Protecting Critical Information Infrastructures

Eduardo Gelbstein

Ed Gelbstein has over 40 years experience in information systems and technology, both in the private and public sectors. His experience includes being Information Technology Strategy Manager for the British Railways and Director of the United Nations International Computing Centre. He was also an advisor to the United Nations Board of Auditors and the French Cour des Comptes. Ed is currently Adjunct Professor at Webster University Geneva and the author of several books and articles as well as a regular speaker at international conference on security, risk, audit and governance.

Resumo
Proteção de Infraestruturas Críticas de Informação

O recurso aos sistemas de informação na gestão e operação de infraestruturas críticas cresceu exponencialmente em todo mundo, sendo que atualmente não existem infraestruturas críticas que não dependam fortemente de software, computadores e redes informáticas.
Nenhuma tecnologia é perfeita e lidar com erros de sistemas faz parte das responsabilidades daqueles que fornecem e operam esta tecnologia. A ubiquidade das redes globais como a internet criou um desafio adicional: tentativas, por vezes bem-sucedidas, de aceder a estas tecnologias por parte de terceiros com a intenção de interromperem estas operações ao abrigo de justificações que vão desde o simples desafio individual, ao ativismo e, potencialmente, a operações de natureza militar ou terrorista.
Os desafios associados à proteção de infraestruturas de informação crítica da qual a sociedade depende para funcionar, são variadas e complexas e têm de lidar com componentes passíveis de gerarem erros: pessoas, processos e tecnologia.
Este artigo fornece uma visão sobre estes desafios e aponta sugestões e referências quanto às melhores práticas.

Abstract

The use of information systems in the management and operation of critical infrastructures has grown explosively around the world and, today, there are such infrastructures that do not have a strong dependency on software, computers and networks.
No technology is perfect and dealing with malfunctions is part of the responsibilities of all those who supply and operate such technology. The ubiquity of global networks such as the Internet has created an additional challenge: attempts, often successful, to access such technologies by external parties intent in disrupting their operations for any of a number of reasons, ranging from "because I can" to activism and, potentially, military and/or terrorist.
The challenges of protecting the critical information infrastructures, on which society depends to function, are many and complex as they have to deal with three imperfect components: people, processes and technology. This article provides an overview of these challenges and includes pointers and references to established standards and good practices.

Social and economic stability require the reliable operation of many Critical Infrastructures. While there are many definitions of what is a Critical Infrastructure, the one adopted by ENISA[1] states:

"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".

These include all utilities such electricity generation and distribution, water treatment, air traffic control, airport and airline operations, railroads and ports, telecommunications, logistics, law enforcement, refineries, banking, finance and many more.

All of these have, at one time or another, suffered disruptions that had significant economic and social costs. All such critical infrastructures have an irreversible dependency on computer systems and networks used to automate and support their operations and it is therefore appropriate to think of them as Critical Information Infrastructures (CII).

For the purpose of this article, the specific and essential characteristics of a CII are that:

- It operates seven days a week, 24 hours a day.
- Their operations require information systems and networks, sensors and other mechanisms for data acquisition.
- Many also operate physical devices ranging from cash dispensers (ATM) to motors (e.g. to switch a railroad track) and robotic systems (e.g. in manufacturing and other continuous processes).
- It is part of a supply chain – operational failure propagates to other entities that may also be CII.

When the objective of cyber-attackers is to – at the very least – cause disruption, CII are attractive targets.

The measures to protect CII described in these pages can be found everywhere and are based on a relatively small number of standards and good practices. However the way in which they are practiced are, like snowflakes, similar but different. The challenge is to demonstrate that they are "good enough" and this is hard enough.

1 European Network and Information Security Agency, www.enisa.europa.eu

Given the frequent, numerous and successful cyber-attacks on such systems and networks by largely unknown players, they should be considered to be potential targets of future cyber-attacks. This, in turn, creates a need for information security to be adequately implemented, managed and assessed.

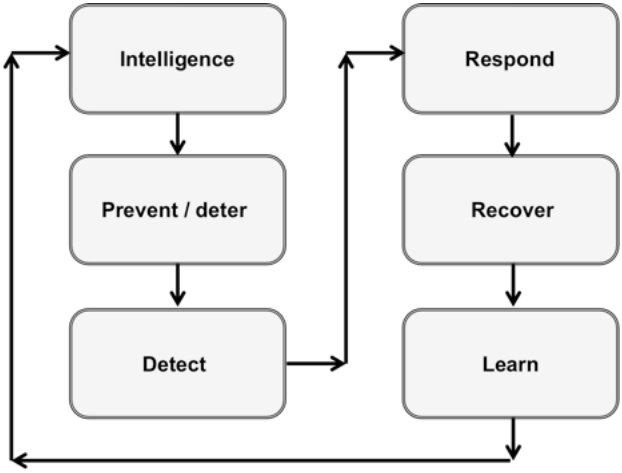
This article makes the assumption that CII operate within several constraints, notably financial, regardless of whether they are in the public or private sector, as well as cultural. The latter include risk aversion and resistance to change as well as difficulties to recruit and retain talented and experienced people.

The objective of information security is to provide adequate assurances of an organisation's information availability, confidentiality and integrity.[2]

The attackers' objectives are the precise opposite: to interfere with access to information, to steal and disclose sensitive or valuable information and to corrupt or destroy data.

The Lifecycle of Information Security

Sustainable security requires (at least) that the six tasks shown in the figure below to be performed adequately.



The main activities, which must be carried out proactively, are:

- Intelligence: this consists of several separate activities carried out by different people.

2 Appendix 1 provides definitions of the main information security terminology.

- Business Impact Analysis (BIA): usually associated with business continuity planning, a BIA identifies the most critical information components and processes of an organization.
- Risk Assessment: a detailed evaluation of the threat landscape of an organization's information covering physical events (such as earthquakes), accidental human intervention (errors, mistakes, ignorance and stupidity) and deliberate human intervention. The latter can be direct (such as fraud by an employee) or indirect (specifically, a cyber-attack). Risk assessment requires that specific attention be given to monitoring and tracking information security events around the world as attacks tactics and techniques change rapidly and, in reality, every organization should consider itself to be a potential target.
- Risk Management Plan: a portfolio of measures, technical and managerial, designed and tested to mitigate the impact of such events.
- Prevent and Deter: A key part of an information security strategy, this consists of protecting the information systems and data, regardless of where they are located, with appropriate tools and processes, ensuring these are up to date, building awareness of good security practices amongst the systems and data owners, those who use the systems and encouraging good behaviour. It must be recognised that a 100% ability to prevent and deter a cyber-attack is not achievable. The information security strategy should define what constitutes an acceptable level of security.
- Detect: the ability to detect an intrusion or attack is essential to take measures to contain and manage the attack. There are many tools (such as Intrusion Detection Systems) that can assist in this activity but none of them is perfect. Recent examples of intrusions that were undetected for a significant period of time were the subject of independent reports[3], and extensive media coverage. Obviously, detection is a pre-requisite to being able to respond.
- Respond: the collection of activities needed to manage an incident effectively, contain and repair any damage, collect information in such a manner that it can be used in evidence (digital forensics), involve law enforcement or other external parties, etc. The speed of response is fundamental to minimize damage and consequent losses.
- Recover: the steps needed to return to normal operations. Depending on the nature of the cyber attack, it may require communications to stakeholders, compensation for losses and reports to regulatory authorities.

3 Available at http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf and http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf.

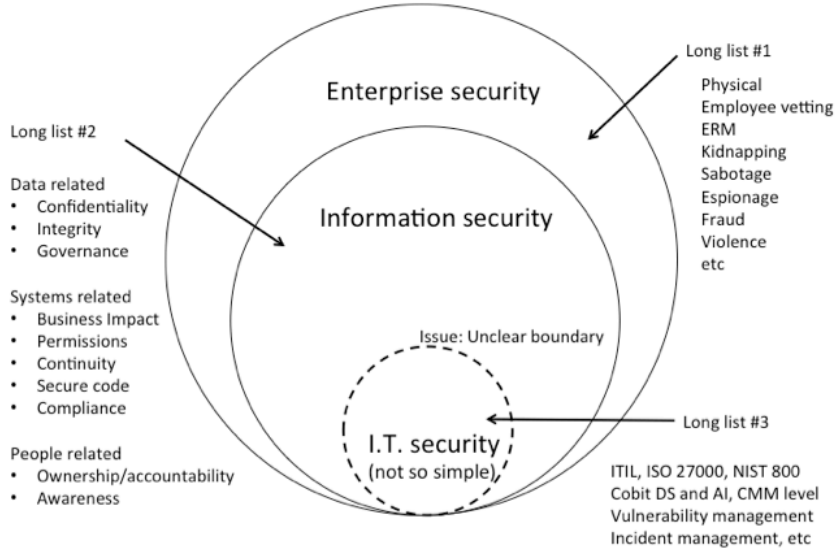
- Learn: every cyber attack represents an opportunity to learn about the effectiveness of information security arrangements, what could have been done better and what steps should be taken to strengthen security.

The converse of this is also true: every attack, regardless of whether it succeeds or fails, provides attackers with information about the security arrangements of the target. Unfortunately, this is an asymmetrical relationship: the defenders need to fight the battle every day while the attackers choose their time and have nothing to lose if they don't succeed.

The Architecture of Information Security

The statement "information security is everybody's responsibility" may appear to be a platitude, but is totally correct. The figure below shows a security architecture in which all the elements must be present and properly managed to deliver a sustainable information security.

It is easy to confuse Information Technology (IT) Security – a discipline in its own right – with Information Security and even then, not to fully appreciate how this interfaces with the overall Enterprise Security. The Figure below, presents a holistic view of how accountability for security is distributed in an organisation.



This discussion begins with the smallest (but visible and talked about) component: I.T. security. This is the technical component that is fully integrated in technical operations, regardless of whether these are provided within the company or by an external third party such as an outsourcing company.

Most people are familiar with words such as "firewall" and "anti-virus" but may not appreciate that these are merely some of the component parts. An appendix to this article gives definitions for the most commonly used terms in information security and the next section will discuss this topic in greater detail.

What the reader is invited to note are the things for which those providing for Information Technology Security are not accountable, amongst them:

- The classification of data and information into categories such as "public", "restricted to…", restricted until…", "confidential", "secret" and other as required to meet an organisation's needs;
- The assessment of the business impact of a security breach;
- The definition of access rights and privileges, i.e. who can be granted access to a network, system or database and, within that access what specifically they are authorized to do;
- Ensuring the quality of software (licensed from a third party or developed in-house). "Software" may include not only applications but also spreadsheets with complex formulae and web pages;

The parties accountable for these activities are those ensuring Information Security, the non-technical component. These parties include the functional managers who "own" computer systems such as Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), and other corporate systems, usually licensed from a vendor and customised to meet the working practices of the organisation. The vulnerabilities of such systems tend to be identified and corrected by their vendors, as they tend to have substantial numbers of clients who would be quick to report them.

In addition, there are "Line of Business Systems", those specifically designed to meet the unique requirements of the core activities of an organisation. These may be highly complex as, for example, those for air traffic control or supply chain management. In addition to their operational criticality, these systems rely on support from a relatively small number of individuals with vital knowledge.

Changes to these systems to enhance their functionality or correct a defect are known to be a time of high risk of malfunction. Moreover, the vulnerabilities of such systems, particularly when they are "one of a kind" are likely to be unknown unknowns.

Critical Information Infrastructures frequently also need another family of computer systems and networks globally referred to as Systems Control and Data Acquisition (SCADA) which are physically distributed and not managed by the IT

function as many of them are embedded into the controls of physical devices and as such, designed and maintained by vendors. Most SCADA devices have been designed to be physically robust and reliable. Security features were, traditionally, not part of the design specification and it can be assumed that many such devices remain in use. The latest generation of SCADA is believed to be considerably more secure as their operational criticality has become clear to their designers.

Other parties with key roles to play in information security include the Procurement function (contracts need to be specific on liabilities should an event occur), the Human Resources function (to report on changes of function, disciplinary action or investigations that would require access rights to the individual to be suspended, etc.), Legal Counsel (on contracts, disciplinary action, the contents of security policies, etc.), and other players will depend on the nature of the organisation.

As information security is tightly linked to enterprise security, there are other components to consider: per-employment checks, the issuance (and control) of credentials to enter a buildings or specific zones of a building, services that allow non-employees access (for example cleaners and vendors' maintenance personnel), the keeping of access logs, investigations, etc. Finally there is the Governance role of executives and senior management. This will be discussed further in the sections that follow.

All of these activities can be undermined if those who use information networks, systems and data are inadequately aware of their responsibilities with regards to information security or, worse, are not sufficiently motivated or engaged with the activities of the organisation and, as a consequence, fail to behave in a manner that protects the information assets of an organisation. Examples of such behaviour include the disclosure of information to unauthorised parties or simply ignoring security policies that rely on their cooperation.

The Components of Information Security

It is well known that a chain is only as strong as its weakest link. This article suggests that the information security chain has five links:

- Governance;
- Technology;
- Processes;
- People;
- Standards and Best practices.

The last of these is probably the strongest while "people", in the author's experience as a practitioner and auditor, almost certainly the weakest. The short discussion that follows attempts to explain why this is the case.

Governance

The governance of information security is a subset of the governance of information systems and technology, which in turn, is a subset of enterprise governance. If and when senior management abdicates its responsibilities for such governance, practitioners are obliged to second guess the organisation's security needs and work on a "best effort" basis.

The three basic governance functions as defined in international standards[4] are to: Direct, Evaluate, and Monitor (ISO 38500, ISO 27014, and other).

Senior management and, ideally, the Board of Directors, should:

- Be informed about information security and its relevance to the organization;
- Set strategy and policy, including the management of non-compliance;
- Provide technical, human and financial resources for information security;
- Assign responsibilities to management and set priorities;
- Monitor the security performance of the organization and initiate corrective actions as required.

Management's role is to assume responsibility for all operational aspects of information systems governance and deal with them proactively:

- Assessing and analyzing the impact of information systems on the organization (BIA);
- Assessing, analyzing, and managing risks associated with information systems;
- Setting information security policy;
- Assigning responsibilities to staff;
- Defining the information security management framework for the organization;
- Implementing security awareness training of all staff,

Standards and best practices for information security governance are listed in Appendix 2.

Technology

The range of technologies in today's organisations is vast, ranging from the data centre components of servers, network devices, storage, power supplies, diagnostic systems, SCADA devices, etc. These are typically "invisible" to the rest of the organisation (except at budget time).

Each of these technical components is a potential source of insecurity in itself, for example by constituting a Single Point of Failure or by containing hidden flaws

4 ISO 38500 (information systems) and ISO 27014 (information security) amongst them.

that make them insecure by design as is usually the case with software. Vendors continually issue fixes (also called patches) to remedy such flaws as and when they are discovered. It's up to the information technology service provider to implement these fixes, some of which are themselves faulty and introduce new vulnerabilities.

There is however, much more technology that introduces security vulnerabilities. A recent concern has been the rapid spread of the "Bring Your Own Device" (BYOD) concept as increasingly IT literate staff no longer wishes to be constrained by corporate technical choices and "insist" on making their own choices, initially for using their home computers and networks and more recently with smart phones and tablets.

Processes

Security practitioners have adopted three fundamental information security principles and turned them into processes – activities that are structured to be consistently repeatable and reviewed and refined to remove all (or as many as possible) systematic errors. These are:

- Need to know: information is classified and access to it is provided to enable a person to perform their tasks, but no more. The technical solutions to achieve these are globally referred to as Role Based Access Control.
- Least privilege: also related to the role of the person accessing systems, this principle defines the actions allowed, ranging from "read only, no printing or downloading allowed" to "create new record".
- Separation of duties: The limiting of individual authorities to ensure that sensitive transactions are reviewed and approved by another person (or more than one). Originally introduced to prevent fraud, this principle has found its way into other domains, such as managing technical changes and monitoring testing.

This is just the beginning of a long list of processes that support information security. The scope of this article does not allow a detailed discussion of all of them. Two key processes that management should be aware of (and control appropriately) are those of:

- Information (and data) classification: briefly mentioned earlier in this article.
- Identity and access management: the steps needed for a person to be given the credentials needed to access corporate networks and systems and their subsequent lifecycle. At the technical level (and mostly hidden from view) is a whole portfolio of processes that include such things as "change management", "configuration management", "promotion from test to produc-

tion", etc. Thick books[5] and many websites describe them in various levels of detail.

- Encryption: a method to render data unreadable to unauthorised parties.

People

Responsibility for information security, although not likely to be mentioned in any job description (other than that of the Chief Information Security Officer) rests with virtually everybody.

Board Members, Executives and Senior Managers have a primary role in Governance.

Functional Managers in Finance, Human Resources, Procurement, etc. are the custodians (some refer to them as "owners") of information assets – applications software and, more importantly, data and information.

The users of such systems and data should have contractually defined accountabilities for protecting such data from disclosure, theft, corruption and deletion. This accountability may have already spread beyond the boundaries of the organisation as information sharing with partner organisations and/or other members of a supply chain demanded it, thus creating an additional challenge for the management of Identity and Access rights.

The same users have, in recent years, challenged corporate technology choices and demand the right of using technologies of their own choice for home computing, smart phone and tablets under the concept of BYOD.

Unless the organisation takes preventive measures to avoid architectural anarchy and place controls on such devices, the risk of malware attacks and theft of intellectual property is increased.

The urge to be "permanently connected" also encourages owners of such devices to use public unencrypted networks, typically the free of charge wireless networks in hotels and coffee bars to access sensitive corporate systems while being unaware how easy it is to intercept such exchanges and also acquire login information such as user names and passwords.

Another people-related challenge relates to the explosive popularity of social networks (there are hundreds of them) and web based discussion sites and blogs which, in the absence of clear policies and controls could constitute a further information security risk.

Last but not least, are the people providing information technology services. They may be members of the organisation, an external service provider or a mix of

5 The Information Technology Infrastructure Library (ITIL), the Data Management Body of Knowledge (DMBOK), the Control Objectives for Information Technology (COBIT) are well established examples.

both. In the latter two situations terms of contract and relationship management become critical activities.

Standards and Best Practices

Information security has been recognised as an important topic for many years and this is reflected in the large volume of standards and best practices currently available. A summary list of the most widely recognised is included as Appendix 2.

The adoption of standards and best practices is essentially optional. It is a fact that these are the result of work and discussions by professional bodies and practitioners over a period of many years. Adopting them recognises that they represent their collective knowledge and experience. On the other hand, not adopting them represents one of two things:

- The organisation that chooses not to adopt such standards and best practices is more advanced in the practice of information security than their latest edition (and no doubt some are);
- The culture of the non-adopters is one of learning from experience (known as being the best teacher and also the most expensive).

Adopting such standards and best practices requires considerable effort and changes to the way security-related activities are conducted. In the first instance, the documents listed in Appendix 2 represent a large amount of information – thousands of pages to read study and understand.

Having got to this point, the next stage consists of conducting a gap analysis to identify the areas where meeting the requirements of the standard or best practice requires activities and/or changes and then carrying them out.

This requires motivation and, most important of all, time. This happens to be the resource of which we all have the least.

The Challenges of Information Security

The previous sections could be regarded as textbook stuff and now is the time to explore why, in practice, all the things mentioned before have not solved that information security "problem".

Governance

A recently published paper[6] discusses the challenges of information security governance (ISG) in some detail. This section summarises its main points as situations that practitioners and auditors encounter regularly.

It is widely advocated that Board Members, Executive and Senior Management play an active role. In practice, this is difficult to achieve because of the numerous and diverse demands on their time. In addition, practitioners are often tempted to use technical, rather than business, language creating a communications barrier and possibly losing credibility in the process.

Another driver for the failure of ISG has to do with the inevitable and human Office Politics that result in a silo mentality of "it's not in my job description" and an unwillingness to share information or collaborate towards a common objective.

Another aspect of weak ISG concerns security policies (and compliance thereto). It's easy and tempting to engage consultants to prepare such policies, which they do using templates. There is absolutely nothing wrong with such templates given that they are based on international standards and best practices.

The issue is a lack of ownership within the organisation that leads to the policies taking a long time to be issued (need to be consulted with Human Resources, Staff Representatives, Legal counsel and others) and then risk being forgotten about, i.e. not updated, not tracked to determine who has read them, if there has been a formal agreement to accept and follow such policies. Unless the policies can be enforced automatically by computer systems, there is a risk they will be ignored.

Technology

Management rely on their technical staff (or that of their service providers) for advice on technologies appropriate to meet their requirements. Technical staff relies on vendors and product reviews by independent industry observers. The truly independent observers are reputable companies that charge for their services, and therefore, not everybody subscribes, relying instead of "free" publications many of which carry advertisements for the same vendors they report on.

Many vendors have long histories and excellent track records for seriousness and quality. This does not stop their marketing departments from being perhaps too optimistic about their products, which invariably claim to be the "ultimate" answer to whatever they specialise in. In the field of information security vendors

6 Gelbstein, Eduardo, 2012. "Strengthening Information Security Governance". ISACA Journal n.º 2.

come and go. The expression *caveat emptor* is just as valid as it was when first stated.

The life cycles of technology are short and the I.T. industry is highly innovative. This means that investment cycles are short and the need to procure new products is constant. Many products can introduce major disruption to an organisation – this was the case with the personal computer, local area networks, graphical user interfaces, the Internet, mobile everything and the potential loss of control of the organisation's technical architecture. This has security implications which need to be balanced against the potential benefits of these innovations.

Processes

The challenge of implementing processes is that of making sure that the right things are done the right way and well enough.

In practice, this easier said than done. In the first instance, consensus (or clear direction) on what are "the right things" is essential, as these are not necessarily the same for all organisations at a given time. What these things are depends on the status of information security management at a given time.

For example, for an organisation that has not reviewed its information security policies for the last six years, the "right thing" may be to do so immediately. Another example could involve a situation where the Chief Information Security Manager is an individual that has no backup in the organisation. Should the situation arise that this person leaves the organisation or is unavailable to work for an extended period of time, identifying a second person to take over would also be the "right thing" to do.

Doing things "the right way" relates to the organisation's willingness to adopt a specific set of standards and/or best practices and implement them, and then ensure that appropriate training is part of the implementation project.

The third part, "well enough" is again an individual assessment driven by the nature of the organisation and its security needs. This is explore further later in this section under Assurance.

Some standards and best practices support a certification of compliance process, notably ISO 27001 "Information Security Management System (ISMS)". There is debate about the value of such certification for three reasons:

- It is possible to obtain it for a limited part of an organisation's information security arrangement.
- That it is only valid for a limited period of time, requiring regular audits and re-certification.
- That it may give management a false sense of security given the changing nature of attacks.

People

The challenges relating to people are enough to fill a book. For the purpose of this article, only two are included:

- Certifications: information security professionals can acquire, in addition to degrees and experience, formal certifications from independent organisation, notably:
  - The Information Systems Audit and Control Association[7] (ISACA) – the Certified Information Security Manager (CISM) and the Certified Information Security Auditor (CISA).
  - The International Information Systems Security Certification Consortium[8] (ISC2). This body can accredit an individual as a Certified Information Systems Security Professional (CISSP) and several others.

Requiring information security professionals in the organisation to have or acquire such certifications is a governance and human resource management question the answer to which has implications in terms of availability and conditions of employment (compensation package).

Another possible certification, internal to an organisation, would be a license to access sensitive computer systems and data, requiring the completion of a number of training modules and a test, the informational equivalent to a driving license.

- Engagement: studies published in the recent past indicate that in many organisations, particularly large one, employee engagement (or lack of it) may be an issue. Disengaged staff have limited commitment to the organisation, seen mainly as a source of income, and are apt to disregard policies and best practices. This makes disengaged staff a security risk.
- Standards and best practices: the challenges here are not simple to resolve: should the organisation adopt standards and best practices? Which ones would be the most appropriate?

While it's tempting to answer the first question in the affirmative, the effort and time involved in doing so are significant if this is to be done well enough. Management and staff commitment are essential to succeed and this cannot be done without adequate resources and determination as doing so is likely to require many changes: cultural, procedural and technical.

The second question is even harder as there are several options ranging from fairly general and non-prescriptive international standards, such as the ISO 27000 series, to national standards in the public domain such as the U.S.'s NIST SP 800 series and others that integrate the perspectives of governance,

7 www.isaca.org.

8 www.isc2.org.

audit and management such as the recently published COBIT5 for Information Security. There is, in the author's opinion, such a thing as "best".

Assurance

The remaining challenge to explore here is that of knowing how good an organisation's information security actually is. There are five complementary approaches to consider, each of them having plus and minus points:

- Information security metrics: it is often said that "you cannot manage what you do not measure" and collecting meaningful information on information security is hard to do. Many publications have long lists of things that *can* be measured. Some metrics can be very useful such as availability, number of dormant credentials (i.e. issued but not used), failed attempts to login, but collecting such data requires resources and judgement needs to be exercised in defining what is worth collecting and analysing. The significant point about metrics is that they are lagging indicators and therefore not useful to predict future performance. The fact remains that attack methodologies and tools continue to evolve and are, therefore, unpredictable.
- Information risk, vulnerability and security self-assessments: a good practice, particularly to identify vulnerabilities and in fact, those accountable for security performance are the best qualified to do this. The minus point is that optimistic bias can find its way into the assessments as not everyone is willing to admit to shortcomings of one's work or organisation.
- Independent certifications: these have been mentioned in the previous section.
- Audits: valuable when carried out by experienced and qualified auditors following formal guidelines. Useless when done by inexperienced people ticking boxes in a form without seeking evidence to support any claims made by the audited. Furthermore, audits are disruptive to day-to-day work and there is rarely a "good time" to be audited.
- Penetration tests: these will really tell an organisation how good their defences are – on condition that the ethical hackers employed are a) very capable and b) independent. A good way to conduct a penetration test would not give prior warning to those responsible for information security. However this may not be a good way to maintain their goodwill and commitment, so it's a delicate decision. It should be noted that the ethical hackers will, as a result of their tests know more about internal security arrangements than the professionals providing this service. Legally binding confidentiality agreements and a large measure of trust are essential.

Conclusions

- Every organisation should consider itself a target of a cyber attack. Many are unprepared.
- 100% information security is not achievable. Technology alone cannot provide security – it needs to be complemented by governance, processes and people.
- Everyone, from senior management to the uniformed (and possibly outsourced) security guard has a role to play to ensure an organisation's information security.
- People are the weakest link in the security chain. The practices that support information security are not self-evident and must be clearly communicated and supported.
- How much insecurity is "acceptable" will vary from one organisation to another.
- Security assurance through metrics, self-assessments, certification, audits and penetration tests needs to be used regularly if information security is critical to the role of the organisation.

Appendix 1
Basic information security definitions and terminology

The objective of **Availability** is to ensure that information can be accessed by those authorised to do so.

The objective of **Confidentiality** is the prevention of unauthorized disclosure of information.

Integrity has the objective of protecting information from unauthorised modification or deletion.

Hacker a person (in fact various types of person) who circumvents the security measures of a computer system. They intent on disruption or other malicious activity are often referred to as "Black Hat Hackers" or "Crackers". Those who use their skills to identify vulnerabilities, with or without the consent of the systems owners are called "White Hat Hackers" or "Ethical Hackers". There are, of course, those who are morally ambiguous, referred to as "Grey Hat Hackers".

Malware is an abbreviation of Malicious Software. This is designed with a multiplicity of purposes, including hostile, intrusive and annoying and used to disrupt computer operations, access private and/or sensitive information and/or take over a user's computer (without their knowledge). Malware can take many forms and evolves continuously. Its various forms include Virus, Worm, Trojan

Horse, Rootkit, Macro, Logical Bomb, and more.

SPAM is (other than the commercial product) unsolicited electronic messaging. While most common in electronic mail it has spread to other activities such as text messages on mobile phones, blogs and other forms of exchanges.

Botnet is a collection of computers connected through the Internet that are under the control of a "bot-herder" or "bot-master", who may have criminal intent – disseminating spam through the target computers – or disruptive intent – launching a Denial of Service Attack on a target organisation. Individual computers are compromised by malware and integrated into the botnet.

Denial of Service (and Distributed Denial of Service) a form of attack intended to temporarily (or indefinitely) interrupt the ability of a computer (such as a server) connected to the Internet to operate. Botnets are often used to achieve this objective.

Firewall is a device (hardware and/or software) designed to control the flow of information in and out of computing devices and, using a set of predefined rules, decide whether or not to allow the data to cross the device.

DMZ, an abbreviation of Demilitarised Zone, is an intermediate network that buffers an organisation's internal and presumed secure network from the Internet, presumed insecure.

SIEM, abbreviation of Security Information and Event Management – such systems provide real-time monitoring, correlate events and provide notifications to operational staff. It also provides storage, analysis and reporting of log data to provide information on trends and potential compliance issues.

Appendix 2
A short (and not comprehensive) list of standards and best practices for information security

International Standard ISO/IEC 38500-2008, "Corporate governance of information technology".

International Standard ISO/IEC DIS 27014-2012, "Information technology – Security techniques – Governance of information security".

International Standard ISO 31000-2009: "Risk Management, Principles and Guidelines".

International Standard ISO 31010-2009: "Risk Management, Risk Assessment Techniques".

"Control Objectives for Information Technology" (COBIT), Version 5, 2012, Information Technology Governance Institute.

"COBIT 5 for Information Security", 2012, Information Technology Governance Institute.

"Information Security Guidance for Boards of Directors and Executive Management", 2nd Edition, 2006, Information Technology Governance Institute.

"Information Security Guidance for Information Security Managers, 2008, Information Technology Governance Institute.

The Risk IT Framework and its Practitioner Guide, 2009, Information Systems Audit and Control Association.

The OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) issued by the Software Engineering Institute at Carnegie Mellon University (USA).

"The Standard of Good Practice for Information Security", 2011, Information Security Forum.

"Information Security Handbook: A guide for Managers" (SP800-100), 2007.

The Data Management Body of Knowledge (DMBOK) published in 2009 by the Data Management Association.

International Standard ISO/IEC 20000-2011 "Information Technology Service Management" (parts 1 to 5).

"The Information Technology Infrastructure Library" (ITIL) Version 4, issued in 2011 consists of five volumes (ISO 20000 is fully compatible with the ITIL framework.

British Standard BS 25999 "Business Continuity Management" (parts 1 and 2) issued in 2006 and 2007.

The "Business Continuity Management Body of Knowledge" is available online and is continuously evolving through contributions from practitioners.

International Standard ISO/IEC 27000 series (from 27001 to 27014 at the time of writing) "Information Technology Security Techniques), latest versions published in 2011.

"The Standard of Good Practice for Information Security", 2011, Information Security Forum.

The USA government series SP-800 (over 100 publications).

International Standard ISO/IEC 27007-2011 "Information technology – Security techniques – Guidelines for information security management systems auditing".

International Standard ISO/IEC 27008-2011 "Information technology – Security techniques – Guidelines for auditors on information security management systems controls".

USA publication NIST SP 800 -53: Recommended Security Controls for Federal Information Systems and Organizations.

The Global Technology Audit Guides (GTAG) issued by the Institute of Internal Auditors which includes GTAG 15 "Information Security Governance" and GTAG 11 "Developing the Audit Plan". The whole collection constitutes a valuable source of guidance for both auditors and practitioners.

The Control Objectives for Information Technology (COBIT) issued by the Information Technology Governance Institute (ITGI) and the Information Systems Audit and Control Association (ISACA). Version 5 was issued in April 2012.

ISACA Auditing Guideline G40: Review of Security Management Practices (2002).