The 5 Waves of Information Security - From Kristian Beckman to the Present

S. H. (basie) Solms

The 5 Waves of Information Security – From Kristian Beckman to the Present

Prof SH (Basie) von Solms

Academy for Information Technology, University of Johannesburg, South Africa
basievs@uj.ac.za

Abstract. This paper gives an overview of the development of Information Security from the early 1980s up to the present time. The paper makes use of two papers by the author, Information Security – the Third Wave (von Solms, 2000) and Information Security – the Fourth Wave (von Solms, 2006), as well as a paper in preparation, Information Security – The Fifth Wave (von Solms, 2010). In the paper in 2000, the First Wave of Information Security was defined as lasting up to the early 1980s. In May 1983 the First International Conference on Information Security (IFIP/Sec 83) took place in Sweden, and was organized by Kristian Beckman. Kristian Beckman was subsequently elected as the first Chairperson of the newly created Technical Committee 11 of IFIP. He died in 1984. Kristian Beckman can therefore be seen to have lived during the First Wave of Information Security, which provides the motivation for the sub title of this paper.

Keywords: Information Security, Kristian Beckman,

1 Introduction

This paper discusses the development of Information Security in terms of 5 Waves.

The First Wave was up to the early 1980s, and is called the Technical Wave. The second Wave was from the early 1980s up to the middle 1990s, and is called the Management Wave. The Third Wave was from the middle 1990s up to about 2005, and is called the Institutional Wave. These 3 Waves are defined and discussed in von Solms (2000).

The Fourth Wave started about 2005 and is called the Information Security Governance Wave. This Wave is discussed in von Solms (2006).

The Fifth Wave, which is called the Cyber Security Wave, started in about 2006, and is discussed in von Solms (2010).

Of course, it must be understood that these 5 Waves are not 'blocks' which started and then ended at a specific point in time – rather they represent new developments which started in a certain period and placed new emphasis on aspects related to Information Security during the last 30 to 40 years, and should therefore be seen as existing in parallel with each other.

This paper will discuss each of these Waves, some in more detail than others, and will then try to draw some conclusions about the future of Information Security.

Paragraphs 2 to 5 will review the first 4 Waves, which will use von Solms (2000 and 2006) as references, with Paragraph 6 briefly evaluating these first 4 Waves, Paragraph 7 will introduce the Fifth Wave, based on von Solms (2010) - a paper in preparation. Paragraph 8 to 10 will provide some discussion about the future, specifically addressing to the concept of professionalism in Information Security, with a short summary in Paragraph 11.

2 The First Wave - Technical

The First Wave of Information Security was basically totally dedicated to the mainframe environment, with dumb terminals and totally centralized processing.

Information Security was limited to simple forms of Identification and Authentication for logging onto the mainframe system, and maybe some crude form of Authorization or Logical Access Control. Most of these functions were handled by the mainframe operating system, which was basically only understood by the technical people, and handled by them. Aspects like policies, procedures awareness etc were not high on the agenda.

As stated above, the realization that the First Wave was not sufficient as far as Information Security is concerned started dawning in the early 1980s.

This realization clearly also dawned on Kristian Beckman, which prompted him to organize the First International Conference on Information Security (IFIP/Sec 83), and to suggest to IFIP (www.ifip.org), then 23 years old, to establish a Technical Committee on Information Security related aspects. As he died in 1984, Kristian Beckman can therefore be seen as living during the First Wave, but with the vision to realize that much more is, and will be needed.

3 The Second Wave – Management

The development of distributed computing, and maybe specifically the personal computer, demanded a lot of other inputs into the Information Security field. The fact that information was not stored on one central well protected computer, but distributed to lots of desk top computers connected by networks, created serious security risks which had to be addressed.

Information Security became a matter which got the attention of Management, and Information Security Managers were appointed. They started creating Information Security Policies and procedures, and organizational structures were created to house Information Security departments. Reporting about the status of Information Security in the company also became a challenge.

These developments of course improved Information Security in general, and emphasized the important aspect that Information Security has a very strong Management Dimension which must be leveraged fully to create a secure environment.

Because of these developments during the Second Wave, companies started investigating aspects related to best practices and standardization in Information Security. Many companies wanted to know what the basic aspects of a good Information Security plan are. Questions asked included:

- How do we compare security wise to our competitors?
- What should be in an Information Security Policy?
- How could they get some form of formal certification for the Information Security status of the company?

Furthermore, the role of the employee as an end user of the system came under the spotlight, and the importance of the Human Dimension was accepted.

This lead to the Third Wave, called the Institutionalization Wave, which became apparent from about the middle 1990s.

4 The Third Wave – Institutionalization

As stated above, the fact that Information Security had a lot more dimensions than just a Technical Dimension, and that Information Security is crucial to the health and strategic future of a company, lead to new efforts to institutionalize Information Security is a company – i.e. to make it part of the culture and way of thinking in a company.

One driver at this point was the idea of international best practices for Information Security, and the arrival of BS 7799 Parts 1 and 2. Part 1 was the first really widely accepted document specifying what aspects related to Information Security should be addressed as a sort of baseline. Part 2 provided the platform to get some international certification against Part 1.

Another driver was the growing emphasis on Information Security Awareness, and the risk that ignorant employees can compromise Information Security measures. Extensive Awareness courses were developed, and employees were drilled to make Information Security part of their, and the company's culture.

During this stage, companies also started to create techniques to measure the status and level of their Information Security compliance, and to report such status to top Management.

During the beginning of the present decade, the importance of good Corporate Governance, and the role that Information Security plays in good Corporate Governance became big news. Furthermore legal and regulatory requirements and the consequences of negligence related to good Information Security, specifically as far as privacy of data and information is concerned, really hit the agendas of Board meetings.

This basically led to the Fourth Wave which can be characterized as Information Security Governance.

5 The Fourth Wave – Information Security Governance

As mentioned, the importance of this Wave became clear during the beginning of the present decade.

Several international best practices for good Corporate Governance appeared, and the role of Information Technology Risk Management and Information Technology Governance were highlighted in many of them. Good Information Technology Governance of course included good Information Security implementations.

Financial information of the company was stored and processed on computers, and if the storage and processing of such information were not properly secured and protected, serious compromises could result. The risk of committing fraud and misusing financial resources by manipulating the company's electronic data stored on its IT systems in an unauthorized way became very clear – and also that top Management is in the last instance accountable.

This growing importance of, and emphasis on Information Security, resulted in the emergence of the concept of Information Security Governance.

The fact that 'Information Security Governance is an integral part of Corporate Governance' became well accepted.

6 Evaluation of Waves 1 to 4

Before we discuss the Fifth Wave, let us briefly reflect on Waves 1 to 4.

Two aspects are important up to this point.

Firstly, it is apparent that all 4 these Waves basically 'point inwards', i.e. they have to do with securing the data and information of the company. The responsibility lies with the company and its employees, and all measures are implemented to this end. The main purpose is to ensure that the confidentiality and integrity of the data and information of the company are maintained at all times – from the company's side.

This resulted in companies rolling out very good security measures, making it very difficult for the criminal elements who wanted access to such data and information, to do so – in many cases a company's IT infrastructure became a well-protected fort.

Secondly, companies rolled out more and more systems based on the Internet and the World Wide Web, making it possible for millions of clients and customers to use such systems – enter the Cyber age!

The direct result of these two aspects was that criminals now moved their attention to the end user. Using the Internet as access medium, with millions of end users with low levels of Information Security awareness and knowledge, the criminal side started having a field day using a wide range of attack mechanisms directed towards the end user – mechanisms mainly based on social engineering.

Their motto became: Do not try to hack into the company's IT systems; it may be very difficult – go for the naïve end user!

This led to the Fifth Wave of Information Security – ensuring Information Security in Cyber space. Let's call that, for lack of a better name, Cyber security.

7 The Fifth Wave – Cyber Security

The Internet is debatably one of the greatest inventions ever developed by mankind, but it has brought with it extremely serious risks. Implementing any Internet-based system means announcing yourself to the rest of the world, thereby providing an opportunity for cyber criminals to attack the system. Cyber criminals are leveraging the growing use of the Internet by companies to deliver services to their clients to commit crime of immense proportions. Malware, phishing, spoofing and other techniques used by such criminals are making the life for any Internet user extremely risky.

The Internet has handed the criminal side an extremely useful way of committing their crimes, and to us as Information Security specialists our greatest challenge – to ensure that such crimes are prevented from happening.

Let us briefly review some recent cyber crime statistics.

7.1 The Sophos Security Threat Report – 2009 (Sophos, 2009)

23 500 infected websites are discovered every day. That's one every 3.6 seconds – four times worse than the same period in 2008

7.2 The CISCO White Paper (CISCO, 2009)

The White paper states that

'Internet users are under attack. Organized criminals methodically and invisibly exploit vulnerabilities in websites and browsers and infect computers, stealing valuable information (login credentials, credit card numbers and intellectual property) and turning both corporate and consumer networks into unwilling participants in propagating spam and malware;

7.3 The UK Cybercrime Report 2009 (UK Cybercrime, 2009)

The report indicate that during 2008, 'cyber criminals committed over 3.6 million criminal acts online (that one every 10 seconds)'.

7.4 The Washington Post (Washington Post, 2009)

'Law enforcement agencies worldwide are losing the battle against cyber crime'.

7.5 'The Internet has become a fundamental business tool, yet browsing the Web has never been more dangerous' (Symantec, 2010)

Surely the Fifth Wave of Information Security is challenging us to provide efficient cyber security.
How should we as Information Security specialists treat this Fifth Wave?
This author claims that

- Some Internet-based systems are Information Security wise 'so close to the edge' that they should rather not be developed
- We have reached the stage where it is impossible to properly secure and protect some Internet-based systems
- Information Security specialists in most cases are not really professionals

This Wave challenges us as Information Security specialists to reconsider our role, and to ensure that we act as Information Security Professionals and not as Information Security Practitioners. This means that we should be more vocal in expressing our concerns about the security of many Internet-based systems.

8 8. Information Security Professionals (ACISP, 2009)

Are we really professionals, as the term is understood in other circles like medicine, engineering etc? Do we belong to a professional body which has a defined Body of Knowledge, an Ethics Code or a Disciplinary Code?

Can we be held accountable for the advice we give about Information Security aspects?

Do we have a 'true' Information Security Profession which is acknowledged internationally? The answer must be 'NO" at this stage!

There are some bodies which do 'certify' people as Information Security Professionals, and that is already a step in the right direction. However, it does not go far enough, and do not create 'true' Information Security Professionals or a 'true' Information Security Profession.

Other initiatives are developing to create a 'true' Information Technology Profession, but that is wider than Information Security. No comprehensive project is presently active to create a true Information Security Professional.

Lacking such formal status, we as Information Security practitioners (not yet Information Security professionals) should act extremely responsible in our advice roles as demanded by the Fifth Wave.

We can find a good example in the way David Parnas acted in the early 1980s.

9 The Strategic Defense Initiative (SDI) and David Parnas (ACISP, 2009)

'The Strategic Defense Initiative (SDI), commonly called Star Wars after the popular science fiction series, was a system proposed by U.S. President Ronald Reagan on March 23, 1983 to use space-based systems to protect the United States from attack by strategic nuclear missiles. It was never implemented and research in the field tailed off after the end of the Cold War.' (Wikipedia)

Prof David Parnas, one of the pioneers in the development of Computer Science and Software Engineering, was at that time a consultant to the Office of Naval

Research in Washington, and was one of nine scientists asked by the Strategic Defense Initiative Office to serve on the "panel on computing in support of battle management".

Parnas resigned from this advisory panel on antimissile defense, asserting that it will never be possible to program a vast complex of battle management computers reliably or to assume they will work when confronted with a salvo of nuclear missiles.

In his letter of resignation he said that it would never be possible to test realistically the large array of computers that would link and control a system of sensors, antimissile weapons, guidance and aiming devices, and battle management stations. Nor, he protested, would it be possible to follow orthodox computer program-writing practices in which errors and "bugs" are detected and eliminated in prolonged everyday use.

"I believe," Professor Parnas said, "that it is our duty, as scientists and engineers, to reply that we have no technological magic that will accomplish that. The President and the public should know that." (The Risk Digest, 1985).

Although Parnas's stand was related to nuclear warfare, which may not be so relevant today anymore, the morale of this story is still the same. Parnas highlighted the reliability issues of the use of computers, because they were important issues concerning the man in the street. It is important to note that Parnas did not say that all computer systems are unreliable – he just said that this specific initiative was dangerous.

The reader may now say that the SDI issues were related to the reliability of nuclear computer systems, and not to the Information Security of commercial systems.

My answer to such a reaction is: 'Is the Information Security of general IT systems today, even though they are now much more business focused, less important, or less complicated?'

Just have a look at paragraph 7 above, or ask a person who lost all his/her money through fraud committed using IT systems whether he sees it as a serious issue or not?

Following Parnas's quote above, I want to state:

'it is our duty, as Information Security specialists (professionals??) to make it heard from all platforms that IT systems are becoming so complex that we doubt whether they can still be properly protected in all cases. The public should know that'

Maybe TC 11 should take a stance on this issue and make a public statement.

10 The Challenge of the Fifth Wave of Information Security

The challenge of the Fifth Wave of Information Security to all of us as Information Security Practitioners/Professionals is to act professionally at all times, meaning that we should not be afraid to warn against the insecurity of many Internet-based systems – that's the challenge of the Fifth Wave of Information Security.

11 Summary

In this paper we reviewed the 5 Waves of Information Security and highlighted the fact that the Fifth Wave is the one which will really challenge Information Security specialist to start acting as Information Security Professionals.

References

1. ACISP 2009, Proceedings of ACISP 2009, Brisbane, Australia, July 2009
2. CISCO, 2009, A Comprehensive Proactive Approach to Web based Threats, www.ironport.com/pdf/ironport_web_reputation_whitepaper.pdf, Accessed May 2010
3. Sophos, 2009, The Sophos Security Threat Report – 2009, www.sophos.com/sophos/.../sophos-security-threat-report-jan-2009-na.pdf, Accessed May 2010
4. Symantec, 2010, The Wild, Wild West Web, Symantec, 2010, http://www.computerworld.com/pdfs/Messagelabs_Wild_Wild_Web.pdf, Accessed June 2010
5. The Risk Digest, Vol 1, Nr 1, 1985 http://catless.ncl.ac.uk/Risks/1.01.html, accessed April 2009
6. UK Cybercrime, 2009, The UK Cybercrime Report 2009, https://www.garlik.com/cybercrime_report.php, Accessed March 2010
7. von Solms, B, 2000, 'Information Security – The Third Wave?', Computers and Security, 9, 2000, pp 615-620
8. von Solms, B, 2006, 'Information Security – The Fourth Wave', Computers and Security, 25, 2006, pp 165 -168

9. von Solms, B, 2010, 'Information Security – The Fifth Wave', 2010, In preparation – to be submitted to Computers and Security
10. Washington Post, 2008, Cybercrime is winning the battle over Cyberlaw, http://voices.washingtonpost.com/securityfix/2008/12/report_cybercrime_is_winning_t.html, accessed June 2010
11. Wikipedia, http://en.wikipedia.org/wiki/Strategic_Defense_Initiative, accessed April 2009