The Evolution of Information Security Goals from the 1960s to today

Yulia Cherdantseva[1] · Jeremy Hilton[2]

[1]Cardiff University
y.v.cherdantseva@cs.cardiff.ac.uk

[2]Cranfield University
j.c.hilton@cranfield.ac.uk

OUTLINE

- Introduction
- The Evolution of Security Goals
  1. The Early Years of Computer Security and the Emergence of InfoSec
  2. From the Ware Report to the Common Criteria
  3. The Proliferation of Computers in the Commercial Sector
  4. The CIA-triad
  5. The Growing Pervasiveness of the Internet and the Emergence of Information Assurance
  6. The extension of the CIA-triad
  7. InfoSec as an Integral Part of Corporate Governance
  8. Privacy
- The Evolutionary Circles of Information Security
- Conclusion

TERMINOLOGY

- ***Security goal*** - the *desirable* security-related property of information or *desirable* ability of an information system, where appropriate (e.g. Reliability, Confidentiality, Integrity, Availability and the like)
- ***Security mechanism*** - a process or technique which helps to achieve one or more security goals (e.g. Authorisation, Authentication, Cryptography)

Y. Cherdantseva & J. Hilton, "The Evolution of Information Security Goals from the 1960s to today", Feb 2012.

WHAT IS IT ALL ABOUT?

- An approach to the evolution of InfoSec, with the focus on security goals
- We concentrate on the period of the last several decades when protection of information has become more challenging following an unprecedented advancement of ICT
- We aim to find answers for two crucial questions:

  What does *secure* mean?

  What *security goals* should be pursued?

Y. Cherdantseva & J. Hilton, “The Evolution of Information Security Goals from the 1960s to today”, Feb 2012.

WHY IS IT IMPORTANT?

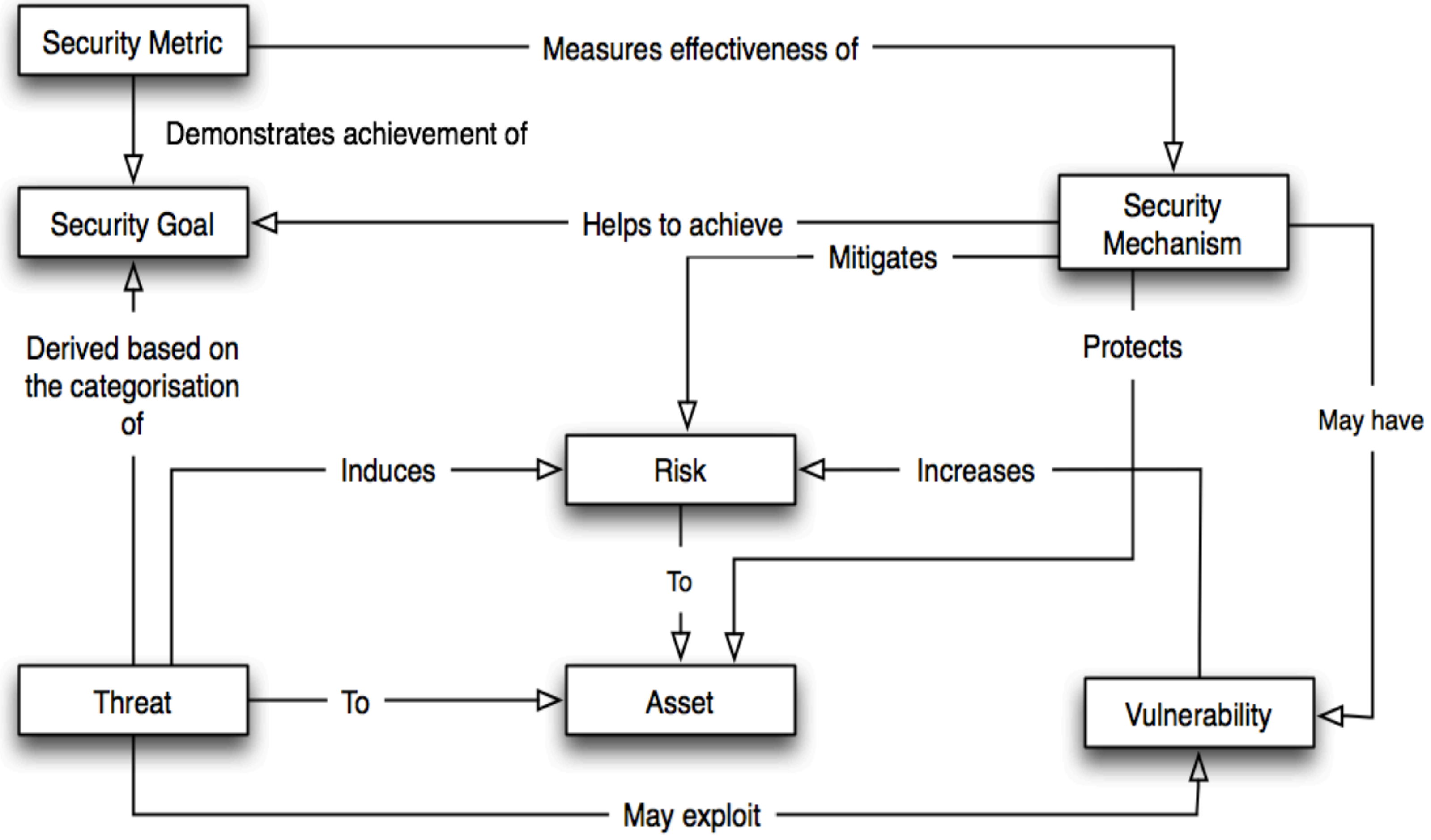
- The examination of the history of InfoSec is important since it enhances the understanding of the current state of the discipline and helps to foresee its future.

- Security goals form an integral part of the overall InfoSec concept.

- Security goals serve as evaluation criteria for information systems and IT security. Hence, a value of the goals analysis is in verifying the adequacy of security evaluation criteria.

Y. Cherdantseva & J. Hilton, "The Evolution of Information Security Goals from the 1960s to today", Feb 2012.

THE ONTOLOGY OF INFOSEC



Y. Cherdantseva & J. Hilton, “The Evolution of Information Security Goals from the 1960s to today”, Feb 2012.

THREAT VS GOAL

- CRAMM (the selection of security countermeasures is based on the threat and vulnerability assessment)
- Microsoft's Security Development Lifecycle (SDL) includes a threat modeling process which is based on STRIDE model

- The CIA-triad
- McCumbers Cube
- Parkerian Hexad
- ISO
- COBIT
- NIST

Y. Cherdantseva & J. Hilton, "The Evolution of Information Security Goals from the 1960s to today", Feb 2012.

ADVANTAGES OF THE GOAL-ORIENTED APPROACH

- It does not require statistics, which is difficult to acquire. On the contrary, for threat-based risk analysis statistics is crucial;
- It is more accessible to management and other non-technical staff, whereas threat analysis requires technical knowledge;
- It captures the essence of the problem and exposes it a high level of abstraction, where as the threat-oriented approach goes into greater detail;
- It guarantees better completeness, while completeness of the threat-based approach depends on the expertise of an analyst;
- It is an inherent human inclination to set goals for activities.

Y. Cherdantseva & J. Hilton, "The Evolution of Information Security Goals from the 1960s to today", Feb 2012.

The Evolution of Security Goals

Y. Cherdantseva & J. Hilton, “The Evolution of Information Security Goals from the 1960s to today”, Feb 2012.

THE EARLY YEARS OF COMPUTER SECURITY

The number of attempts to breach computer security was low due to the several reasons:

- computers were expensive, rare and closely safeguarded,
- there were very few programming experts as the discipline was new and computers were programmed in difficult machine languages.

The main focus of Computer Security (CS), a predecessor of InfoSec, was Reliability of rare and high-priced machines.

Information protection was achieved mainly through the control of physical access to computers.

Y. Cherdantseva & J. Hilton, "The Evolution of Information Security Goals from the 1960s to today", Feb 2012.

THE EARLY YEARS OF COMPUTER SECURITY

- In the 1970s, the first personal computers appeared, but there was no considerable concerns about InfoSec
  1. machines were stand-alone and controlled by a single individual,
  2. the software was unique.

- The threat to information has greatly increased in the late 1970s following the development of cheap and standardised software.

Y. Cherdantseva & J. Hilton, “The Evolution of Information Security Goals from the 1960s to today”, Feb 2012.

THE EMERGENCE OF INFOSEC

- With the hardware and software getting more affordable and effective, the subject of protection has changed from computers processing information to the information itself.
- Consequently, the goals of the information protection discipline have changed: whereas previously Reliability of computers was dominant, at this stage, Confidentiality, Integrity and Availability started to acquire importance.
- The shift in the focus from protection of computers to protection of information (and a subsequent change of goals of the discipline) marked the emergence of InfoSec from CS.

Y. Cherdantseva & J. Hilton, "The Evolution of Information Security Goals from the 1960s to today", Feb 2012.

FROM THE WARE REPORT TO THE COMMON CRITERIA

- The RAND Report R-609, *Security Controls for Computer Systems* ("The Ware Report") 1970
- *Computer Security Technology Planning Study* ("The Anderson Report") 1972
- Both reports are focused on protection of classified information in the military or government environment. Hence, although the reports provide extensive classifications of threats to information, both primarily concentrate on protection of information from external disclosure (**Confidentiality**).

Y. Cherdantseva & J. Hilton, "The Evolution of Information Security Goals from the 1960s to today", Feb 2012.

FROM THE WARE REPORT TO THE COMMON CRITERIA

In 1975, Saltzer and Schroeder stated that at that time security specialists distinguish three categories of threats to information:

- unauthorised information release (Confidentiality);
- unauthorised information modification (Integrity)
- unauthorised denial of use (Availability).

Since then the concept of three major categories of threats and the related security goals have become the underlying philosophy of InfoSec.

Y. Cherdantseva & J. Hilton, “The Evolution of Information Security Goals from the 1960s to today”, Feb 2012.

FROM THE WARE REPORT TO THE COMMON CRITERIA

- The InfoSec research before the early 1980s was sponsored by the military agencies (Confidentiality).
- This research significantly influenced future development of InfoSec:
  - ✓ The Anderson Report, the Ware Report >>
  - ✓ "Criteria and Evaluation" program (NSA) >>
  - ✓ *Trusted Computer System Evaluation Criteria* ("The Orange Book") >>
  - ✓ "Rainbow Series" >>
  - ✓ Common Criteria (ISO)
- The initial defense-focused approach to InfoSec with the emphasis on Confidentiality, affected many security-related documents and widely used standards.

Y. Cherdantseva & J. Hilton, "The Evolution of Information Security Goals from the 1960s to today", Feb 2012.

THE PROLIFERATION OF COMPUTERS IN THE COMMERCIAL SECTOR

- Computers gradually started to proliferate in the commercial sector, bringing with them security concerns.
- Industry's involvement in the InfoSec research, demanded the revision of the existing research findings.
- There are four major differences between the military and commercial sector:
  1. In the defense sector protection of information must be achieved almost at any cost. In the commercial world the cost of information protection should be balanced with the risk to business.
  2. The defense sector expects a well-funded, technically strong enemy. In the commercial environment a threat often comes from an insider or inattentive employee.
  3. The defense environment assumes cleared people working in a physically protected environment under the military discipline. The commercial world rarely operates in a physically protected environment; the staff is not necessarily trusted and acts under the civilian law.
  4. The motivation of the defense sector is based on the law, orders and regulation. The motives of the commercial world are costs and benefits.

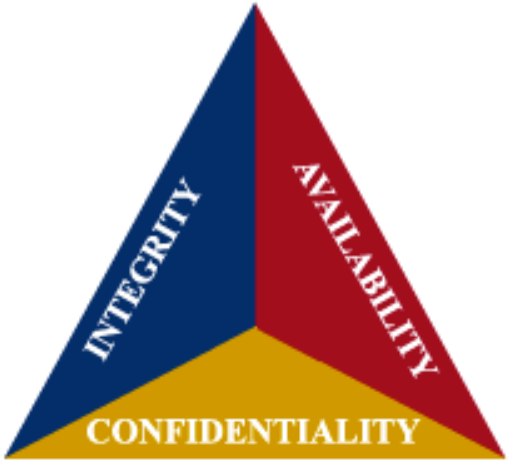
Y. Cherdantseva & J. Hilton, "The Evolution of Information Security Goals from the 1960s to today", Feb 2012.

The Proliferation of Computers in the Commercial Sector

- The recognitions of these differences in the following research lead to the change of priorities among the security goals.
- In 1987, Clark and Wilson depicted this change. Among the security threats they recognised the most dangerous threat for commercial enterprises to be an unauthorised modification. Consequently, the related security goal – Integrity – began to gain a priority.

Y. Cherdantseva & J. Hilton, “The Evolution of Information Security Goals from the 1960s to today”, Feb 2012.

THE CIA-TRIAD



- ✓ 1986-1987
- ✓ Leo, Owens and Tipton
- ✓ Johnson Space Center
- ✓ JSC-NASA Information Security Plan ("The Pink Book") 1989.

- The CIA-triad was not intended to be a precise and comprehensive definition of InfoSec.
- The definition was intended to convey the overarching goals of InfoSec to business and engineering management in a terminology that will be easy to understand.

Y. Cherdantseva & J. Hilton, "The Evolution of Information Security Goals from the 1960s to today", Feb 2012.

THE GROWING PERVASIVENESS OF THE INTERNET

- More essential services began to work online
- Availability started to gain appreciation
- The weighty role here played The Morris Worm (the first denial-of-service attack on the Internet. It was launched in 1988. The Worm caused a devastating effect on the overall perception of security and reliability of the Internet and finally anchored the important place of Availability among the security goals)

Y. Cherdantseva & J. Hilton, “The Evolution of Information Security Goals from the 1960s to today”, Feb 2012.

THE EMERGENCE OF INFORMATION ASSURANCE

- In 1998, Information Assurance (IA) - a concomitant discipline of InfoSec - emerged.
- According to the original definition, IA is concerned with Non-repudiation and Authentication in addition to the CIA-triad.
- IA emerged to address the threats, induced by the growing networks, that were deemed to be out of the InfoSec scope.
- Since IA focuses on security of information systems, rather than on protection of information as such, security goals here describe the desirable properties of information systems, rather than properties of the information. This, possibly, explains the fact that Authentication was included in the list of the IA goals.

Y. Cherdantseva & J. Hilton, "The Evolution of Information Security Goals from the 1960s to today", Feb 2012.

THE EXTENSION OF THE CIA-TRIAD

- In 1998, Parker criticised InfoSec definitions of being limited to the CIA-triad and claims it being dangerously incorrect.
- Parker hexad: **Confidentiality, Integrity, Availability, Possession or Control, Authenticity and Utility**.
  - ✓ **Possession** -"the holding, control, and ability to use information".
  - ✓ **Utility** - "usefulness of information for purpose".
  - ✓ **Authenticity** - "the conformance to reality" and "extrinsic value or meaning of the information with respect to external sources".

Y. Cherdantseva & J. Hilton, "The Evolution of Information Security Goals from the 1960s to today", Feb 2012.

THE EXTENSION OF THE CIA-TRIAD

- Following the evolution of business needs and ICT, the list of security goal has broadened.
- BS7799 Part 1:1995

  InfoSec is associated with the protection of Confidentiality, Integrity and Availability.
- BS ISO/IEC 2001:2005

  InfoSec in addition to the CIA-triad is concerned with Authenticity, Accountability, Non-repudiation and Reliability.

Y. Cherdantseva & J. Hilton, “The Evolution of Information Security Goals from the 1960s to today”, Feb 2012.

THE EVOLUTION OF SECURITY GOALS (1990s-early years of 21 c.)

INFORMATION SECURITY AS AN INTEGRAL PART OF CORPORATE GOVERNANCE

- ✓ the Turnbull Guidance *"Internal Control: Guidance for Directors on the Combined Code"*,
- ✓ the American Institute of Certified Public Accountants (AICIPA) standards,
- ✓ the King report on Corporate Governance,
- ✓ the OECD Principles of Corporate Governance
- ✓ the 8th audit directive of the European Union
- ✓ the Sarbanes-Oxley Act (SOX).

- InfoSec was previously deemed to be low level activities and the responsibility of the technical personnel
- The documents attracted the managers' attention to risk management, the effectiveness of internal controls and to InfoSec in general

Y. Cherdantseva & J. Hilton, "The Evolution of Information Security Goals from the 1960s to today", Feb 2012.

INFORMATION SECURITY AS AN INTEGRAL PART OF CORPORATE GOVERNANCE

- The ultimate goal of Corporate Governance is effective and secure business performance.
- InfoSec no longer puts the main emphasis on Confidentiality.
- Validity (as conformance to reality), Completeness and Accuracy of information become essential. This enriches understanding of such goals as Integrity and Authenticity.
- The business needs give rise to additional security goals: Transparency and Auditability.
- Efficiency and Cost-effectiveness of security measures - became new, additional goals of InfoSec.

Y. Cherdantseva & J. Hilton, “The Evolution of Information Security Goals from the 1960s to today”, Feb 2012.

PRIVACY

- ✓ 1973, *Records, Computers and the Rights of Citizen* brought to life the Code of Fair Information Practice (FIP).
- ✓ 1977, *Personal Privacy in an Information Society*
- ✓ 1980, the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*

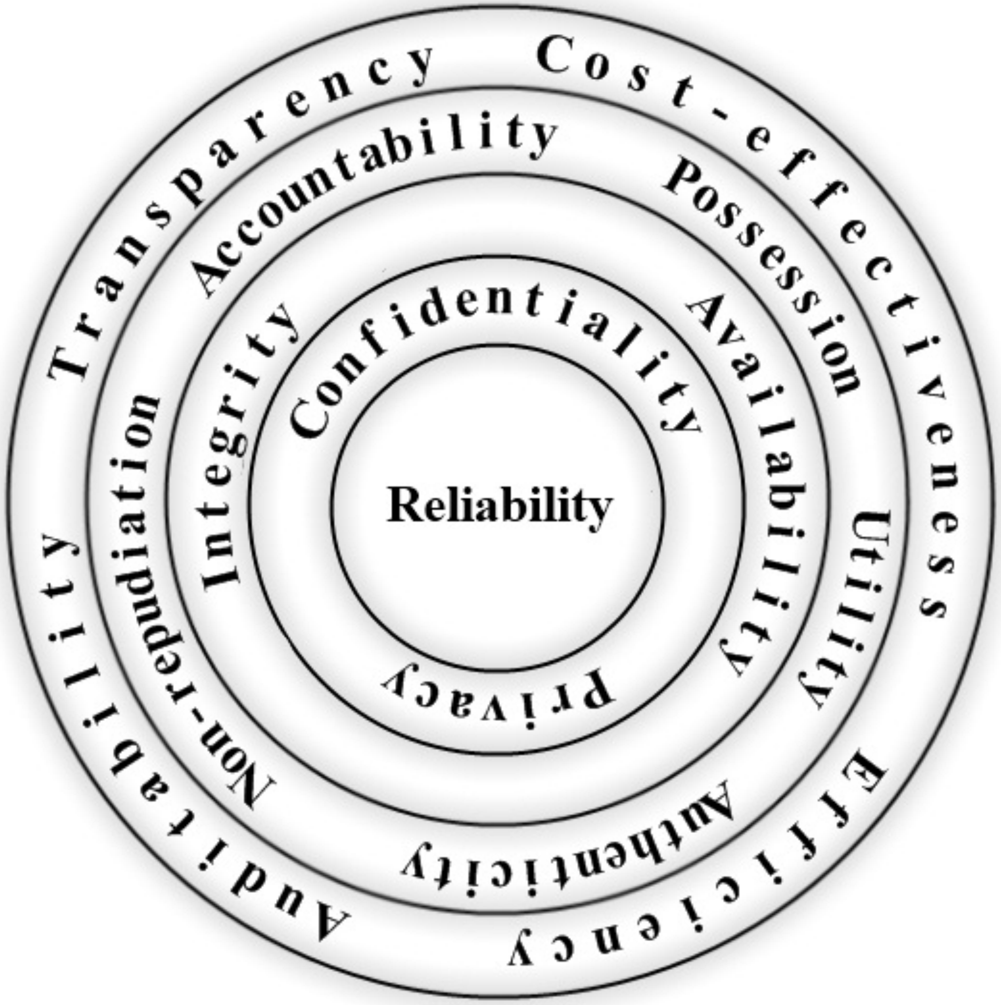
- The weaknesses of the FIP are rooted in allowing many exemptions and in self-regulation.
- Privacy legislation, generally, fail to keep pace with the advances of ICT.
- Many principles are still not consistently enforceable by law in many countries.

The evolutionary circles of Information Security

- A set of relevant security goals changes and grows as a result of the discipline's scope getting broader.
- The evolutionary circles illustrate the growth of InfoSec and the change of security goals.
- Each evolutionary circle includes security goals that were in the realm of the discipline at that particular stage.
- The nested circles visualise that the previously critical goals do not disappear from the InfoSec arena; they stay relevant, but become a part of a greater set of valid security goals.
- The newly emerging goals attract more attention, leaving the old goals in the shadow.

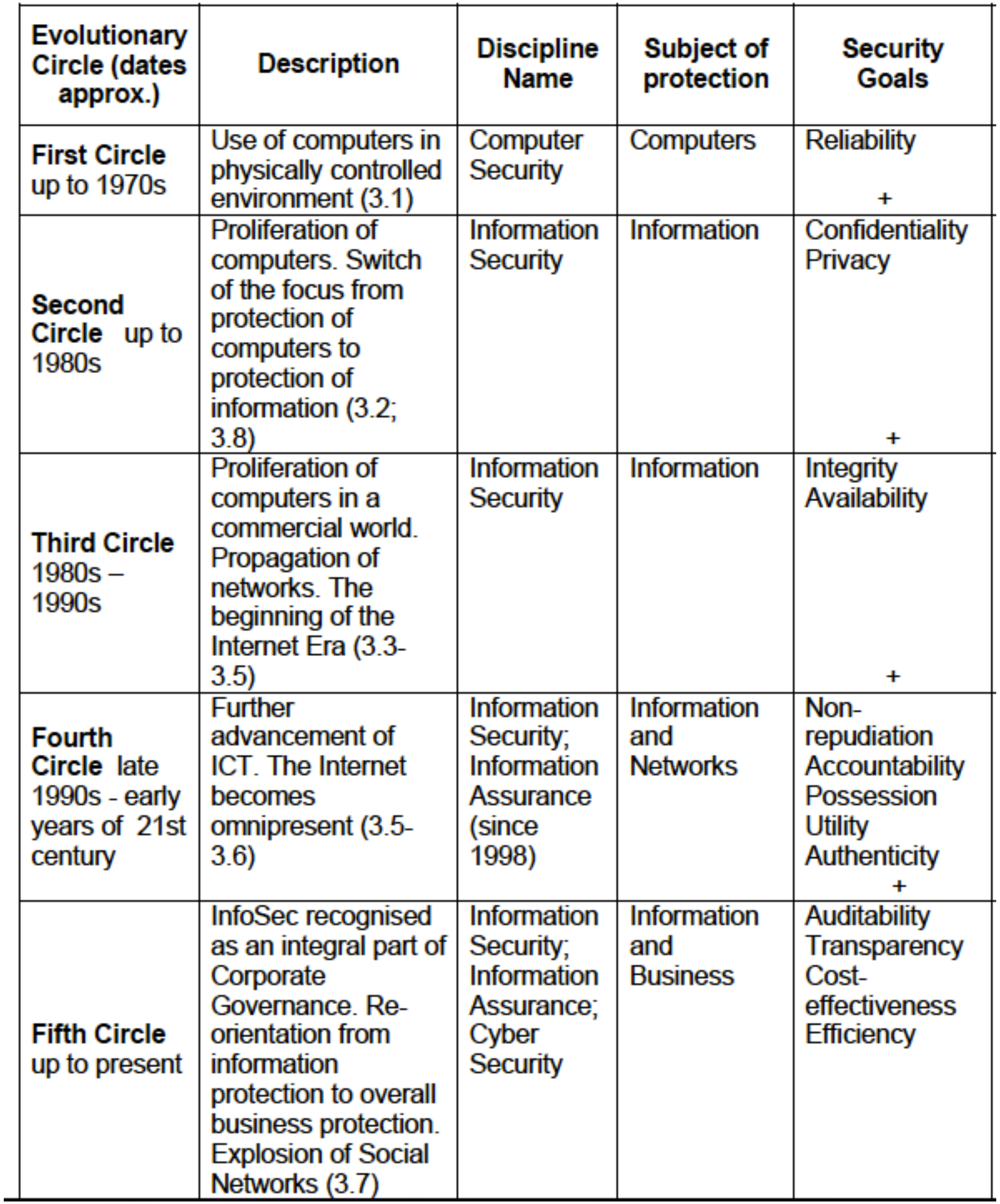
Y. Cherdantseva & J. Hilton, "The Evolution of Information Security Goals from the 1960s to today", Feb 2012.

The evolutionary circles of Information Security



Y. Cherdantseva & J. Hilton, “The Evolution of Information Security Goals from the 1960s to today”, Feb 2012.

The evolutionary circles of Information Security



Evolutionary Circle (dates approx.)	Description	Discipline Name	Subject of protection	Security Goals
First Circle up to 1970s	Use of computers in physically controlled environment (3.1)	Computer Security	Computers	Reliability +
Second Circle up to 1980s	Proliferation of computers. Switch of the focus from protection of computers to protection of information (3.2; 3.8)	Information Security	Information	Confidentiality Privacy +
Third Circle 1980s – 1990s	Proliferation of computers in a commercial world. Propagation of networks. The beginning of the Internet Era (3.3-3.5)	Information Security	Information	Integrity Availability +
Fourth Circle late 1990s - early years of 21st century	Further advancement of ICT. The Internet becomes omnipresent (3.5-3.6)	Information Security; Information Assurance (since 1998)	Information and Networks	Non-repudiation Accountability Possession Utility Authenticity +
Fifth Circle up to present	InfoSec recognised as an integral part of Corporate Governance. Re-orientation from information protection to overall business protection. Explosion of Social Networks (3.7)	Information Security; Information Assurance; Cyber Security	Information and Business	Auditability Transparency Cost-effectiveness Efficiency

Y. Cherdantseva & J. Hilton, “The Evolution of Information Security Goals from the 1960s to today”, Feb 2012.

Conclusion

- The set of security goals is neither fixed, nor given.
- Security goals are changing over time in response to the evolution of society, business needs and ICT.
- An InfoSec professional should be alert to the rapid evolution of a valid collection of security goals and should be ready to conduct, regularly, an insightful analysis of security issues posed by emerging technologies

Y. Cherdantseva & J. Hilton, "The Evolution of Information Security Goals from the 1960s to today", Feb 2012.

CONCLUSION

"What does a *secure* system mean?"

Any list of goals is only complete until
a new threat and
a new corresponding goal
emerge.

Y. Cherdantseva & J. Hilton, "The Evolution of Information Security Goals from the 1960s to today", Feb 2012.