Whitman, M.E. and Mattord, H.J., 2015. *Principles of information security.* London: Cengage Learning.

The following resource(s) will be made available on *my*LMS, which you must check regularly:

- Assignment specification
- Blended learning items
- Continuous assessments
- Exam scopes
- Important notifications from your lecturer
- Module guide
- Module announcements

## Recommended Resource(s)

Take note that all disciplines and their corresponding textbooks are frequently updated. Therefore, you should use the latest editions, where available. Recommended resources should be used for research purposes. There is a range of resources related to this module, including the following:

**Textbook(s)**

Boyle, R.J. and Proudfoot J.G. 2014. A*pplied Information Security: A Hands-On Guide to Information Security Software:* 2nd ed. UK: Pearson.

Boyle, R.J. and Panko, R.R., 2014. *Corporate computer security.* Prentice Hall Press.

Coleman, D. 2014. *Certified Wireless Network Administrator Official Study Guide: Exam CWNA-106.* John Wiley & Sons.

Geers, K. 2011. Strategic Cyber Security. Tallinn Estonia: CCD COE Publication.

Gollmann, D. 1999. Computer Security. New York: John Wiley & Sons.

Pfleeger, C. et al. 2015. Security in Computing. Pearson.

Quinn, J. 2016. Ethics for the Information Age. Pearson.

Stallings, W. & Brown, L. 2015. *Computer Security: Principles and Practice.* Pearson.

Stallings, W. & Brown, L. 2015. *Computer Security: Principles and Practice.* Pearson.

Van Wyk, K. et al. 2015. *Enterprise Software Security: A Confluence of Disciplines.* Pearson.

**Online Document(s)**

Eslambolchi, H. 2012. *Cyber Security Principles and its Challenges in 21st Century.* [Online] Available at: http://2020vp.com/cyber-security-challenges-in-21st-century/. [Accessed: 11 November 2018].

**Website(s)**

Web pages provide access to a further range of Internet information sources. Lecturers may download the web-related material for you to access offline. You must use this resource with care, justifying the use of information gathered.

Stay Safe Online. 2017. [Online] Available at: https://www.staysafeonline.org/stay-safe-online/keep-a-clean-machine/malware-and-botnets [Accessed: 11 November 2018].

spaces.internet2.edu. N.d. Cybersecurity Awareness Resource Library. [Online] Available at: https://spaces.internet2.edu/display/2014infosecurityguide/Cybersecurity+Awareness+Resource+Library [Accessed: 11 November 2018]

## Supporting Documents

Geyer, L., Levin, A., Makati, P., Pierce, R., Potter, M., and Wheeler, A. 2019. *PIHE Guide to Referencing (Harvard Referencing Method).* Unpublished document. Pearson Institute of Higher Education

## Essential Requirements

- Access to a resource centre or a library with a wide range of relevant resources including textbooks, newspaper articles, journal articles, organisational publications and databases.
- Access to a range of academic journals in electronic format via PROQUEST or other databases.
- In addition to textbooks, access to Internet sources and the utilisation of GNS3 Software is essential.

## ICT Requirements

| ICT Required | Reason | Lecture Week(s) |
|---|---|---|
| Access to IT labs for practical (in addition to normal lecture hours) | Lab work | 9 – 12 |

All lab work must be completed on desktop computers.

## Formative Assessment(s)

**Continuous Assessments**

Continual formative assessment is conducted so that you are given feedback on your progress in the achievement of specific learning outcomes. The formative assessment tasks occur every fortnight and can take the form of one of the following:

- A five-item multiple choice test
- A short-questions test
- Construction of concept maps
- Take home tests with long questions

- Short practical tasks
- Short class presentations

Students could be expected to complete assessments on *my*LMS as well as other digital platforms.

Guidelines for online *my*LMS assessments:

- Time limits should be checked before commencing assessments.
- Ensure that the Internet connection is stable.
- In some cases, assessments are not available indefinitely and will only be available for a day or two.
- Marks may only be available (with a memorandum) after all students have attempted the assessment after the assessment due date.
- Two attempts may be awarded in cases where there is poor Internet connection. Note that no more than two attempts may be awarded in some cases.

**Test(s)**

There will be only one theoretical test for this semester. The test will count 20% towards the final mark.

If a test is missed because of illness, a doctor's note must be presented within 48 hours of the missed test to the Academic Manager/Administrator/Coordinator.

To make up for this missing assessment, you may be able to write a deferred test. However, in order to gain entry to this test, you will have to follow various procedures and meet certain criteria. You must complete a *Deferred Test Application Form* available on *my*LMS. You will be required to pay a non-refundable fee per application. Each test missed requires a separate application. This will be your only opportunity to make up for a missed test.

It is the students' responsibility to collect their tests and verify their marks on the day they are handed out. No adjustment of marks will be entertained beyond the date scripts are returned to students after marking.

**Assignment(s)**

There is only one assignment for this module. This assignment will be completed individually. The assignment is based on understanding the theory covered in class and its application to practical case studies. In order for students to achieve a 50% pass rate on the assignment they should spend approximately 15 - 20 hours working on the whole assignment. This assignment will count 20% towards the final mark.

Assignments must be submitted on or before the due date to the lecturer in class or as per arrangement. Five percent (5%) will be deducted for every day that the assignment is late, up to a maximum of three days. Assignments that are more than three days late will be awarded a zero.

## Summative Assessment

Summative assessment is concerned with the judgement of learning in relation to the exit-level outcomes of the qualification. Such judgement includes integrated assessment(s), which test your ability to integrate the larger body of Social Practices and Security knowledge, skills and attitudes that are represented by the exit-level outcomes as a whole.

## Plagiarism

All assignments and reports must be submitted to the online similarity checker (Turnitin) available on *my*LMS prior to being submitted for marking. When submitting your assignment/report, it is compulsory to submit the entire Turnitin report. Marks will be deducted in accordance with the institutional policy.

Also, when submitting assessments, you should include the completion and signing of the applicable Assessment Coversheet as an acknowledgement that the work submitted is your own original work, except for source material explicitly acknowledged. This declaration will serve as proof that you are aware of the Institution’s policies and regulations on academic integrity.

## Final Mark

In order to pass the module, a sub-minimum mark of 40% or higher is required for the examination and a final average of 50% or higher is required for the entire module.

The final mark is calculated as follows:

**Coursework Mark** [(Continuous assessment percentage × 0.10) + (Test percentage × 0.20) + (Assignment percentage × 0.20)] + **Examination Mark** [(Project percentage x 0.10) + (Examination percentage × 0.40)]

## Details of Assessments

| Methods of Assessment | Weighting[1] | Dates |
|---|---|---|
| **Semester 1** | | |
| Assignment | 20% | 16/03/2020 – 20/03/2020<br>Scope of coverage: Weeks 1 – 7 |
| Test | 20% | 14/04/2020 – 17/04/2020<br>Scope of coverage: Weeks 4 – 8 |
| Deferred Test | | 28/04/2020 – 30/04/2020<br>Scope of coverage: Weeks 4 – 8 |
| Continuous Assessment | 10% | Lecturer will stipulate the date(s) of these assessments and scope of coverage. |
| All formative marks captured | | 21 May 2020 |
| Project | 10% | 11/05/2020 – 15/05/2020<br>Scope of coverage: Weeks 6 – 12 |
| Initial Examination | 40% | 1: 25/05/2020 – 08/06/2020 |
| Supplementary/Deferred Examination | | 1: 29/06/2020 – 10/07/2020 |

## Putting Together a Portfolio of Evidence

You must demonstrate, through the presentation of evidence, that you have met all module requirements within the qualification being undertaken. To do this, you must organise your evidence into what is known as a 'portfolio'.

[1] Refer to the **Conditions of Enrolment**, available on *my*LMS.

A portfolio will take time and effort to complete. It is a means of focusing and demonstrating to others your strengths and achievements. A portfolio is an important resource that you may find useful to retain once you have achieved your qualification, particularly when applying for future positions.

You are encouraged to read more about building a portfolio and to begin populating your evidence to illustrate your full skill-set to future employers.

## Consultations

Consultation times will be pinned onto the lecturer's office door/notice board. You must give lecturers 24 hours' notice for appointments. Meetings can be requested in-class or via email. It is important that you detail the requirements (chapter, section, etc.) for your consultation.

## Module Content

You are required to attend all classes. In addition, exercises and activities, which are supplied by lecturers, are compulsory.

Continuous assessments may run throughout the semester.

**Semester 1: Schedule**

| Lecture Weeks | Topics and Assessment Criteria Covered | Assessments | References |
|---|---|---|---|
| **1**<br>1: 03/02/2020 – 07/02/2020 | Introduction to Information Security<br>AC: 1.1, 1.2 | | • Chapter 1 |
| **2**<br>1: 10/02/2020 – 14/02/2020 | The Need for Security<br>AC: 1.1, 2.1, 2.2 | | • Chapter 1, 2 |
| **3**<br>1: 17/02/2020 – 21/02/2020 | Legal, Ethical and Professional Issues<br>AC: 3.1, 3.2, 3.3 | | • Chapter 3 |

| | | | |
|---|---|---|---|
| **4**<br>1: 24/02/2020 – 28/02/2020 | Risk Management: Identifying, Assessing and Controlling Risks<br>AC: 4.1, 4.2, 4.3, 5.1, 5.2 | | • Chapter 5 |
| **5**<br>1: 02/03/2020 – 06/03/2020 | A Blueprint for Security Planning for Continuity<br>AC: 6.1, 6.2, 6.3, 6.4 | | • Chapter 4 |
| **6**<br>1: 09/03/2020 – 13/03/2020 | Available Technologies (Firewalls, Remote Access and VPN) and Cryptography<br><br>Project Setup<br>AC: 7.1, 7.2, 7.3, 8.1, 8.2 | | • Chapter 6, 7, 8 |
| **7**<br>1: 16/03/2020 – 20/03/2020 | Available Technologies (IDPS) and Cryptography<br><br>Project Software Installation<br>AC: 8.3, 9.1, 9.2, 9.3 | Assignment due | • Chapter 7, 8 |
| **8**<br>1: 23/03/2020 – 27/03/2020 | Hacking Methods and Tricks of the Trade; Security from the Other Side<br><br>Practical on Cyber Security<br>AC: 6.5, 10.1, 10.2 | | • Chapter 2, 12<br>• Appendix A |
| 1: 30/03/2020 – 03/04/2020 | **Academic and Work Readiness Mastery** | | |
| 1: 06/04/2020 – 10/04/2020 | **Semester Break** | | |

| | | | |
|---|---|---|---|
| **9**<br>1: 14/04/2020<br>– 17/04/2020 | Cyber Security<br>AC: 10.1, 10.2 | Test | • Appendix A |
| **10**<br>1: 20/04/2020<br>– 24/04/2020 | Practical on Cyber Security<br>AC: 10.1, 10.2 | | • Appendix A |
| **11**<br>1: 28/04/2020<br>– 30/04/2020 | Practical on Cyber Security<br>AC: 10.1, 10.2 | Deferred Test | • Appendix A |
| **12**<br>1: 04/05/2020<br>– 08/05/2020 | Practical on Cyber Security<br>AC: 10.1, 10.2 | | • Appendix A |
| **13**<br>1: 11/05/2020<br>– 15/05/2020 | Revision | Project due | |
| **Revision**<br>1: 18/05/2020<br>– 22/05/2020 | **Revision and examination preparation** | | |
| 1: 25/05/2020<br>– 08/06/2020 | **Initial Examination** | | |
| 1: 29/06/2020<br>– 10/07/2020 | **Supplementary/Deferred Examination** | | |
| 20/07/2020 | **Semester 2 Teaching Period Continues** | | |

# Appendix A

This appendix should be referenced when studying the content and the assessment criteria for the week(s) listed below.

| | |
|---|---|
| **Week** | 9 - 12 |
| **Learning Outcome** | LO10 |
| **Assessment Criteria** | 10.1, 10.2 |

## Cybersecurity

**Introduction**

Modern societies have become increasingly dependent on ICTs that offer both opportunities and challenges with respect to improvements in the quality of life of people and the communities in which they live. For although the use of ICTs offers several potential benefits (including improvements in efficiency and reduction in costs, and widespread access to information and services), they also expose individuals, organisation and nations to new risks, including those that result from Internet-related security breaches and misuse of cyber-power (i.e. the ability to use cyberspace to create advantages and influence events within and outside of cyberspace).

Cybersecurity is a dynamic and growing industry. As an academic discipline, cybersecurity has never been more important. It has evolved from a relatively obscure concentration into a highly complex, interdisciplinary field – rich in both research possibilities and real-world applications.

Cyber-threats against individuals, governments and businesses are continually taking on newer, more complex and more dangerous forms. At this moment, highly skilled cyber attackers around the world are in the process of crafting revolutionary attack methods to thwart the latest cybersecurity innovations. As a consequence, cybersecurity professionals today must possess a range of academic and technical skills to secure information and infrastructure, and combat new attacks.

**Why are we talking about cybersecurity?**

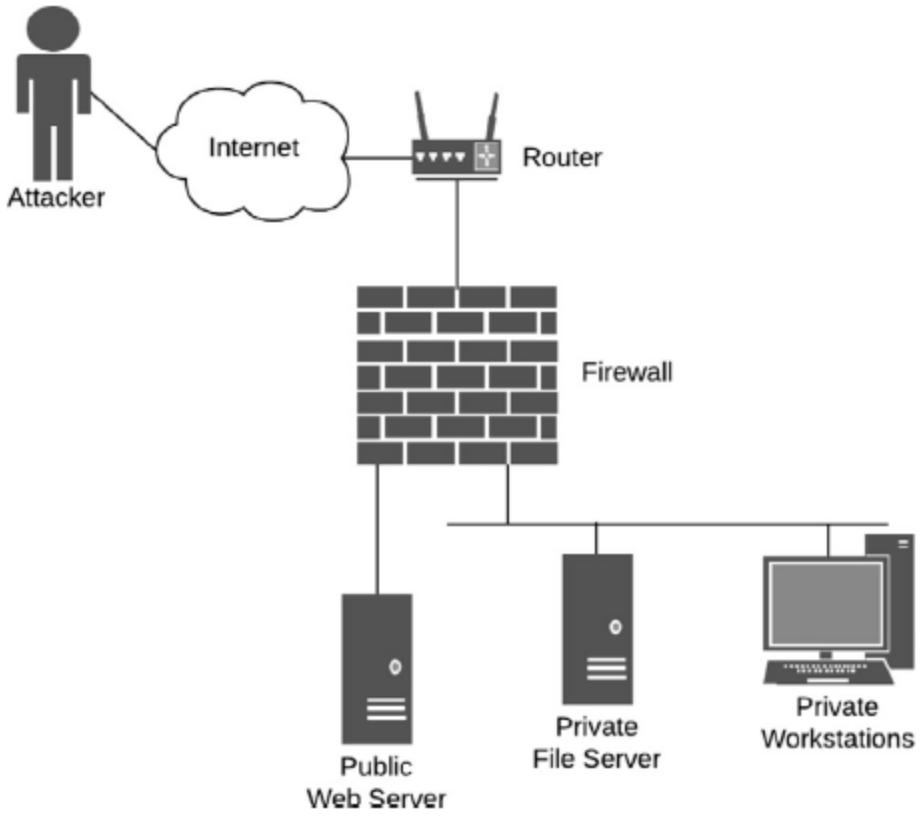


**Figure 1: Typical network design for a small to medium size organisation**

Source: Noam [et al.] 2015

Figure 1 shows a typical network with an attacker on the other side of the Internet. This kind of network topology is common for local corporate networks that are connected to the Internet. Such corporate networks typically consist of a Web server, a file server and a cluster of workstations. This network setting is commonly used in cybersecurity research and training, as well as in the operative networks of real-world mid-size corporations.

Statistics and examples demonstrate the scope and diversity of the various global cybersecurity threats. With regard to cybercrime, which may be construed as a threat to national and international economic security, the 2012 Norton Cybercrime Report estimates that 556 million victims fall prey to this each year (Keevy, 2016). This report states that one-and-a-half million victims are thought to be targeted daily and that cybercrime results in financial losses of US$ 110 billion per year, 42% of which is lost due to fraud. The following are some of the major cases in cyber-attacks reported in the last decade:

**Case 1: Internet under siege**

- February 7 – 9, 2000 Yahoo!, Amazon, Buy.com, CNN.com, eBay, E*Trade, ZDNet websites hit with massive denial of service (DOS)
- U.S. Federal Bureau of Investigation (FBI) officials have estimated that the attacks caused $1.7 billion in damage

**Case 2: Slammer worm**

- January 2003 Infects 90% of vulnerable computers within 10 minutes
- Effect of the worm
    - Interference with elections
    - Cancelled airline flights
    - 911 emergency systems affected in Seattle
    - 3 000 Bank of America ATMs failed
- No malicious payload!
- Estimated $1 billion in productivity loss

**Case 3: September 11**

- Wireless tower on top of Trade Center destroyed
- AT&T has record call volumes
- 'Flash' usage severely limits availability
- Rescue efforts hampered

**Cybersecurity perspective**

Many aspects of our lives rely on the Internet and computers, including communications (e-mail, cell phones, and texting), transportation (traffic control signals, car engine systems, and airplane navigation), government (birth/death records, social security, licencing, and tax records), finance (bank accounts, loans, and electronic pay checks), medicine (equipment, medical records) and education (virtual classrooms, online report cards, research). Consider how much of your personal information is stored either on your own computer or on someone else's system. How is that data, and the systems on which that data resides (or is transmitted), kept secure? Cybersecurity involves protecting the information and systems we rely on every day – whether at home, work or school.

**Information security vs cybersecurity**

The term ‘cybersecurity’ is often used interchangeably with the term ‘information security’, but it is important to differentiate between the two terms.

**‘Information security’ defined**

As mentioned in the previous study units, the aim of information security is to ensure business continuity and minimise business damage by limiting the impact of security incidents (Von Solms, 1998).

Whitman and Mattord (2009) define information security as “the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information” (Whitman and Mattord, 2009, p. 8).

Von Solms et al (2013) argue that cybersecurity goes beyond the boundaries of traditional information security to include not only the protection of information resources, but also that of other assets, including the person him/herself.

**Cybersecurity defined**

According to H.R. 4246 ‘Cybersecurity Information Act’, cybersecurity is:
“The vulnerability of any computing system, software program, or critical infrastructure to, or their ability to resist, intentional interference, compromise, or incapacitation through the misuse of, or by unauthorized means of, the Internet, public or private telecommunications systems or other similar conduct that violates Federal, State, or international law, that harms interstate commerce of the United States, or that threatens public health or safety.”

Cybersecurity can also be defined as: “Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.”

“Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access” (http://whatis.techtarget.com/definition/cybersecurity)

Cybersecurity covers the fundamental concepts underlying the construction of secure systems, from hardware to the software to the human computer interface, with the use of cryptography to secure interactions.

### The relationship between information security and cyber security

Just as information security expanded on the concepts of ICT security in order to protect the information itself, irrespective of its current form and/or location, cybersecurity needs to be seen as an expansion of information security. Cybersecurity should be about protecting more than just the information, or information systems resources, of a person/organisation. Cybersecurity is also about the protection of the person(s) using resources in a cyber-environment and about the protection of any other assets, including those belonging to society in general, that have been exposed to risk as a result of vulnerabilities stemming from the use of ICT. The relationship between these three overlapping concepts is illustrated in Figure 2.

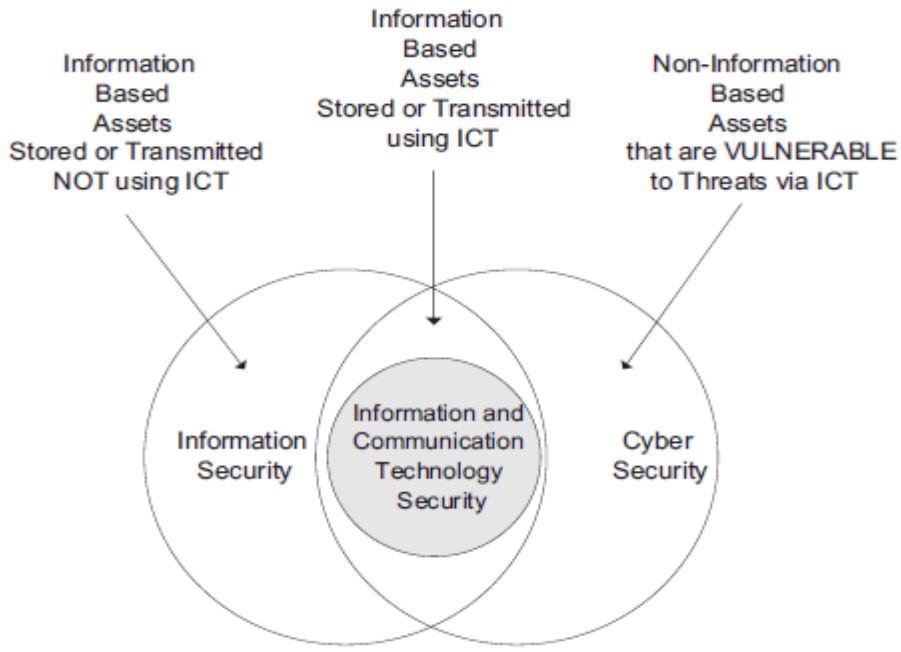


**Figure 33: The relationship between information and communication security, information security and cybersecurity**

Source: Von Solms [et al.] 2013

### Principles of cyber security

As discussed in study unit 1, the computer security industry developed a standard for computer security called the **C.I.A. triangle**. The **C.I.A. triangle** is based on the three characteristics of information that give it value to organisations: confidentiality, integrity and availability. These form the core principles of cybersecurity:

- Confidentiality: Information which is sensitive or confidential must remain so and be shared only with appropriate users.
- Integrity: Information must retain its integrity and not be altered from its original state.
- Availability: Information and systems must be available to those who need it/them.

**Why cybersecurity is important**

The following are some of the reasons why cybersecurity is important:

1. The increasing volume and sophistication of cybersecurity threats – including targeting phishing scams, data theft and other online vulnerabilities – demand that we remain vigilant about securing our systems and information.
2. The average unprotected computer (i.e. does not have proper security controls in place) connected to the Internet can be compromised in moments. Thousands of infected web pages are being discovered every day. Hundreds of millions of records have been involved in data breaches. New attack methods are launched continuously. These are just a few examples of the threats facing us, and they highlight the importance of information security as a necessary approach to protecting data and systems.

**How can you protect yourself or organisation against cyber-threats?**

It is important that we each understand the risks as well as the actions we can take to help protect our information and systems. They are as follows:

- Properly configure and patch operating systems, browsers and other software programs.
- Use and regularly update firewalls, anti-virus and anti-spyware programs.
- Use strong passwords (combination of upper and lower-case letters, numbers and special characters), and do not share passwords.
- Be cautious about all communications; think before you click. Use common sense when communicating with users you do and do not know.
- Do not open e-mail or related attachments from untrusted sources.
- Allow access to systems and data to only those who need it, and protect those access credentials.
- Follow your organisation’s cybersecurity policies, and report violations and issues when they occur.

**Cybersecurity risks/threats**

There are many risks, some more serious than others. Some examples of how your computer and systems could be affected by a cyber-security incident – whether because of improper

cybersecurity controls, man-made or natural disasters, or malicious users wreaking havoc – include the following as described below:

**Cyber bullying**

According to Martin and Rice (2011), several recent studies have found that technology is increasingly used to bully, “cause embarrassment, invoke harassment and violence, and inflict psychological harm”. This could lead to “severe and negative impacts on those victimized”.

**Cyber terrorism**

In the USA, critical infrastructure is defined as “the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof” (Department of Homeland Security, 2011). Infrastructure that delivers electricity and water, controls air traffic, or supports financial transactions is seen as “critical life sustaining infrastructures” and all directly depend on underlying communications and network infrastructure (The Whitehouse, 2011, p. 3). The protection of such critical infrastructure forms an important part of cybersecurity and is included as an important national imperative in national cybersecurity strategies (Minister for the Cabinet Office and Paymaster General, 2011, p. 39; The Whitehouse, 2011, p. 13).

Cyber-terrorists or enemy specialists may target a country’s critical infrastructure via cyberspace. This could either be indirectly, for example by influencing the availability of information services using denial-of-service attacks or, more directly, through an attack on the national electricity grid.

**Cyber-espionage**

Cyber-espionage is another major threat to national and international cybersecurity, and this has also become more prevalent. Perhaps the best recent example of this type of cybersecurity threat were the ‘spear-phishing’ attacks carried out against Google in 2011, allegedly by Chinese intelligence personnel or China-based hackers (, 2018). A ‘spear-phishing’ cyber-attack is an advanced ‘phishing’ operation.

**Denial-of-service**

This refers to an attack that successfully prevents or impairs the authorised functionality of networks, systems or applications by exhausting resources. What impact could a denial-of-service have if it shut down a government agency’s website, thereby preventing citizens from accessing information or completing transactions?

What financial impact might a denial-of-service have on a business? What would the impact be on critical services such as emergency medical systems, police communications or air traffic control? Can some of these be unavailable for a week, a day or even an hour?

**Malware, worms and Trojan horses**

These are spread by e-mail, instant messaging, malicious websites and infected non-malicious websites. Some websites will automatically download the malware without the user's knowledge or intervention. This is known as a 'drive-by download'. Other methods will require the users to click on a link or button.

**Botnets and zombies**

A botnet, short for 'robot network', is an aggregation of compromised computers that are connected to a central 'controller'. The compromised computers are often referred to as 'zombies'. These threats will continue to proliferate as the attack techniques evolve and become available to a broader audience, with less technical knowledge required to launch successful attacks. Botnets designed to steal data are improving their encryption capabilities and thus becoming more difficult to detect.

**'Scareware' – fake security software warnings**

This type of scam can be particularly profitable for cyber criminals, as many users believe the pop-up warnings telling them their system is infected and are lured into downloading and paying for the special software to 'protect' their system.

**Social network attacks**

Social network attacks are major sources of attacks because of the volume of users and the amount of personal information that is posted. Users' inherent trust in their online friends is what makes these networks a prime target. For example, users may be prompted to follow a link on someone's page, which could bring users to a malicious website.

**Penetration testing**

A penetration test, sometimes 'pentest', is a software attack on a computer system that looks for security weaknesses, potentially gaining access to the computer's features and data. It is a proactive and authorised attempt to evaluate the security of an IT infrastructure by safely attempting to exploit system vulnerabilities, including OS, service and application flaws, improper configurations, and even risky end-user behaviour. Such assessments are also useful in

validating the efficacy of defensive mechanisms, as well as end users' adherence to security policies.

**Why perform penetration testing?**

**1. Security breaches and service interruptions are costly**

Security breaches and any related interruptions in the performance of services or applications can result in direct financial losses, threaten organisations' reputations, erode customer loyalties, attract negative press and trigger significant fines and penalties.

**2. It is impossible to safeguard all information, all the time**

Organisations have traditionally sought to prevent breaches by installing and maintaining layers of defensive security mechanisms, including user access controls, cryptography, IPS, IDS and firewalls. New vulnerabilities are discovered each day, and attacks constantly evolve in terms of their technical and social sophistication, as well as in their overall automation.

**3. Penetration testing identifies and prioritises security risks**

Penetration testing evaluates an organisation's ability to protect its networks, applications, endpoints and users from external or internal attempts to circumvent its security controls to gain unauthorised or privileged access to protected assets. Test results validate the risk posed by specific security vulnerabilities or flawed processes, enabling IT management and security professionals to prioritise remediation efforts.

**4. To find vulnerabilities and fix them before an attacker does**

Sometimes the IT department is aware of reported vulnerabilities, but they need an outside expert to officially report them so that management will approve the resources necessary to fix them. Having a second set of eyes to acknowledge/examine a critical computer system is a good security practice.

**5. Find holes now before somebody else does**

At any given time, attackers are employing any number of automated tools and network attacks looking for ways to penetrate systems. Penetration testing provides IT management with a view of their network from a malicious point of view. The goal is that the penetration tester will find ways into the network so that they can be fixed before someone with less than honourable intentions discovers the same holes.

6. **Report problems to management**
7. **Verify secure configurations**
8. **Security training for network staff**
9. **Discover gaps in compliance**
10. **Testing new technology**

**How often should you perform penetration testing?**

Penetration testing should be performed on a regular basis to ensure more consistent IT and network security management by revealing how newly discovered threats or emerging vulnerabilities may potentially be assailed by attackers.

The following are some of the scenarios that should be followed in penetration testing:

- New network infrastructure or applications are added.
- Significant upgrades or modifications are applied to infrastructure or applications.
- Security patches are applied.

**How can you benefit from penetration testing?**

Penetration testing offers many benefits, allowing you to:

- Intelligently manage vulnerabilities: Penetration testing provides detailed information on actual, exploitable security threats. By performing a penetration test, you can proactively identify which vulnerabilities are most critical, which are less significant, and which are false positives.
- Avoid the cost of network downtime: Recovering from a security breach can cost an organisation millions of dollars related to IT remediation efforts, customer protection and retention programmes, legal activities, discouraged business partners, lowered employee productivity and reduced revenue.
- Meet regulatory requirements and avoid fines: Penetration testing helps organisations address the general auditing/compliance aspects.
- Even a single incident of compromised customer data can be costly in terms of both negatively affecting sales and tarnishing an organisation’s public image. With customer retention costs higher than ever, no one wants to lose the loyal users that they have worked hard to earn, and data breaches are likely to turn off new clients. Penetration testing helps you avoid data incidents that put your organisation’s reputation and trustworthiness at stake.

**Penetrating testing tools**

- Various penetration tools are available. Below is a list of some of these tools:
- Metasploit

- Nessus vulnerability scanner
- Nmap
- Burp suite
- OWASP ZAP
- SQLmap
- Kali Linux
- Jawfish

Metaploit is the most popular pentest tool.

**BackTrack**

BackTrack is a Linux-based penetration testing arsenal that aids security professionals in the ability to perform assessments in a purely native environment dedicated to hacking. BackTrack is a well-known, specialised Linux distribution focusing on security tools for penetration testers and security professionals, but it now offers a lot in terms of forensics.

BackTrack promotes a quick and easy way to find and update the largest database of security tools collection to date. Users range from skilled penetration testers in the information security field, government entities, information technology, security enthusiasts, and individuals new to the security community.

**Advantages and disadvantages of BackTrack**

**Advantages**

1. BackTrack 5 has all the tools that you need for testing network security, and it is nicely presented.
2. It offers a slew of security and forensic tools on a live DVD, ready to use.
3. It is based on Ubuntu Lucid (10.04 LTS) with Linux kernel 2.6.38 and some patched Wi-Fi drivers to allow injection attacks.
4. BackTrack provides users with easy access to a comprehensive and large collection of security-related tools, ranging from port scanners to Security Audit.

**Disadvantages**

Documentation is scarce and often out-dated, and upgrading from previous release is not supported.

**Tools in BackTrack**

BackTrack arranged tools into 12 categories:

Use the links to the tutorial.

1. Information gathering
   http://searchsecurity.techtarget.in/tip/BackTrack-5-tutorial-Part-I-Information-gathering-and-VA-tools
2. Vulnerability assessment
   http://searchsecurity.techtarget.in/tip/BackTrack-5-Guide-II-Exploitation-tools-and-frameworks
3. Exploitation tools
   http://searchsecurity.techtarget.in/tip/BackTrack-5-tutorial-Part-3-More-on-exploitation-frameworks
4. Privilege escalation
   http://searchsecurity.techtarget.in/tip/BackTrack-5-guide-4-How-to-perform-sttealth-actions
5. Maintaining access
6. Reverse engineering
7. RFID tools
8. Stress testing
9. Forensics
10. Reporting tools
11. Services
12. Miscellaneous

Read more on how to use these tools on the official BackTrack website:
http://www.backtrack-linux.org/wiki/index.php/Main_Page
See toolbox for backtrack installation, configuration and exercises.

**Challenges of cybersecurity**

Successfully combating cyber-threats is not an easy task. Many companies and nations have spent millions of dollars in infrastructure and research to try combat cybercrimes. However, this comes with many challenges, some of which are listed below:

- The number of threats that are faced is constantly increasing.
- Convenience/functionalities/usability vs security: Users want useful and/or fun technology.
- The Internet has become the primary computing platform.
- Evolving technologies.

- New technology may bring new vulnerabilities.
- Evolving tactics by attackers.
- Ineffective sharing of threats and mitigation information.
- Insufficient cybersecurity workers.
- Insufficient funds to curb cyber-threats.

**Conclusion**

Cybersecurity is an inter-disciplinary field, and success depends on many factors, including technology, economics, usability and psychology. Cybersecurity is perhaps the most difficult intellectual profession on the planet. Due to the pace of technological change and broader developments in threats in the online environment, it is necessary to undertake ongoing evaluation and regular reviews of the appropriateness of an organisation's cybersecurity policies. It is also important that enough time and resources be dedicated to finding cybersecurity threats and solutions, and that preventive steps are taken to circumvent these threats.

**Bibliography**

Define cyber security. 2016. [Online] Available from: http://whatis.techtarget.com/definition/cybersecurity [Accessed: 20 November 2018]

Paul, T. 2018. *China's Alleged Supply Chain Hack: Explaining the Controversy around Bloomberg's 'Big Hack' Reporting.* [Online] Available from: https://supchina.com/2018/10/16/explaining-the-controversy-around-bloombergs-big-hack-reporting [Accessed: 20 November 2018]

Keevy, J. 2016. *More people in SA victims of cybercrime.* [Online] Available from: http://www.insurancegateway.co.za/Swaziland/PressRoom/ViewPress/URL=More+people+in+SA+victims+of+cyber+crime+1#.Vp4b13YrLIU [Accessed: 20 November 2018]

Martin, N. & Rice, J. 2011. *Cybercrime: understanding and addressing the concerns of stakeholders.* Computers & Security, 30:803-14.

Noam, B. & Cleotilde, G. 2015. *Effects of cyber security knowledge on attack detection.* Office and Paymaster General. 2011, p. 39; The Whitehouse. 2011, p. 13

Whitman, M.E.; Coles, M.J. & Mattord, H.J. 2009. *Principles of information security.* 2nd ed. London: Cengage Learning.

Whitman, M.E.; Coles, M.J. & Mattord, H.J. 2012. *Principles of information security.* 4th ed. London: Cengage Learning.

Von Solms, R. & Van Neerk, J. 2013. *From information security t*