Information security for non-technical managers

Dr Eduardo Gelbstein

bookboon
The eBook company

Dr. Eduardo Gelbstein

Information security for non-technical managers

Information security for non-technical managers
1st edition

ISBN 978-87-403-0488-6

Contents

About the author

With nearly 50 years experience in the private and public sectors in several countries, Ed has been active in information security through publications, international conferences, workshops and also as an auditor.

After many years as a senior Information Technology manager in the pre-privatised British Rail, he joined the United Nations as Director of the International Computing Centre, a service organization providing services to many international organisations. Following his retirement, he was invited to joint the audit teams of the United Nations Board of External Auditors and those of the French National Audit Office (*Cour des Comptes*), activities he continued for several years.

He is currently a Senior Fellow of the Diplo Foundation, an entity that provides online training to diplomats around the world. He is also a faculty member of Webster University, Geneva, Switzerland and a guest speaker at the Geneva Centre for Security Policy. He remains a contributor to security conferences in Europe, the Arabian Gulf and Africa.

His publications include several books and articles in peer-reviewed journals. Amongst them:

"Quantifying Information Risk and Security", ISACA Journal, July 2013.

"Demonstrating Due Diligence in the management of Information Security, ISACA Journal, January 2013.

"Strengthening Information Security Governance, ISACA Journal, November 2012

"Planning an I.T. Audit for a Critical Information Infrastructure", Chapter 11 of the book "Securing Critical Infrastructures and Critical Control Systems – approaches for Threat Protection" edited by Christopher Laing *et.al*. IGI Global, November 2012

"Law and Technology – Cyberwar, Cyberterrorism and Digital Immobilization", co-authored and co-edited with Professor Pauline Reich, IGI Global, November 2012

"Data Integrity, the poor relation of Information Security", ISACA Journal, November 2011

"Crossing the Executive Digital Divide", Diplo Foundation, Geneva, 2006

"The Information Society Library", a collection of 9 booklets (3 of them on security), Diplo Foundation, Geneva, 2003 (in support of the first World Summit of the Information Society)

"Information Insecurity", United Nations Secretary General's Information and Communications Task Force, September 2002

Ed can be contacted at gelbstein@diplomacy.edu

Introduction

Purpose of this book

This non-technical book is intended for those who seek a broader understanding of information security and what needs to be done to protect information assets and what their role should.

These short chapters aim to give a concise overview of why the information security "problem" has not been solved and what is involved in using computer systems and networks in a connected world in which over 2 billion people have access to the Internet and over 4 billion have mobile phones. Many of them also have enough knowledge of how these things work to be able to disrupt them.

In writing this book, the author considered the elements of 5W1H: What, Why, Who, Where, When and How. A focus on "What" and "Why" was felt to be appropriate. "Who" applies to the reader as well as to service providers, system designers and all attackers. "Where" is everywhere across national boundaries. "When" is now.

The "How" part of this discussion goes beyond the intent and scope of this book. Much material is available and some is mentioned in Chapter 9.

One of the many challenges of managing information security in the corporate world is that of scale: small organisations (for example and I.T. team of less than 5 to 10 people) may not have access to the skills and experience to do many of the recommended practices and, at the other end, very large organisations that may have several I.T. teams at various locations may lack the "human touch" and rely on bureaucratic procedures and technologies. The appropriate approach should be part of Information Security Governance as there is no single right answer.

Readers unfamiliar with some of the terminology – there seem to be new words invented all the time – are encouraged to consult an online encyclopaedia or use a search engine.

Key points from the various chapters

- "Cyberspace" is inherently insecure (Chapter 1).
- The terminology of "cyberspace" is ambiguous and can lead to misunderstandings and confusion. Many basic terms have disputed definitions and spelling (for example cyber-war and cyber-weapon). The same is true for the concepts of "information security" and "information technology security" (Chapter 2).
- Dependency on information systems, services and technologies has become irreversible. There is adequate knowledge on how to protect them through many standards, good practices and guidelines. However, more needs to be done to apply this knowledge in practice (Chapter 2).
- Those intent on disrupting information systems and data (suggested name: "hackers") can be anyone, anywhere. It is prudent to assume they are talented, knowledgeable, motivated and dedicated, perhaps more so than those accountable for maintaining security in an organization (Chapter 2).
- Security professionals and Senior Management have different perceptions of the importance of this topic. This results in poor dialog and weak governance. As a result, many organisations are not well prepared to respond to a security incident. (Chapter 5).
- 100% information security is unachievable, as it would require the four components on which it relies to be perfect. These components are: governance, people, processes and technology (Chapter 5).
- Information security has become a stable and recognized profession but it is not regulated. Unlike a doctor in medicine or an aircraft pilot, anyone can be a practitioner (Chapter 6).
- The speed of technical innovation and enthusiasm for new products conspire against "security by design", largely absent in the products on which cyberspace relies. In safety industry accidents are thoroughly investigated to discover their root cause, which is then removed by design (Chapter 7).
- Understanding and quantifying the impact of security events on an organisation (referred to as Business Impact Analysis) is fundamentally important to ensure that preventive and protective measures are applied where it matters most (Chapter 8).
- Information security deals with uncertainty rather than risk, as incidents are targeted, not random events. Moreover risk (for which there are several overlapping definitions) is in the future and human ability to make predictions has a poor track record (Chapter 8).
- Information security is not someone else's job: everyone has a role. Many may not be aware of this.

1 Information security in context

In this chapter we consider

- A short history of information technologies, its side effects and unintended consequences
- Why information security and information technology security have become important
- The ubiquity and irreversible dependency of information technologies

> There are technical aspects that make cyberspace inherently insecure
> and are virtually impossible to completely "fix".
>
> Alexander Klimburg, Editor and co-author: National Cybersecurity Framework Manual, NATO CCDCOE, 2013

1.1 A short history of information technologies and their side effects

Those of us who worked in research laboratories close to the leading edge of technical innovation in the 1960s and 70s, look at today's technologies with amazement, if not incredulity. Many industry leaders failed to anticipate how these technologies would change the world:

- In 1943, Thomas Watson, then President of IBM, predicted that: "I think there is a world market for maybe five computers".
- In 1977, Ken Olsen, then President of Digital Equipment Corporation said that: "There is no reason for any individual to have a computer at home". The company no longer exists…

These transformational successes include digital integrated circuits ("chips") and the DARPANet (precursor of the Internet) of the mid 1960s, the personal computers, optical fibre networks and cellular telephony of the 1970s. Then came graphical user interfaces (such as the Apple Mac in 1984 and Windows in 1990), the World Wide Web (1991) and Google (1998). The first model of the (Apple) iPhone was launched in 2007 and the first model of the iPad followed in 2010. This innovation has not stopped and shows no signs of doing so. If anything, it may be accelerating.

Those visionary enough to believe these technologies would transform the world who were prepared to invest in them (a real gamble) have become amazingly wealthy. Those of us who are more conservative thinkers and somewhat risk-averse wish we had.

On the other hand there have been many failures – ideas, products and services that showed considerable potential but did not succeed. How many remember companies like Wang (a leader in word processing and mini-computers in the late 1970s or Altavista, a search engine launched in 1995.

This rapid wave of innovation, that some call a *Technami*, brought with it side effects and unintended consequences. Information insecurity is one of them and has become a matter of concern. The Technami continues: recent innovations include cars that do not need a human driver, robotic surgery machines (still controlled by a human but this may change), flexible and wearable devices and new approaches to military electronics.

Information technology products are supplied on an "as is" basis, with limited warranties and, in the case of software, licenses that exclude the vendor from liabilities for the consequences of malfunction or failure. Most End User License Agreements (EULA) are long and hard to understand by a layman, who has to accept the terms and conditions to install the software. Many of the "apps" designed for smartphones and tablets may not have had adequate quality assurance and some have been shown to contain malicious software (malware).

This is unlike the situation of the pharmaceutical industry: a license to sell a product requires extensive testing following strict protocols. When sold, the product includes a leaflet describing possible side effects and contraindications. This process does not always ensure that products are safe enough and several had to be withdrawn from the market. However, this is better than "you bought it, now good luck".

1.2 Why information security is increasingly important

We now know that undesirable things happen in cyberspace. The list that follows is not exhaustive as human ingenuity keeps developing new ways to exploit insecurity:

- Financial loss: in 1995 a British bank with a long history went out of business, then in 2008 a French bank lost over 6 billion Euro. In 2011 a Swiss bank operating in London lost 2 billion dollars. In the three cases through insider misuse or abuse. These were not unique situations.
- Denial of Service attacks – these overload a system, usually a website or an electronic mail service so that it cannot function. Such attacks are easy enough to carry out and are usually successful.
- Sabotage of networks or computer systems to interfere with their operation.
- Use of malicious software to take control of a computer or computer system for any of many possible reasons.
- Theft of Intellectual Property – including industrial espionage.
- Theft of Personally Identifiable Information – a breach of privacy leading to impersonation.
- Corruption or destruction of corporate data or software – frequently using malicious software.

There are growing concerns about the threat of cyber attacks on critical infrastructures such as utilities (power, water, communications, transport, hospitals, etc.) as well as on law enforcement and emergency services.

Politicians around the world have also accepted that there is a threat that entities playing a critical role in national security, such military facilities and operations in the field, may the target of a cyber attack.

Individuals are also targets, for example by:

- Infecting a personal device with malicious software (virus, worm, Trojan Horse, Rootkit, etc.).
- Losing control of a personal device that is used without their knowledge of consent to disseminate spam or carrying out a Denial of Service (zombie, botnet).
- Impersonation – senior executives in Interpol and NATO have had – without their knowledge or consent – Facebook pages about them created and exploited to acquire "friends". These were then requested to provide information. The individuals concerned were unaware of this.

- Abuse of trust – an academic researcher created accounts in Facebook, Twitter, Linkedin and other social media for a bright young woman (Robyn Sage) with impressive credentials. So impressive that many not only wanted to be linked to her, but offered her employment (unseen) or shared sensitive documents to seek her opinion. In reality Robyn did not exist – her identity was part of research into how trust is used and abused in social networks.
- Identity theft – including data on bank accounts, credit cards, etc., causing individuals financial losses that are complex to unravel.
- Blackmail – for example by encrypting the data in a computer and demanding payment to provide the decryption key.
- Attacks on mobile phones with the primary objective of financial theft. etc.

1.3 Ubiquity and irreversible dependencies

Could one imagine an environment today without information technologies (I.T.), mobile devices or the Internet? There are few places left where only a few privileged individuals have the technical and financial means to avail themselves of such tools, and the number is steadily decreasing.

Statistics published by the Internet World Stats estimated that by mid 2012 there were over 2 .4 billion Internet users (have you noticed that only drug dealers and the I.T. industry refer to their clients as "users"?). Other sources give comparable numbers. The International Telecommunications Union, an organization of the United Nations reported that in October 2012 there were over 6 billion mobile telephone subscribers. At that time the world population was just over 7 billion, many of whom subsist on less than $2 a day.

Clearly, information and the technologies that enable access to it have become "must have" items, not only for individuals but also for nations and businesses of all kinds. The enthusiasm for new gadgets and services defies belief. The launch of a new product can cause people to queue overnight in the street waiting for the store to open.

While this may not be obvious to the general public, technologies are not perfect. Besides, the ways in which users protect their systems and data are not perfect either and neither are the users themselves – errors are made by everyone (chapter 6 will return to this topic).

Many are also unaware of their role in protecting their personal information and the corporate information of their employer. The rest of this book concentrates on the need for good information security and what this involves.

2 Lessons identified in the last ten years

In this chapter we consider

- How ambiguity in the language of information security leads to misunderstandings and confusion
- The major information insecurity target areas: crime, critical infrastructures, government, the military and individuals
- Why many organisations are unprepared despite the standards, guidelines and good practices available
- The asymmetric nature of what has become a war of attrition
- How maintaining security is everybody's job

2.1 The semantics of information security

> … confuse their language so they will not understand each other.
>
> Genesis 11:7, the Bible, New International Version, © 2011

The vocabulary of information security continues to grow. A substantial part of it consists of technical jargon e.g. botnet, rootkit, public key, etc. These are fairly meaningful to the initiated and mysterious to the rest. The media have adopted the word "cyber" and make frequent use of it. Politicians have adopted it too even though there are multiple and rather inconsistent definitions.

When William Gibson created the word "Cyberspace" in his 1984 novel *Neuromancer* he contributed a word that would be greatly misused and abused without questioning. Later in his life Gibson said that it was an "evocative and essentially meaningless buzzword".

There is no agreed definition for "cyberspace". It certainly includes the worlds of data and software. Some argue that it also includes network and computing infrastructures. Most agree that the Internet is part of cyberspace and that the Internet is only a component of it.

Similarly there is limited agreement on definitions for "cyber-war" and "cyber-terrorism" and no agreement on how to spell them: as two words (cyber war), hyphenated as above or as one word (cyberwar). Things like this are important to legislators, diplomats and lawyers.

There is even limited consensus on the definition of cybersecurity (regardless of how it is spelled). For this book, the concepts of "Information Security" and "Information Technology Security" will be used throughout and are discussed in Chapter 3.

Ambiguity and linguistic confusion do not end here as other words are also used freely without widely accepted and agreed definitions. Another such word is "hacker" who can be anybody, anywhere:

- A hacker can be a computer programmer who combines curiosity, knowledge, creativity and cleverness to achieve a given objective. This was the original meaning of "hacker".
- A hacker can also be someone who bypasses or interferes with a computer's security and/or software and data.
- Hackers range from individual youngsters with some knowledge of computing (Script Kiddies), using tools available online.
- Others work as groups referred to as Hacktivists (one such group calls themselves "Anonymous";
- Then come cyber-mercenaries, professional security people working with criminals.
- There are those in military and law enforcement organisations – the media often refers to them as "cyber-armies".
- There are also those working for non-State actors ("terrorists").

To complicate matters, one person could be several of the above at any one time.

2.2 The major target areas in information insecurity

A report published by the NATO Cooperative Cyber Defence Centre of Excellence[1] (CCD-COE) defines five domains where information insecurity is an issue and discusses them separately given that the requirements and actions are different, but with areas of overlap. These domains are:

- Cybercrime
- Critical Infrastructure Protection
- Cyber Military Defence
- Intelligence and Counter-Intelligence
- Internet Governance.

This book will only explore the first three given the limited availability of public information on Intelligence and Counter-Intelligence and the complex nature of Internet Governance as it includes technical, legal, socio-economic and global political elements.

2.2.1 Cybercrime

Bank robber Willie Sutton (1901–1980) is reported to have said that he robbed banks "because that's where the money is." As money dematerialised into the ones and zeros of the digital world, it should not be surprising that crime has followed it into the digital world.

The only international instrument to address this topic is the Council of Europe Convention on Cybercrime (2001). It is open to accession to all countries, and in early 2013, only 39 countries have ratified or accessed the Convention and 10 more have signed the convention but not ratified it. (the United Nations has 193 Member States.)

The estimated but unconfirmed amount of cybercrime amounts to hundreds of billions of dollars a year. It is likely that some cybercrimes are not reported by the victims to avoid undermining public and shareholder confidence. Such crimes take place across borders and the perpetrators can, and do, place technical and legal barriers to their detection, arrest, extradition and trial.

Cybercrime takes many forms. From a corporate perspective, the main concerns are the theft of Intellectual Property and fraud. The same is true for other forms of data leakage where sensitive information ends up with parties not supposed to have it. Other forms of corporate cybercrime include sabotage and/or extortion.

Individuals are also targets of cybercrime such as identity theft, where a third party can collect sufficient information about a person to be able to impersonate them (and often bankrupt them) by obtaining documents, loans and credit cards details.

"Phishing", targets individuals (privately and at work) by using electronic communications pretending to be from a trusted entity, such as a bank, to either personal information such as passwords or credit card details and/or get them to click on a link in the message. This action takes them to a believable copy of the trusted entity's website that also asks to "confirm" personal details and also infect their computer with malware.

There are others preying on the gullible who are adept at extracting money from their victims through deception. These range from pretending to be a relative of a bank or government official in a distant country asking for assistance to transfer a huge sum of money, provided the victim makes a payment in advance to facilitate the process…

Then there is the lonely soldier (or potential distant bride) who needs money for a ticket, surgery, or other plausible reason – just a small advance that will be repaid in no time at all. Despite the publicity these receive, there is no shortage of victims. Cybercrime is not likely to stop in the near future.

2.2.2 Critical Infrastructure Protection

There are many definitions for a Critical Infrastructure. For example the European Network and Information Security Agency (ENISA), part of the European Union, describes them as:

"Those interconnected systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy".

The specific and essential characteristics of a Critical infrastructure are:

- It operates 7 days a week, 24 hours a day AND:
- Their operations require information systems and networks, sensors and other mechanisms for data acquisition.
- Critical infrastructures are frequently required to operate physical devices such as cash dispensers (ATM), motors (to switch a railroad track) and robotic systems (in manufacturing).
- It is part of a supply chain – failure to operate propagates to/from other entities that may also be critical infrastructures, creating a domino effect.

This definition applies to utilities (electricity, gas, water), transportation (air traffic control, airport operations, railways), all continuous manufacturing (oil refineries, glass and paper processing), banking (ATM networks and online), telecommunications (fixed line and mobile telephony, internet service providers) and many more. All of these are "invisible" when operational. When they fail, this almost invariably makes the news headlines.

Attacks on critical infrastructures are becoming more sophisticated: a significant event was the use of the Stuxnet software to disrupt Iran's uranium enrichment processing facilities, first made public in June 2010.

Experts have described Stuxnet as a "military-grade cyber-missile" and software experts that analysed Stuxnet[2] reported that: "We've definitely never seen anything like this before". The journal Computer World called it "one of the most sophisticated and unusual pieces of software ever created".

Since then there have been other successful attacks on critical infrastructures in many countries. One attack in August 2012 had as its target Saudi Aramco where the Shamoon virus infected 30,000 personal computers, deleted their data and replaced it with images of a burning U.S. flag. The source of the attack remains unidentified.

Cyber-attacks and the prospect of a cyber-war (an event for which there is no agreed definition so far) expose the operators of critical infrastructures to disruptions and the corruption or destruction of data.

2.2.3 National security and defence

As in the two previous sections, the targets may be very specific and the attackers may be different. There is unconfirmed talk of "cyber armies" active in several countries. When such activities are discussed in public, they are referred to as being limited to "defensive capabilities". In October 2011 however, General R. Kehler, of the U.S. Military Strategic Command stated that: "…need to define Rules of Engagement for Offensive Computer Warfare".

There is media speculation that offensive capabilities are already in place or being developed in several countries.

While from an information security perspective, the three domains discussed here have many elements in common, one of several challenges is whether or not to extend, amongst other, the Laws of Armed Combat (the Geneva and The Hague conventions) to include cyber weapons and define what may constitute protected targets in the event of cyber-conflict.

However, the problem will not go away even if such laws are updated and new Treaties are signed, because non-State actors wilfully ignore conventions or treaties.

2.3 What needs to be done to strengthen security is well known but not done well enough

This subtitle is a modification of the title of a report published by the U.S. General Accountability Office (GAO) in December 2011. Managing information security requires a focus on many disparate activities, in particular:

- Selecting and adopting standards, good practices and guidelines and ensuring these are complied with (Chapter 4)
- Building awareness of information security issues among the workforce and service providers (Chapter 4)
- Identifying the most critical information systems and data, their vulnerabilities and the extent to which their risk exposures require mitigation actions (Chapters 5 and 8)
- Defining the impact of security events on business processes and the organisation as a whole (Chapter 8)
- Defining what the organization considers to be an acceptable risk (Chapter 8)
- Reviewing all of the above for their appropriateness.

2.4 Certifications

Information Security is not a regulated profession and therefore there is no requirement for any form of certification. Where information security is critical, it may be justified to require such certifications. These fall in three categories: organisational, professional and personal.

Organizational certifications include, for example, compliance with ISO 27001 "Information Security Management System" and the U.S. Federal Information Security Management Act (FISMA). Some may be optional (ISO 27001) while others may be mandatory in specific fields of activity such as the Payment Card Industry Data Security Standard (PCI-DSS).

Professional certifications are optional for individuals but employers may choose to make them a requirement. There are several certifications, such as those from the Information Systems Audit and Control Association (ISACA): CISA: Certified Information Security Auditor, CISM: Certified Information Security Manager and CRISC: Certified in Risk and Information System Control.

There are also those of the International Information Systems Security Certification Consortium (ISC^2), including CISSP: Certified Information Systems Security Professional and CSSLP: Certified Secure Software Lifecycle Professional and other. In addition, vendors and training companies also offer various certifications.

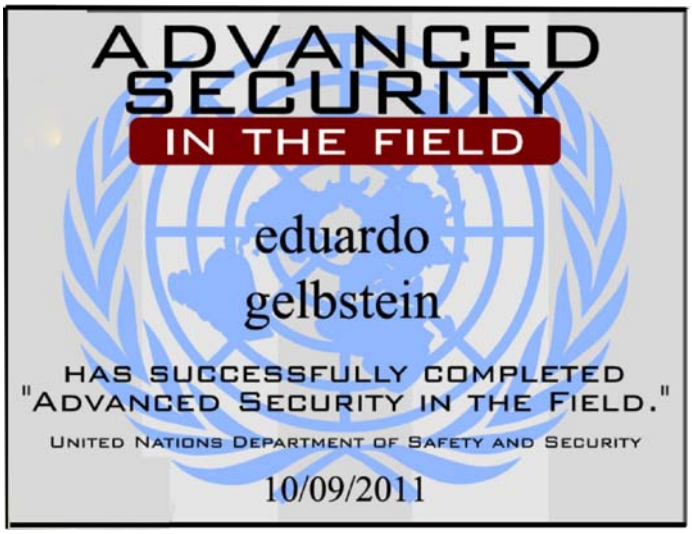

Figure 1: example of a personal certification

The third category is equivalent to a driving license and requires individuals to complete a training or awareness programme and pass a test.

Such certifications have been developed and tested over many years by several organisations. One example is the Security in the Field certificate that the United Nations requires those who travel to a field location to have. This particular certification is valid for three years after which the course and test have to be retaken.

2.5 Asymmetries and consequences

It should have become apparent that, when it comes to information insecurity, attackers have clear advantages:

- No need to be physically present at the location to carry out an attack:
  - There are exceptions – e.g. when the target is not connected to a global network such as the Internet. This was the case in Natanz, Iran, where the systems controlling the enrichment centrifuges were isolated from the Internet and where the malware was introduced using a flash memory device.
- No penalty for failure: every interaction with the defences of a computer network or system provides the attacker with insights that help prepare subsequent attacks.
- No administrative obstacles to overcome: the attackers' key resource is knowledge and their requirements for tools and technology are modest. Their acquisition process is certain to be simpler than corporate procurement, necessitating various levels of approval.

- Those responsible for maintaining the security of information assets are often handicapped by other factors, notably:
    - Pressure to contain or reduce costs
    - Inability to develop strong business cases for expenditure and resources.

2.6 Maintaining security is everybody's job

Technical progress has created an environment that allows access to information resources

- To multiple individuals (internal to the enterprise or not)
- From multiple locations (offices, homes, on the move)
- Using multiple networks (corporate, Internet, home, commercial wireless, telephone)
- With multiple devices (corporate and home computers, tablets, smartphones)

In this environment, many elements are not under corporate control and it is not possible therefore to expect someone else to be whole accountable for the security of information assets. Everybody should be ready to make an effective contribution.

2.6.1 Awareness of the relevance of information security to the specific organisation

Some contracts of employment include clauses specific to information security such as the non-disclosure of proprietary, sensitive or otherwise classified information. Government departments may require the signature of something equivalent to an Official Secrets Act.

Similar criteria may apply to customer information, ranging from name, address and contact information to customer status, e.g. credit rating, bank balances, etc. These may be subject to national legislation such as Data Protection and Privacy.

The disclosure of thousands of diplomatic exchanges by a service member of the U.S. military, the "Wikileaks" affair of 2010, was one situation where an individual with the authority to access information misused this privilege to act as a whistle-blower for reasons unknown, regardless of the consequences to the organisation and the individual.

2.6.2 Human error

Nobody is perfect and unintended actions may impact information security. Working to meet a tight deadline, being distracted, lacking focus due to multitasking, interruptions, feeling unwell, etc., are all drivers for human error. Lack of familiarity with procedures and/or systems as well as reliance on temporary personnel can also result in human error.

There are controls to reduce the possibility of human error. Segregation of Duties being perhaps the most commonly applied – until the trend for the "Lean Enterprise" reduced staff numbers to the point that more and more responsibility was placed on individuals without recourse to an independent check for the accuracy and appropriateness of their actions.

2.6.3 Social engineering

Social engineering predates "social networking" by many years and is best described as "the art of human hacking". Deception and manipulation are embedded in human nature and good practitioners do not need technical skills to break the barriers protecting information assets – they simply ask for the information or for the elements needed to access it. Research carried out in the UK in recent years revealed that many people would disclose their access identifier and password in exchange for a bar of chocolate. Please keep reading…

This chapter explored "lessons identified" – this is not the same as "lessons learned".
The next chapter discusses how information security is defined.

3 Defining information security

In this chapter we consider:

- Availability, Confidentiality, Integrity and other concepts
- The various layers of security and how they relate to information

The previous two chapters discussed "security" without actually defining it, on the assumption that it is such a common concept that everyone understands what it means. Sadly, this is not completely true because of the linguistic ambiguity and confusion discussed earlier.

3.1 What is meant by "Information Security"

In the 1990s, emerging information security standards[3] defined information security as consisting of three elements:

- The preservation of confidentiality: ensuring that information can only be accessed by those authorised to do so
- Maintaining integrity: safeguarding the accuracy and completeness of information and that no unauthorised changes are made
- Ensuring availability: ensuring that authorised parties can access to information when required.

This definition is reflected in the international standard ISO 27000 and is widely used. Security practitioners have proposed additional components. In 2002, D.B. Parker proposed three additional elements:

- Authenticity: ensuring that the parties in an electronic transaction are who they claim to be and that the components of the transaction are genuine.
- Possession and Control: loss of possession and control of data creates the risk of loss of security. Example: a laptop computer forgotten and unrecovered at an airport security point.
- Utility: the ability to use the information. For example suppose that encrypted data is provided to an individual together with the encryption key but the recipient loses the encryption key. The data remains available, authentic and confidential, it retains the original integrity and is in the intended person's possession. But as it is not usable it has no utility.

Electronic commerce added one more element: Non-Repudiation: The mechanism that ensures that a party to a transaction cannot deny having received a transaction and neither can the other party deny having sent it.

3.2 Differences between Enterprise security, Information security and Information Technology security

The management of information security relies on three distinct areas of accountability. These are not always well linked or coordinated as their management is placed in different organisational structures which may not even talk to each other. These are shown in Figure 2.

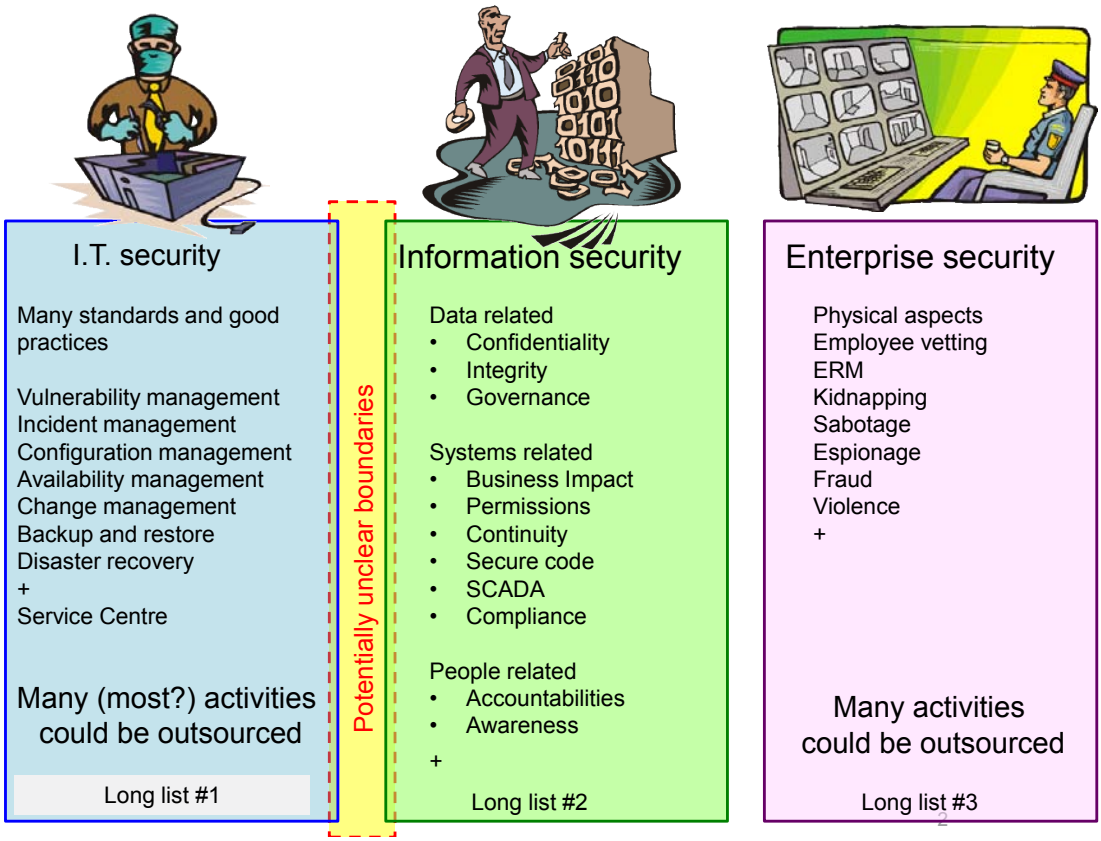

Figure 2: the organisational pillars of corporate information security

3.2.1 Enterprise and Physical Security

There are few organisations that do not have some form of physical security and someone responsible for it. The presence of receptionists or uniformed guards to control access is familiar to everyone.

But, do they and their colleagues, many "behind the scenes", have responsibilities for information security? In fact, they do, together with other units. This starts with pre-engagement background checks for or with the Human Resources function. These may cover prospective employees and also consultants, external auditors, vendors and other visitors. The strictness of such checks should reflect the sensitivity of the individual environment.

Physical security also monitors access controls and ensures that sensitive areas can only be accessed by those specifically authorised to do so. In addition, they take measures to ensure that equipment and data owned by the organisation are not removed without authority (easier now, given the miniaturisation of devices), and, that any devices lost or stolen are dealt with appropriately, including remote blocking and wiping clean their content.

This is followed by credentialing, which may take the forms of a "VISITOR" label or a badge programmed to open predefined doors and/or be used as a token to access a computer system.

The physical security team is also responsible for dealing with suspected or actual breaches of security and this may include investigations, seizure and maintenance of a legally acceptable chain of evidence and, when necessary collecting all credentials and items owned by the organisation before escorting a sanctioned person out of the building. Such actions are notified to the HR department who then takes all the necessary employment and administrative steps of separation, in particular ensuring that the person's access to computer systems and data privileges are terminated.

3.2.2 Information Security

An organisationally dispersed activity, this deals with the actual information assets of the organisation, in whatever form they are kept (paper or electronic) and wherever they are kept (archives, the computer "cloud", an outsourcing company, an employee's home, etc.).

A requirement for confidentiality implies that the "owner" or "custodian" of the information is the only party with the necessary knowledge to define what should be confidential and under what conditions. The process for doing this is called Data Classification.

There are many ways of classifying data and organisations have their own criteria for doing so. This is fine, as long as these criteria are applied consistently and systematically. One "easy" (= lazy) way is to say: "Everything is confidential" and accessible only to those specifically authorized to access a specific item. This may sound tempting but the amount of data held by organisations is huge: intellectual property, commercial, operational, legal, financial, HR, procurement and much more…. In a large organisation, assigning access rights to individuals and maintaining them as they change jobs is unrealistic.

At the other extreme, there are those who say "we are proud of our transparency and have nothing to hide, so don't classify anything". This is naïve. Every organisation, however simple or small has data it should not make public, for example the address and bank information of an employee (for privacy reasons), details of commercial proposals during a bidding process (commercially sensitive), valuable proprietary information, and more.

There are several possible classification categories between "Top Secret" and "Public", such as Restricted to (*a defined group*), Embargoed until (*a given date*), etc. Each category clearly defined and supported by clear rules. The right balance between restrictions and openness may not be obvious but, without it, the organisation is either tied up in knots or exposed.

There is an additional managerial challenge: every part of the organisation relies on specific computer networks and applications. The management of the specific business process and its tools needed to support them are accountable for ensuring that the rights of individuals accessing these systems or "permissions" are consistent with their roles and responsibilities.

For example, a bank employee working in a provincial branch would have no reason to access data on clients at other locations. If access is enabled there is a need to define that define what the person is allowed to do with the data (read only, download, update, create, delete).

This is an onerous task which when not appropriately managed, may result in people accumulating access rights (usually referred to as "permissions") as they move through the organisation as a result of promotion or reorganisation.

In practice, it is hard to create a detailed and complete list of permissions when one does not already exist. There are tools supposed to facilitate this process. Newer enterprise systems include tools to define Role Based Access Controls (RBAC). These controls and any temporary exceptions to them, , require management attention and regular validation.

3.2.3 Information Technology Security

Perhaps the most visible and talked about component, this belongs in a technical environment that has its own culture and language. Essential to protect information from unauthorized access and modification, these activities may not reside in the organisation as is the case when information technology operations and services are provided by an external supplier. Such suppliers are usually providers of outsourcing, offshoring, 3rd Party services, temporary staff and others.

It is usual to find a Chief Information Security Manager (3.4) in the I.T. department with well defined responsibilities and objectives.

None of topics in this section can be said to have "a right answer" and there are many books where they are discussed.

The next chapter examines the managerial challenges information security presents to an organisation.

4 Managing information security in the enterprise

This Chapter examines

- The components of security governance
- Managing for security: standards, good practices and guidelines
- What makes a good Chief Information Security Officer?
- Your role as a manager

Society operates on the basis of trust, a complex subject with ethical and social implications. Trust represents a belief in the honesty, fairness and goodwill of the parties concerned. Chapter 2 showed that trust in cyberspace has been deliberately broken often over many years.

Loss of trust led to the development of standards, good practices, guidelines, information security policies, legislation and other measures considered necessary for the protection of information assets.

> Fidarsi è bene. Non fidarsi è meglio.
> (To trust is good. Not to trust is better)
>
> Italian proverb

Achieving a satisfactory level of information security requires many things to be done and these things requires leadership and management if they are to be performed well enough. To illustrate this, consider the analogy of an orchestra and its conductor:

The conductor provides leadership by making it clear to the musicians, every one a professional and the "manager" of a musical instrument, what is expected of their performance as part of a group. The conductor does not need to by able to play every instrument in the orchestra but must have credibility and gain the respect of the players.

A brilliant conductor can get good performances from a mediocre orchestra. When a not-very-competent conductor ends up in front of a first class orchestra, its members will usually perform well by ignoring the conductor. When the conductor and the orchestra are both mediocre, the outcome will be, at best, mediocre.

4.1 Information Security Governance

The purpose of information security governance is to evaluate, direct and monitor the actions taken to meet the organisation's requirements and how well these are executed. The purpose of this is to reduce the business risks of operational disruption, loss of sensitive data, litigation and failing to comply with regulatory and legal requirements. Information security governance (ISG) needs to be carried out at a level that can decide on:

- The organisation's security strategy that reflects known and emerging risks
- The organisation's security policies
- Accountabilities for information security across the organisation
- The allocation of human and financial resources
- The adequacy of past performance.

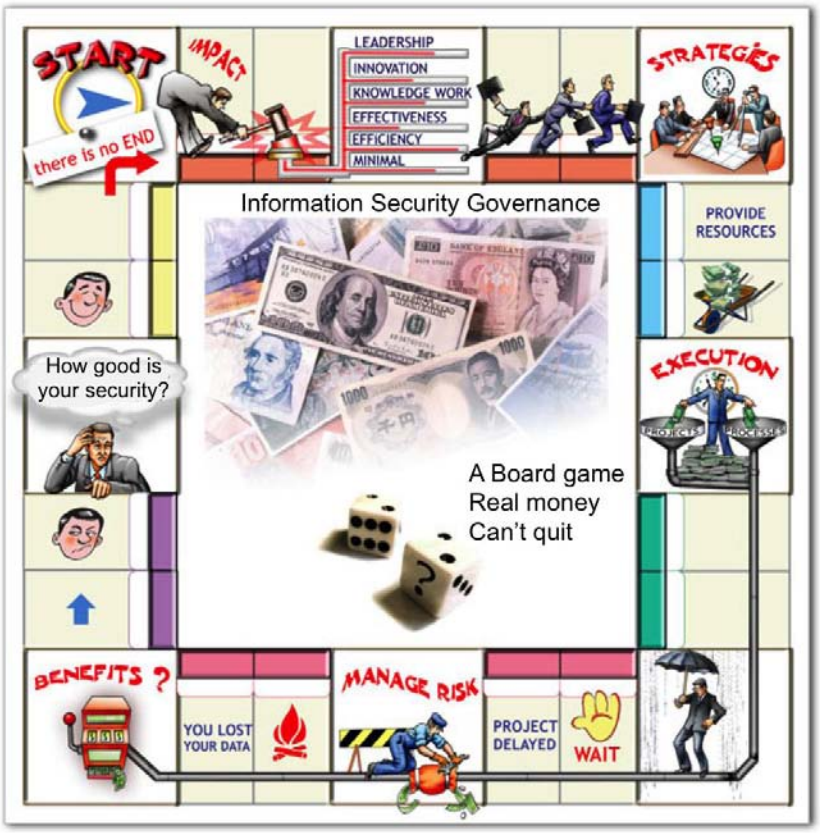

Figure 3: Information Security Governance as a Board game (played with real money)

4.2 The components of information security governance

4.2.1 The organisation's security strategy

In the eyes of executives and senior management, information security is a business support function, no doubt important, but also an element of cost to the business. Therefore, an information security strategy describes how to migrate from an "as is" situation to a target destination. By doing this, senior management decides how to best spend the (invariably limited) organisation's funds.

As information security expenditures target hard to quantify future risks and outcomes, a good strategy aims to reduce the risk of something really bad happening, which thus becomes a hypothetical benefit.

Comparing intangible cost-avoidance projects (such as security) against more conventional profit-oriented investments has no easy answers.

The information needs to support an information security strategy includes:

- Relevant audit recommendations and the status of their implementation
- Past information security incidents and their operational and financial consequences
- Security metrics such as Performance and Risk indicators
- An assessment of the extent and quality of existing controls (as provided by Internal Audit);

- Business Impact Analysis
- An Information Risk Register, including the status of planned mitigation actions
- Information security intelligence ("what is going on out there?")
- Status reports on compliance (regulatory, legal and with internal policies)

The information security strategy should have sufficiently detailed descriptions of the organisation's objectives, it's priorities and how it proposes to organise and fund the programme

4.2.2 The organisation's security policies

> Never issue a security policy that you cannot or will not enforce.
>
> Statement by a speaker (who does not wish to be named) at a Security Conference

These constitute a set of documents describing specific requirements and rules that must be complied with. For clarity and conciseness, each policy should cover a single area. For example, a "Password" policy would cover the rules and regulations for creating, maintaining and changing them.

A corporate portfolio would contain several policies, e.g. on: Appropriate Use of information resources, Use of unencrypted public Wi-Fi networks, Installing software on devices used to access corporate data, etc. The SANS Institute has comprehensive lists as well as policy templates (see Chapter 9). There are other sources for such templates and also consultants offering this service.

For such policies to succeed, they should be reviewed and approved by those who may have to deal with non-compliance issues, usually the Human Resources function and Legal Counsel. Consultation with representatives of the workforce may be a good move.

Issuing and disseminating policies is a challenge: The easiest way consists of posting the policies in a corporate Intranet and relying on employees to find them and take note of them. It is unreasonable to expect such an approach to be effective. The proverb that says that "you can take a horse to water but you cannot make it drink" says it all.

At the other extreme, there are ways to ensure that every employee receives a copy of the policy, acknowledges receipt and signs a document stating intention to comply. This document is filed in the HR record of each individual. This is too complex.

The selected approach should reflect the importance of information security to the specific organisation and it's culture.

4.2.3 Accountabilities for information security across the organisation

The easiest way to ensure that key tasks will **not** be performed is lack of clarity on who is accountable for what. In large organisations, where size and complexity require formal procedures, accountabilities are also incorporated in job descriptions to avoid the "not in my job description" syndrome that exists particularly when dealing with disengaged employees.

In addition there are roles to be assigned to people outside the I.T. function (external or internal) to define access account needs, system and data privileges, approve exceptions, etc., as described below.

4.2.4 Resource allocation, human and financial

Possibly the most critical governance task, it requires decisions consistent with the assessed:

- Current information security performance, i.e. is it good enough?
- Knowledge, experience and certifications of those accountable for information security
- Extent and quality of existing controls (does Internal Audit consider them adequate?)
- Is information security part of the Cost of Doing Business or a corporate investment? How should such expenditures be justified
- Suitability of current performance and existing controls
- Future human resource needs to support information security activities.

The quality of these decisions will define whether the information security strategy succeeds or fails.

4.3 Managing for security

Figure 4 illustrates the basic steps involved in managing information security in an effective way:

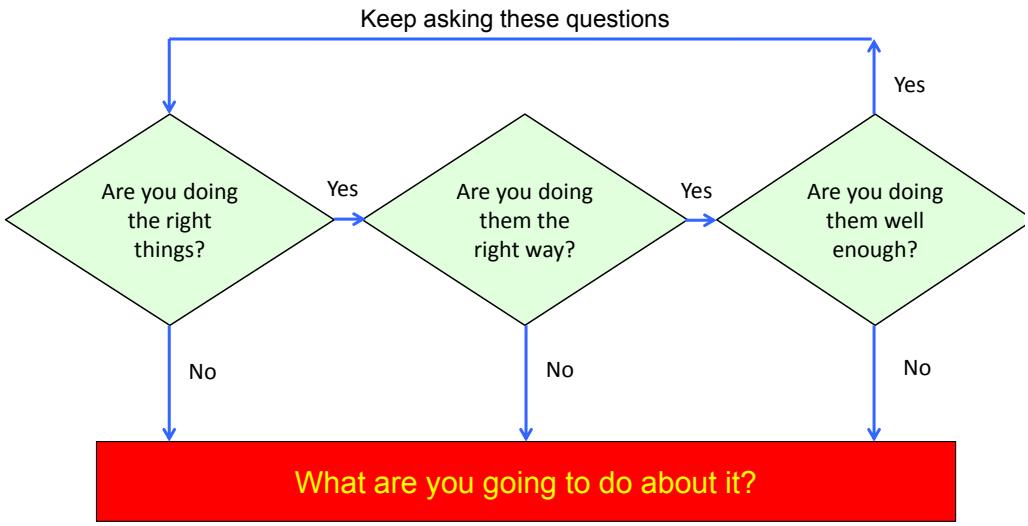

Figure 4: Managing execution for security

Execution – returning to the symphony orchestra model, a good performance requires every player to give her or his best towards it. In information security, this requires a clear understanding of roles and responsibilities, knowledge of the relevant business processes and the role of information systems and data in supporting them, experience, motivation and commitment.

The three questions in the figure apply to everything we undertake. Success requires all three to be answered by "YES" and when the honest answer is "NO", there will be no improvement without action.

This section aims to provide pointers to the reader to what are "the right things", "the right way" and "well enough". Every organisation may have different sets of answers to these questions, which is to be expected, as there are many options to choose from.

4.3.1 Are you doing the right things?

The "right things" include topics such as:

- Having an effective security governance mechanism
- The adoption and implementation of standards, guidelines and good practices. There is no such thing as a "best" practice – such published practices are compromises by committees
- Having clear definitions of objectives, targets, accountabilities resources, metrics, etc.
- Having clear and enforceable security policies
- Establishing a programme of briefings and training on information security.

If the answer to this question is NO, the organisation is exposed. At best, people will need to guess what is expected of them and/or not have the skills or resources required to do their work.

4.3.2 Are you doing the right things the right way?

Instead of developing and writing their security policies (not a trivial task) there are those who opt for an easier way to do this: buy standard templates for such documents, do a quick Search and Replace, print the documents and put them in a filing cabinet. This creates the belief that "it's done". This approach is far removed from being a good practice.

The same is true for engaging consultants to do this without participation and commitment from the workforce. Consultants can add value through their experience but, at the end of the assignment, they'll leave to go to another client. After they have gone, nobody in the organisation will feel ownership of this work. In the end this will once again end up in a filing cabinet.

There are other activities that need to be done the "right way" in line with the chosen standards and good practices. These choices are influenced by national and organisational cultures, government and regulatory requirements, and the preferred practices of service providers, outsourcers and organisational practitioners.

If the answer to this question is NO, it would be good to explore why not. Many reasons can be imagined: lack of time, lack of funding, lack of knowledge, technical arrogance ("we know better"), lack of clarity as to whose decisions these are, etc.

4.3.3 Are you doing the right things the right way well enough?

It is possible that the answers to the two previous questions were YES and this is good thing. However, doing things well enough requires knowledge, dedication, discipline and employee engagement.

When any of these are missing, tasks will be executed in an unsatisfactory way and be supported by excuses: "Sorry, I did not have time to do the data backup for this critical system and the data is now lost", or "Sorry, I did no do the test on this modification as I was sure it would be OK" (guess what: it wasn't).

If the answer to this question is NO, the organisation has a management problem that may require injections of motivation, training, and recruitment and, possibly, more drastic actions.

4.3.4 Standards, guidelines and good practices

Many sets of standards and good practices for information security have been produced. These are the work of professional bodies, working groups of dedicated practitioners. As technologies change fast, none of these documents can be considered to be "definitive". Some of the items in the list that follows are widely accepted to be Good Enough:

- The ISO 27000 family of standards for the management of information security: These documents are published by the International Standards Organisation, regularly reviewed and updated.
- The NIST SP800 series of documents, published by the Computer Security Division of the U.S. National Institute for Science and Technology. Consisting of well over hundred documents, these are also regularly updated.

Other relevant guidelines and good practices cover more specific segments of the practice of information security. Amongst them:

- The Information Technology Infrastructure Library (ITIL) covers generic process descriptions. These aim to improve the consistency with which processes are implemented and executed. ITIL is widely used around the world and led to the development of the international standard ISO 20000 on I.T. Service Management.
- The Control Objectives for Information Technology (COBIT), issued by the Information Technology Governance Institute (ITGI) and the Information Systems Audit and Control Association (ISACA). Its current scope covers governance, planning and organisation, acquisition and implementation, service delivery and monitoring. COBIT 5, issued in 2012, includes separate publications dedicated to information security.
- The Data Management Body of Knowledge (DMBOK) dealing with all aspects of managing data resources.

This list is just the "tip of the iceberg". Which, if any, should be adopted is defined by the security strategy of the organisation, its culture and language (all the above are available in English and some have been translated into other languages).

Adopting and implementing any or all of the above requires a considerable learning and training effort followed by a commitment to change daily practices and strive for continuous improvement. Change is hardly ever welcomed and, more often than not, vigorously resisted.

4.4 What makes a good Chief Information Security Officer (CISO)

In the beginning… (20 to 25 years ago) information security was integrated in the I.T. function and seen as a technical role. Times have changed, and so have the multiple possible roles of information security professionals.

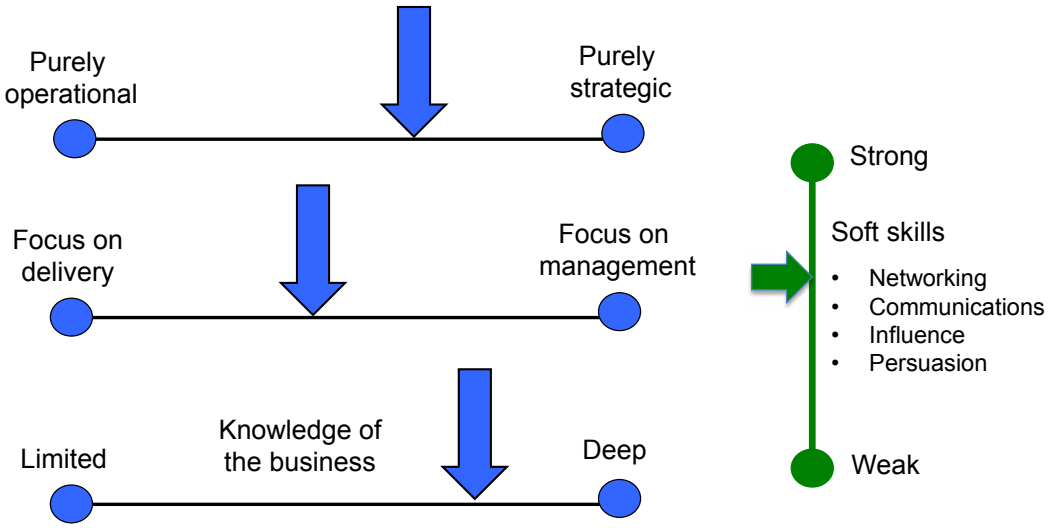

Figure 5: Different types of CISO

The arrows in Figure 5 can be positioned anywhere along the line between the points describing the role of a Chief Information Security Officer. Senior management (including the Chief Information Officer) needs to define which choices are most appropriate for their organisation.

4.4.1 Is the role operational or strategic?

A strategic role requires interaction with several managers, including the Chief Information Officer, Chief Security Officer, Chief Risk Officer, Internal Audit, General Legal Counsel and multiple Business Units – as well as with executive management and the board of directors. This requires the CISO to have good knowledge of the business and soft skills: communications, interpersonal relations, negotiations and ethics. In addition, presentation and credibility are essential.

4.4.2 Focus on delivery or on management?

Service delivery is a technical job requiring knowledge of products and procedures. These individuals are often invisible to the organisation and the need for soft skills is less critical.

Operational management requires the CISO to manage the activities and performance of several technical specialists and have a good knowledge of related disciplines such as risk management, business continuity, intellectual property protection, data leakage and integrity issues, regulatory compliance, privacy, forensics and investigations, etc.

4.5 **Your** role as a manager

It may not appear in your job description but security really is "everyone's job". Managers have to:

4.5.1 Develop security awareness

Whenever any one says: "I did not know", this creates a vulnerability and thus, a risk to the organisation. Individuals in your team should be familiar with the need for maintaining security and also with the organisation's information security policies and why compliance is important.

4.5.2 Manage internal threats

This is part of every manager's accountabilities and includes identifying and addressing instances of:

- Non-compliance with policies;
- Disengaged and demotivated, employees;
- All forms of sabotage, lost equipment or data, the theft of intellectual property and other unauthorised disclosures, fraud, etc.

The Human Resources function, Legal Counsel and Corporate Security should be consulted on these matters and their advice on investigations is essential before any action is taken.

4.5.3 Sponsor and practice good digital hygiene

Hospital infections were rampant in the 19th Century and even the early 20th Century. Good hygiene and antibiotics transformed this, except now hygiene needs to be strengthened again because of unintended consequences such as the emergence of antibiotic resistant bacteria. The following are good hygiene practices:

- Protecting equipment and data against loss or theft and prompt reporting whenever this happens;
- Maintaining software updated (particularly end-user owned equipment)
- Applying well designed non-guessable passwords and, better still, using two-factor validation and never sharing such passwords with others
- Installing and maintaining up-to-date tools to prevent unauthorized access (e.g. firewall) and block or remove malicious software (e.g. anti-virus)
- Taking appropriate care not to disclose sensitive information through Social Media (e.g. Facebook, Twitter, Linkedin)
- Using encryption to protect sensitive data if this is aligned with the organisation's security policies
- Making copies of information (backup) and preserving them in a secure manner (encrypted, secure cabinets, etc.)

The next chapter discusses internal sources of insecurity by exploring four domains of vulnerabilities.

5 The four domains of vulnerabilities

In this chapter we take a closer look at the various things that create vulnerabilities that may result in information security breaches

- Information Security Governance
- People (I.T., management and others)
- Processes (in I.T. operations, applications, support, data and project management, incident response, disaster recovery, business continuity and crisis management)
- Technologies

Vulnerability refers to an inability to resist a hostile environment. Things that are man-made are never 100% invulnerable. Besides, information technologies are subject to failure and obsolescence.

Anything that can go wrong will do so at the worst possible time.
Anything that could not possibly go wrong is only waiting for the opportunity.

One of many formulations of Murphy's Law

5.1 Governance vulnerabilities

Information Security Governance (ISG) is often less than successful for a number of the reasons:

- Executives and Senior Managers have many diverse topics to deal with and face heavy demands on their time. ISG adds to their workload and covers a topic they may be unfamiliar with. Therefore it gets displaced by other priorities.
- Inability to value the organisation's information and data. This inhibits informed discussion on the needs for security and the resources to be assigned to this.
- Each organisation has a unique culture, which includes "politics". This can cause problems when functional silos seek to maximise their influence and budgets.
- A lack of willingness to enforce policies, which renders them useless.

5.2 People vulnerabilities

It should not come as a surprise that people at all levels of the organisation are the weakest element of information security. After all, people play a role in information security activities – amongst them:

- End users
- Project managers and implementers
- Designers (from a relatively simple spreadsheet to complex software and networks)
- Requesters and authorisers (for creating accounts and defining access rights and privileges)
- Systems and data owners (or custodians)
- Technical roles in service delivery and support
- Strategy and policy designers (at the functional, departmental or enterprise level)
- Buyers (corporate and individual)
- Consultants and/or auditors
- Other.

The vulnerabilities associated with these roles fall into four categories:

5.2.1 Lack of knowledge/awareness/training

The management and maintenance of information security are not intuitive tasks. However, unlike driving a car, they can be carried out without having to provide a certification or a license.

Some measures to strengthen information security can be automated and enforced. One example is requiring an end user to change their password every month. This is good, but not knowing how to design an adequate password, someone may select "123456" or a date of birth. Worse, when several passwords need to be created and maintained, they are likely to be written down and even placed in a conveniently visible place.

Placing policies, guidelines and recommended practices somewhere in a corporate Intranet is less expensive than providing awareness sessions, tutorials and other forms of training. However, pressures to reduce expenditures make these an easy target for budget cuts.

5.2.2 Accidental and unintended actions

Even with the best training, people are fallible and a security incident caused by human error cannot be excluded. Errors can arise through pressure to meet a deadline, stress, fatigue, not following rules and policies, etc.

Individuals can also be victims of deception and act against the interests of the organisation, by e.g. disclosing confidential information. Services such as text messaging, blogs and social media have made this easy to do. Social engineering in the form of deception is not uncommon. Somebody may claim they are calling from the Help Desk to ask an individual to confirm their password. They do.

5.2.3 Deliberate actions

A well established concern: an individual (employee, consultant, contractor, cleaner, security guard, etc.) motivated to act against the organisation. Fraud, theft of intellectual property, data corruption, sabotage and extortion, do happen and are sometimes not detected for a considerable time.

5.2.4 Lack of engagement

A hard vulnerability to deal with: individuals who don't care about information security, guidelines or policies. Unmotivated or disgruntled for real or perceived grievances, these individuals should be regarded as "toxic" as their behaviour can be contagious.

When their contracts of employment and the culture of the organisation makes it difficult or impossible to sanction their behaviour, they can become over-confident – once upon a time one such person told their boss: "I don't want to and you can't make me". What the boss did is another story.

5.3 Process vulnerabilities

There are many definitions of what is a "process". For this book, a process is: a set of related tasks, carried out by people and/or tools that transforms inputs into outputs. Processes should be carried out systematically to achieve consistency, remove errors and support improvements. The Capability Maturity Model (CMM) is used to define the level to which a process has been formalised. This maturity is defined in five levels:

1. Initial: an undocumented, usually unrepeatable process (also referred to as chaotic or ad-hoc);
2. Repeatable: the process is at documented to a point that it may be possible to repeat the same steps each time it is carried out;
3. Defined: the process is defined in detail in terms of work instructions or procedures) and implemented consistently;
4. Managed: the process is quantitatively managed with agreed metrics;
5. Optimised: process is managed to include continuous optimisation or improvement.

While the principles of process management are simple enough to understand, the higher maturity levels are hard to achieve, as this requires a sustained effort over a long time. Operating at level 1 is asking for trouble. Level 3 should be considered a desirable initial target.

The challenge of reducing process vulnerabilities begins by identifying those processes that are critical to information security, and, having done so, adopting the standards, guidelines and good practices that best match the organisation's culture and requirements.

Mapping such processes against information security needs, requires consideration of:

- Processes owned by service providers (internal I.T. departments and external service providers);
- Processes owned by system designers and implementers;
- Processes owned by system and data owners;
- Processes owned by end users.

5.3.1 Processes owned by service providers

Management should not be particularly concerned with which, if any, of the available frameworks has been adopted, unless there are frequent performance problems and/or audit recommendations highlight specific areas of risk.

Good practice establishes formal Service Agreements with internal service providers that specify performance targets and how performance will be measured. When the service providers are external to the organisation, such agreements are defined in legally binding contracts. These also specify performance targets, how performance will be measured and reported and make provision for penalty clauses when performance fails to meet the agreed levels.

5.3.2 Processes owned by system designers and implementers

Software development may have started as a craft and became more formalised and structured over the years. The Software Development Life Cycle (SDLC) model is well established (there are other models, e.g. agile programming). In essence SDLC has three major domains:

Planning: begins with identifying the need and making the business case, then specifying the requirements, deciding whether to buy or build, requesting offers, evaluating them, etc., until a decision is taken.

Implementing: developing or adapting software to meet defined needs, documenting and testing to the point that it becomes possible to support future changes and enhancements.

Deployment: the software is approved for installation in a service provider's production environment and is subject to maintenance (the removal of errors) and supporting end users.

Usually done by vendors or specialised companies, there are several guidelines and good practices that describe the numerous processes in detail with the objectives of providing Quality Assurance and future maintainability. One such set of guidelines is the Software Engineering Body of Knowledge (SWEBOK).

There is, however, a "however": Many end users are computer literate to the extent of designing and implementing sophisticated software, from complex spreadsheets to web pages, without thinking of such activities as software design. As a result, good practices may not be followed and the resulting product may not be adequately documented or tested. Despite this, they are put to use in order to support critical activities and decisions.

5.3.3 Processes owned by system and data owners

There is an old expression about data and computers: Garbage In Garbage Out (GIGO). This is as true today as it was when first stated.

The process of Identity and Access Management (IAM) is fundamental to information security. It defines the specific individuals that need an account to access specific systems. A Help Desk or similar group will create such accounts but accountability for requesting and approving their creation, modification or termination remains with the systems owners. Such approvals (or denials) should be traceable.

Having created an account for an individual, the next step is to define what data this person can access and what operations can be performed on it. For example, an Accounts Payable employee should not have access to the Human Resources records. Similarly, a Payroll employee should not have the authority to modify someone's pay without proper controls.

Accounts and permissions need to be managed through a lifecycle that reflects career moves, promotions, disciplinary actions, etc., from the day they are created until the individual leaves the organisation. Vulnerabilities are created when these activities are left "for another day" due to other priorities or pressures to reduce costs.

Data related processes fall in three categories: data quality, data classification and system permissions. The Data Management Body of Knowledge (DMBOK), a book of some 500 pages, gives a detailed set of guidelines for managing data. Data quality, while essential, has limited impact on security.

Data classification is closely tied to confidentiality. Classification requires data owners to assign data to a category in a set that applies to the whole organisation. Typical labels for such categories include Secret, Confidential, Restricted, Embargoed until, and Public. Failure to classify data is an invitation for it to leave the organisation without proper control.

5.3.4 Processes owned by end users

The popularity of small and powerful devices (lightweight computers, notebooks, tablets and smartphones) and their rapid adoption by the population at large together with the trend to use such personal devices in the work environment – the "Bring Your Own Device" extends the need for security processes to be owned by end users whenever these devices access or store sensitive data.

While the basics, such as keeping software updated, using anti-virus software, making backup copies of data, etc., briefly mentioned in 4.5 should be well known, in practice they may not be the case. Many people do not appear to be concerned about the risks of not doing so. In addition, social networks and free /low cost downloads of software, particularly Apps for smartphones and tablets, have all introduced new risks.

5.4 Technology vulnerabilities

Technologies are prone to failure. This may be gradual, as when corrosion weakens a bridge, or sudden: the lights go out. Failures may be contained through checks and maintenance and some may be repairable. Not always, as the damage may be too big to repair (e.g. the nuclear plants at Fukushima) and becomes irreversible.

Failures in information technologies are rarely gradual. Hardware failures are often repairable, but not always: a fire (or flooding) in a computer room may require the replacement of all the equipment. Software failures due to design errors (bugs) are fixable provided time and expertise are available.

Failures due to a cyber-attack have unpredictable consequences: A cyber-attack on the administrative systems of Saudi Aramco in October 2012 infected 30,000 computers and erased all of their data. Cleaning and testing each of these 30,000 computers and recovering their data (or at least part of it) were major projects.

5.4.1 Lack of security by design – lessons to be learned from the safety industry

Information security has always been a source of concern. In the early days of computing, it focused on access controls for a small number of people.

When personal computers emerged in the 1970s, they were primarily for enthusiasts, often I.T. people, and were not deployed in organisations until the mid 1980s. The basic design of such computers did not include security features. Malicious software appeared a few years later – the word "virus" was first used in 1984 – and at first it was essentially a nuisance. Personal computers were not yet networked and infections spread through the exchange of floppy disks . Current designs still require the user to obtain additional products (e.g. antivirus, encryption, electronic document "safes").

Work towards what we now call the Internet started in the mid 1960s as a restricted resilient network. Its designers did not expect that it would become a global network with major security implications. The impact of malicious software on the Internet was discovered in 1988, when a program written by a student (the Morris Worm) spread rapidly through the Internet and caused it to grind to a halt. The designer of this worm is reputed to have said "I should have tried it on a simulator first".

Mobile phones appeared in 1973 as a portable device to make voice calls. They have developed into "smartphones" and "tablets", powerful devices that, like personal computers, do not incorporate security as an intrinsic part of their design – other than perhaps requiring (the optional) use of a four digit personal identification number (PIN).

The safety industry, found in extractive industries, construction, transportation, manufacturing, health care and other, learns from experience. Their views are that bad practices exist and lead to near misses e.g. the hammer that falls from the top of scaffolding but does not hurt anyone. Near misses are rarely reported. "Luck" being what it is, does not always work to the organisation's favour and minor incidents occur on a regular basis. These are reported and become part of the safety at work statistics.

From time to time, a major incident will occur. The safety industry promptly carries out investigations to identify the root cause and take steps to remove it. Such modifications are extensively tested before being made operational. An example in 2013 involved a whole fleet of new airplanes (Boeing 787) that were grounded for several months until a design modification was tested to the satisfaction of certifying authorities. At present, this is not the case in the I.T. industry.

The concept of unintended consequences goes back to the late 1700s. These include benefits, negative side effects or perverse effects contrary to what was intended. Innovation in information technologies has brought all three, none of which could have been envisaged a priori. In the world of I.T.:

Unexpected benefits include the ability to interconnect the world and provide easy access to information and services and enable new forms of entertainment and business.

Negative side effects include the emergence and spread of malicious software, a measure of loss of privacy and many opportunities to waste time.

Perverse effects count among them all forms of cybercrime, successful attacks on critical infrastructures, theft of intellectual property and potentially, new forms of warfare.

Three additional areas of vulnerability domains meriting management attention are SCADA, Cloud computing and Mobile devices:

SCADA is the acronym for Systems Control And Data Acquisition: devices and networks interfacing with the physical world ranging from relatively simple controls of air conditions and lifts, closed circuit TV and sensors in surveillance, ATMs, etc. to complex distributed systems in the control of manufacturing processes, utilities and transport. These rarely are the responsibility of an I.T. function and are designed for simplicity and reliability, not security.

Cloud computing is the shorthand description for computing resources delivered through the Internet. In this environment computer hardware and software is managed by a third party and is shared amongst several clients. This offers simplicity and lower costs by not having to have a corporate infrastructure. If the connection to the Internet is lost for whatever reason – from denial of service attacks to physical damage to the network lines – all the services delivered through the Cloud will be unavailable until the disruption is fixed.

The mobile world is subject to new challenges ranging from malicious software targeting portable devices, data theft, loss or theft of devices and, increasingly, other issues emerging one at the time, such as the ability to geo-locate an individual through their devices creating risks that are not yet fully understood.

The next chapter discusses other factors that contribute to information insecurity all of which should be of concern to management.

6 Other drivers of information insecurity

In this chapter we consider other factors that management should be concerned about.

> Good managers remove obstacles, provide help and acknowledge effort.
>
> Well known but not always applied advice to managers (source unknown)

Maintaining good enough information security in an organisation is a complex. Many believe someone is doing this and that they don't have any responsibility for it. This chapter explores topics that are not covered by standards, guidelines or good practices and yet, can be found (if recognised) everywhere.

When they remain unrecognised and/or nobody is accountable for them, they add to the information **in**security of the organisation.

6.1 Causes for concern

6.1.1 Internal to the organisation

Executive detachment: Good governance requires commitment and support from the top. Without it people have no choice but to guess what is expected of them and make a best effort to get things done.

At the most senior levels of any organisation, detailed knowledge is unavoidably diluted and the demands on their time are many. Getting their attention requires good communications skills, a clear business case and the ability to deliver the message in a short time.

Organisational culture and politics: A fact of life. To play the game requires knowing who has influence in the organisation and how to create a meaningful dialog with them. Failure to do this will neutralise the best efforts of those whose role is to strengthen security.

Silo mentality: Lack of cooperation between functions is not uncommon in politicised organisations. When this is entrenched, only transformational leadership can change the status quo. This is harder to achieve in large organisations than in smaller ones. From an information security perspective this means one thing: TROUBLE.

Digital Natives[4]: Articles published in 2001 introduced the terms "digital native" and "digital immigrant". Digital Natives are the generation that had the opportunity to interact with digital technologies from an early age, understand their concepts and have an intuitive approach to them. Digital natives drive the End User Revolution discussed below.

Digital immigrants retain many elements of their before-the-digital-era approach and use the digital world with some effort. These are the people who have to read manuals…

Disposal and recycling: Another governance issue relates on the retention and disposal of data to ensure that devices are not discarded containing corporate data. It is prudent to involve legal counsel before taking action and then taking appropriate steps to erase all data from such devices.

6.1.2 Funding information security expenditures

Funding information security is part of governance. Executive detachment and organisational politics can make this a controversial topic.

There are those who argue that protecting the organisation's information requires investments. This leads to the question "what is the return on security investments?" Others argue that funding security is part of the cost of doing business and that such expenditures should be aligned with the value of the assets to be protected, in the same way as insurance premiums. Both arguments are valid and remain an unresolved semi-philosophical debate.

Funding information security covers activities in different parts of the organisation such as:

- Technical purchases for the I.T. service provider (if internal) and for assorted items across the organisation (e.g. anti-virus products, tokens for authenticating end users, equipment and software upgrades and maintenance, etc.)
- Consultancy and audit services for updating information security strategy and policies, Business Impact Analyses and Risk Assessments (Chapter 8)
- Training and awareness material as well as workshops and certifications
- Resourcing a continuing data classification programme
- Ensuring disposals are carried out without exposing the organisation's data.

Separating those activities specifically dedicated to security from other operational I.T. activities is not easy. Notwithstanding, published evidence indicates that I.T. expenditures are typically in the order of 3 to 5% of an organisation's total expenditures and that information security represents around 5% of this.

A Gartner Group report[5] for the year 2012 shows that the average expenditure per employee per year in the U.S. was $13,600. For a working year of 220 days, the daily I.T. expenditure per employee is $62, of which about $3 are for information security. This is comparable to the price of a cup of coffee.

The relentless pressure to reduce expenditures frequently requires the financial justification of things that are not easily quantified, such as the Return on Investment (ROI) on data or of protecting reputation.

The expenditure part of an ROI analysis for information security is straightforward. Experienced practitioners know that some items can be safely left out of the calculation, e.g. the cost of procurement, maintenance fees and installation costs. The Benefits part is like a work of fiction in which it is relatively easy to come up with "good" numbers.

Risk is in the future and data to support reliable predictions is not available. This means that whatever numbers are presented as benefits cannot be validated, let alone guaranteed. These numbers are conditional on several (implicit) assumptions such as: that the product proposed works as promised by the vendor, that it has been correctly installed and configured and that those using it know what they are doing. These are not always the case.

There is also the implicit risk that the pursuit of cost savings can result in Budgetary Anorexia (or Saving Money Regardless of Cost (SMRC)) that may end up being counterproductive. Typical SMRC actions include:

- Salami approvals – one at a time with a focus on cost reduction
- Selection of the lowest bidder regardless – this not always a successful strategy
- Deferring expenditures as in: "surely this can wait another year"
- Postpone recruitment as in: "work smarter, not harder"
- Limited or no Segregation of Duties – an open door to incorrect or untested changes
- Rigid remuneration – leading to the inability to recruit and retain the talent required.

When all of these are used consistently, it is very likely that experienced staff will look for a job elsewhere and find it as such people are in short supply.

6.1.3 The end user revolution

Digital natives have taken to recent innovations with great enthusiasm, to the extent of queuing overnight outside a store in order to buy the latest object of desire. This is fine in their private domain as individuals are free to do whatever they like and/or can afford.

These devices are finding their way into the corporate environment, as individuals feel empowered to challenge corporate standards and insist that they be allowed to use their device, service or application. This has led to the Bring Your Own Device (BYOD) movement and organisations are struggling to understand and manage the security implications of this. As BYOD continues to expand it seems that where already established it has become irreversible.

This means that people can access (and also download and store) sensitive corporate data with a device outside the organisation's security architecture. What's more, such a device may contain applications (Apps) unknown to the organisation. These free or low cost Apps, designed by unknown individuals and without security certification, may well include malware. To add to the pain, this corporate data may be accessed from anywhere, e.g. a coffee shop offering "free Wi-Fi" that being unencrypted allows a third party to acquire the data.

At the other extreme, tight security measures encourage digital natives to bypass the organisation's restrictions by copying sensitive information to their accounts in the Cloud where it will be unprotected. This makes a hacker's work so much easier…

Other new risks generated by digital natives include the use of social networking to share sensitive information with their peers. Digital natives show a much greater level of trust in people they meet online than digital immigrants. Remember the Robyn Sage story in Chapter 1?

6.2 External factors: the constantly changing landscape

There is no indication or reason to believe that the rate of innovation in information systems and technology will slow down in the foreseeable future.

6.2.1 Technology will continue to evolve

It can be expected that devices will be faster, smaller and lighter, have longer battery life and be touch-screen based. Their lifecycle from purchase to perceived obsolescence will continue to be short.

Increasingly, appliances will contain new technologies and be connected to the Internet. Many already are – in lifts, air conditioning systems, vending machines, etc. and could become targets for disruption. Future promises include cars and surgical robotic systems.

Creative people will make available new online services – the so-called Web 2.0 was a surprise to most people and services such as blogs, sharing audio and video, multi-player gaming, social networks, online auctions and so much taken for granted may well be complemented by currently unimaginable offerings.

6.2.2 Growing challenges in identity and privacy

As social animals, people want and need to interact with each other in a way that allows some measure of control. In cyberspace it is important to be able to trust the identity of individuals to prevent fraud and strengthen national security.

Organisations need to ensure that the individuals they deal with are who they say they are, and that they are authorised to do what they do. Individuals want to be trusted and need to trust organisations they interact with to safeguard their personal information.

In addition to passwords (something you know), many organisations now use additional techniques to authenticate individual such as cards or tokens (something you have) used as a second identification factor. At the high end there are devices that scan a fingerprint or an eye (something you are).

6.2.3 Weapons grade malware

Ever since the Stuxnet malware became public knowledge in 2010, there have been concerns that it was proof that targeted attacks could be launched against anyone and that it opened the door to the militarisation of cyberspace.

Two articles published in The Economist, the latest at the end of March 2013, entitled "The Digital Arms Trade" and a previous article of April 2008, entitled "Computer Security: Pain in the aaS" discussed Crimeware As A Service, highlight the existence of a market for expertly designed software attack tools. These are reported to sell for sums that, compared to military equipment, are small.

Will cyberspace become a new domain of battle? Possibly.

6.2.4 Security certifications will increase in importance

As stated earlier, information security is an unregulated profession. Several bodies offer certification of compliance either with a standard or set of good practice while others issue certificates attesting to the knowledge and experience of individuals in specific areas of information security.

It is likely that, as senior management appreciates the importance of information security, there will be a trend towards requiring such certifications as a condition of employment.

6.3 Information security should not inhibit innovative thinking

Innovative technologies open up opportunities and bring with them unknown side effects and unanticipated consequences. Living with uncertainty and risk is unavoidable and the managerial challenge is one of understanding its ability to manage technology-driven change.

To protect the organisation, Chief Information Security Officers tend to be cautious and are often referred to as "Dr. No". This works well in risk-averse organisations where being a technology laggard is considered prudent behaviour but can be frustrating to the workforce when their personal technologies are more advanced than those in the corporate environment.

At the other end of the spectrum, those with a greater appetite for risk and early adopters of innovative technologies can give grasp opportunities to develop business services and solutions ahead of others and benefit accordingly. Management should recognise from the outset that being ahead of others implies learning from experience about side effects and unintended consequences.

The next chapter examines the challenges of measuring what may be immeasurable…

7 Measuring security

In this chapter we consider the possibilities of putting numbers to a topic that is hard to measure:

- Security metrics – can security be measured and, if so, how?
- What should be reported, when, to whom and how?

7.1 Measuring Information Security

Wouldn't it be good if your organisation could say "our security level last month was 82.5"? Unfortunately, this is not possible and represents a challenge because there is no simple way to express in numbers a complex concept such as security.

The same is true of many other things, such as pain and love… Perhaps it's for this reason that Albert Einstein's office in Princeton had a sign stating: "Not everything that counts can be counted. Not everything that can be counted counts".

Could you even tell how good your information security is right now? How good should it be? Or, how about being able to state that: "our security level in the last month was better than at this time last year"? This may just be possible provided the concepts of "better" or "worse" are clearly defined, understood and agreed.

But this does not mean that the situation is hopeless. This chapter proposes one realistic approach: using Risk Indicators (risk is discussed Chapter 8).

> "You cannot manage what you do not measure."
>
> Transformed, inaccurate and misattributed. Lord Kelvin's original was substantially different.

In 1893, William Thompson (Lord Kelvin) said: "If you can measure that of which you speak and can express it by a number, you know something of your subject; but if you cannot measure it, your knowledge is meagre and unsatisfactory." Lord Kelvin had a point and the (over) simplification is misleading as the management of complex situations inevitably implies incomplete, sometimes not measurable and/or unavailable, information.

There are huge amounts of security related information that could be collected. The areas of vulnerabilities in Chapter 5 and the areas of concern in Chapter 6 lend themselves measurement. The same applies to operational matters such as intrusions and other incidents and financial data on security expenditures.

There are many sources listing possible information security metrics (e.g. NIST SP800-53 revision 2 and COBIT 5 for Information Security). Collecting, analysing and reporting all this information are resource intensive tasks but this does not guarantee that all these metrics will be useful to a particular organisation. Knowing what to measure, how to do it and how to communicate the results can help improve security's efficiency, effectiveness and the reputation of your organisation.

7.1.1 Why it makes sense to have security metrics

There are many good reasons for making the effort to have a set of security metrics. Perhaps the most important one is that in the absence of metrics the organisation relies on FUD – Fear, Uncertainty and Doubt and, as Lord Kelvin said, your knowledge is meagre and unsatisfactory. More specifically, there are four domains where such metrics are relevant, even necessary:

Regulatory compliance: Information security incidents may cause an organisation to fail to meet the requirements set by legislation. This may have legal, financial and reputational consequences. Metrics can put the security incident in context and provide factual information to demonstrate that appropriate due diligence had been exercised.

Financial management: Investments need to be made regularly in various aspects of information security and metrics should demonstrate that past security investments were justified.

Organisational effectiveness: Metrics can also be used to demonstrate to the organisation's stakeholders the effectiveness of the information security programme.

Operational: Of primary interest to the Chief Information Security Officer and also process, system and data owners. WARNING: there are many such metrics but of limited value to business managers.

7.1.2 What makes a metric useful?

Security metrics are particularly useful when they provide early warning of potential security hotspots. Such metrics are called "Leading indicators". A security metric is definitely not useful when the response from those to whom they are reported is "so what?"

To avoid the "so what" response, the metric should be capable of illustrating what the risks are, their potential impact and where they may arise highlight in sufficient detail the business processes and resources threatened. This enables managerial insights into the value of any improvements made by mitigating problems before they arise.

Managers should not have to ask: "what are you going to do about this?" the security practitioner should anticipate such a question in their report. In the perfect world, the manager should ask instead "is there anything I can do?"

Useful metrics share the following characteristics:

Business focus: The choice of metrics should be such that they are focused on supporting the business and meaningful to business managers. Specifically, metrics should make explicit how information security incidents impact the organisation's objectives, by quantifying the cost avoidance or risk reduction of the overall security program.

Quantifiable: Numbers increase the objectivity and validity of data and enable further analysis and comparisons.

Obtainable: Metrics data should not require complex tools or convoluted procedures to obtain them. They should be easily collected through interviews or from data collected through business and I.T. processes.

Repeatable: Measurements should be able to be repeated in a standard way at specified intervals to identify trends or identify changes that are the result of mitigating actions

Trending: Repeated measurements highlight change and allow decision makers to assess the effectiveness of the information security strategy and how this is executed.

7.1.3 Examples of relevant security indicators

Historical information, particularly audit reports, can be useful. Recent reports that include recommendations on information security should be taken seriously because:

- They are (supposed to be) based on verifiable facts, not opinions
- They reflect business needs rather than technical purity. Ideally, the recommendations are linked to the organisation's Business Impact Analysis and Risk Register
- They are reached through formal established frameworks such as the Control Objectives for Information Technology (COBIT), the General Technology Audit Guidelines (GTAG) of the Institute of Internal Auditors and/or other guidelines.

Other valuable historical information are reports on investigations conducted after serious security incidents. These should explain how the incident occurred and which vulnerabilities were exploited.

All indicators that support comparison and trend analysis are valuable by definition. An example of a useful metric would look like this:

Security awareness: % of employees that have satisfactorily completed a programme. The definition of such a metric should be complemented with details of:

- What evidence is collected and what is the source of data
- The frequency of measurement

The portfolio of metrics should be large enough to be valuable but not so large that it becomes a massive project in its own right and the output is too large to be manageable.

Topics that merit being supported by useful metrics should include those that support reporting of changes and trends in:

Policy Management review
Implementation status of audit recommendations
Human resources accountable for information security activities – for example:
Implementation status of Risk Register high impact mitigation measures
Process Maturity levels for information security related tasks
Financial resources dedicated to information security activities
Change and Configuration management
Tests of incident management and crisis management plans
Extent of implementation of Role Based Access Controls (RBAC)

7.2 Reporting information security metrics

Given that there are books dedicated to security metrics, this discussion will not go further. The reality is that it is possible to collect huge amounts of data on information security, most of which will not meet the characteristics listed above.

Busy people in functional jobs normally prefer ad-hoc reports issued on a Need To Know basis. This shifts responsibility for deciding who should know "what and when" to those collecting and analysing data. Easier said than done.

Self-service dashboards buried in an Intranet seem like a good idea but, in practice, not many have the time or the inclination to look for more information as they are already drowning in too much of it.

A sensible approach would require those accountable for the various aspects of information security to be good communicators and decide what can be covered by informal conversations in the lift or cafeteria and what needs a formal report addressed to individuals with the power to authorize actions.

Senior management should be regularly updated on three topics:

- Intelligence about information security threats and recent exploits
- Resources, particularly in the form of Key Risk Indicators (for example "a key information security person has handed in their notice and there is no obvious candidate to take up their role")
- Non-compliance with policies and procedures.

The next chapter gives an introduction to two tools that provide the means to identify the areas where security has the greatest role to play: Business Impact and Risk Management.

8 Other information security topics

In this chapter we present in summary form other topics relevant to information security that merit a book in their own right

- Business Impact Analyses – BIA
- Information Risk Management (three books are available in the Bookboon collection)
- Business Continuity and Crisis Management
- The legislative landscape

8.1 Business Impact Analysis (BIA)

It's always "going to be OK" when it's not happening to you.

Source unknown

A BIA, in its simplest form, identifies WHAT information systems and services are vital for the survival of an organisation when a disruptive event happens. It should also identify how long it would take for such an inability to perform business processes to hurt the business.

In addition, a BIA should also identify WHICH internal and external individuals whose knowledge and expertise are critical when things go wrong. The outcomes of a BIA are shown in Figure 6[6].

Such analyses require the commitment and active involvement of managers familiar with the business, its processes and their criticality. Carrying out a BIA is a managerial task requiring consideration of several impact dimensions:

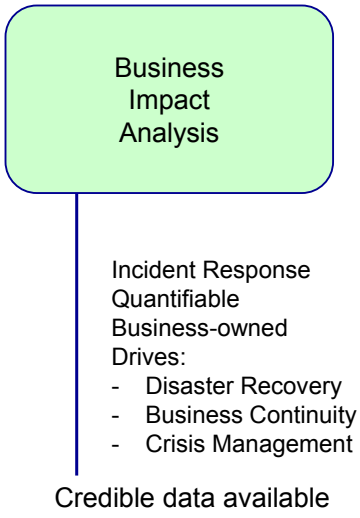

Figure 6: Purpose of a BIA

- **Operational** – factors such as impact on customers, advantages to competitors, effect on suppliers and on the business's supply chain, consequences on the workforce;
- **Financial** – ranging from increased expenditures to address the disruption to the loss of revenue arising from an inability to deliver services to the loss of share value;
- **Contractual and legal** – an inability to meet contractual obligations for e.g. service or product delivery;
- **Reputational** – perhaps the hardest to evaluate but nonetheless significant in the longer term;
- **Societal** – particularly in the case of Critical Infrastructures and Emergency Services where disruption has significant consequences on the population at large;
- And other appropriate to your business.

The BIA process needs to be revisited regularly to reflect changes in business processes, computer systems and services and organisational structures.

Once an incident has been identified (not always immediately) and reported to the I.T. service provider, the response to the incident involves several steps, typically:

Step 1: Containment – i.e. limiting the impact by, for example, quarantine of the facilities affected. This requires those responsible for containment to have a good understanding of the risks involved in taking (or not taking) action

Step 2: Evidence gathering and preservation – When dealing with Step 1, any evidence found should not be disturbed or contaminated. This may be used subsequently to identify the cause and may be needed if legal action is intended. Preserving evidence must conform to national legal standards.

Step 3: Communicating the incident to those who need to know. Failure to do so may delay the resolution of the incident and hamper any subsequent investigation. Serious security incidents raise confidentiality issues that may be of a commercial and legal/regulatory nature.

This may not be enough and it may be necessary to invoke other measures, such as Disaster Recovery, Business Continuity and Crisis Management. These are briefly discussed in 8.3.

8.2 Information Risk Management

Some practitioners advocate that Risk Management should come first. However, this experience-based book considers that you cannot go anywhere without first knowing where you are starting from. BIA is the mechanism that provides this knowledge.

There are many books on Risk Management and Information Risk. This short section highlights the most important concepts and factors to take into account when assessing information risk as part of information security management.

8.2.1 Risk and Uncertainty

> The gambling known as business looks with austere disfavour to the business known as gambling.
>
> The Devil's Dictionary, by Ambrose Bierce, 1906

The linguistic ambiguity discussed earlier, causes many people to use the words "risk" and "uncertainty" interchangeably, but they mean different things:

Risk has several context-dependent definitions (in finance, insurance, medicine, information systems, etc.). One generic definition is that it is: "a probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through pre-emptive action."

Information security standards recognise that information security risks are hard (if not impossible) to quantify. Therefore their definitions do not refer to "probability". The International Standard ISO 27005:2008 defines risk as "The potential that a given threat will exploit vulnerabilities of an asset and thereby cause harm to the organisation."

Terms such as 'potential" and "likelihood" invite subjective judgements to be made and therefore, any evaluations of information security risk should not be treated as a "fact" but as an informed guess.

It is good to remember that risk assessments in other domains – foreign currency exposures, changes in share price and other economic domains are also not robust and rely on the same words, "potential" or "likelihood". These mask uncertainty – trying to address things we don't fully understand.

This is nothing new, as Aristotle (384–322 BC) is credited to have said: "it is likely that something unlikely will happen". This remains true today and is referred to as "known unknowns" and "unknown unknowns".

Pre-emptive action requires an ability to predict the future with a degree of accuracy, given that threats can arise from natural forces (e.g. the Fukushima earthquake and tsunami), accidental human actions such as traffic accidents, domestic fires, disclosures of confidential information in social media, and deliberate human action (fraud, sabotage, terrorism and the rest).

Deliberate actions are not random events and this makes them unpredictable. Uncertainty can be reduced, amongst them intelligence (in the military sense), obtained from sources assessed as trustworthy enough. However, there have been examples of intelligence thought to be good at the time that, in the end, turned out to be bad.

Another is scenario planning (or war games) in which a group of knowledgeable and experienced participants explore "what if" situations using creativity (and some would say paranoia) to describe how deliberate actions could develop and attempt to have a range of answers to the 5W1H. This approach can work quite well and is extensively applied. It is, however, not perfect.

In both cases there are several factors to assess with incomplete information, such as the threat's intent (nature, accidental or deliberate), its capability, particularly if human and deliberate e.g. amateur hacker versus cyber-army professional and everything in between, as well as the opportunity, such as remote access versus authorized insider.

8.2.2 Risk Management: purpose and main activities

The purpose of Risk Management is to protect an organisation from threats that can disrupt its activities. Figure 7[7] presents the main elements of risk management and the areas of information needed to conduct them.

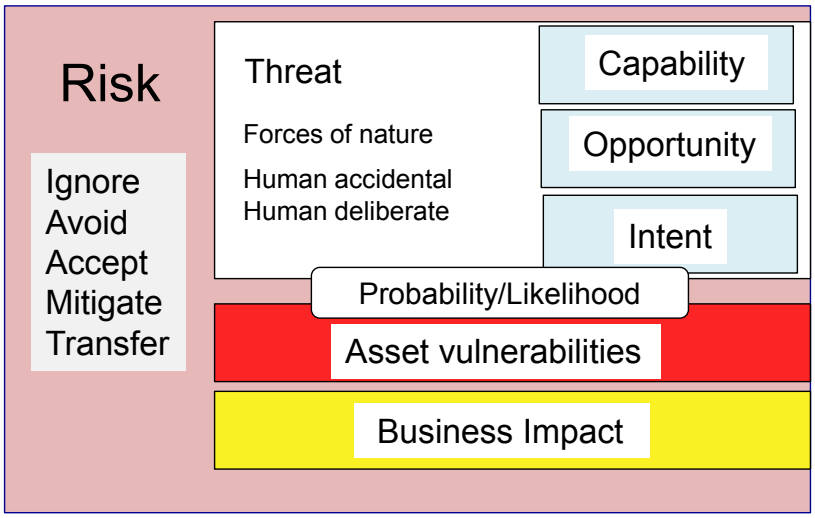

Figure 7: components of risk

There are several frameworks to assess information risk management. The author is most familiar with the ISACA IT Risk Framework and with OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). Information about both can be found in Chapter 9.

8.2.3 Risk management outcomes

An information risk management initiative should add value to the organisation. To do so, the outcomes of such initiatives should include:

- A detailed programme for the management and mitigation of information risks;
- The integration of the risks into the Enterprise Risk Management programme using common definitions;
- A Risk Register that includes descriptions of the strategy to be applied to each: ignore, avoid, accept, mitigate or transfer;
- Determine and implement effective countermeasures to those risks;
- Where required, assess the return on investment of the countermeasures.

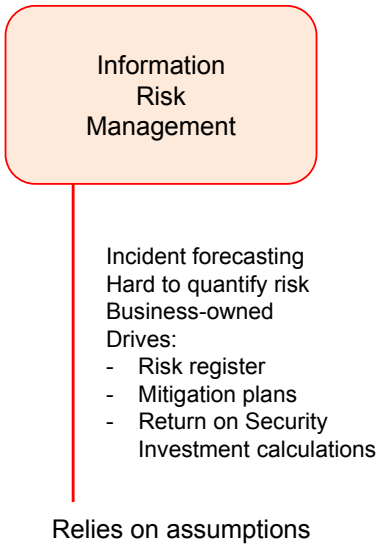

Figure 8: summarises the above.

8.3 Planning for survival

> By failing to prepare, you are preparing to fail
>
> Origin uncertain – attributed to Benjamin Franklin, Winston Churchill and others

Even experienced optimists accept that an information security incident is inevitable as 100% security is unachievable – and, as discussed in Chapter 7, security metrics are in short supply. Preparedness is the only alternative to having to improvise when an incident occurs.

There are several levels of preparedness beginning with the information systems and services providers. Their areas of accountability would normally include:

- Mechanisms to support incident reporting, analysis, containment and resolution
- Where the impact of an incident is assessed to be high, this may require the establishment of an Emergency Response Team capable of providing 24*7 cover
- Support to an investigations team and knowledge of how to collect and preserve evidence
- Contingency plans to allow systems and services to continue to operate
- Disaster Recovery plans. These are intended to provide infrastructure and operations capabilities at another location. These plans assume that such operations cannot continue at the original location due to forces of nature (e.g. earthquakes, weather conditions) or deliberate actions such as sabotage, terrorist attacks, etc.

It should be noted that Disaster Recovery plans focus on physical infrastructure and will be of limited use if software or data have been corrupted through some form of cyber-attack.

The next level of planning for continued operations is that of Business Continuity Planning and addresses the possible unavailability of offices, access to buildings or significant interruptions of utilities. Business Continuity Planning is not the responsibility of information systems and I.T. operations providers.

Crisis Management is the third major component of responding to information security events. It differs from the above two insofar that it involves parties outside the organisation, i.e. stakeholders, the media and others depending on the nature of the organisation.

8.4 The legislative landscape

As mentioned earlier, the Council of Europe Convention on Cybercrime is an established instrument that addresses the cross-border nature of cybercrime. There is also the European Union Directive 95/46/EC on Data Protection, of which a draft intended to supersede it was made public early in 2012.

These complements national portfolios of legislation. As technical innovation is faster than establishing legislation there remain many grey areas. These y vary from country to country. Corporate legal counsel is best qualified to identify applicable legislation and brief those responsible for the implementation and operation of computer systems and services about them.

9 Conclusions

> The conclusion, in which nothing is concluded.
>
> Samuel Johnson, in "The History of Rasselas".

It would appear that Information Security is one of the issues that has no solution and its practitioners continue to express concerns about pretty much the same topics they have been discussing for many years, namely:

- The lack of adequate metrics to describe security and risk
- The speed of technical innovation that forces everyone, from practitioners to users, to be in learning and catch-up mode
- The unknown consequences of being an early adopter of innovative technologies
- The challenges of building awareness of how to keep corporate data secure amongst both management and the workforce
- The skills of assorted people (hackers) intent on fraud, espionage, theft of intellectual property or simply disruption
- The apparent lack of interest in the subject shown by senior management and executives
- The constant search for resources as new technologies find their way into every area of activity and play an increasingly critical role.

Will this change in the near future – perhaps, but it would be a good thing if it did and did so for the better.

It is good to remember the Greek mythology story of Pandora's box. Pandora was expressly told by Zeus not to open it but she did. By doing so, all the evil in the world was released before she could close it again and the only thing that remained in the box was hope.

Small actions – downloading a piece of software to a personal device – may look simple and innocent but may turn out to have serious consequences. This is not helped by popular magazines for I.T. enthusiasts which are full of "advice" on downloads, gadgets and modifications to the configuration of devices (such as jail-braking or making changes to a register) which may be OK for an individual but disastrous to an enterprise. Good luck!

10 References

There are many of publications on information security. Starting about 25 years ago, it includes books, academic research, conference proceedings, standards and good practices, vendor literature and many journals and websites. There are also professional networks and numerous blogs.

The list below does not attempt to be comprehensive and focuses on publications that the author believes could be useful to those interested in the topic who are not security practitioners.

10.1 Downloadable free of charge:

Information Security Guidance for Boards of Directors and Executive Management, 2nd Edition, 2006 Information Systems Audit and Control Association (ISACA) www.isaca.org

Convention on Cybercrime (2001), The Council of Europe www.coe.int

Cybersecurity Guidance Is Available But More Needs To Be Done To Promote Its Use, GAO 12-92, December 2011 **NB:** the U.S. Government Accountability Office has over 350 documents on aspects of computer security, at: http://www.gao.gov/browse/topic/Information_Security/

National Institute for Science and Technology (U.S.), Computer Security Resource Centre, http://csrc.nist.gov/publications/PubsSPs.html
The Special Publications series SP 800 is a collection of over one hundred documents on good practices

SANS Institute: Information Security Policy – a development guide for large and small organizations
SANS Institute: Security Policy Roadmap – process for creating security policies
http://www.sans.org/security-resources/policies/

National Cyber Security Framework Manual, 2013, NATO Cooperative Cyber Defense Centre of Excellence, http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), a set of tools and techniques for risk-based information security assessment and planning www.cert.org/octave

There are also hundreds if not thousands of websites covering information security. The one at www.csoonline.com is regarded as reliable.

10.2 Material requiring purchase

Business Model for Information Security (BMIS), 2010, ISACA can be purchased from the ISACA Bookstore (free to ISACA members)

Control Objectives for Information Technology (COBIT) for Information Security and the associated Practitioners Guide, Version 5, 2012, ISACA

The ISO 27000 series of standards on various aspects of the management of information security. www.iso.org

General Technology Audit Guide (GTAG) 15: Information Security Governance, IIA GTAG 15, 2011, The Institute of Internal Auditors (http://www.theiia.org)

Managing the Human Factor in Information Security, by David Lacey, 2009, Wiley

10.3 Topics not covered in this book

To keep this book to a reasonable length, several topics were left out altogether, including

- Guidelines and good practices for personal "digital hygiene" – how to reduce the security risks of cyberspace (malicious software, fraud, loss of privacy, identity theft, disclosures, and more)
- A guide to the terminology – several online encyclopaedias provide trustworthy information
- Discussions on how malicious software (virus, worm, rootkit, etc.) and attack tools (botnet, zombie devices, SQL injection, etc.) – encyclopaedias are, again, a good source
- Security audits and Ethical hacking

11 Appendix: Acknowledgements

The author is indebted to many people and organizations for their patience, support and willingness to collaborate with many projects, including the preparation of this book. In particular:

Organizations:

IGI Global, publishers of academic books, including Law and Technology and Securing Critical Infrastructures, for their editorial guidance and comments.

The ISACA Journal and its editorial team, for their editorial guidance and permission to selectively quote from published articles.

The Geneva Centre for Security Policy for allowing me to join their workshops and discussions that resulted in the publication of the NATO CCD COE "Framework for National Information Security Strategies" published in March 2013.

The MIS Training Institute for Europe, Middle East and Africa, for the opportunity to speak at their conferences, meet and discuss these topics with hundreds of knowledgeable practitioners.

Webster University Geneva, for providing me access to Gartner Research and processing this text through the Ithenticate service to ensure all copyrighted material has been adequately acknowledged.

Graphics:

Diplo Foundation (www.diplomacy.edu) for their kind permission to modify and use Figure 3
The Hemera 1 Million Box of Art – royalty-free clip art used in Figure 4
The ISACA Journal, as mentioned in the Endnotes.

Many individuals provided valuable candid comments on the draft of this book and their input is gratefully acknowledged. The author apologises for any errors in this book. They are unintended and entirely mine. Readers willing to provide comments and corrections would allow any possible new editions to be improved.

12 Endnotes

1. National Cybersecurity Framework Manual, Edited by Alexander Klimburg, NATO CCDCOE, 2013
2. The Future of Cyberwar, by James P. Farwell; Rafal Rohozinski, Survival, Global Politics and Strategy, January 2011.
3. ISO 27000 series, Information Security Management, International Standards Organisation.
4. "Digital Natives, Digital Immigrants", by Mark Prensky, from "On the Horizon", NBC University Press, 2001.
5. "I.T. Metrics: Staffing and Expenditure Report", Gartner Research Note G00248502, February 2013.
6. Source: ISACA Journal, Volume 4, © 2013, ISACA, All rights reserved. Used by permission.
7. Source: ISACA Journal, Volume 4, © 2013, ISACA, All rights reserved. Used by permission.
8. As footnote 7.