Background to the Development of a Curriculum for the History of "Cyber" and "Communications" Security

William Caelli, Vicky Liu, Dennis Longley

Background to the Development of a Curriculum for the History of "Cyber" and "Communications" Security.

William Caelli[1], Vicky Liu[1] and Dennis Longley[2]

[1] Science and Engineering Faculty, Queensland University of Technology, 2 George Street, Brisbane, Qld. Australia
w.caelli@iisec.com.au, v.liu@qut.edu.au
[2] International Information Security Consultants Pty Ltd, 21 Castle Hill Drive South, Gaven, Qld. Australia..
d.longley@iisec.com.au

Abstract. For any discipline to be regarded as a professional undertaking by which its members may be treated as true "professionals" in a specific area, practitioners must clearly understand that discipline's history as well as the place and significance of that history in current practice as well as its relevance to available technologies and artefacts at the time. This is common for many professional disciplines such as medicine, pharmacy, engineering, law and so on but not yet, this paper submits, in information technology. Based on twenty five elapsed years of experience in developing and delivering cybersecurity courses at undergraduate and postgraduate levels, this paper proposes a rationale and set of differing perspectives for the planning and development of curricula relevant to the delivery of appropriate courses in the history of cybersecurity or information assurance to information and communications technology (ICT) students and thus to potential information technology professionals.

Keywords: information assurance education, cybersecurity education, data network security, Internet security, history of computing, history of communications technology, information security, convergence

1 Introduction

Why teach the history of cybersecurity and/or information assurance? The answer is that at least three distinct themes can be determined in relation to the position of cybersecurity/information assurance history in the creation, development and presentation of courses of study in the area. These are:
1. any profession that claims to be so, acknowledges and builds upon its history;
2. the profession of cyber and network security or information assurance should be no different in this way from any other profession such as medicine, law, science, military affairs and others and should build upon general education in the ICT area for both specialist and general professional activity in the discipline, and

3. the challenge is to make such history relevant to students in the age of total convergence in the information technology area and to relate it to current practice, products and systems.

The environment in which an educated cybersecurity professional will practice has been envisaged by Al Gore, former Vice-President of the USA in the following way in his book *"The Future"* [1]:

"The emergence of a planet-wide electronic communications grid connecting the thoughts and feelings of billions of people and linking them to rapidly expanding volumes of data, to a fast growing web of sensors being embedded ubiquitously throughout the world, and to increasingly intelligent devices, robots, and thinking machines, the smartest of which already exceed the capabilities of humans in performing a growing list of discrete mental tasks and may soon surpass us in manifestations of intelligence we have always assumed would remain the unique province of our species; "

Given this scenario, vaguely reminiscent of the envisaged "*Noosphere"* of Vernasky and Chardin [2] and even the planetary intelligent machine of the *"Krell"* in the 1952 movie, *"The Forbidden Planet"*[3], loosely based on a Shakespearean play, the security and protection of such an information environment takes on new meaning and urgency.

In summary, for any discipline to be regarded as a "professional" undertaking, and whose members may then be accepted and treated by society at large as true "professionals" in that specific area, the discipline must ensure that its practitioners clearly understand that discipline's history as well as the place and significance of that history in current practice. This includes a clear understanding of the *"what/how/why"* of currently available technologies, including professional practice procedures and the like, as well as of ICT artefacts, including base products, integrated systems, services, etc.. This commonly forms an educational base for many professional disciplines such as medicine, pharmacy, engineering, law and so on but not yet, this paper submits, for information technology although references have been made to such histories on some curricula proposals and final versions as discussed later. This paper discusses such history against the consideration of the need for education and training of specific cybersecurity/information assurance professionals. The specific case of education and training in military level cyber-operations is not included in this discussion but is worthy of further analysis. It also has resonance with the more general requirements for cybersecurity awareness in any ICT education program.

Based on twenty five elapsed years of experience in developing and delivering cybersecurity courses at undergraduate and postgraduate levels, this paper proposes a rationale and set of differing perspectives for the development of curricula relevant to the delivery of an appropriate course in cybersecurity history to information and communications technology (ICT) students and thus potential information technology professionals. It does not propose specific curricula in a normal sense, as a set of topics, learning outcomes and the like but rather discusses the bases on which such selections could be made. It proposes particular emphasis on explanation of historical matters as these relate to information technology from differing perspectives which must be understood and catered for by the ICT professional in practice, e.g. interactions with users, managers and other ICT professionals. Particular emphasis is

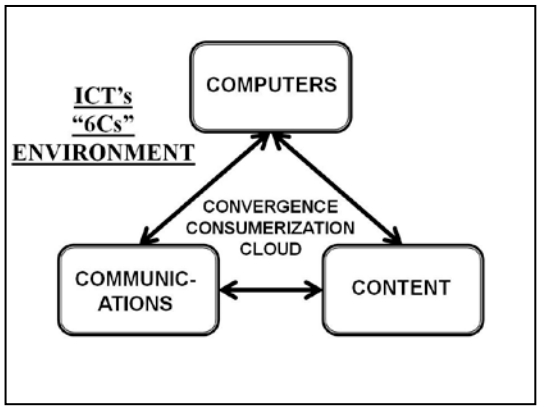

Figure 1: 6C Environment for ICT

placed on the role of the ICT "professional" through education at the university undergraduate level in general as well as via specialised postgraduate cybersecurity program. It proposes that the basis for this curriculum could be set out on the grounds of perception of four distinct generations of information technology professionals within the information technology and data communications network environments in which they worked along with the growing perception of the related science and technology. One aim is to be able to invigorate students in a way that enables them to be able to understand and appreciate the background to any current cybersecurity product, system or service offering from, or claim made by, the ICT industry in general and the specific cybersecurity industry more particularly. The aim is to cover such developments over the last 50 to 60 years in both technological and societal contexts, winding up in an age of total convergence of computers, communications and content (3C) and to thus provide students with an engaging insight into "how we got here" and "why" products, systems and services are what they are and/or what they should be. A particular emphasis is placed on relating this history to the requirements of protection in a globally connected information services environment based around associated data networks and the environments in which new graduates will be employed.

Simply put, the current information environment may be considered the result of convergence of computers, communications and content, commonly referred to here as 3C. Further, 3C has to be considered in the context of a further set of three factors. These include the convergence just mentioned, consumerisation of the ICT products, systems and services offered by the industry itself and finally the result of "cloud" computing service offerings on an international scale that brings a global information environment service into being, together nominated in Figure 1 as the "6C" situation..

2 Roles and Functions of the ICT and Cybersecurity Professional.

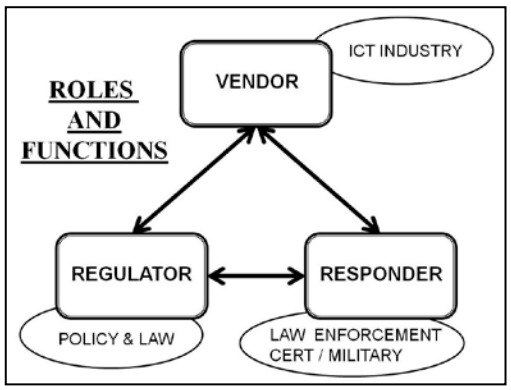

Figure 2 : Roles and Functions

Depending upon where an ICT or cybersecurity professional finds their professional practice employed, their responsibility, and thus need to understand the historical background

to the discipline, may be tailored as needed. As illustrated in Figure 2, roles played and functions undertaken may vary between activities:
* within a traditional ICT vendor, under the usually accepted meaning of the term "ICT industry", as distinct from users or consumers of its products, systems or services but including development of applications for such technologies and artefacts for sale or deployment;
* related to the role of an appropriate regulator responsible for associated policy, law and regulation in the cybersecurity realm; and
* associated with a responder to attacks on or malfunction of information systems including law enforcement and military entities, internal or external response teams, etc.

3 Structures and People.

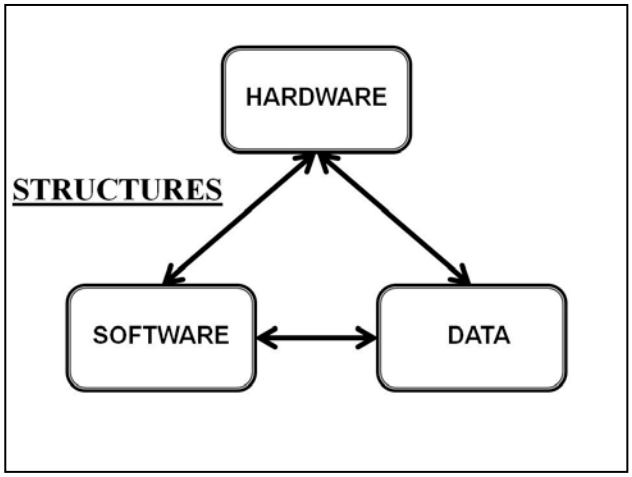

Figure 4 : Structures relevant to Cybersecurity

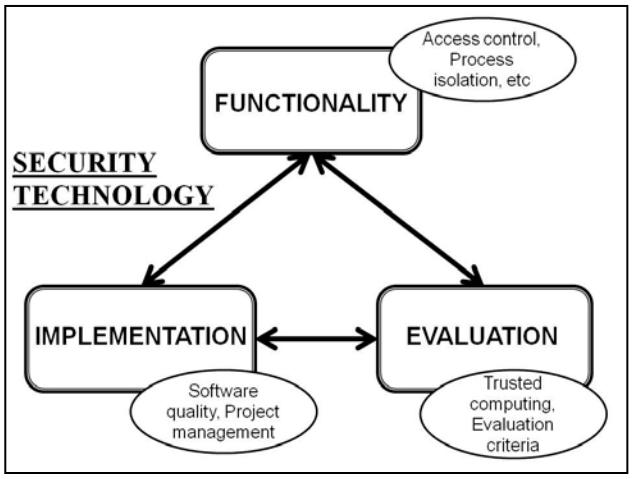

Figure 3 : Security Technology

The existence of underlying security technologies and systems in any information system can be seen as being related to three distinct aspects, viz. hardware, software and data as in Figure 3. In turn, the historical context of the development of associated security technologies in each of these areas sets the scene for today's product, systems and services offerings. For example, the computer and data network "add-on" security industry is now a very large global activity that, it could be argued, owes its very existence to the failure of the normal ICT industry to provide adequate, proven and reliable security features within the base products it offers. Thus, it is necessary to understand

the historical context to the three aspects, again, of any information security product or system. Its functionality specification, its reliable and verifiable implementation in a secure manner itself and, finally, its independent evaluation must be determined by the ICT professional as being fit for the purpose claimed, as illustrated in Figure 4.

4 Policy, Laws and Regulations.

The cybersecurity professional will be involved in either development of public policy and law/regulations relevant to information systems or responsible for the interpretation and implementation of relevant technologies, products, systems, services, policies and procedures for an owner/manager of that information system or even a combination of both of these. At the extreme end of the ”spectrum”, the ICT cybersecurity professional may be regarded as a member of the military, involved in cyber operations in response to attack or a member of law enforcement / response teams concerned with investigation of such attacks. In this sense the cybersecurity professional may take on a role of user, manager or professional in the ICT area or be responsible for liaison with people designated in those functions, as illustrated in Figure 5. The question is one of creating appropriate educational curricula to meet these varying situations and requirements. Examples assist in clarifying these concepts. The cybersecurity professional may be responsible for the creation and dissemination of user procedures for use of information system resources in a company, including, for example development and propagation of a bring-your-own-device (BYOD) policy. At the management level, the cybersecurity professional should normally be involved, but often is not, in the requirements definition and procurement activities related to information systems creation and deployment. In this case, for example, some form of labelled “mandatory access control (MAC)” functionality may be favoured over “discretionary access control (DAC)” but this must be specified at procurement time.

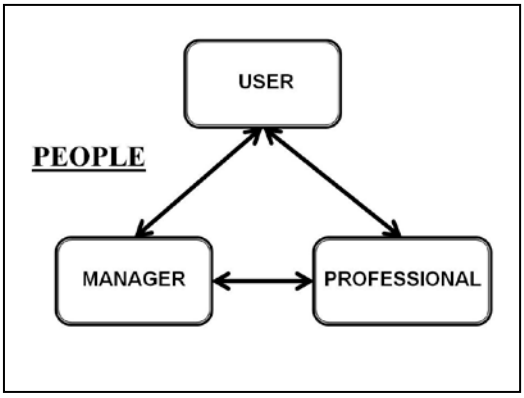

Figure 5 : People / roles and functions.

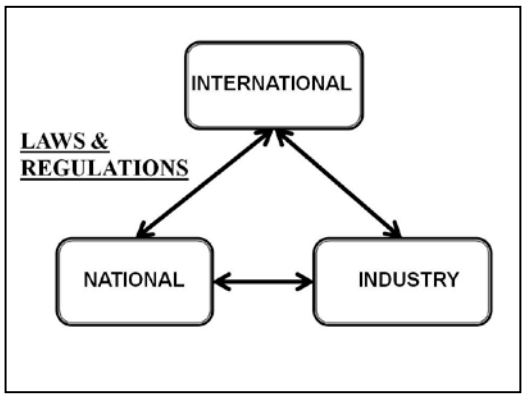

Figure 6 : Legal and Regulatory Regimes

The cybersecurity professional must in turn become familiar with the relevant legal and regulatory regimes appropriate to the enterprise involved, including consideration of these parameters at the international, national and industry levels, as in figure 6.

Examples here may range for export restrictions on advanced cryptographic systems under the *"Wassenaar Arrangement"* [4] to industry specific regulations, such as the USA's HIPAA requirements for the healthcare industry at a national level and then to PCI-DSS contractual obligations in the payment card area.

5. Real Curricula and Industry Training.

At present it appears that full elucidation of the history of information assurance, information security or cybersecurity, under whichever term it may be defined, and the significance of that history in explaining the "why" of current information assurance schemes is severely limited if not totally lacking. For example, the following topics may illustrate the problem:

- *"C2 by '92"* [5] and the failure of mandatory regulations in information assurance in the USA for government/defence procurement;
- the Microsoft *"Palladium / NGSCB"* [6] project for the "hardening" of the Windows based PC in the early 2000s;
- IS 7498-2 [7] and the security architecture for the open systems interconnection (OSI) model and structures for computer connectivity on a global scale;
- the *"Rainbow Series"* of specifications for "trusted computing" from the USA's Department of Defense, particularly the preface to the 1983 *"Orange Book"* or *"TCSEC / Trusted Computer Systems Evaluation Criteria"* explaining the rationale for the publication[2];
- the MULTICS memory segmentation and capability architecture and associated "ring" protection scheme, later embedded into the Intel iAPX-286 and later microprocessors, and so on.
- market failure of "B2" / mandatory access control based, or similarly oriented, operating systems such as Digital Equipment Corporation's (DEC) SEVMS, Gemini Inc. GEMSOS, Secure XENIX, USA's National Security Agency's (NSA) SELinux and SE Android, etc.
- development of the *"Wassenaar Arrangement"* covering export of "dual-use" technologies and artefacts including cryptographic systems and advanced secure computer systems as well as reverse engineering technologies;
- lack of incorporation or acceptance of appropriate and defined security structures into the overall Internet TCP/IP and DNS structures; and so on.

[2] "The criteria were developed with three objectives in mind: (a) to provide users with a yardstick with which to assess the degree of trust that can be placed in computer systems for the secure processing of classified or other sensitive information; (b) to provide guidance to manufacturers as to what to build into their new, widely-available trusted commercial products in order to satisfy trust requirements for sensitive applications; and (c) to provide a basis for specifying security requirements in acquisition specifications.

Some curricula already exist in the information assurance area and even, by implication, in the cybersecurity/cyber operations arena. Examples of these follow.

a. IEEE/ACM

The November 2012 *"Ironman"* version [8] of the IEEE/ACM's body of knowledge (BOK) definition in the area of "information assurance and security" has been published as document CS2013 as part of the overall computer science curriculum. It acknowledges that the situation in this area is "unique" in that relevant matter overlap with all the other areas defined in the computer science curriculum. It states as follows:

"In CS2013, the Information Assurance and Security KA is added to the Body of Knowledge in recognition of the world's reliance on information technology and its critical role in computer science education. Information assurance and security as a domain is the set of controls and processes both technical and policy intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, and confidentiality and providing for non-repudiation. The concept of assurance also carries an attestation that current and past processes and data are valid. Both assurance and security concepts are needed to ensure a complete perspective. Information assurance and security education, then, includes all efforts to prepare a workforce with the needed knowledge, skills, and abilities to protect our information systems and attest to the assurance of the past and current state of processes and data."

However, any historical perspective in this area is separated into an overall "history of computing" section in the BOK. However, the complexity related to inclusion of information assurance curricula into IT programs aimed at the development of the normal IT professional has been a topic of discussion for many years and was clearly alluded to in the earlier ACM IT curriculum guidelines of 2008 [9].

b. USA – Committee on National Security Systems

Documents labelled broadly as *"4011"* to *"4016"* set out "training" requirements for various positions in relation to information assurance functions within the USA's Federal Government, Department of Defense and allied organisations [10]. The history of information security gets mentioned but does not receive any detailed analysis of its place in the educational program.

c. International Information Systems Security Certifications Consortium (ISC^2) – CISSP[3]

This organisation, established in 1989, has developed a certification program for information security professionals given the "*Certified Information Systems Security Professional (CISSP")* designation. It has associated with it a *"Common Body of Knowledge (CBK)"*. The process of personal accreditation under the scheme involves study and examination coupled with designated years of experience for various levels of certification, now expanded beyond the original CISSP. The CBK is described by ISC^2 as follows:

[3] One of the authors, Caelli, is a Fellow of ISC^2.

"The (ISC)² CBK is a taxonomy - a collection of topics relevant to information security professionals around the world. The (ISC)² CBK establishes a common framework of information security terms and principles which allows information security professionals worldwide to discuss, debate, and resolve matters pertaining to the profession with a common understanding."
It sets out a number of domains relevant to the security professional but does not emphasize the historical background to the domains of interest that are set out.

d. Universities and Colleges.
Many universities and colleges in the USA participate in that country's *"National Centers of Academic Excellence (CAE)"* program of its National Security Agency and Department of Homeland Security [11]. These educational institutions, however, adhere to the defined CNS and related curricula. In the separate NSA sponsored area of "cyber operations" education a separate curriculum is published with particular emphasis on the data networking arena. Many also participate in the activities of the "*Colloquium for Information Systems Security Education (CISSE*)[4]", a not for profit society based in Maryland, USA.

e. Other Organisations

i) ISACA[5]
This organisation, formerly the *Information Systems Audit and Control Association*, now just uses its acronym as its name. It also offers a range of industry certifications knows as CISA/CISM/CGEIT/CRISC depending upon an individual's role and certification requirements. In an established manner ISACA publishes its knowledge requirements list as the *"2013 Candidate's Guide to the CISM ® Exam and Certification"*. Once again, while acknowledged, the historical context to the various topics outlined is not given any detailed reasoning or background. Concentration is largely, as may be expected, on the "what" and "how" of the topics.

ii) SANS Institute, EC-Council, CREST (UK) and others.
Other industry level organisations also exist to provide information assurance education and training. Once again, however, the concentration is on the "what and how" aspects of cybersecurity with some emphasis on sub-sets of the overall information assurance area, e.g. CREST (UK) which describes itself as follows:
" The Council for Registered Ethical Security Testers. CREST exists to serve the needs of a global information security marketplace that increasingly requires the services of a regulated and professional security testing capability."

[4] One of the authors, Caelli, is a member of the Board of CISSE.
[5] One of the authors, Caelli, is an Honorary CISM of ISACA.

6 Conclusions.

A trained cybersecurity technician should be able to readily answer questions related to the "what and how" of any relevant information security matter. However, a cybersecurity professional should be readily able to answer the *"Why is it so?"* question, the catch-phase of the late Professor Julius Sumner Miller, a prominent physics educator and TV presenter [12]. While numerous industry based education and training groups exist and offer various levels of certification, many of which are accepted by both the private sector and government organisations, including defence related entities, curricula do not emphasize historical background to the topics outlined and thus the "why" of many aspects of information assurance / cybersecurity.

References

1. Gore, Al : The Future: Six Drivers of Global Change, Random House; 2013.
2. *"Noosphere"*, http://en.wikipedia.org/wiki/Noosphere
3. *"The Forbidden Planet"*, http://en.wikipedia.org/wiki/Forbidden_Planet
4. *"The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies"*, http://www.wassenaar.org/
5. *"Computers at Risk: Safe Computing in the Information Age"*, National Academies Press, 1990.
6. Levy, S.: *"The Big Secret: An exclusive first look at Microsoft's ambitious plan to remake the personal computer to ensure security, privacy and intellectual property rights. Will you buy it?"*, Newsweek, July 1, 2002
7. ISO 7498-2:1989 : Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture, http://www.iso.org
8. Computer Science Curricula 2013, Ironman Draft (Version 1.0) February 2013; http://ai.stanford.edu/users/sahami/CS2013/ironman-draft/cs2013-ironman-v1.0.pdf
9. Lunt, B. et al: *"Information Technology 2008, Curriculum Guidelines for Undergraduate Degree Programs in Information Technology"*, ACM/IEEE 2008.
10. Committee for National Security Systems, http://www.cnss.gov
11. National Centers of Academic Excellence, http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml
12. Wikipedia entry: http://en.wikipedia.org/wiki/Julius_Sumner_Miller