Information Assurance Programs at Tertiary Level

Henry B. Wolfe
University of Otago, Dunedin, New Zealand

hwolfe@commerce.otago.ac.nz

Abstract

This paper highlights the rationale for all IT degrees being focused on Information Assurance holistically throughout the entire degree. It takes a look at the failure of industry to produce an operating system that provides user control of system activities and primarily serves the user rather than other special interest groups (Microsoft, Digital Rights Management, other applications vendors, etc.)

Keywords: cryptography, forensics, information assurance, education.

Introduction

Information Assurance (IA) is the current euphemism for computer security. No matter what it is called, the importance and relevance of this function increases from day to day.

In the 1950's computers had not yet emerged from the scientific community and found their way into business use. In those days, information was processed using punched cards as the data storage medium. Each function (i.e. sequence check, calculate, copy, print reports, etc.) was performed on a single machine and each of these was controlled by a plugboard and had to be programmed (specific plugboard setups) for each operation. It was a good place to learn and understand how information was created, verified, processed, stored, and protected. Computing in the business sense took hold in the early 1960's and has grown into what we know today.

In the early years, we didn't have attacks on our IT functions. There was no vector other than a physical attack. Protection of these functions and equipment was minimal (physical barriers to access for the most part) and usually the place in budget terms where cuts could be made without jeopardizing corporate goals. Security was considered an overhead line item.

In today's world, Information Assurance can no longer be considered "overhead". It is a primary requirement for all organizations (in some jurisdictions its protection is enshrined in legislation). It also no longer encompasses only the computer function and physical facility.

Various anecdotal estimates boil down to the notion that if an organization were to lose its IT capacity for more than three days, it would most likely cease to exist.

Therefore, justification for Information Assurance is really no longer necessary. It now becomes an issue of what our statutory responsibilities are and how IA measures adopted (or not adopted) im-

pact our liability or risk. That risk can come from law enforcement or in the form of stockholder proceedings brought against the company and its directors - both jointly and severally. These now are perceived as “real” risks.

It serves no purpose to run through a list of potential risks to the IT function. Any such list would be incomplete since new attack strategies and techniques are being developed continuously. Suffice it to say that there are many serious risks that each organization (and individual) must protect themselves from.

IA as mentioned before is holistic and encompasses all aspects of IT including but not limited to policy, backup strategies, disaster recovery/continuity planning, firewalls, intruder detection, intruder protection, anti-malware protection, cryptography (for protecting the privacy and integrity of data in transit and data at rest), electronic forensics, etc.

In order to be in a position to properly and completely protect the IT function, it is necessary to understand these and many other topics. No single measure makes the infrastructure safe. Each risk and corresponding protective measure must be addressed and considered as it applies to the specific organization. Ignoring any of the potential risks and their respective protective measures may make it possible for the IT function to be attacked successfully.

This really boils down to the fact or notion that all IT professionals need to be indoctrinated and educated in the discipline of Information Assurance. Currently, most universities do not have an IA degree program nor do they spend much time, within the terms of their IT degrees, on all inclusive security and defensive techniques and tactics. The time for that to change is now. The world runs on systems controlled by IT. The adequate protection of this vital function cannot be ignored. IT degrees that do not have a mandatory component of information assurance and networking throughout are obsolete.

Information Assurance Education

If one were to differentiate between computer security and information assurance you would have to consider IA as the protection of the entire IT function rather that just focusing on computer security (although computing tends to be central to the IA function). This includes user training, control and audit procedures, electronic forensics, and physical plant among other elements.

User training is vital to IA . Half of the “Attacks or Misuse Detected in the Last 12 Months” are caused by insiders (The annual *CSI Survey 2007: The 12th Annual Computer Crime and Security Survey* states that insider abuse of network access is the most prevalent problem. (59%) pp12-13. Obtain a copy from http://www.gocsi.com). Internal controls and audit are also vital. The problem cannot be eliminated, but it may be reduced substantially by using and improving these measures.

In order to defend an organization’s IT infrastructure, those responsible for that must be thoroughly trained in IA techniques and tactics. Within the set of techniques currently used in IA are many disciplines. Each is comprehensive enough for whole careers to be established in the discipline. For example, cryptography or forensics are separate specialties that provide an entire career path. Yet these topics must be included in IA training. Defending a network against the many external risks is another such example. IA training needs to indoctrinate the student with more than just a cursory awareness of the techniques. Each of the many parts that make up the whole must be clearly defined and demonstrated. The individual roles in and importance to the holistic picture of IA needs to be incorporated into this training.

Some academics, in my humble opinion, seem to have a disdain for the idea of "training". If it is not theoretical, then it should be taught in a vocational institution rather than a university. Whether we call it training, indoctrination, exploring theory and practice is not really germane to the issue. What is important is that all IA techniques and measures are fully identified, explained, demonstrated (where possible), relevant exercises given, and yes, the theory behind each should be a part of the foundation introduction for each element.

The next objection by some academics is that practical topics do not produce relevant research and/or publications (**See:** *Appendix A for specific criteria*). The field of Information Assurance provides a rich source for many and varied research projects all of which can produce important and relevant publications. For example, one of my students who was studying electronic forensics, did some experiments on host protected areas (a technique to place information on a hard drive in a way and in a place that it is protected from access through the normal processes of the operating system). Forensic tools are designed to capture the entire contents of a hard drive for evidentiary purposes (from the first bit at the first addressable location to the last bit at the last addressable location). This student found out through his experiments (and proved) that certain forensic tools did not capture information stored in this area. The finding was published in the appropriate refereed Elsevier journal (Bedford, 2005) for all to learn from. This resulted in forensic products being improved and in eliminating a hiding place that could be used by the bad guys.

The notion that there is no room for "good" research is actually nonsense. Cryptographic researchers spend their whole careers doing nothing but research on cryptographic techniques, algorithms, proofs, and methods of attack. Their results comprise the content of several refereed journals. My example is not an isolated instance. It is used to make the point: that IA is not only a practical field of study but that it provides many opportunities for research, experimentation and quality publications.

What's the Status of IA Education?

In 1998, the President of the United States issued Directive #63 (Presidential Decision Directive/Nsc-63, 1998) that started the ball rolling on the creation of such a degree structure. The justification for this initiative was to improve the security of the US national information infrastructure by raising the knowledge, experience, and exposure of IT graduates to the importance of IA and IA techniques.

The task was assigned to the National Security Agency (NSA). For those who do not like the intelligence community let me point out that these folks, as a result of the strict vetting procedures and extremely high intellectual and experiential standards required for entry, tend to be superior in their abilities. NSA, never the less, conspired, conferred and collaborated with the public sector, the private sector and the academic community to produce an IA degree structure that is sensible, considered, and complete in its content.

That structure was used to invite US universities to apply to become Certified Centers of Academic Excellence in Information Assurance (CAEIAE) ("Application Procedures & Requirements," n.d.). In order to receive that accolade, each university is required to implement the IA degree structure and have their program evaluated against ten pertinent criteria ("Criteria for Measurement," n.d.). The applicant university must achieve a minimum score for each of the ten criteria in order to become certified. The first universities were certified in 1999. Today there are eight-five (85) US universities who are currently certified ("Institutions," n.d.). This certification is not forever and must be renewed every three years (More information about this program may be obtained from the NSA site established to promote this certification program at

http://www.nsa.gov/ia/academia/caeiae.cfm). This is one example of a successful program that is currently operational.

Other countries have shown an interest in protecting their respective information infrastructures and have designed programs of their own, either using the NSA model as a starting point or creating their own from scratch, and are in the process of mounting or designing and implementing such degree programs. Some examples are England, Australia and New Zealand and I expect that there are others.

The NSA model is excellent - thorough and complete. It has been collaboratively designed by some pretty smart people and has a proven track record so it provides a good starting point. No matter what the source, provided that the design is thorough, all universities that offer IT degrees need to have a look at and consider the possibility of altering their own IT degree structure to incorporate some, most or all of the NSA model content (see the *.pdf* documents listed in the References section of this paper).

In today's business world, one of the imperatives is to protect the information infrastructure. We all depend on its availability and integrity. What would happen if the stock market were to be electronically destroyed? What would happen if the air traffic control system were electronically destroyed? What would happen if the banking systems were electronically destroyed? What would happen if the utilities control systems (electricity, gas, water, etc.) were electronically destroyed?

Just think for a minute about the chaos that would occur if even one of these systems were to be successfully attacked and destroyed. If all were destroyed simultaneously, we would be returned to the "dark ages". The rule of law would cease to exist and it would be survival of the fittest (or the most well armed). The point is that we as a society cannot afford to allow that. In order to avert this from happening in the future, we need to educate IT professionals and users. They need to understand the importance of their actions when connected to the Internet. We need to produce IT professionals better prepared to defend their organization's IT function.

Some Obstacles

The first obstacle is usually the university itself. This kind of initiative, no matter how sensible and responsible that it may seem, has a tendency to be resisted by academics in general. It is often expressed that IA being "forced" on them is an interference with their "academic freedom". In other words, they resent that such an initiative originates from outside academic circles (i.e. government, business, etc.).

One possible solution to this problem is for the IA degree to be initiated from within academia as either a new IT degree or as a replacement for an existing IT degree or as a modification/realignment of an existing IT degree.

The next obstacle or probably more appropriately the main obstacle is funding. New programs need new funding (usually). Sourcing that funding can be and usually is an issue.

If the entire degree (all of the courses - this is rarely the case) needs to be funded, then finding the big bucks may be a problem. In most cases, many of the required courses will already exist within the university courses offered (for example, accounting, business law, statistics, etc.). What has to be remembered is that the IA degree is meant to produce graduates with an ethos of ethics, responsibility and an IA focus. Many courses may be perfectly adequate without any alteration. Others may need only minor additions (computing specific courses: programming, net-

working, database, etc.) Those additions will promote and highlight IA issues providing an underlying theme throughout the degree period, reinforcing the need and importance of IA.

New courses may include topics like cryptography, electronic forensics, policy, continuity planning and other specialist topics that may not currently be available within the university structure. (See Appendix B: Sample Structure for a Bachelor's Degree in Information Assurance.). Of course these need qualified instructors/teachers/professors and appropriate resources (software and sometimes specialist hardware). Some of these specialist resources can be fairly expensive. So new funding will be needed for new courses and their support.

In the main, the actual new money required should not be so much as to make the program an impossibility. The upside to this whole proposal is that these degree courses have become popular and student numbers tend to produce fund recovery - beginning to pay for themselves quickly. If the US experience can be considered as a model, the fact that the initial seven universities has grown steadily to eighty-five since 1999 should give some credibility to the idea. Each program appears to have been successful and their graduates are sought after.

Finally, selling such a program should be pretty easy. The facts surrounding the need for such degree programs are clear and logically sound. The need within the IT community for people trained in IA is also clear. So we have a market for the graduates. We have a market for the degree program - both of which justify pursuing the IA degree strategy.

Some Thoughts about IT Professional's Performance

Before beginning, it needs to be stated that I am not a Luddite. For the entire fifty years that I have been an IT professional, I have reveled in and looked forward to each new technological innovation. Rather than jumping on the current fad bandwagon, I have selectively exploited these innovations and enjoyed every minute of it.

However, there are a few issues that a proper IT education possibly could have perhaps prevented. When the PC came along many of us exploited it to its fullest and continue to do so. The early PC was fully in our (the users') control. It did not do anything that we did not command it to do. Security was easy. If we followed a few simple rules we could easily be assured that our IT function (and data) would be protected.

As it turns out, early operating systems were not very user friendly and we had to remember specific command line instructions in order to operate our PC. Some small improvements were made to make that a bit easier (batch files, menu programs, etc.) but we were still in control.

Word processing was possible requiring less than 100,000 bytes of memory. For that we had the ability to type and edit text, control and change fonts, format text, spell check, grammar check, mail merge, and consult a thesaurus. Really, these are the foundation operations that any word processing requires. We didn't have any graphic capability.

The Task Manager tells me that in order to edit this paper, it requires Word® to be memory resident - taking up forty-five (45) ***megabytes***. With no document loaded it only takes twenty-nine (29) ***megabytes*** to be resident. These numbers appear to vary by ten or so megabytes for no explicable reason. The paper, by the way, is 72,000 bytes in length. What's wrong with this picture?

What is it exactly that we are getting from the forty-five (45) megabytes that Word® requires? The argument that memory is cheap, computers are very fast, and disk storage is cheap and fast does not explain away bloated poor quality inefficient software. Writing applications in some voluminous inefficient programming language is probably very profitable for the vendors of such

software because it can be done faster (and therefore cheaper) but faster is not necessarily better in this situation.

In the early days of computing, programmers created tight code that was fast - it performed very efficiently. Because it was tight and small, it was easy to document, test and debug.

It could easily be argued that I wish to return to the good old/bad old days. That is not what this is about. Rather, it is about education – the education of a whole generation of computer programmers, most of whom do not really understand what exactly is happening within the computer. They can issue a single command that does many things and not need to understand any of it - just the outcome.

The argument for that is that it is cost effective. Perhaps, but it seems to me that an IT professional should know about his/her craft, tools and how to use them to their greatest extent.

Let's just return to the notion that the user should be in control of his/her computer and its activities. Today's operating systems control our PC. We do not. The operating system performs many functions that we have no control over and most likely do not know about. These have been designed to make it easier for dummies to operate - and they are successful in that respect.

However, these systems make believe that they are policemen deciding what to do in regard to digital rights management for example. Why does my operating system need to do that? That function does not in any way improve the performance or operation of my PC. Actually, digital rights management has absolutely nothing to do with my computer and is only relevant to copyright holders. They however, have captured those who produce operating systems influencing the design of a tool that is meant to serve the user and corrupting that into a policing tool.

Some operating systems and applications report back to their master or masters at their discretion and without our permission or knowledge. When did we give up control of our PC?

If proper IT education was in place for the last thirty years, these things would probably not have happened. We would be using efficient software designed to fulfill our needs as users without respect to any other special interest entity. There is no need for our software to report our activities or status to anyone. What purpose does that serve? What exactly is the benefit to the average user of this imposed surveillance? Why don't we have an option within the application and/or operating system to just turn these functions off?

Perhaps we need two settings for software and operating systems: 1) for dummies who don't care about their privacy or control of their PCs and the other 2) for those who wish to control what their PC is doing and who it is conversing with.

Conclusions

We've gotten a little bit away from the initial subject, but it seems to me that we have failed to produce strong IT professionals over the past many years and that its time to wrest control back. The new crops of IT students need to be instructed in the efficient use of programming tools - where efficient doesn't just mean produce fast. They need to understand the importance of Information Assurance as it applies to organizational systems and networks as well and to individual and personal systems. They need to know that information technology is perhaps the most strategically important activity that occurs in any organization and that it continuity, availability and integrity must be protected without exception.

Additional Sources of Useful Information:

Resource List:

NSTISSI No. 4011, *National Training Standard for Information Systems Security (Infosec) Professionals*, published by **N**ational **S**ecurity **T**elecommunications and **I**nformation **S**ystems **S**ecurity, 20 June 1994, 29 pages, ***http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf***.

CNSS Instruction No. 4012, *National Information Assurance Training Standard for Senior System Managers*, published by the **C**ommittee on **N**ational **S**ecurity **S**ystems, June 2004, 20 pages, ***http://www.cnss.gov/Assets/pdf/cnssi_4012.pdf***.

CNSS Instruction No. 4013, *National Information Assurance Training Standard for System Administrators (SA)*, published by the **C**ommittee on **N**ational **S**ecurity **S**ystems, March 2004, 56 pages, ***http://www.cnss.gov/Assets/pdf/cnssi_4013.pdf***.

CNSS Instruction No. 4014, *National Information Assurance Training Standard for Information Systems Security Officers*, published by the **C**ommittee on **N**ational **S**ecurity **S**ystems, April 2004, 66 pages, ***http://www.cnss.gov/Assets/pdf/cnssi_4014.pdf***.

NSTISSI No. 4015, *National Training Standard for System Certifiers*, published by **N**ational **S**ecurity **T**elecommunications and **I**nformation **S**ystems **S**ecurity, December 2000, 32 pages, ***http://www.cnss.gov/Assets/pdf/nstissi_4015.pdf***.

CNSS Instruction No. 4016, *National Information Assurance Training Standard for Risk Analysts*, published by the **C**ommittee on **N**ational **S**ecurity **S**ystems, November 2005, 38 pages, ***http://www.cnss.gov/Assets/pdf/cnssi_4016.pdf***.

CNSS Instruction No. 4017, *National Information Assurance Training Standard for System Security Engineers*, to be published by the **C**ommittee on **N**ational **S**ecurity **S**ystems, Under Development - **NOT** yet available ***http://www.cnss.gov/Assets/pdf/cnssi_4017.pdf***.

NOTE: The Internet is a fluid living thing with more than 460 million active hosts. What is valid today may not be valid tomorrow. One or more of these addresses may no longer be active but give them a try.

References

Application Procedures & Requirements. (n.d.). Centers of Academic Excellence, National Security Agency. Available at http://www.nsa.gov/ia/academia/caeiae.cfm

Bedford, M. (2005). Methods of discovery and exploitation of Host Protected Areas on IDE storage devices that conform to ATAPI-4. *Digital Investigation, 2*(2). Oxford, England: Elsevier Science. ISSN: 1742-2876.

Criteria for Measurement. (n.d.). Centers of Academic Excellence, National Security Agency. Available at http://www.nsa.gov/ia/academia/caeiae.cfm

Institutions. (n.d.). Centers of Academic Excellence, National Security Agency. Available at http://www.nsa.gov/ia/academia/caeiae.cfm

Presidential Decision Directive/Nsc-63. (1998). Retrieved from http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

Appendix A

Criteria required to become a Certified Center of Academic Excellence in Information Assurance (of the ten - those that specifically describe expected academic rigors).

Criteria 4: Academic Program Encourages Research in IA

The academic program encourages research in IA. Provide examples. This criterion focuses on STUDENT-based research and is important because research fuels the relevancy and currency of IA curricula.

Criteria 6: Faculty Active in IA Practice & Research & Contribute to IA Literature

It is clearly demonstrated that the faculty is active in current IA practice and research, and contributes to IA literature. Substantiate depth and length of faculty expertise through submission of biographies.

Criteria 9: Declared Center for IA Education or Research

The university has a declared center for IA education or a center for IA research from which IA curriculum is emerging. The center may be school or university-based. (Example: The Computer Science Department has an officially designated "Center for IA Studies" with a clear link to and sponsorship by the College of Engineering Sciences, with a charter signed at least at the College of Engineering level) Provide documentation of the designation of the Center (e.g. the charter), signed by the Dean or higher, and the mission statement.

Appendix B

Sample Structure for a Bachelor's Degree in Information Assurance

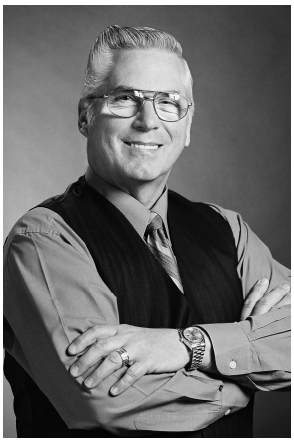
Title	Paper Description
Year One	
Introduction to Accounting & Reporting	Intro - Basic concepts, principles and techniques of financial accounting
Introduction to Business Law	Basic business law - emphasis on using & meeting statutory requirements
E-Business & Information Systems Dev.	Foundation topics for developing information systems & applications
Quantitative Analysis for Business	Descriptive and inferential statistics - application to business research & practice
Law of Obligations in Business	Law of contracts, torts, intellectual property, sale of goods, etc.
Computer Programming	Algorithm development - art & craft of computer programming
Information Assurance I	Introduction to the ideas and ethos of protection of the IT function
Computing for End-Users	Graphics oriented presentation techniques.
Year Two	
Programming & Problem Solving	Programming in modern programming languages
Information Assurance II	Techniques for protecting the IT function
Database Design & Management	Topics related to relational database design, construction & management
Communications Skills	Critical understanding of communications theory, processes, & techniques
Algorithms & Data Structures	Data abstraction & their various types and uses within algorithms
Introduction to Networking & Protocols	Exploration of networking theory, principles & tools - foundation for net admin
Policy & Continuity Planning	The corner stones of IA: policy, disaster recovery planning and backup
Year Three	
Effective Programming	Reliable implementation of algorithms and systematic verification
Information Assurance III	Designing and implementing Audit and Control processes and measures
Network Design & Administration I	Network admin practices, tools, and security techniques (Novell & Windows)
Network Design & Administration II	Internet, firewall & server construction, operation and maintenance (Linux)
Applied Cryptography	Mathematical understanding of basic principles of cryptography
Database Systems	Database design, tuning, object, and distributes systems

Business Ethics	Ethical issues in business including ethical theory and reasoning

Year Four

Information Assurance IV	Risk analysis and advanced techniques for protecting the IT function
Networking & Security I	Administering and protecting a local area network (comprised of the three LANs)
Information Assurance Project I	Practical project (variable topics) applying IA techniques
Networking & Security II	Administering and protecting a local area network continued
Information Assurance Project II	Practical project (variable topics) applying IA techniques continued
Computer Forensics	Policy, first responder and the technology of electronic forensics

Biography



Dr. **Wolfe** has been an active computer professional for 49 years. In 1979 Dr. Wolfe took up an academic post at the University of Otago and for the past twenty or so years has specialized in computer security (and is currently in the process of designing and creating an Information Assurance degree – based on the NSA model). During that period he has earned an international reputation in the field of forensics, encryption, surveillance, privacy and computer virus defenses.

Dr. Wolfe writes about a wide range of security and privacy issues for *Computers & Security*, *Digital Investigation* (where he is also an Editorial Board Member), *Network Security*, the Cato Institute, *Cryptologia* (where he is also an Editorial Board Member), and the *Telecommunications Reports*. He is a Fellow of the New Zealand Computer Society. He is also a member of Standards New Zealand SC/603 committee on Security, Secretary of the *AsiaCrypt* Steering Committee (representing New Zealand), a member of the New Zealand Law Society's Electronic Commerce Committee, and was on the Board of Directors of the *International Association of Cryptologic Research* finishing up in January 2003.