2010

Making Information Security Acceptable to the User

Andrew Jones
Khalifa University of Science Technology and Research

Thomas Martin
Khalifa University of Science Technology and Research

Originally published in the Proceedings of the 1st International Cyber Resilience Conference, Edith Cowan University, Perth Western Australia, 23rd August 2010

MAKING INFORMATION SECURITY ACCEPTABLE TO THE USER

Dr. Andrew Jones[1,2] and Dr. Thomas Martin[1]

[1]Khalifa University of Science Technology and Research
Sharjah, United Arab Emirates
[2] Edith Cowan University
andrew. jones@kustar.ac.ae

Abstract

The security of information that is processed and stored in Information and Communications Technology systems is an ongoing problem that, as yet, has not been satisfactorily resolved. Software developers, system architects and managers all aspire to use technology to provide improvements in the protection of information that is processed and stored on these systems. However, they are working in an environment where the threats to the information, the technologies in use and the uses to which the technologies are being employed are changing at a pace which is faster than can be effectively addressed.

This paper looks at the underlying environment of the technologies, social and economic change and the factors that affect how the end user perceives and interacts with the technologies.

Keywords: Information Security, Human Factors

INTRODUCTION

All organisations are facing the increasingly complex problem of securing their information and the systems that contain it. Information technology has become more useful and more useable, the initial capital costs and ongoing costs have dropped. All of this has lead to a greater dependence on ICT. In an effort to address the problem, an increasing number of legal and regulatory requirements have been introduced. Unfortunately these are, in many cases, almost unenforceable or pointless, as they have been brought into effect with a range of requirements to meet laws in individual countries and to meet perceived national and business sector specific requirements.

While work continues at many levels, experience of the past shows that to deliver international legal harmonisation of individual national laws takes a long time, it is set in an environment where the technology and the use and misuse that arises from it are changing rapidly.

The technologies that are being used, and in particular the Internet, are now almost ubiquitous and global and as a result there is inconsistency and confusion in the standards that should be applied to the protection of information. Security of information and information assets is not a problem that has only arisen with the increasing use of Information and Communications Technologies (ICT) to process, store and transmit information. As with many things in ICT, it is an old problem that has moved to a new environment. In the days before computers and mobile devices, sensitive information was stored in filing cabinets, safes and storage vaults. To protect this information, we relied on the vetting of staff, locks and bars and dedicated security staff that carried out periodic checks to ensure that the storage area had not been breached or if it had, then to report it within an acceptable period. As with any system that relies on human input, this was not foolproof and security breaches occurred on a regular basis with those that were detected being reported. Most of the reported security breaches were as the result of carelessness, accidents, theft or the illicit copying of documents. With the ever increasing use and complexity of ICT, the security of information has been addressed through the application of more and more technical solutions.

In part this is because the people that use the systems to carry out their roles within organisations for the most part only understand how to use the functionality of the ICT system that supports them in achieving their goals. Systems have been developed to meet the broadest possible consumer audience with the result that the unit cost has decreased significantly over time. ICT systems tend to be generic in nature and contain functionality that far exceeds the needs of most users. In the past, the tools that a person was provided with were the minimum that was required for them to carry out their role, for example a pen, pencil, paper, ruler, eraser (something to write with and make corrections with) or perhaps a typewriter. Now, with almost any ICT system, they will be provided with a suite of office tools (Word processor, spreadsheet, database system, presentation software) and

with this there will almost always be additional applications such as email and even instant messaging. Then there will be system administration tools to manage the information and security tools to protect it. In doing this we have gone from providing the tools essential to complete the task at hand to providing a very rich environment in which there are far more tools and applications than are required. In this environment, it is not reasonable to expect that the end-user will have a good level of knowledge of the existence of many of the functions available on the ICT systems. As a result the security measures required to protect the information that is stored and processed by these applications and systems has been automated wherever possible. This appears to be a rational development when the very use of ICT systems is itself an automation of the manual processes that preceded them.

Unfortunately we live in an imperfect world and the result of this apparently rational development has been a significant reduction in the level of security that is afforded to many of our sensitive items of information when we store them on an ICT system. When the processes used to produce, modify, maintain and store information were manual, a breach in security would result in the exposure of a limited number of documents, from a single document to a file to a filing cabinet. Paper documents also have the advantage, from a security point of view, that they were relatively heavy and bulky. This, together with the fact that they were visible, gave the potential for accurate indexing and regular audits, where they could be accounted for and for regular 'weeding' where documents that were no longer required could be extracted and destroyed. Even the destruction of the documents could be observed and certified.

DIGITAL DATA STORAGE

Now, with digital storage devices increasing their capacity with near exponential growth, the situation has changed. The volumes of documents that are stored on digital media have grown significantly (if you run out of storage space, you just get a bigger disk or ask for more space on the server). Coupled with this is that in the new digital storage media, the filing and indexing of information is all carried out in a 'virtual' environment. What the user sees is only a representation of what is actually happening. The document that they 'save' to a location in the filing system of the ICT system may well have a number of other copies created and stored unbeknownst to the user. Some of these are created for good system management and user support functions such as the recovery of documents that have been lost during a system failure or similar events, others for reasons known only to the software developers. One of the prime drivers for the destruction of obsolete documents has been lost because now storage space is readily available. Coupled with this is the fact that there is no longer an easily understandable visualisation of the volume of information being stored (you are no longer confronted with boxes of documents in the corridor or full shelves). As a result, the pressure to manage the level of information that is stored has decreased. Even when it comes to the destruction of information on the ICT system, all is not as the user sees it. When a document is deleted and disappears from the index system, it hasn't really been deleted – it has just been moved, in most cases to the 'recycle bin' (in paper terms, it has been thrown in the bin, but has not been shredded or burnt) and can be recovered. When the recycle bin is emptied, the user may be forgiven for thinking that they have now, finally got rid of it. Unfortunately this is not true, as the only thing that has been deleted is the reference to the location where the file was stored. Even at this stage, the file can be recovered if that storage space has not been re-used (and even if it has, then part of the file may still be recoverable). In fact the only realistic way for the average user to ensure that the document has been destroyed is to overwrite all of the unallocated space on the disk with a predetermined or random character string. Is it realistic to expect that the average user, for whom the ICT system is just a tool to carry out their tasks, will have the interest, the knowledge, the time and access to appropriate tools to do this? If the information is of significant value, even this may not be enough and the information may still be recoverable according to Guttman.

When dealing with the physical containers that stored information, it was relatively easy to validate that the measures taken by one organisation were of a similar standard to those taken by another organisation with which it wished to share the information. It was possible to check the efficacy of the security measures because there was a long history of their use and tests could be carried out and the results measured. While this still largely holds true for the protection of the physical assets, it does not hold true for those assets that are stored in the digital domain. One of the problems is that different organisations are likely to have different requirements and the individual technologies and security measures that they impose will vary and change over time with the result that it is extremely difficult to compare the security measures of two different systems.

This is very different from the past where, although the measures employed to provide security such as the type of door, wall or lock might vary, the function and purpose was easily understood and it could be tested and visually inspected. Even the average user could be expected to do this to some extent, as they are the same types

of measures that they encounter in the home. In the digital domain, very few of the tools that are used have been tested. Even when they have, the standard against which they have been tested, the results of the tests and the products performance against them are often difficult to understand.

With ICT systems, the measures that are used to protect the information differ from those used in the physical domain because they are largely hidden from the user. The security measures have been developed to achieve their function with a minimum of user interaction or visible signs of activity. Most ICT security measures work as background tasks (firewall, IDS, malware scanning) while the user is productively engaged in the work required for their role. As a result the user is not aware that it is taking place or whether the security measure is actually working at all. The ICT security aware person will have a higher level of sensitivity to the messages that the security tools occasionally show on the screen, but for the average user these are largely meaningless. In addition, the average user does not have the level of access required, the knowledge nor the tools to take action if there was an indication of a problem.

With physical and procedural security measures the user is aware of many of the measures in place which are both visible and involve a human interaction (e.g. locks on doors, bars on windows, document audits and security guards). With ICT systems, the firewall, the IDS, the anti-malware and many of the access control devices are setup and configured by system administration staff and work without direct interaction with the user. This is, in part, because the system designers have 'improved' the human-computer interface to reduce the level of inconvenience that the legitimate user has to overcome in order to carry out their role. In doing so, they have made the security measures less obvious.

Information security in computing terms was defined as early as 1987 in a survey as ensuring the Confidentiality, Integrity and Availability (CIA) of information. All three of these aspects of security are important in the functioning of any organisation, but it is the issue of confidentiality that is most normally thought of when the term security is used.

During the early days of computer technologies, when access to information systems was largely limited to government organisations and academic institutions, governments took an approach to information security that was based on the concept that only absolute security was acceptable. As the use of computer processors and ICT became more widely used, it became increasingly clear that this was both unaffordable and unachievable. The approach that was subsequently adopted was one of 'risk management'. In this approach the security measures that were implemented were designed to be appropriate to the sensitivity of the information to be protected. This has to be measured in terms of the impact to the organisation if the security is breached and the level of threat that exists to that information. While this approach was initially adopted in the early 1990s, it has not yet achieved a realistic level of maturity. It is not surprising there are difficulties in creating methods for the accurate determination of risk in an environment where the threat and the technology employed are constantly changing. One of the problems with a risk management approach have been that in the area of ICT systems, there is a relatively short history and there is no depth of historical information available on which to base the risk decisions. Another is that ICT systems are not geographically bounded and they exist in a global infrastructure rather that at a physical location. There is also little experience in how to define the risks or measure the effectiveness of a combination or ICT risk mitigating countermeasures. This is further complicated by the fact that the technologies that are being used in the workplace have become increasingly affordable and are being used in the home. As was said previously, user's experience with physical security measures used in the home does contribute to being better prepared in the office. However, now we are seeing ICT technology being used, not the security measures and this has resulted in people who apply limited or no security to their home computing environment applying the same to their work environment.

Individuals are now utilising the same hardware and software both at work and in the home. In many cases, the user actually has a wider range of technology (MP player, games console, SatNav system, personal video recorder, etc.) and a more modern computer in their home.

When the use of such technologies in the home is combined with a number of changing work practices (including more frequent mobility, home working and the greater acceptance of the use of work computers for personal correspondence and web browsing) it is not surprising that people increasingly tend to think of their work computer in the same way that they think of their home computer. The security requirements that the individual in their home have for their personal information, if they have considered it at all, are normally far lower than those which are required to properly protect an organisation's information assets. Few users will give these concepts of security a moment's thought, nor the risks that they accept by not taking suitable measures to protect the information that they process or store on the range of devices that they own. As a result,

the information that belongs to the organisation, whether processed on one of their personal devices or the ICT system at work is likely to receive the same level of consideration as their personal information.

Another complicating factor is that the same infrastructure (the Internet) is being used to support both the user's personal requirements and that of the organisation. For the organisation, this is cost effective and not only allows organisations to interact with each other and their customers, but also allows business to take place over the common infrastructure. This has creates a number of risks as it reveals an organisation's ICT infrastructure to the global population of Internet users. This exposes the organisations to attacks from any computer that is connected to the Internet, which means that they are exposed to attacks from anywhere in the world, at any time. In the past, when the information was paper-based, an attacker would normally have to physically make a trip to the location where the information was stored and overcome the physical and procedural measures that had been put in place. This reduced the number of potential attackers and also provided the opportunity to identify and capture the attacker. Because the access to the information is now through electronic means, there is no longer any need to physically travel to the site where the information is stored and the potential threat spectrum has increased dramatically.

The range and diversity of ICT technologies that are currently utilised to provide security to systems causes a further complicating factor as the functionality of different technologies and tools overlap and their quality varies. While physical security measures and tools have been developed and tested over a considerable period of time, those used in computer security have, for the most part, not been exposed to the same level of scrutiny. The effectiveness of physical security measures can be tested in isolation and the efficiency of a lock, for example, can be tested using an industry wide accepted set of tests. Once it has been tested and the characteristics of a lock or a security door are known, it is likely to remain in production for a significant period and a large number produced. On the basis of having passed the tests, the lock or the door will have known characteristics and be trusted to meet them. While other locks or doors that fail the tests or are not tested will still be produced, they will not be used in situations that require a provable level of security.

Security measures for ICT systems are, on the other hand, extremely difficult to test. They have to rely on other elements of the system, (e.g. operating systems) and work in an environment where other tools and applications may affect their performance. The great diversity of available security measures complicates the task. There is also a high cost of in-depth testing of ICT security measures, compounded by the limited period during which the security tools have value before they are found to be inadequate as a result of the fast moving pace of development in computer technology. While the testing of a lock may take hours or days, the testing of an ICT security device is likely to take months. Even when tested by one of the 'certified' laboratories, there is not likely to be potential for long production runs for the product and as a result, the cost of a tested product is likely to be considerably higher than one that has not been tested. For the user of an ICT system, these issues will not normally be apparent as they are addressed by the management of the organisation and the ICT system or security staff.

With physical, procedural and personnel security measures, the user has an understanding of their effectiveness and their benefits from their personal life, as they use the same types of tools and techniques to protect their homes and their cherished and valued possessions. If they feel they have items of value, people will utilise high quality door and window locks and will fit intruder and fire alarm systems to achieve a feeling of 'safety' from the knowledge that their items of value cannot easily be stolen or destroyed. The value of using good security measures in the home environment is reinforced by insurance companies that give the owner the benefit of lower premiums if they consider the measures that have been taken are effective and reduce the likelihood of loss.

Unfortunately, people do not apply the same level of security protection to their 'invisible' assets', the information that is stored and processed on computers. In most cases this is because people have no idea of the value of their stored information or indeed, have no knowledge of some of the information that is stored on their digital devices. People are only now starting to realise the impact on their personal finances, and their lives in general, that result from identity theft or fraud. Even with this increased awareness, people are, for the most part, intrinsically naive and trusting. When using the internet, this can result in them falling victim to malicious attacks on their computers, social engineering, scams and the theft of personal information.

The general lack of awareness and understanding of the risks to information security is the result of a combination of contributory factors. One of these is that information stored on digital media, unlike that which is stored in paper form, does not take up large volumes of physical space. Digital storage media is now extremely cheap and if the computer disk is full, it is cheap and easy to add another disk. One of the effects of

this is that people do not 'weed' out the information that they no longer require for their personal life or business – there is not the same imperative to do so and it is a time consuming process. A related issue is that, unlike paper, when a record is destroyed on a computer, it can normally be recovered by employing easily accessible and simple-to-use tools. This is not commonly understood and most people believe that a file which has been deleted from a computer is not recoverable. In contrast to the physical world, where if a person was scammed or conned out of money or it was stolen the victim would probably eventually realise the loss, in the virtual world the loss of information is normally transparent. In the physical world the theft of a document or an asset require its removal, which should eventually be noticed, whereas the 'theft' of digital information leaves the original asset in place with no apparent trace that it has been touched.

Another factor is that with physical objects they possess, people normally have a good understanding of the value, whereas with information they are responsible for, very few people or organisations can place a realistic value on it. Both physical objects and intangible assets such as information cost money to produce or obtain. But physical objects have a predictable ongoing value, whereas intangible assets such as information are more difficult to value (having been generated as a result of effort in terms of man hours and computer processing). As a result most individuals and indeed many organisations have not considered the intrinsic value of the data that they possess, either in terms of the cost of replacing it or its intellectual value.

We are in the process of migrating to what is known as an information society, where information has started to have a much greater value than before. There is now a knowledge economy and the volumes of data that are generated and stored have grown on a massive scale. Unfortunately, the majority of individuals that depend on, and contribute to, this information society have no concept of how it may affect them.

The first computers that were developed had very limited processing power and storage capacity, were limited in numbers, extremely expensive and were used by exclusive groups with specialised requirements. As the technologies on which these computers relied developed and they became more widely used, they have continued to become less expensive, have greater processing and storage capacity and have increasingly become essential business tools and eventually also household items. With the extended capability, reduced cost and more widespread use of the technologies, an escalating number of people have gained access to them. As a result of this massive expansion in the number of users, the majority of whom were no longer computer specialists, and the increasing complexity of the networks and functionality of the computer, it became necessary to 'hide' many of the operations of the computer from the user. In the early days, users had to learn to enter commands to instruct the computer on the required operation and any constraining parameters, but the introduction of graphic user interfaces (GUIs) where the user clicks on an icon on the screen allowed for a massive increase in the numbers of people who were able to use computers.

One of the effects of introducing the GUI was that many of the processes that take place within the computer were no longer giving visible feedback to the user. The approach that has been adopted by information security has been based on the same concept that was adopted for the GUI, which is to automate as many of the processes as possible and have the software deal with them rather than the user. This has allowed non-information security literate users to operate systems in a relatively secure manner, whether for business or for pleasure. In business this is essential to allow the user to utilise the computer as a tool to help them to carry out their tasks and for personal use to browse the internet, use it for online shopping, correspond and play interactive games, without having to give specific thought to the risks that the activities may expose them.

This is a trade off that will always be present if there is a need for personnel who are not trained in the specific technologies or the security measures being used in ICT systems. In the physical world security personnel in the form of police officers and security staff are employed to provide a basic level of security to allow people to carry on with their lives and tasks in a relatively secure manner. The same philosophy is applied to the cyber world, with system administrators, information security staffs and specialist law enforcement officers employed to achieve a similar outcome. However, with networked ICT systems this takes place in a global environment and while the security and system administration staff can deal with the assets of the organisation, there is no 'Internet police force'.

A security breach in the cyber environment can have a significantly different impact to one that takes place in the physical world. If a document is mislaid or lost in the physical environment, then a search can be conducted and an assessment made of what has probably happened to it can be made. It may have been inadvertently destroyed, misfiled, lost in transit or stolen, but the volume of information that has been compromised will normally be of limited amount. If computer data is compromised, then the potential damage will normally be orders of magnitude greater.

If a house is broken into, then the assets of an individual or a small group are at risk. If a company premises are broken into then a small company or an element of a larger company's assets may be compromised. In both cases, there is a strong likelihood that the attack will be detected. However, when a computer is broken into the likelihood of the attack being detected is much lower and not only are the assets of the owner at risk, but the computer itself may then be used to attack other ICT systems attached to the network.

It is clear from the number of reported information security breaches and the levels of identity theft, hacking and malicious software in circulation, that the current approach to security is not effective. Achieving an appropriate and adequate level of security always carries a cost, but as mentioned earlier, governments and organisations realised around 20 years ago that absolute security was neither affordable nor, in many cases, achievable. The balance is to determine what level of risk is acceptable and then put in place effective security measures to achieve it.

A DIFFERENT APPROACH

Given that the required level of security is not currently being achieved, an alternative approach that might improve the way users perceive information security would be to reverse the approach of obfuscating the processes on the ICT system and make the security processes more visible to the user. In order to achieve this, it would be necessary to shift the balance from the computer dealing with all of the security issues in the background and provide the user with better visibility of the security processes that were taking place and the events that they were detecting. The negative impact of this is that it would undoubtedly result in lower levels of productivity for the users as they would have to respond to events that the ICT system was detecting.

Within organisations there would be a requirement for additional information security staff to address the problems that the users identified, whether real or false alerts. However, in a relatively short period of time, with the proper support and education, this would result in a greater awareness by the user of what security relevant activity was taking place on their system. It would also be likely to have the benefit that the users would become more aware of changes in the way their ICT systems were operating and increase the likelihood of them noticing when they were not performing as they should.

The reality is that while the implementation of security for ICT systems does not currently work well, to move towards the suggested type of approach would be a risk management decision that each individual business would have to make. They would have to decide whether the additional cost of reduced productivity was balanced against an improvement in the security of the information that they rely on.

Improvements in the security of ICT systems could also be achieved by a number of other approaches. One of these would be in the area of software development. If the quality of the software that is used on ICT systems was improved, the potential vulnerability of the systems would be reduced because there was better written code with fewer weaknesses in use. In no other area of our lives do we accept products of such poor quality and with such little recourse to corrective action. In addition, together with the improvement in the quality of the software itself, the messages that it generates for the user could be improved to give the user meaningful information, rather than the commonly seen 'error codes' or other meaningless messages. Because the users have been conditioned to it by the software developers, very few users ever read the end-user licence agreements or terms and conditions for the software and services that they use. Most users will automatically hit the accept button or tick the accept box. A belief that has developed, with experience, is that the software will eventually do what you wanted it to if you do hit the cancel/next/OK button has also supported this behaviour.

If the way that people perceive and interact with information security measures is to improve, then one issue that has to be addressed is to separate out and make distinct the security messages that are shown to the user from all of the other system and software generated messages that they receive. This, together with well constructed and helpful messages, would highlight the fact that the message was security relevant. Doing this gives the potential for the provision of guidance with regard to the actions that need to be taken by the user and the level of importance. In order to achieve this, software developers would need to seek the assistance of security staff, users and even psychologists to ensure that messages that are presented when an event occurs convey meaning in a form that is understandable by the majority and that the instructions or advice is relevant and achievable.

Whenever the subject of information security is addressed there is a need to improve the awareness of the users and also for training of specific staff. Information security is neither obvious nor intuitive. This type of activity has, in the past, normally been undertaken with a view to the cost of delivery of the training and undertaken by

the organisations technical or security staff that understands the technology. While cost effective, these are not necessarily the people most suited to the development and delivery of material to improve awareness. The effect of such activities could, for the most part, be considerably improved by using people with good communication skills who can produce and deliver material that is both interesting and understandable.

Because of the way ICT systems are designed and developed in most organisations, security is perceived as an inhibitor to productivity. This is largely a result of the security functionality of ICT systems not being designed in from the beginning. When it is retrofitted it does not appear to be an integrated part of the system. The implementation of the security measures in this way is likely to impede the functionality of the systems. If security is designed into systems from the earliest stages of their development, it will be better integrated, more cost effective and more efficient.

Security is currently seen as an activity that only has penalties for poor behaviours and that has no obvious positive impact on the user. An approach that might be considered for improving ICT security would be to offer incentives for acting in a positive manner with regard to security. This might be implemented in a number of ways, depending on the organisation, but the effect that could be achieved is to attract attention to ICT security within the organisation and change the way in which it is viewed by staff. One example of this is the Massachusetts Department of Environmental Protection 2010 Small System Security Award. The aim of this initiative was to acknowledge small systems within the organisation that had been proactive in enhancing the security of their system and to help encourage all small systems to consider security within their existing structure. A recent article in CSO online suggests a number of ways to change the perception and knowledge of the users. These include: providing treats, training, effective messages on the screen and probably most importantly, management demonstrating that they support the culture by their own behaviour. Activities such as this can be used to change the user's perception of security and as a result, change their behaviour.

CONCLUSION

The security functionality of ICT systems is not currently easily visible to the user, except for messages that are difficult to understand or meaningless. The security regimes that have been put in place are, in the main, based on punitive actions for transgressions with no reward for positive activities. While this environment exists, there is little chance that the user's perception of ICT security will improve. It is possible that with co-ordinated effort from groups that range from software and system developers to ICT security and administration staff, security and training course developers, that user's perception of and engagement with ICT security can be improved. Naturally, there will be a significant cost. If organisations also take action to promote positive behaviour with regard to ICT security by changing the organisational culture and by rewarding positive behaviour then the users are likely to respond and any positive activity incentive scheme will also focus attention on the topic of ICT security and help to keep it in the forefront of users thoughts.

REFERENCES

Gutmann, P. Secure Deletion of Data from Magnetic and Solid-State Memory, Sixth USENIX Security Symposium, Pp. 77–90 Of The Proceedings, 1996, http://www.usenix.org/publications/library/proceedings/sec96/full_papers/gutmann/index.html

Clark. D.D., Wilson. D.R., A Comparison of Commercial and Military Computer Security Policies, IEEE, 1987

Odlyzko, A.M.: Economics. Psychology, and Sociology of Security, http://www.dtc.umn.edu/~odlyzko/doc/econ.psych.security.pdf (accessed 14 Dec. 2009)

Barrett, L. Identity Theft Cost Victims $54B in 2009, Esecurity Planet, 12 February 2010, http://www.esecurityplanet.com/trends/article.php/3864616/Identity-Theft-Cost-Victims-54B-in-2009.htm

Wintour, P. Lost in the Post - 25 Million at Risk after Data Discs go Missing, The Guardian, 21 November 2007, http://www.guardian.co.uk/politics/2007/nov/21/immigrationpolicy.economy3

Krebs, .Payment Processor Breach May Be Largest Ever, Washington Post, 20 January 2009

Massachusetts Department of Environmental Protection, 2010 Small System Security Award, http://www.mass.gov/dep/water/drinking/10secur.pdf

Agle, A. Seven Practical Ideas For Security Awareness, CSO Online, 02 June 2009, http://www.csoonline.com/article/493941/seven-practical-ideas-for-security-awareness