

The Information Society Library
GETTING THE BEST OUT OF CYBERSPACE

INFORMATION SECURITY AND ORGANISATIONS

A NON-TECHNICAL GUIDE
TO PLAYERS, OFFENCES
AND EFFECTIVE DEFENCES

Stefano Baldi • Eduardo Gelbstein • Jovan Kurbalija



P R E F A C E

There is no shortage of books on all matters relating to information management and information technology. This booklet adds to this large collection and attempts to do a number of things:

- offer non-technical readers an insight into the few principles that are important and reasonably stable;
- present the material in a context relevant to the work of those involved in international relations;
- awaken the curiosity of readers enough that they will progress beyond this booklet and investigate and experiment and thus develop knowledge and take actions that will meet their particular needs.

The format of these booklets and their contents evolved from courses given by the authors over the last few years in various environments and the feedback of the attendees. Readers' feedback on these booklets would be greatly appreciated by the authors so that future editions can be improved. The coordinates of the authors are given at the end of this booklet.

Acknowledgement

One of the authors of this booklet is also the co-author of the book *Information Insecurity*, published in September 2002 by the UN Information and Communications Technology Task Force and the UN Institute for Training and Research (UNITAR).

Most of the material in this booklet is new and has a practical focus that does not duplicate the above-mentioned book.

ISBN 99932-53-03-0

Published by DiploFoundation

Malta: 4th Floor, Regional Building
Regional Rd.
Msida, MSD 13, Malta

Switzerland: c/o Graduate Institute of International Studies
Rue de Lausanne 132
CH-1211 Genève 21, Switzerland

E-mail: diplo@diplomacy.edu
Website: <http://www.diplomacy.edu>

Edited by Hannah Slavik and Dejan Konstantinović
Cover Design by Nenad Došen
Layout & prepress by Rudi Tušek

© Copyright 2003, Stefano Baldi, Eduardo Gelbstein and Jovan Kurbalija

Any reference to a particular product in this booklet serves merely as an example and should not be considered an endorsement or recommendation of the product itself.

CONTENTS

Setting the scene	5
Introduction	7
What does information security mean to an organisation	8
A brief historical review	8
Cyberspace as a frontier land	9
Organisations under siege	12
Information security definitions	15
Residual risk	15
Value of information assets	16
Vulnerabilities	17
Threats	19
Availability	20
Confidentiality	21
Integrity	21
Information insecurity players and offences	23
Information insecurity players	25
Good guys	25
Very special guys	25
Bystanders	26
Obstacles	26
Bad guys	27
Trusted insiders	29
The catalogue of information security offences	30
Building effective security	33
Things we (should) know about effective security	35
About what needs to be done	35
About exposures	37
About critical infrastructures	38
The international standard ISO 17799	39
Using established standards and codes of practice	39
Dealing with the organisational aspects of information security	49
Ensuring the right technical approach is taken	49
The information insecurity timeline	51
Preparing for information insecurity	51
Monitoring systems and traps	52
Monitoring systems against internal attacks	52
Reacting to an information security incident	53
Digital autopsy of a security breach or cyber-attack	53
Employees' freedom of expression, monitoring and civil rights	55
Concluding remarks	56
About the authors	58



SECTION



1

Setting the scene

You would be surprised how many blue-chip companies and dot-com sensations do not have someone in their organisation who is competent to answer even simple questions.

*Richard Power, Editorial Director,
Computer Security Institute quoted in PC Week, August 1999*

INTRODUCTION

Why does the Information Society Library include booklets (*Good Hygiene for Data and Personal Computers* and *Information Security and Organisations*) on what seems to be a technical subject dealing with computers, viruses and topics of this nature?

Readers may point out that in their organisations it is the responsibility of the technically trained employees to take care of information security, as indeed should be the case. However, this booklet will show that although firewalls, encryption and other tools are all necessary and should be fully utilised, they are not sufficient in themselves to address the problem.

Information security goes much further than dealing with viruses and hackers. Today, most of the impact caused by viruses and hackers is just an expensive nuisance. A good deal of effort to clean up the mess left behind is also involved. Nevertheless, information security has the potential to become a major social, economic and legal problem.

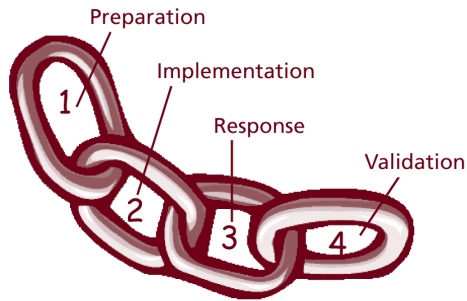
Organisations working in the international arena need to deal with a number of security problems, including the possibility of becoming a target for coordinated attacks by hacktivists, industrial spies, unethical vested interests and organised crime. “Trusted” insiders can also commit serious fraud or acts of sabotage against them.

Such attacks have become much easier in the last ten years for several reasons:

- greater ease of access as networks become more interconnected;
- growing level of computer skills among the general population;
- accepted realisation that *all* computer systems have vulnerabilities;
- permanent game of catch-up by information technology professionals that results in many known vulnerabilities remaining uncorrected.

Information security should be regarded as a system of linked activities, many of which are technical in nature. At the same time, several

information security issues require managerial decisions that should not be abdicated to technical staff.



These activities are shown as four links in a chain (see the graphic above), the strength of the chain being determined by its weakest link.

Senior management has a major role to play in protecting an organisation's information assets, particularly during the preparation stage. Management is responsible for providing the resources necessary for implementation and response and ensuring that security arrangements are regularly validated.

When these activities are not conducted effectively, senior management will be, at best, a mere bystander and at worst, an obstacle to good security practices. These potential roles will be explored further in the pages that follow.

WHAT DOES INFORMATION SECURITY MEAN TO AN ORGANISATION?

A BRIEF HISTORICAL REVIEW

The need for information security is not new. It emerged at more or less the same time as the invention of writing. In fact, more than two thousand years ago in ancient Greece, messages sent by officials from one part of the country to another were sealed, encoded and entrusted to a loyal messenger.

Writing, mathematics and geometry all have long histories. Human-kind learned how to make use of them to create tools many thousands of years ago. The knowledge and experience acquired in tool-making was put to good use by all societies. They were also applied to creating a certain category of tools which societies could use to defend themselves and acquire territory from other societies: weapons. Electronics, computing and related products are no different in this respect: they can be used to create weapons as well as useful tools.

The virtual world of information existing in the electromagnetic spectrum started in the mid 1800s. The first operating telegraph was established in 1844. Figures from 2003 show that some 1.3 billion telephones exist worldwide, most of them capable of connecting to other telephones anywhere in the world.

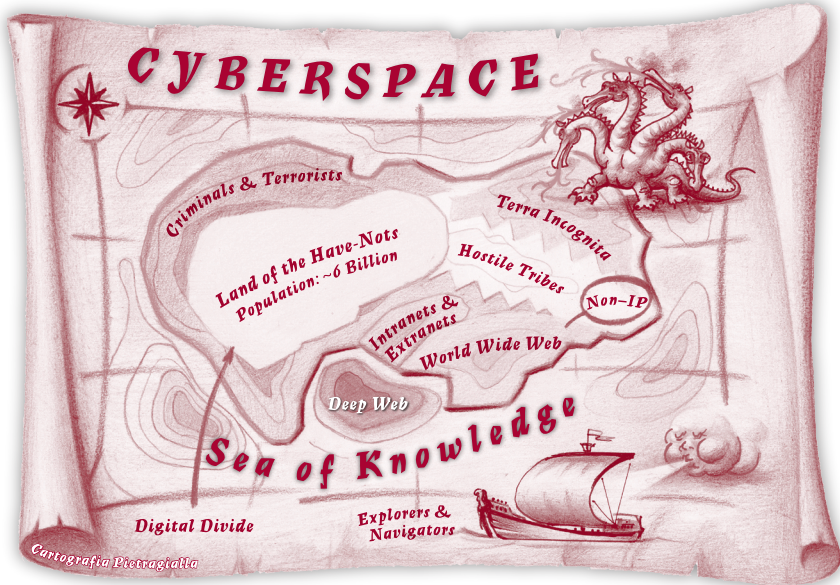
In addition, more than 600 million individuals have access to the Internet – an amazing number given that the World Wide Web was only invented in 1989. A profusion of other networks link the world through copper wires, optical fibre networks, radio and microwaves as well as satellites.

The word “cyberspace” was first used in William Gibson’s 1984 science fiction novel *Neuromancer*, and has been adopted to represent the inter-related world of data and software. Cyberspace is virtual because of its intangible nature. The word Infosphere (derived from the concept of the biosphere) is also used to describe this virtual environment.

CYBERSPACE AS A FRONTIER LAND

The development of the relatively new world of cyberspace has similarities with past exploration and the conquest of new territories. In the early stages of exploration, new territories, known as frontier lands, mark the end of “civilisation and culture” and the beginning of “lands of opportunity”.

There has always been a need for detailed maps of frontier lands. As frontier lands have few or no laws, those brave enough to explore them find many freedoms to exploit. In line with this analogy, in 2002 the Director of Europol, Jürgen Storbeck, described the Internet as “a new sphere of life and a new scene of crime”.



A plausible map of cyberspace today might look somewhat like the island shown above. The landscape has few details, and some features may not be in the right place or to the right scale.

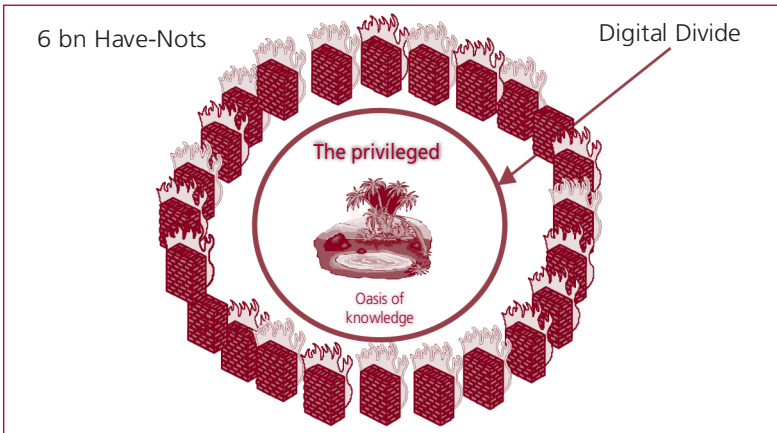
The existence of the “Digital Divide”, the boundary between those who have access to the “Sea of Knowledge” and those who do not, is generally recognised. The other major features shown are also generally known: “Criminals and Terrorists”, for example, exist and exploit the frontier land-like nature of cyberspace.

“Hostile tribes” (for example, Hackers) are known to be present, but in unknown numbers. The “World Wide Web” and the “Deep Web”, as well as “Intranets and Extranets”, are all becoming highly visible features of the landscape. However, the land of “Non-IP” should not be ignored: IP stands for Internet Protocol and the land of “Non-IP” comprises all the information and communications systems that do not use this Internet standard. These include:

- the vast majority of telephone and satellite networks;
- local area networks linking computers inside a building;
- all proprietary networked computer systems used by businesses and intelligence, defence and police services.

There is a clear trend towards the connection of non-IP systems to the Internet. This has an impact on their information security needs.

This map of cyberspace represents the optimists' view. The pessimists, many of them working in information security, also look upon cyberspace as a lawless frontier land but their map is very different. In their map, the "Sea of Knowledge" is only an oasis. A walled city has been built around it to defend it, and the walls represent the "Digital Divide".



In this scenario, "cyber-terrorism" is the activity of individuals or small groups which interfere with the operation of cyberspace and launch attacks on the walled city.

In the world of information security, two key questions can be asked: To what degree will the (fire)walls be effective in repelling such attacks? Is a definitive victory possible?

The challenges of this particular scenario are summarised in three questions to which the answer appears to be "No":

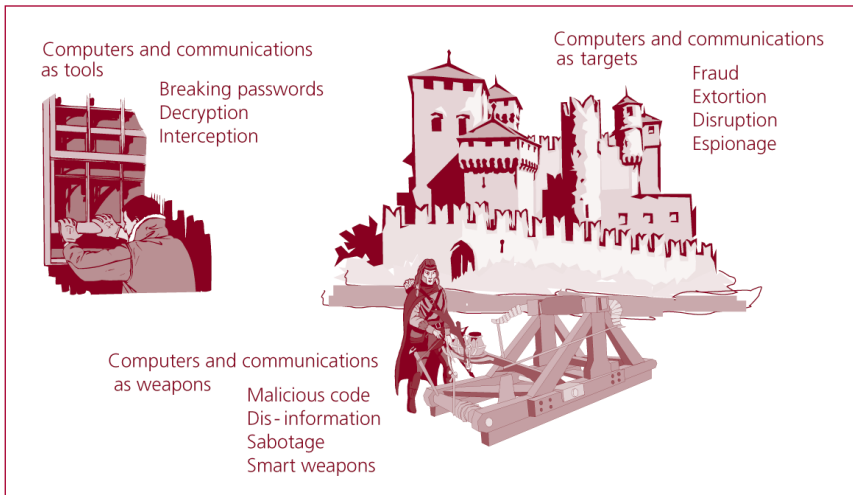
- Do we really know who the cyber-attackers might be?
- Do we know who designed the Code Red, Nimda, Slammer and Fizzer worms, let alone all the other malicious code making the rounds recently such as the Blaster worm and Sobig.F?
- Can we exclude the possibility that these examples of malicious code were just proofs of concept, with military-strength versions to follow?

ORGANISATIONS UNDER SIEGE

Today, in a large part of the world, few professional activities do not use information technologies in one way or another. Moreover, in most cases these technologies play critical roles – for example in the operation and management of critical infrastructures such as electricity generation and distribution, financial systems and transport.

The same critical dependency involving a wide spectrum of information gathering, analysis, discussion and negotiation exists for those involved in knowledge-based work, ranging from statisticians to diplomats.

Cyber-attackers use these tools in their work just as much as professionals, for example to intercept data traffic on networks or to obtain access to computer systems by capturing or breaking passwords. Other members of the hostile tribes, such as cyber-criminals and cyber-terrorists, also use information tools as weapons.



Sometimes these weapons take unexpected forms. For example, a computer virus, which is just a string of ones and zeros, is only considered a weapon when it is used with the intent to cause damage.

Cyber-weapons can also take physical form, for example, directed high-energy beams, which can physically damage equipment, or smart electronic components in more conventional weapons.

From the point of view of planning effective defences, the challenge is to protect computer and network systems that others see as potential targets.

A strong asymmetry exists between what it takes to build something and what it takes to destroy it.

There are three distinct types of attack, each with different consequences requiring different protection strategies.

Physical attack

This is the most visible and tangible type of attack, although it can be considerably more subtle than the one shown in the picture here. Obviously, it requires physical access to the rooms where communications and computing equipment is located.



Once access is obtained, the use of water, fire, explosives, high energy weapons or tools to cut cables can all have severe consequences as the time needed to restore order and reliable operations is considerably greater than that needed to cause the damage.

Syntactic attack

This is a subtler form of attack, consisting of making a computer system perform functions it was not originally designed to perform. An attacker gains access to a target system and takes control of certain functions.

Example no. 1: An insider obtains the access rights of a system administrator. These rights are then used to provide unauthorised user names and passwords to individuals outside the organisation, which will give them access to private documents or other intellectual property.

Example no. 2: A hacker gains access to a computer and installs software on it that allows the hacker to gain control of the computer without the owner knowing it. The hacker has turned the computer into a “zombie” and together with other “slave” computers uses it to launch

coordinated Denial of Service attacks against a third system by flooding it with requests for web pages or e-mail messages.

Example no. 3: A hacker (or a criminal) intercepts and diverts treasury payments.

A knowledgeable person can carry out such attacks and not be discovered.

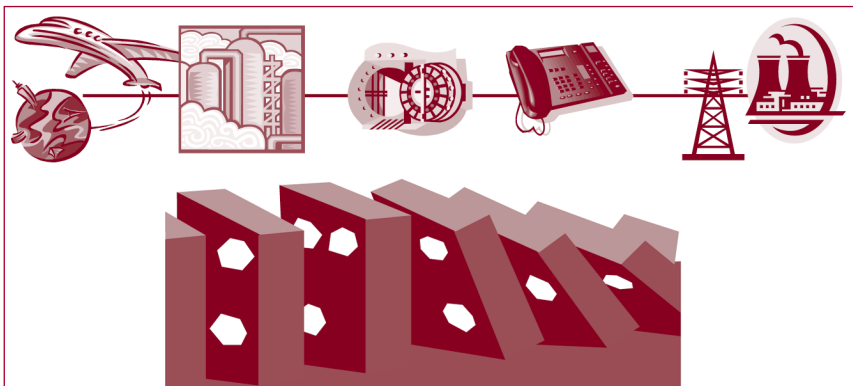
Semantic attack

An insidious form of attack occurs when the content of documents, web pages or databases is changed, particularly when such changes are subtle. There are many examples of intruders changing the contents of web pages, as these types of attack receive considerable publicity.

Of greater concern is the possibility that such changes are made to databases of major social importance, such as those of social security, taxation and student records. Carried out over a long period of time, such changes could have a cumulative disruptive effect considerable enough to lead to the loss of confidence in the systems' integrity.

A final consideration for this section is the increasing interconnectedness of computer networks and systems. This trend creates an ever-greater risk of disruption to the orderly operation of society.

The domino effect comes into play when the information systems of critical infrastructures are successfully targeted. The increasingly international nature of electricity grids, global telecommunication (including the Internet), banking and finance, distribution and logistics, as well as



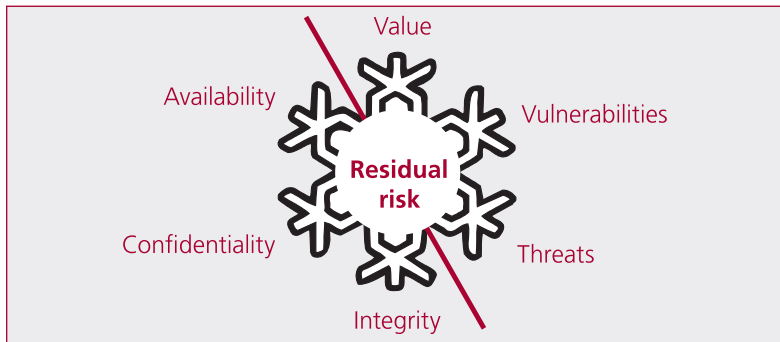
transport systems, leads to mutual interdependence. This means that an attack on any one of these systems could easily propagate to others.

These systems are the likely targets of cyber-terrorism and cyberwar. As a separate booklet (*Hactivism, Cyber-terrorism and Cyberwar*) in this series argues, such cyber-attacks are no longer far-fetched terrorist attack or war games scenarios, but real threats.

INFORMATION SECURITY DEFINITIONS

Information security is defined through seven parameters. Six of them can be divided into two distinct groups:

- targets (availability, confidentiality and integrity); and
- context (value of the assets to be protected, vulnerabilities and threats).



The seventh parameter, residual risk, needs to be examined before these two groups can be discussed further.

RESIDUAL RISK

It is possible to make anything very secure, even extremely secure. However, there is no way to make things totally secure – 100 percent security is unachievable in all domains.

It is possible to make buildings fireproof and earthquake proof, within limits. The cost and complexity of doing so may become prohibitive for the intended use of such a building (or information system if that is the

case). This compromise between survivability and affordability implies the acceptance of a residual risk.

Defining what constitutes an acceptable residual risk is the responsibility of senior management.

Organisations operating critical infrastructures or services, international organisations operating in areas affected by natural or man-made disasters, the military and emergency services, as well as financial institutions, all by their very nature demand a low degree of residual risk.

However, it is important to state that significant improvements in security can be achieved simply by getting the basics right and by increasing awareness of the subject among the affected employees.

As security measures become more complex they also become less manageable. Therefore, somewhat paradoxically, having more security measures in place can actually make an organisation less secure.

VALUE OF INFORMATION ASSETS

An asset is any item to which an organisation or an individual assigns value in financial or other terms. In the context of this booklet, such assets include:

- private, confidential and secret documents and messages in e-form – although the same considerations apply to paper files and archives;
- data and databases that impact day-to-day operations (logistics, field operations, money transfers);
- intellectual property in all its forms.

It is difficult to put monetary value on information assets as these do not appear in an organisation's financial accounts and no standard techniques are available to quantify them. The activities related to securing the information assets of organisations are frequently regarded as costs rather than benefits.

However, information value, expressed in financial terms, is available: In 1999, the American Association of Fraud Examiners reported that the average computer crime involved an amount of US\$2 million, whereas the average bank holdup involved a sum of “just” US\$14,000.

The economic damage caused by information insecurity is very high. It is estimated that the Code Red worm that circulated in 2001 required US\$2.6 billion to clean up.

VULNERABILITIES

Vulnerabilities are imperfections and defects in the items and activities needed in the operation and management of information assets.



In an article in the June 2002 issue of *Management* magazine, Colin Shaw (from Price Waterhouse Coopers) stated that nearly one half of the 560 US companies his firm surveyed expect cybercrime to be the number one fraud concern of the future.

To summarise, such vulnerabilities can be divided into two groups: those inherent in information technology products and those related to activities carried out by human beings.

Product vulnerabilities

Software

All software has defects (also known as bugs). Most of the time these remain invisible, but sometimes they make an unwelcome appearance. There are several reasons for this, in particular:

- software development is more of a craft than an engineering discipline;
- software is designed to perform clearly defined functions. It is rarely, if ever, designed to ensure that functions not part of the original definition *cannot* be performed;
- software is hard to create, read, document and test. Furthermore, the effort put into testing is usually limited so deadlines and budgetary targets can be met.

These vulnerabilities can be exploited in order to force the software to perform functions not envisaged by the programmers.

Commercially available software packages including operating systems (e.g. Windows) and

If debugging is the process of removing bugs, then programming must be the process of putting them in.

— well-known computer industry saying

applications (e.g. Excel, Lotus Notes, Oracle, SAP) also contain programming errors and vulnerabilities. The terms and conditions of software licences absolve vendors from any liabilities arising from such errors and vulnerabilities.

Hackers systematically look for these vulnerabilities and imperfections. Ethical hackers who find them communicate this to the software vendors to allow them to prepare updates and plugs to fix them. Other hackers exploit the vulnerabilities and imperfections to cause disruption or benefit from them.

Software which is in wide use around the world, such as the Windows operating system and the browser and e-mail packages bundled with it (Internet Explorer and Outlook Express), receive a great deal of attention from hackers as attacking such products maximises the impact of their intention to spread malicious code.

Commercial and in-house custom built software may receive less attention from “casual” hackers but this does not reduce the risk of attack. In terms of cybercrime and cyber-terrorism, attacking such systems may be more lucrative or devastating. The motivations of a hacker intending to circulate a virus or worm through e-mail, and those of one planning to mount a successful attack on a global funds transfer system are fundamentally different.

Processes

The security features of even the best software in the world will be determined by how the software is installed and configured. A firewall installed with some or all of its features turned off is not going to be of much help, and just having a firewall may provide a false sense of security.

Similarly, new servers come with a default system administrator login (e.g. SysAdmin or Sys_Admin). A good system administrator will *immediately* modify these with a well designed, hard to break user ID and password. However unbelievable this may sound, this is not always done and any half-sensible hacker will begin by checking if the default login is still valid.

Technology is dominated by two types of people: those who understand what they cannot manage and those who manage what they cannot understand.

Anonymous

Another frequent security violation occurs when the access rights of employees are not updated immediately upon a change in their status, in particular when they leave an organisation.

Security practitioners are well aware that most security failures are due to simple omissions or a few individuals failing to adequately perform their duties. There are few things more dangerous than the combination of goodwill and stupidity.


THREATS

The threats faced by information and communications systems are fundamentally different for several reasons:

- the duration of attacks is short and prior warnings are rare;
- data-thugs, cyber-vandals, criminals or cyber-terrorists do not need to have physical contact with the victim;
- attackers have a wide range of motives;
- attackers are knowledgeable, creative and one step ahead of the defenders;
- it is easy to hide in cyberspace and the risk of detection and retribution are low.

Other asymmetries will be discussed later in this booklet.

It should be noted that the whole field of information security is characterised by profound asymmetries. This is true for the whole spectrum of attacks, including cyberwar and cyber-terrorism. For a long time, books on military strategy have stated that asymmetries are always ex-

<p>Policies Technologies Operating Processes Staff and ERT Contingency plans Crisis management Much to lose</p> <p>DEFENDER</p> <p>also</p> <p>Proportionality E-evidence</p>		<p>ATTACKER</p> <p>Has easy access to know-how Operates with minimal infrastructure Gains new knowledge about defences with every attack Has nothing to lose</p>
<p>Cost, Effort, Traceability, Risk, Impact, Motivation</p>		

exploited by the side that cannot win with traditional forms of attack and warfare.

First and foremost, every attack informs the attacker about how good an organisation's defences are without revealing anything about the attacker. Other asymmetries include:

- The **cost** of mounting a cyber-attack (a few personal computers, some software tools and know-how) is almost trivial compared to the cost of building, implementing and operating defences.
- The **impact** of disrupting the operation of a critical infrastructure or business activity is much greater than that of finding and apprehending the culprit.
- The **motivation** of the attacker is invariably greater than the motivation of the defender.
- Attackers face no **risk** when operating from a distance. Even an insider involved in an attack may remain undetected long enough to make a getaway. Besides, legislation is not always in place to deal with such actions (the Council of Europe's Convention on Cybercrime was signed in November 2001 by 33 countries, but has not yet entered into force).

Cyber-attackers rarely, if ever, give prior warnings.

AVAILABILITY

Availability is a measure of the fraction of time that an information resource (system, network, database or application) is accessible and usable when a user needs it. It is usually expressed as a percentage. In practical terms, this means the following:

- An availability of 99.9% means that – excluding planned outages – the facility will operate as desired at all times other than a cumulative 8 hours in a year.
- An availability of 99.99% requires the cumulative non-operational time not to exceed 50 minutes in a year.
- An availability of 99.999% (commonly referred to as “five nines”) requires the cumulative non-operational time not to exceed 5 minutes in a year.

Systems and facilities operating twenty-four hours a day, seven days a week, can achieve such high availability targets, but at a cost. Technical and management costs rise quickly, as does the complexity of the arrangements required to meet tighter availability targets.

CONFIDENTIALITY

Confidentiality is the requirement that information not be disclosed or provided to anyone not specifically authorised to have it, regardless of whether they are individuals, entities or processes.

Techniques such as access controls, authentication and encryption are used to enforce confidentiality.

INTEGRITY

Integrity is the trait guaranteeing information has not been changed, destroyed or lost in an unauthorised or accidental manner. In addition, implicit in the concept of integrity is the assurance that the information is suitable for the intended purpose (correctness integrity) and that the originator of the information is reliable (source integrity).



SECTION



2

Information
insecurity
players and
offences

“Only the Paranoid Survive”

Title of 1999 book by Andrew S. Grove, founder of Intel

INFORMATION INSECURITY PLAYERS

This section discusses the various types of individuals active in the field of information insecurity, and the roles they play.

GOOD GUYS

These are individuals whose primary role is to protect their organisations and their own data and systems from all forms of cyber-attack. Motivated by their work ethics and professionalism, they act in the best interests of their organisations and often derive a high level of job satisfaction.



“Good guys” include Chief Information Officers or Directors of Information Technology, information security team members, aware end users and ethical hackers.

VERY SPECIAL GUYS

Almost always external to the organisation, these individuals play key roles in defining security. They include vendors, security consultants and auditors.

Not everybody is willing to categorise them as good guys – vendors, for example, knowingly deliver products with vulnerabilities and disclaim all liabilities for their consequences. Security consultants, when engaged, must be highly trustworthy because they will come to know as much, if not more, about the security arrangements of an organisation as those responsible for the organisation’s daily security.



Technically trained employees often regard auditors with suspicion because they tend to see auditing reviews and reports as being critical of their activities, rather than as a means of reducing the organisation’s overall risk.

BYSTANDERS

Likely to be the most numerous group in organisations, they are also potentially dangerous. Bystanders are all those employees who do not believe that they have a role in protecting the information assets of the organisation where they work, and therefore fail to apply an appropriate level of care to information security matters.



The booklet in this series, *Good Hygiene for Data and Personal Computers*, was written with the purpose of helping bystanders become aware of the issues and activities that need to become a part of their work routine in order to avoid undermining their organisations' information security.

Typical bystanders' security shortcomings include writing down passwords, and often posting them visibly in their work areas, using easy-to-guess passwords, allowing visitors to use their computers, failing to place their documents in shared network drives that are systematically backed up and more.

OBSTACLES

It is a fact of corporate life that obstacles exist in every organisation. They come in two categories – individuals opposed to security as a matter of principle and individuals opposed to security because of constraints placed upon them.



The existence of the former can lead to tragic consequences as they can frustrate the security personnel to the point that they may lose interest in safeguarding the interests of the organisation or, worse, quit and go to work somewhere else, given that knowledgeable information security experts are in short supply.

Even when their actions are driven by real constraints, executives should carefully weigh the need for adequate checks and balances to avoid the trap of “saving money regardless of cost” or making the jobs of security staff impossible by, for example, refusing to

deal with complex issues such as compliance with policies or providing appropriate resources.

BAD GUYS

Hackers in their various guises



The history of codes and ciphers is almost as old as the history of writing itself. Hacking and malicious code have a history as long as that of computing.

Every code ever invented was broken eventually – hence, the purpose of any code is to prevent the opposing side from *immediately* decoding information, in the hope that by the time the code is broken the information will no longer be relevant.

Anyone can become a hacker – it is no longer necessary to be a “mathematical genius”. The skills needed to write and exploit malicious code and penetrate networks are within the grasp of almost anybody interested in this activity.



The activities of hackers are frequently referred to by the media as “hacktivism” or “cyber-terrorism” to produce eye-catching headlines. Another booklet in this series (*Hacktivism, Cyber-terrorism and Cyberwar*) is devoted to these specific topics.

Thus, hackers come in various categories, starting with Script Kiddies, the least knowledgeable of all hackers, who buy or copy tools and techniques from others. Many tools and details of malicious software can be obtained for free or for a nominal sum from websites and hacker clubs.



The number of institutions where hackers can gain formal training appears to be increasing. These institutions are legal and may in future provide valuable training for security administrators.

In addition, hackers are better organised to share information about their successes than Chief Information Officers and Chief Security Officers are to share information about their problems, let alone their fail-

ures. This is understandable as every organisation needs to protect its reputation and public image. Public admission of security failures by a bank, stock exchange or similar organisation for which public trust is vital, could be catastrophic.

Vendor websites and e-zines give detailed descriptions and explanations of software vulnerabilities to help system and network administrators take appropriate actions to deal with them. Hackers also follow these announcements and act quickly to exploit such vulnerabilities in order to gain access to protected systems and networks.

Hackers can get training almost anywhere in the world. Catching a hacker is hard work and involves the setting of elaborate traps, as it is very easy for hackers to hide their identities and locations in cyberspace. Furthermore, it is impossible to determine whether an attack comes from “private individuals” or if the attackers are acting on behalf of a group or even a country.



Even if a hacker is identified and caught, the legal repercussions are usually light and penalties are minimal. Kevin Mitnick (the US super-hacker) spent time in prison but was fined only around US\$5000. The 19-year-old Dutch hacker who wrote and propagated the “Anna Kournikova” virus was sentenced to 150 days community service (his lawyer appealed this sentence).

While the methods of all hackers are pretty much the same, hacker affiliation and motivation influence choice of targets and persistence in the attacks. In addition to the enthusiasts described above, the family of hackers includes:

- criminals, and in particular members of organised crime – motivated by money;
- hacktivists – motivated by causes in which they believe passionately;
- spies (industrial and others) – motivated by the need for better intelligence about competitors and real or potential adversaries;
- cyber-terrorists – motivated by political or fundamentalist beliefs.

TRUSTED INSIDERS

The trusted insider is a major risk. These individuals enjoy privileged access to an organisation's systems and facilities. Insiders can be unaware of security issues, trusting and full of goodwill (easily exploitable by social engineering), malicious or suborned by a third party.

Insiders have the knowledge, access rights and possible motivation to act against the interests of the organisation that employs them, either directly or indirectly. The motivation may vary from financial gain (through the diversion of funds, creation of dummy transfers or accounts, and blackmail) to revenge (individuals who are disgruntled for any real or imagined reason). Other insiders may be influenced, suborned or blackmailed by external parties.

The concept of the "insider" has a wider meaning than before because of the growing use of contract staff (e.g. temporary assistance, consultants) and the use of outsourcing for software development, maintenance and operations support.

Outsourcing has become a global industry with a turnover of some US\$100 billion per year. A substantial part of outsourcing work has moved to countries where the earnings of ICT personnel are much lower (as much as 90 percent lower) than in the US and Europe. Countries with a substantial presence in software development include India, China, Russia, the Philippines and Pakistan.

The usual measures of conducting background checks, closely supervising the activities of such personnel and carrying out security vetting are, in most cases, not available or not under the control of the client. Thus, when software developed through outsourcing is destined for a critical infrastructure system or a major global commercial enterprise, it creates a potential security issue.

One important fact about cyber-attacks is that when carried out intelligently, they are hard or even impossible to detect. Cyber-fraudsters have gotten away with many offences and those cases that were detected, were discovered by accident, not design. "Smart terrorism" will no doubt take advantage of this too.

THE CATALOGUE OF INFORMATION SECURITY OFFENCES

Offences can be grouped into four distinct categories:

- network related offences including interference, sabotage and hiding in cyberspace;
- access related offences including hacking and the distribution of malicious code;
- data related offences including modification and theft;
- computer related offences including fraud and forgery.

Within these four categories are many variants, some of which are presented below as examples:

Disinformation and propaganda – Activities here range from official “hearts and minds” campaigns through formal websites to the spoofing or altering of the contents of other organisations’ websites. These activities are better categorised as hacktivism, although the popular press tends to refer to them as cyber-terrorism.

Sabotage – These are activities involving the intentional insertion of malicious code (such as logic bombs, Trojan Horses, viruses or worms), deliberate interference with the configuration of servers, computers and other equipment as well as the prevention of scheduled backups.

Cyber-hooliganism – Cyber-hooliganism involves defacing and spoofing electronic mail and websites and spreading malicious code without a truly destructive payload. Cyber-hooligans cause widespread disruption and economic damage, but do not actually damage data or infrastructures.

Theft and fraud – Intellectual property, money and/or information taken without permission by an individual for personal gain or extortion/blackmail of a third party falls within this category.

Industrial espionage – The organised theft of intellectual property (including software) is an old activity carried out for profit by professionals.

Organised crime – It operates outside legal jurisdiction and remains hidden and untraceable. Its activities cover a wide range including extorting payments from companies whose systems they have penetrated,

the perpetration of major fraud by intercepting, modifying and diverting treasury and payment traffic and stealing confidential information with a high market value.

Organised crime can also track the activities of individuals to support its other activities: kidnapping, blackmail, theft of personal information (e.g. credit cards) or ID theft. The traditional activities of organised crime, such as pornography, prostitution, money laundering and drug and arms trafficking also benefit from the facilities provided by cyberspace, in particular the ability to operate remotely and be largely untraceable.

Semantic attacks – Here instead of disabling or destroying systems, the data is modified so that any outputs based on it become untrustworthy. This can be done with databases and websites, as well as by hijacking or spoofing the electronic mail of one or more individuals.

An example is the targeting of a country's social security or tax data. If a semantic attack is conducted subtly, by the time it is discovered the original data may be unrecoverable. Financial institutions, as well as those of intelligence, defence and police, are well aware of such possibilities and their data backups and recovery procedures are believed to take these possibilities into account. However, many other institutions optimistically believe that such action is “unlikely”.

Cyber-terrorism – Activities conducted by individuals or groups separate from (but possibly sponsored by) a country with the intention of disrupting civil society (e.g. interfering with just-in-time deliveries, air traffic control, banks and financial institutions as well as other critical infrastructures) are classified in this category. Such attacks would, in practice, be indistinguishable from those of a state sponsored cyberwar and unless hostilities are formally declared, it would not be easy to immediately ascertain who the attackers are or from where the attacks originated.



SECTION



3

Building effective security

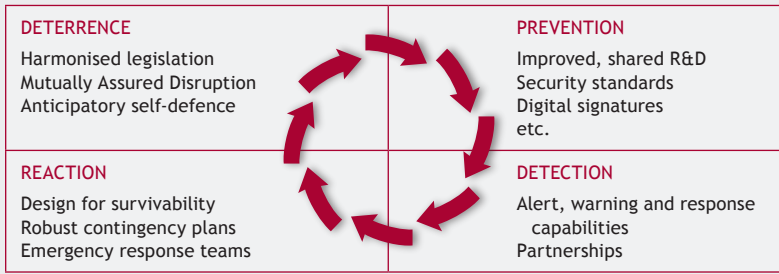
*Information security is not a technical matter,
it is a way of life.*

Anonymous

THINGS WE (SHOULD) KNOW ABOUT EFFECTIVE SECURITY

About what needs to be done

Humankind has a long history of dealing with crime and war. Defence requires actions in four categories: deterrence, prevention, detection and reaction. In the particular case of cyberspace, these can be interpreted as follows:



Deterrence: Good legislation is generally considered to be the best deterrent against cybercrime and cyber-terrorism. However, current national and international legislation does not appear to prohibit the production, distribution or possession of malicious code unless it is used to commit a crime.

At present, legislation dealing with cybercrime is available in approximately 40 countries (out of a total of 200). One international cybercrime agreement is the Council of Europe’s Convention on Cybercrime, signed in November 2001 by 33 countries, but not yet ratified by the five countries necessary for it to come into force (the situation as of August 2003).

It is possible to envisage that a number of organisations, such as those responsible for national security, could be in a position to respond to hacker attacks in kind. The authors could not find any official government statements that such retaliation has taken place. However, many press reports describe hacker groups from countries involved in political disputes responding to each other’s cyber-attacks by using similar techniques.



Smart hackers are likely to use operating systems other than Windows to more effectively resist a counter-attack in kind. Linux is not the only alternative; another variant of UNIX called FreeBSD (<http://www.freebsd.org>) is also quite popular among the technical community. This precludes the danger of viruses, worms or other code that exploits weaknesses in the Windows environment.

Another point to consider is that if a hacker has hijacked another computer to carry out an attack, with or without permission, the retaliatory counter-attack will illegally hack an innocent system.

Prevention: Prevention is the collected knowledge, experience and best practices that provide an appropriate level of security. Equivalent to secure locks and alarms for protecting a home, preventative measures include improved software and hardware design, security standards and practices, digital signatures, encryption and other tools that create obstacles for potential attackers.

Public/private sector cooperation, as well as international cooperation, are essential for the development of this area. One such example is the InfraGard initiative in the US.

Address <http://www.infragard.net/about.htm> Go Links Norton AntiVirus

InfraGard
Guarding the Nation's Infrastructure

About InfraGard

Organization

InfraGard is a Partnership between Private Industry and the U.S. government (represented by the FBI). The InfraGard initiative was developed to encourage the exchange of information by the government and the private sector members.

Private sector members and an FBI field representative form local area chapters. These chapters set up their own boards to govern and share information within the membership. Each chapter is also part of an organization which is InfraGard.

The Federal Bureau of Investigation play the part of facilitator by:

- gathering information and distributing it to members
- educating the public and members on infrastructure protection
- disseminating information through the InfraGard network
- producing valuable analytical products on information received through the InfraGard network
- opening the doors of communication between government and private sector members.

Detection: Detection is the vital component needed to enable a rapid response to security breaches. Several technical measures can be implemented to detect attempts to intrude into a network or computer. In addition, Computer Emergency Response Teams (CERTs), that of Carne-

gie Mellon University in the US perhaps being the best known, provide reliable information about threats. The statistics published by CERT (<http://www.cert.org>) clearly indicate that the number of vulnerabilities reported and the number of attacks continue to rise steadily (having doubled annually over the past six years).

Reaction: Reaction is a major subject in itself and deals with the best ways to resolve problems and restore normal operations. The issue of what constitutes an appropriate and coordinated response at the national and international levels remains open to debate.

About exposures

All networks are at risk of attack by both unknown hackers and those with access to inside knowledge (employees, former employees, vendors' employees, trainers, consultants and many others who are essential components of today's complex environment).

Our increasingly networked society and business environment heighten the challenge of maintaining security. Companies establish partnerships which require interconnected systems and networks to participate in electronic commerce and to allow them to operate within each other's supply chains.

The cost, complexity and effort of achieving a low residual risk are very high. Systems that are not connected to shared infrastructures (not only the Internet but also networks of other organisations) stand the best chance of surviving a cyber-attack.

The most visible effects of cyber-attacks are found on the Internet. However, the most damaging and expensive are, and will continue to be, in business services and military systems. Many of these services and systems are either not connected to the Internet, or are connected behind several layers of protection.

While attacks on these services and systems require knowledge restricted to a small number of individuals and sophisticated access facilities, the risk of such actions being facilitated by an insider cannot be excluded. This creates an ethical problem for employers.

About critical infrastructures

Critical infrastructures and functions fall into four categories:

- national public administration (government departments, public services and publicly owned industries such as electricity, water, air traffic control and telecommunications);
- national intelligence, defence, police and emergency services;
- international organisations performing critical activities that could, if seriously interfered with, have serious consequences in the short term – examples include UN peacekeeping operations, NATO, and numerous humanitarian organisations;
- infrastructures owned and operated by the private sector (which may be involved in the same areas of activity as those listed in the first point above).

Because of their role in the functioning of society, security managers in critical infrastructures have to accept, and fulfil, a number of special responsibilities:

- Their computing and networking systems and facilities must be designed to be highly secure.
- They must continually monitor for vulnerabilities, threats and potential attacks.
- They must have effective Emergency Response Teams as well as detailed and tested arrangements to deal with security incidents.
- They must have proven and tested disaster recovery, business continuity and crisis management plans and processes.
- They must have an adequate number of trusted, qualified and experienced security staff.
- The interface between the critical infrastructure and the public Internet, if there is one, must be particularly well configured and managed.
- They should seek, achieve and maintain formal certification for their security arrangements.
- They must maintain effective coordination and communication with other critical organisations to which they are linked or which depend on the services they provide.

None of the above tasks can be described as simple. They are made all the more complex whenever such critical infrastructures are outside the

private sector, as a number of common characteristics are shared regardless of geographical location:

- slow and complex procurement, recruitment and implementation;
- rigid budgets subject to political decisions;
- fixed, sometimes non-competitive, pay scales;
- little reward for success.

These limitations frequently result in one or more of the following situations:

- many inadequately protected systems;
- not everything is properly configured and installed and vulnerabilities are accepted as “inevitable” because of a lack of available resources;
- inadequate, if any, training on computer and data hygiene, security, policies and best practices;
- questionable and untested security practices;
- variable, sometimes doubtful, security clearance procedures;
- little or no use of Total Quality Management.



Security audits may be infrequent. Certification is not a common practice and disaster recovery and business continuity plans may exist but are often untested. This all works against effective security and as good ICT talent is in short supply, public administration frequently ends up with second best. The fact that these staff members work within a “comfort zone” of secure employment is a problem, as is the lack of physical security.

THE INTERNATIONAL STANDARD ISO 17799

Using established standards and codes of practice

Several standards and best practices have been established in the field of information security. This booklet uses the framework of the international standard ISO 17799, “Code of Practice for the Management of Information Security”, which allows for a cross-reference of the following discussion with a well established and respected document.

The Geneva based International Standards Organisation (ISO) published the first edition of this document in 2000. Its precursor was the British Standard BS 7799 (Part I), the “British Standards Institute Code of Practice for Information Security Management”, which was first issued in 1995 and subsequently adopted in a slightly modified form by a number of other countries.

The British standard now includes a Part II, which includes a specification for an Information Security Management System (ISMS.) The intention is that formal certification should be carried out against Part II of the standard.

The discussion that follows is based on ISO 17799 and not the more recent British standard. It identifies and describes ten guiding principles, presented in summary form. This discussion should not be considered a replacement for the full text of the document.

Although ISO 17799 is described as a standard, it is not prescriptive. For example:

- It does not state that “you must have a firewall”, but instead puts forward that “precautions are required to prevent and detect the introduction of malicious software”.
- It does not state that “*your* system must be the same as *my* system”, but instead puts forward that “it is essential that an organisation identifies *its* security requirements.”

Guiding principle no.1: Security policy

Purpose: To provide management direction and support for information security. The standard recommends the following framework:

- establishment of a top-level management security forum;
- provision of individual security awareness training;
- risk management as a management approach;
- compliance with the appropriate legislation (e.g. the European Data Protection Directive).

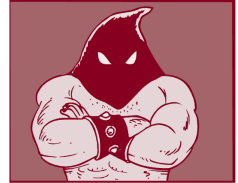
A policy document would, at a minimum, contain sections on:

- an organisation’s need to have a contingency plan;
- the need for effective data back-up;
- avoiding malicious software;

- procedures for controlling access to systems and data;
- procedures for reporting security incidents;
- procedures for policy non-compliance, malicious activity, inappropriate use, etc.

The detailed writing of security policies can be based on ready-made policies that can be purchased from specialised sources or outsourced to a suitable consultancy. However, senior management should not abdicate its responsibility to make key decisions with financial and ethical implications, or those effecting human resources.

The modern corporate environment sometimes imposes measures to deal with non-compliance that strongly resemble the stark, quick and severe punishment of centuries past. However, this is not always the case. Both managers and staff should be clearly informed of the consequences of not complying with prescribed policies.



Guiding principle no. 2: Security organisation

Purpose: To manage information security within the organisation with particular emphasis on:

- maintaining the security of organisational information processing facilities and of assets accessed by third parties;
- maintaining the security of information when the responsibility for information processing and service delivery has been outsourced to another organisation.

Security organisation should provide for, at the very minimum:

- establishing an internal forum for information security;
- arranging the coordination of information security;
- allocating information security responsibilities to nominated functions/ individuals;
- identifying the risks associated with third party access to data and information;
- ensuring that security requirements are specified in contracts with third parties;
- determining security requirements in outsourcing contracts.

In situations where information security is critical, the Chief Executive may consider requiring the most senior person responsible for this matter, either the Chief Information Officer or the Chief Security Officer (or equivalent titles), to formally document all system and process vulnerabilities. The person holding this position may also be required to sign a statement on the security status of the information assets in the same way that the Chief Financial Officer is expected to sign the financial statements of the organisation and have them subjected to an independent audit.

Guiding principle no. 3: Asset classification and control

Purpose: To identify the scope of information security management and ensure that information assets are given an appropriate level of protection.

An organisation implementing ISO 17799 must determine which of its information assets may materially impact the operation and delivery of its business activities if they were to become unavailable or degraded.

This in turn requires an analysis of the probability (risk assessment) that a given threat will exploit a specific weakness and cause loss or damage to an asset or group of assets. Risk is defined by the combination of value, vulnerability and threat.

All assets relevant to the scope of the Information Security Management System must be identified and assigned a nominated “owner” or custodian.

Guiding principle no. 4: Personnel security

Purpose: To reduce the risks of human error, theft, fraud or misuse of facilities, in particular:

- by ensuring that all end-users are aware of information security threats and concerns and that they can support the organisation’s security policies in the course of their normal work routine;
- by working to minimise the damage caused by security incidents and malfunctions as well as to learn from such incidents.

Typically, the necessary tasks to meet this requirement are:

- including security considerations and responsibilities in job descriptions and staff contracts as well as in the contracts for temporary staff, contractors and consultants granted access to systems and facilities;
- end-user training and awareness programmes;
- developing response methodologies and practices in the event of malfunctions and security incidents.

Guiding principle no. 5. Physical and environmental security

Purpose: To prevent unauthorised access, damage and interference to business premises and information and, as a result:

- prevent loss, damage or compromise of assets and/or an interruption of business activities;
- prevent the theft of information and/or information processing facilities.

Usual practices in the implementation of environmental security include:

- defining and implementing a security perimeter;
- establishing physical access controls (e.g. smart cards, keypad and secret codes and their associated monitoring);
- defining secure working areas and associated practices;
- ensuring the continuity and security of power supplies;
- developing practices for the disposal of equipment (which may contain licensed software and data and thus fall under the scope of the security policy).

However, many of these practices are not systematically applied. Consequently, an additional good practice is to conduct unannounced checks on a fairly frequent basis. It is not unusual for secure doors to be wedged open (“we are waiting for a delivery”) or for unescorted visitors to be allowed access to computer rooms (“we know this person”).

The widespread use of notebook computers, personal digital assistants and wireless networks make this task more complex.

Guiding principle no. 6: Operations management

Purpose: To ensure the correct and secure operation of information processing facilities in order to:

- minimise the risk of systems failures;
- protect the integrity of software and information;
- maintain the integrity and availability of information processing and communications facilities;
- ensure the safeguarding of information on networks;
- ensure the protection of the supporting infrastructure;
- prevent damage to assets and interruptions to business activities;
- prevent the loss, modification or misuse of information exchanges between organisations.

The minimum components of these practices are:

- fully documented operational procedures (typically comprising Availability and Performance Management, Incident and Problem Management as well as Change Control and Configuration Management, among others);
- clear assignments of individual responsibilities;
- protection against malicious software;
- housekeeping (for example, registering and maintaining the records of users, inventories and resource usage);
- network management;
- media handling and its security;
- exchanges of information and software with other parties.

There are many ways to obtain best practice information about this domain. One example is the Information Technology Infrastructure Library (ITIL), originally developed more than ten years ago by the UK government's Central Computing and Telecommunications Agency (CCTA) and now managed by an autonomous entity: <http://www.itil.org.uk>. Obtaining such information is necessary but not necessarily sufficient. Responding to hackers may require the organisation under attack to use "guerrilla" tactics of its own.

Guiding principle no. 7: Access control

Purpose: To control access to information in order to:

- prevent unauthorised access to information systems;
- prevent unauthorised computer access;
- ensure the protection of networked services;
- detect unauthorised activities;
- ensure information security when using mobile computing and teleworking facilities.

Even though individual users may legitimately need access to an organisation's systems, data and information, their rights do not have to include universal access to all information assets. Therefore, an organisation needs to define who has the rights to access what and when.

The usual activities associated with access control include:

- definition of the access control requirements (with a focus on confidentiality);
- managing the access rights of individual users;
- defining the responsibilities of individual users;
- defining the appropriate mechanisms for access to a) the network; b) applications; and c) operating systems;
- policies and practices for monitoring system access and use;
- policies and practices for granting remote access to teleworking staff, from mobile devices, etc.;



These issues require particular attention when the activities are outsourced. It is strongly recommended that the right to audit the outsourcer should be part of all such contracts.

Guiding principle no. 8: Systems development and maintenance

Purpose: To ensure that security is built into information systems in order to:

- prevent loss, modification or misuse of user data in applications systems;
- protect the confidentiality and integrity of information;
- ensure information systems and support activities are conducted in a secure manner;
- maintain the security of application system software and data throughout the lifecycle of such systems.

This would normally require:

- defining the security requirements of systems and computer applications;
- defining the role of cryptographic controls;
- ensuring the security of system files;
- ensuring the security of development and support processes.

Applications development is an activity which is increasingly being outsourced, and the same recommendation applies: the right to audit the outsourcer should be part of all such contracts.

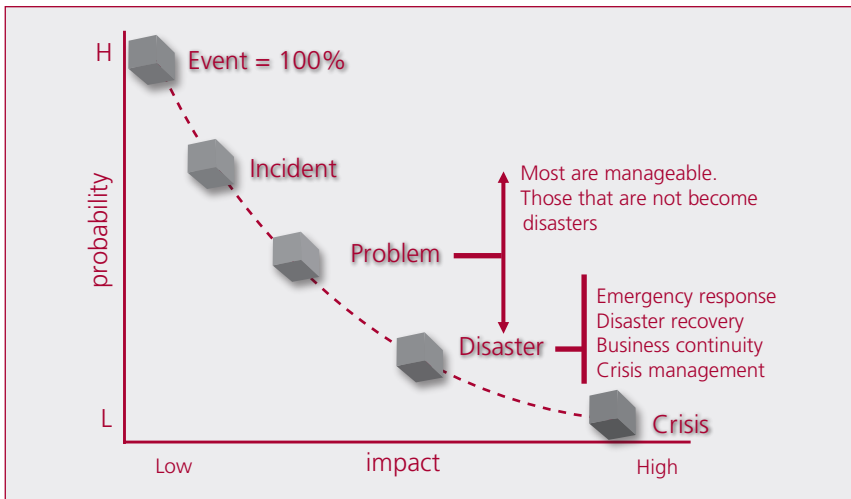
Guiding principle no. 9: Business continuity management

Purpose: To counteract interruptions of business activities and protect critical business processes from the effects of major failures or disasters.



Based on ample evidence, business continuity practitioners say the following:

Fail to Plan = Plan to Fail



This chart illustrates the relationship between the probability of occurrence and the impact of the different situations that can arise in the realm of information security.

Security *events* are those minor IT incidents that are invariably sprung on us: an urgent security patch to install, a new virus that appears before the anti-virus software vendors have issued the antidote or an employee who forgets his or her password and unsuccessfully attempts to login five times. Such incidents have a 100 percent probability of occurring. They are a part of life.

Events that are not resolved quickly or easily and need to be passed on to technical or other forms of support, become *incidents*. By their very nature, incidents have a visible impact and it is good practice to record them.

Incidents that cannot be dealt with within a suitable time-frame, so as not to affect the operations of an organisation (it could be minutes for a critical infrastructure or hours for an academic institution), become *problems*.

Problems are invariably brought to the attention of senior management simply because of their impact. Problems that cannot be fixed risk becoming *disasters* that can interrupt business operations for an undefined period of time.

Disasters can be categorised using the ABC method, depending on the location and nature of the disruption. In an A (Area) type disaster, an entire area is affected; in a B (Building) type disaster, a building or building complex, and in a C (Content) type disaster, the ability of an organisation to access and process the information it needs for its operations is affected. Type C disasters are usually associated with information and communications technology problems ranging from malicious code to technical problems that cannot be resolved quickly.

The impact of the various types of disasters depends on the nature of the activities of a given organisation. A street demonstration that prevents free movement in a particular area for a day is not strictly speaking a disaster for a public administration office. However, it can be for an emergency room in a hospital.

Disasters often degenerate into *crises*, at which point it becomes necessary to deal with the media.

An effective response to disasters occurs in four stages:

Emergency response: This is the set of actions to be taken immediately upon the detection of a potentially major problem, to determine if it

can be contained and resolved without significant disruption to business operations.

Disaster recovery: This is the responsibility of the parties providing communications and operations management, i.e. an essentially technical process which relies on the use of other, often distant, facilities with an adequate replica of the affected infrastructure.

Business continuity: In this stage, clearly defined and essential activities can continue to be carried out from another location if necessary. This is the responsibility of senior management and involves staff who must be available and ready to assume these responsibilities as and when required.

Crisis management: This is another senior management responsibility. It involves communicating with all stakeholders and other important parties once a disaster has taken place and the business continuity arrangements have been put in place.

In practice, it is not uncommon for organisations to pay lip service to these four stages. They are complex, expensive and inconvenient, particularly during testing.

Such plans need constant reviewing and updating, as well as testing, if they are to be of any use in case of a disaster. The literature of disaster recovery and business continuity is replete with sad stories of plans that proved worthless with catastrophic results for the respective organisations.

Guiding principle no. 10: Compliance

Purpose: To avoid breaches of any civil or criminal law or of statutory, regulatory or contractual obligations, and to comply with organisational security policies and maximise the effectiveness of system audit processes.

This requires a thorough knowledge of the legislative framework within which the organisation operates, as well as a review of the security policy from this perspective.

A system audit becomes an essential part of the compliance process. Another controversial aspect of compliance involves the monitoring of an organisation's personnel to see how well it complies with the organisation's security policies. This entails monitoring employees' activities and has the potential to raise the issue of appropriate use of the employer's systems and facilities.

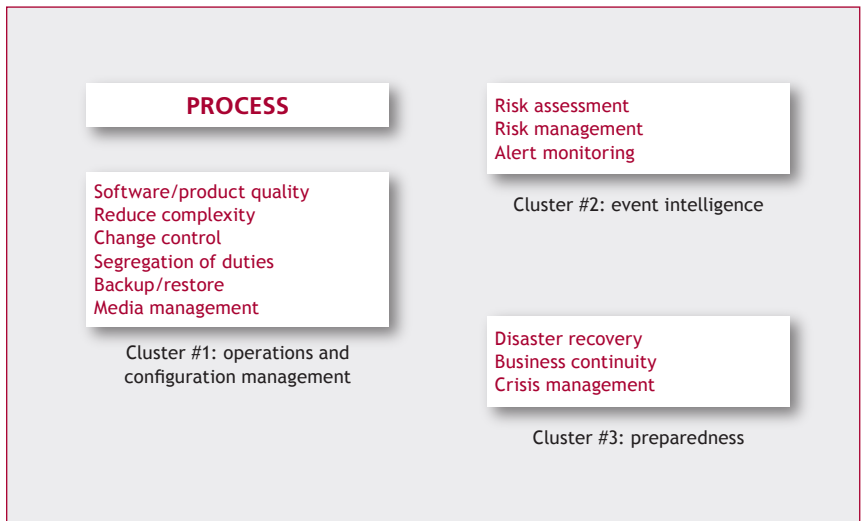
DEALING WITH THE ORGANISATIONAL IMPLICATIONS OF INFORMATION SECURITY

While ISO 17799 and other such standards (see also the Section *Preparing for information insecurity*) provide good frameworks, they also raise several complex issues for senior management:

- agreeing how much should be spent on information security;
- agreeing on the criteria for justifying investments and expenditures for information security;
- understanding and managing the impact of bystanders and obstacles;
- defining the appropriate balance for information security policies and the consequent impact on personnel: somewhere between a laissez-faire approach and a dictatorship;
- dealing with security breaches;
- appropriate response against malicious action by a trusted insider;
- whether or not to seek certification.

Ensuring the right technical approach is taken

The technical implementation of information security measures requires multiple structured processes to be developed. These can be grouped into three clusters, shown in the diagram below.



Operations and configuration management is the basis of all operations in a computer or telecommunications centre. There are three proven complementary approaches:

Approach no. 1: The KISS principle

KISS stands for “Keep It Simple, Stupid!” as complexity is known to be the enemy of manageability.

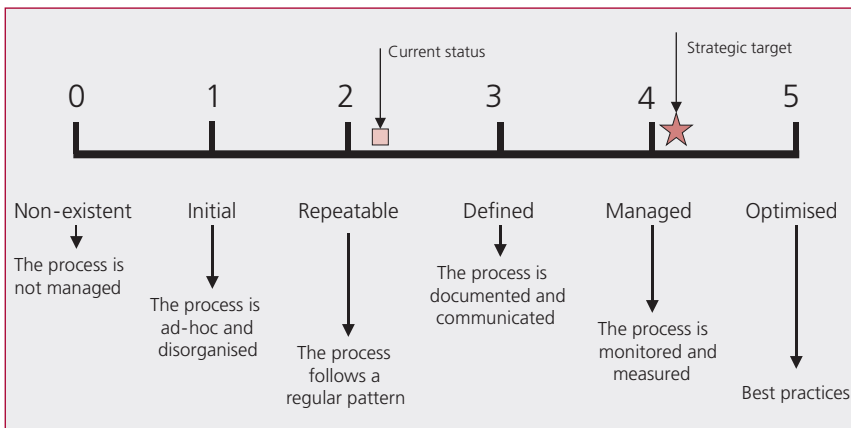
Approach no. 2: Adopt proven best practices

As much as creative technical people like to think they know better, much can be said for avoiding reinventing the wheel, particularly where this risks derailing the operations of a whole organisation. There are many ways to obtain best practice information. The Information Technology Infrastructure Library referred to earlier in this booklet is one such example.

Approach no. 3: Adopt the Total Quality Management approach

Formalised in the family of standards collectively known as ISO 9000, Total Quality Management complements the previous two approaches by emphasising a formal approach to the documentation of how processes are conducted, collecting data on systematic problems and focusing on continuous process improvement to eliminate them.

The Information Systems Audit and Control Association (ISACA) uses ISO 9000 as the basis for defining process maturity. The diagram below illustrates the levels of organisational maturity as defined in the guidelines for the Control Objectives for Information Technology (COBIT).



Obviously, working at a level of maturity of 0 or 1 is not a particularly effective way to manage a critical task such as information security. However, the migration to level 4 or 5 may require a significant cultural change in the information technology staff, as well as significant effort to achieve the required level of maturity.

The information insecurity timeline

The timeline for information insecurity has three stages: Before, During and After.

Preparing for information insecurity

The ISO Standard 17799 provides a structure of activities to improve information security. This short section places these activities in context and prescribes a timeline. Preparation is clearly the first necessary activity.

We prepare for security in our homes as a matter of course, as in most societies it is not practical to live in a house without the means to protect personal security and property. However, every situation is different. The level of security will depend on the value of the items we wish to protect and the threats against which we seek such protection. In the end, we all ensure that our property has sufficient locks and possibly, depending on who we are, and where, burglar alarms, secure fences, guard dogs and other additional protective measures.

Even then, we know from experience that 100 percent security cannot be achieved – professional thieves will defeat the best “secure” locks. In addition, every measure of security we implement will subsequently constitute an obstacle to our personal access: two locks on the door, a burglar alarm that needs to be reset within 30 seconds, and so on and so on.



Even though ISO 17799 has its critics and is not perfect, it still offers a good description of minimum requirements. For those interested, other standards do exist, for example, the SAS 70 (<http://www.sas70.com>): the Statement on Auditing Standards Number 70 developed by the American Institute of Certified Public Accountants (AICPA). Another example is the NIST's 800-37 put forward by the Computer Security Resource Centre of the US National Institute for Standards and Technology (<http://csrc.nist.gov>).

All information security literature emphasises that security is both a technical and a managerial problem.

Monitoring systems and traps

This booklet should have by now made it clear that malicious code, such as a virus, is only one form of attack, and therefore *antivirus software* is just one of the many tools that protects information systems and networks.

Cyber-attackers do not give warnings about the timing and nature of their attacks. Firewalls and intrusion detection systems of two examples of tools used as protective shields against external attacks.



Intrusion detection systems (IDSs) monitor computers and networks for possible security breaches: either external attacks or misuses from within the organisation. Intrusion detection systems include such functions as:

- ability to recognise typical attack patterns;
- analysis of abnormal activity patterns;
- analysis of system configurations and vulnerabilities;
- tracking security policy violations.

Honeypots are systems (combinations of hardware and software) deliberately designed to attract potential hackers in order to learn how they operate and manage to break into and exploit protected systems. A well designed honeypot will appear to be a valuable resource to a hacker and give no indication that he or she is being tricked and monitored.

The main benefit of a honeypot is that it reveals the vulnerabilities of the security arrangements and provides pointers for the creation of more secure systems.

Highly sophisticated honeypots have been used to track down and identify hackers.

Monitoring systems against internal attacks

The most damaging attacks against information systems are invariably launched by trusted insiders. There are many products designed to search for unusual activity in systems and networks to provide indications of potential misuse or sabotage. The implementation of such sys-

tems creates ethical and legal issues that need to be dealt with on a case by case basis.

Intrusion detection systems, honeypots and internal monitoring systems generate massive amounts of information (including false positive alerts) and the resources and effort involved in making effective use of them must not be underestimated.

Reacting to an information security incident

Adequate preparations will pay off the day that a cyber-attack takes place. Following is a short sequence of actions (their discussion goes beyond the scope of this booklet) that must take place in such an event:

- tactical warning (monitoring, detection and reporting);
- activation of the Emergency Response Team;
- damage control;
- activation of contingency plans;
- attack assessment and collection of forensic evidence;
- restoration of networks, systems and data to “normal” status.

These activities are the responsibility of a technical team, either from the organisation or from the outsourcer if the services are provided by an external company. The role of senior management is to concentrate on the effectiveness of the contingency plans and crisis management as and when it becomes necessary.

Digital autopsy of a security breach or cyber-attack

After an information security event has taken place and the situation has been restored to normal, conducting a detailed review of what allowed the incident to take place is recommended.

For a cyber-attack involving the penetration of a network or computer system, it is vital to identify the mechanism used to achieve this and discover the exact nature of the vulnerability that allowed it. As discussed earlier, such vulnerabilities can be technical or procedural. In both cases, it is prudent to take corrective action immediately upon discovery.

When the review identifies a lack of due diligence or malicious intent on the part of an employee, the problem becomes complicated. It may

be necessary to take disciplinary or legal action against the individual concerned.

This requires senior managers to avail themselves of digital forensics, the study of information technologies as they relate to the law. Digital forensics deals with the preservation, identification, extraction and documentation of computer evidence.

Who needs to use digital forensics? In practice anyone who needs to handle a case of fraud, sabotage, industrial espionage or other offences.

Who needs evidence? Executives and managers, criminal and civil lawyers, insurance companies, and law enforcement officials as well as individuals. Such evidence must be obtained and secured in such a way as to retain its legal value.

Evidence can be *visible* – in the form of unencrypted stored data in a computer or data intercepted as it flows openly over a network. Other, more complex forms of evidence also exist.

Visible-invisible evidence is information that is deliberately hidden through the use of passwords, encryption or information hidden in another file. Steganography is one example of a technique used to hide data.

In an investigation, logs, also part of the visible-invisible evidence, may additionally show activity at unusual times or missing sequential numbers.

Invisible-invisible evidence falls into two categories: 1) that which has not been hidden by an individual but by the system itself, as is the case with Windows temporary files, swap files, Internet temporary files, etc.; and 2) that which has been hidden deliberately, including files erased by an individual (as opposed to deleted files which can usually be recovered).

Securing evidence requires a comprehensive knowledge of all the applicable legislation. A number of elements are common to such legislation, including, but not limited to:

- documenting the time, date and circumstances of the seizure;
- collecting all physical evidence associated with the event (Post-It™ Notes, desk calendars, notebooks, manuals, contents of waste baskets, floppy disks);

- labelling all evidence in a clear manner;
- discovering *all* files (normal, deleted, password protected, encrypted and hidden);
- recording all serial numbers, documenting the system layout, etc.;
- transferring all items under investigation to a secure, access restricted location, taking particular care not to expose them to electromagnetic interference;
- creating a secure set of no less than two copies of everything using disk imaging techniques, keeping one copy in an evidence container.

The key point is that unless evidence has been collected, kept, analysed and disclosed, in full compliance with the applicable legislation, it risks being dismissed by a court of law.

It is strongly recommended that both the internal auditors of the organisation and the legal counsel be closely involved with these processes.

Employees' freedom of expression, monitoring and civil rights

Many organisations and companies have introduced tighter control of the activities of their employees. Initially, tools for such control simply monitored Internet usage and produced reports of, for example, the time spent by employees accessing websites and the list of the websites they most frequently accessed.

Since then, monitoring has become more complex for three reasons: employee productivity, information security and legal liabilities. The following discussion will focus on information security.

The need for information security introduces a rather unpleasant principle, “trust no one”, which may offend those diligent employees who work with nothing but good intentions.

Regrettably, over the years it has become clear that the actions of malicious insiders are the most detrimental to an organisation and often the hardest to detect. The latest generation of monitoring systems may look to some like something out of George Orwell’s novel *Nineteen Eighty-Four*.

Top of the line systems of this kind are not in widespread use, as they are complex to implement and manage. One such system collects and correlates information from physical (typically access control) and computer systems to identify and track where unauthorised users are accessing computer resources.



According to the annual study on workspace monitoring by the American Management Association, the number of companies in the US performing 'active monitoring' of employees rose from 45 percent in 1998 to 78 percent in 2001; e-mail monitoring rose from 27 to 38 percent over the same period. Most companies give the following reasons for monitoring: legal liability, productivity and protection of their trade secrets and intellectual property.

It is assumed that in order to facilitate acceptance, most employers would advise their employees that such systems are in use as part of the organisation's formal security policy. Nonetheless, it is an employer's prerogative to decide whether and how to monitor its staff's activities.

CONCLUDING REMARKS

These are early days in the management of information security and matters are unlikely to become less complicated. Among the emerging headaches facing Chief Information Officers and IT Managers are:

- the creativity and ability of the growing international community of hackers, hacktivists and other players;
- the potential for malicious software to become seriously damaging, by deleting or corrupting corporate document repositories, databases or systems data;
- the explosive growth of documents and other forms of information in digital form whereby storage (as well as backups and disaster recovery) become a significant technical and operational challenge;
- the security implications of wireless networking (such as WiFi), which are being deployed ahead of effective security solutions for them;
- the proliferation of small, easy to lose, portable devices such as Personal Digital Assistants (PDAs) containing corporate data

- and documents as well as possibly automated mechanisms for accessing corporate networks (a large number of software packages and applications will offer to “remember your password”);
- the emerging world of mobile computing and teleworking and the problem of “junior” using father’s access to the corporate network from home to “download interesting stuff from the Web”.



The intention of this booklet is not to scare readers, but to highlight the need for vigilance and preparedness. The following basic rule should never be forgotten:

Better safe than sorry.

ABOUT THE AUTHORS

Stefano Baldi

Stefano Baldi is a career diplomat in the Italian Ministry of Foreign Affairs, Counsellor at the Permanent Mission of Italy to the UN – New York. He has also served at the Permanent Mission of Italy to the International Organisations in Geneva, where he has developed several initiatives for the use of information technologies (IT) in the diplomatic community.

Baldi has an academic background in demography and international social issues. He also lectures on the use of internet for ministries of foreign affairs and missions at DiploFoundation's Postgraduate Diploma Course on Information Technology and Diplomacy. Baldi's most recent research focuses on the impact and future developments of information technology in international affairs.

<http://baldi.diplomacy.edu>

baldi@diplomacy.edu

Ed Gelbstein

Eduardo Gelbstein is a Senior Special Fellow of the United Nations Institute for Training and Research (UNITAR) and a contributor to the United Nations Information and Telecommunications (ICT) Task Force and to the preparatory work for the World Summit on the Information Society. He is the former Director of the United Nations International Computing Centre.

In addition to his collaboration with the United Nations, he is a conference speaker and university lecturer reflecting his 40 years experience in the management of information technologies.

He has worked in Argentina, the Netherlands, the UK, Australia and after joining the United Nations in 1993, in Geneva (Switzerland) and New York (USA). He graduated as an electronics engineer from the University of Buenos Aires, Argentina in 1963 and holds a Master's degree from the Netherlands and a PhD from the UK.

gelbstein@diplomacy.edu

Jovan Kurbalija

Jovan Kurbalija is the founding director of DiploFoundation. He is a former diplomat with a professional and academic background in international law, diplomacy and information technology. Since the late 1980s he has been involved in research on ICT and law. In 1992 he was in charge of establishing the first Unit for IT and Diplomacy at the Mediterranean Academy of Diplomatic Studies in Malta. After more than ten years of successful work in the field of training, research and publishing, in 2003 the Unit evolved into DiploFoundation.

Jovan Kurbalija directs online learning courses on ICT and diplomacy and lectures in academic and training institutions in Switzerland, the United States, Austria, the United Kingdom, the Netherlands, and Malta.

The main areas of his research are: diplomacy and development of the international regime on the Internet, the use of hypertext in diplomacy, online negotiations, and diplomatic law.

jovank@diplomacy.edu

NOTES

NOTES

NOTES