1-1-2010

How do you make information security user friendly?

Andrew Jones
Edith Cowan University

10.1016/j.istr.2010.04.001

AUTHOR QUERY FORM

ELSEVIER	**Journal:** ISTR **Article Number:** 2153	**Please e-mail or fax your responses and any corrections to:** **E-mail:** corrections.eseo@elsevier.tnq.co.in **Fax: +31 2048 52789**

Dear Author,

Any queries or remarks that have arisen during the processing of your manuscript are listed below and highlighted by flags in the proof. Please check your proof carefully and mark all corrections at the appropriate place in the proof (e.g., by using on-screen annotation in the PDF file) or compile them in a separate list.

For correction or revision of any artwork, please consult http://www.elsevier.com/artworkinstructions.

Articles in Special Issues: Please ensure that the words 'this issue' are added (in the list and text) to any references to other articles in this Special Issue.

Uncited references: References that occur in the reference list but not in the text – please position each reference in the text or delete it from the list.	
Missing references: References listed below were noted in the text but are missing from the reference list – please make the list complete or remove the references from the text.	
Location in article	**Query / remark** **Please insert your reply or correction at the corresponding line in the proof**
Q1	Kindly check the affiliations and corresponding author details.

Electronic file usage
Sometimes we are unable to process the electronic file of your article and/or artwork. If this is the case, we have proceeded by:

☐ Scanning (parts of) your article ☐ Rekeying (parts of) your article ☐ Scanning the artwork

Thank you for your assistance.

INFORMATION SECURITY TECHNICAL REPORT XXX (2010) 1–4

available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodinf.htm

Information Security Technical Report

How do you make information security user friendly?

Andrew Jones [a,b,*]

[a] *Khalifa University of Science Technology and Research, United Arab Emirates*
[b] *Edith Cowan University, Australia*

1. The past and the present

The security of the information assets is a requirement for all types of organisation, whether to protect the business or to meet legal or regulatory requirements. The security of information is not a new problem that has arisen with the increasing use of computing to process store and transmit information, it is just an old problem in a new environment. Before computers, we had filing cabinets, storage vaults and safes that valuable organisational information was stored in. To protect this information, we relied on locks and bars and security staff that checked that the secure storage areas had not been breached. The system was not foolproof and there were regular security breaches reported as the result of either carelessness or the theft/copying of documents. With the uptake in the use of computing, information security has increasingly been seen as a technical 'computer' problem. One of the problems that arise from this is that different organisations are likely to have different requirements and the individual technologies and security measures that they impose will vary. This is very different from the past where, although the type of lock might vary, the function and purpose was easily understood and could be visually checked. Another problem is that the measures used to secure information on a computer, as opposed to most other areas of security, are largely hidden from the user and have been made to achieve their function without visible signs of activity and are not visually checkable. (Testing whether a password or encryption system is working is not as simple as tugging on a lock to make sure it has engaged). With physical security measures the user is conscious of many of the measures in place which are visible and involve a human–human interaction (e.g. security guards to authorise access, locks on doors and bars on windows). With computer systems, the firewall, the IDS and many of the access control devices work without direct interaction with the user as system designers have 'improved' the interface to reduce the level of inconvenience that the legitimate user has overcome in order to carry out their role. In doing so, they have made the security measures less obvious.

Security in computing terms was a term coined as early as 1987 in a survey (Clark and Wilson, 1987) as ensuring the Confidentiality, Integrity and Availability (CIA) of information. While all three of these aspects of security are important in the functioning of any organisation, it is the confidentiality issue that is most readily thought of when the term security is used.

In the past, during the early days of computer technologies, governments took the approach that only absolute security was acceptable. As the use of computers became more widespread, they eventually came to realise that this was both unaffordable and unachievable. In order to adopt a more achievable (and affordable) stance, a risk based approach was eventually adopted. One of the shortcomings of this approach has been that in the area of computer systems, which have a relatively short history and where the environment is fast changing, with new technologies arriving on the market at regular intervals, there is no depth of historical information available on which to base the risk decisions. There is also little experience in how to define the risks or measure the effectiveness of a combination or risk mitigating countermeasures. Over the same period, the technologies that are being used in the workplace have become increasingly affordable and are increasingly being used in the home.

This has exacerbated the issue of the confidentiality of information in a number of ways.

The individual is now utilising the same hardware and software, both at work and in the home, or in many cases, has a more modern computer at home. When this is coupled with changing work practises such as home working and the increasing acceptance of the use of work computers for personal correspondence and web browsing, people will tend to consider the work computer as they do their home computer. The security requirements of the user for personal information, if they are considered at all, are normally far lower than those which are required to properly protect an organisation's information. Many home users have no concept of a requirement for information security or the risks that they, often unknowingly, accept by not taking measures

* Khalifa University of Science Technology and Research, United Arab Emirates. Tel.: +9716 5043501; fax: +9716 5611789.
E-mail address: andrew.jones@kustar.ac.ae

1363-4127/$ – see front matter © 2010 Published by Elsevier Ltd.
doi:10.1016/j.istr.2010.04.001

Please cite this article in press as: Jones A, How do you make information security user friendly?, Inform. Secur. Tech. Rep. (2010), doi:10.1016/j.istr.2010.04.001

to protect the information that they process or store on their computers. As a result of this, the information that belongs to the organisation, whether processed on the personal home computer or the computer at work is likely to receive the same level of consideration as their personal information.

Another complicating factor is that the same network (the Internet) is being used to support both the organisational and personal requirements. For the organisation, this is cost effective and not only allows organisations to interact with individuals, but also allows commerce to take place over the common infrastructure. Unfortunately this has creates a number of risks and a potential cost, in that it 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, any attacker would normally have to physically make a trip to the location where the information was stored. This reduced the number of potential attackers and also provided the opportunity to identify the attacker and capture them. Because there is no longer any need to physically travel to the site where the information is stored, the potential threat spectrum has increased dramatically.

The scope and diversity of the technologies that are currently in use to provide security to information systems cause 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 had the same exposure or received the same level of scrutiny. There are a number of reasons for this, ranging from the diversity of available measures, the high cost of in-depth testing and the limited period during which the security tools have value before they become obsolete or are found to be inadequate as a result of the fast moving pace of development in computer technology.

For the user of the computer, many of these issues never gain any visibility. They are addressed by the management of the organisation and the computer system or security staff. The user has an understanding of the effect and benefit of physical and personal security from their personal life as they use the tools and techniques to protect their homes and the articles that they cherish and value. People will utilise high quality door and window locks and will fit intruder and fire alarm systems to give them a feeling of 'safety' and that the items that they value cannot be stolen. The value of using good security measures in the home environment is reinforced by the companies that provide their insurance, which give them the benefit of lower premiums if they consider the measures to be strong and reduce the likelihood of loss.

Unfortunately, people do not apply the same level of security protection to their 'invisible assets' (Odlyzko), the information that is of value to them that is stored and processed on computers. People are only now starting to realise the damage that can be caused to their personal finances as a result of identity theft or fraud. Even with this increasing level of awareness, people are intrinsically naive and want to be helpful. In the world of networked computers, this leaves them exposed to hacking attacks on their computers, social engineering and scams.

The general lack of awareness of the risks to information security is the result of a combination of contributory factors. The first of these is that, unlike information that is stored in paper form, digital information does not take up significant physical space. The storage media is also extremely cheap and if the computer disk is full, it is easy to add more storage. As a result of this, people do not 'weed' out the information that they have stored – there is no imperative to do so and it is time consuming. Another issue is that, unlike paper, when a record is destroyed on a computer, it can normally be recovered by the use of trivial and easily accessible tools. This is not commonly understood and people believe that a deleted file is not recoverable. Also, where in the physical world, if a person was scammed out of money or conned, it is likely that they would eventually realise the loss, in the virtual world, the loss of information is transparent. The theft of a document or physical asset require its removal, which may be noticed, whereas the theft of digital information leaves the original document with no trace that it has been touched.

A third factor is that, unlike physical objects, people do not normally have a good understanding of the value of the information that they own. Physical objects cost money to produce or obtain and have a predictable ongoing value. Intangible assets such as data may cost money to obtain but are more likely to be generated as a result of effort in the 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 own.

Society has gradually migrated to an information society where information has much greater value than in the past. There is now a knowledge economy and the volume of data that are generated and stored has grown on a massive scale. Unfortunately, the majority of individuals that contribute to, and depend on, this information society have no concept of how it relates to them.

The first computers that were developed were limited in numbers, extremely expensive, had very limited processing power and storage capacity and were used by an exclusive group of users with specialised requirements. As the technology on which computers rely developed, they became less expensive, had greater processing and storage power and the computer gradually became a common business tool and eventually also a household item. In the process, as more people gained access to them, it became increasingly necessary to 'hide' the operation of the computer and to make its interface more intuitive and user friendly (the graphic user interface or GUI) as the users moved from dedicated computer staff to people with no technical knowledge or skill. This resulted in many of the processes that were taking place within the computer not being visible to the user. After all, why trouble the user with information that they would not understand and that, potentially, they might either accidentally or purposefully use to damage the operation of the device?

The current approach to information security has been based on the same concept that the development of the computer has followed, which is to automate as many of the processes as possible and hide them from the user. This has allowed non-information security and technology literate users to operate the systems and achieve the required

Please cite this article in press as: Jones A, How do you make information security user friendly?, Inform. Secur. Tech. Rep. (2010), doi:10.1016/j.istr.2010.04.001

outcome, whether for business or for pleasure. In business this is essential to allow the user to utilise the computer as a tool in support of their tasks and in personal use to play interactive games, browse the internet and correspond without thought of the risks that the activities may expose them to.

This is a trade off that will always be present. In the physical world we employ security personnel in the form of police officers and security staff to provide a basic level of security. The same philosophy is applied to the cyber world, with system administrators, information security staffs and specialist law enforcement officers working to achieve the same outcome. However, with the networked computer this takes place in a global rather than a local environment and with no 'Internet police force'. Unfortunately, the result of a breach of security in the cyber environment may be significantly different to one that takes place in the physical world. If a house is broken into, then the possessions 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 at risk. When a computer is broken into, not only are the assets of the owner at risk, but the computer may be used as a vehicle to attack a large number of other computer systems attached to the network.

2. A new approach

It is clear from the number of reported information security breaches and the level of identity theft that the current approach is not effective. One approach that might improve the way users perceive information security would be to reverse the current trend of obfuscating the processes on the computer and make the security processes more visible to them. This would shift the balance from the computer being used as a tool that dealt with all of the security issues in the background but would undoubtedly have the impact of lower levels of productivity for the user as they would have to respond to events that were being notified to them by the computer. In organisations it would also require additional information security staff to address the problems that the users identified, whether real or imaginary, but would result in a greater awareness by the user of what was taking place on their computer. It would also potentially have the benefit, over time, of the users becoming more attuned to changes in the way their computer systems were operating and increase the likelihood of them noticing when something was wrong. This would be a risk management decision that businesses would have to make while taking account of the cost of reduced productivity when balanced against an improvement in the security of the information that they rely on.

It is interesting to note that a number of studies have shown that the average user will automatically hit the cancel, next or OK button for a message on a computer screen without reading the message that was related to the choice. Very few users ever read the end user licence agreements or terms and conditions for the software and services that they use and will automatically hit the accept button or tick the accept box. This attitude has developed as a result of poor software construction and the presentation of many meaningless or unintelligible messages being presented to the user. 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 information security 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 and has the potential to provide guidance with regard to the actions that need to be taken and the level of importance.

To achieve this, the security staff and software developers will have to seek assistance from psychologists and normal users to ensure that the messages that are presented convey the meaning in a form that is understandable by the majority and that the instructions or advice is relevant and achievable.

Whenever information security is addressed there is a requirement to undertake a programme to improve the awareness of the users and also for training for specific staff. This has always been undertaken with a view to the cost of delivery and is normally undertaken by the technical staff that understand the technology but are not necessarily the most suited to development and delivery of material to improve awareness. The programmes could, for the most part, be considerably improved by ensuring that the material that is delivered is prepared by people with good communication skills who can produce material that is both interesting and understandable.

In most organisations, security is currently perceived to be an inhibitor to staff attempting to carry out the tasks that they are paid for. This is largely because the security functionality in information systems is often not designed in from the beginning and as a result is retrofitted and may not appear to be an integrated part of the system. By implementing security in this manner, it is also more likely to cause an impediment to the systems functionality. If security was designed into systems from the earliest stages of their development, it could be better integrated, more cost effective and more efficient.

Security is currently seen as a barrier that has penalties for poor behaviours. It has no obvious positive impact on the use. Another approach that could be considered for improving information security would be to offer staff incentives for acting in a positive manner with regard to security. The way in which this might be implemented would vary from organisation to organisation, but the effect that could be achieved is to attract attention to information security within the organisation and change the way in which it is viewed by staff. It could also be a method to change the users perception of security and as a result, change their behaviour.

3. Conclusions

While the security functionality of Information and Communications Technologies (ICT) remains hidden from the user with the exception of hard to understand or meaningless

Please cite this article in press as: Jones A, How do you make information security user friendly?, Inform. Secur. Tech. Rep. (2010), doi:10.1016/j.istr.2010.04.001

messages and punitive actions, there is little chance that the perception of information security will improve. It is possible that with effort from a range of groups from system developers to people with a good knowledge of security and training course developers, that the way in which people perceive security can be improved. Organisations can also take action to promote positive behaviour with regard to information security by changing the way in which they implement it and by rewarding positive behaviour. Some form of positive activity incentive scheme could focus attention on the topic of security and change the perception of the users. This would result not only in security becoming better understood and more accepted, but would also lead to an improvement in the overall level of security of information systems.

REFERENCES

Clark DD, Wilson DR. A comparison of Commercial and Military computer security Policies. IEEE; 1987.

Odlyzko AM. Economics, psychology, and sociology of security, http://www.dtc.umn.edu/odlyzko/doc/econ.psych.security.pdf. accessed 14.12.09.

Please cite this article in press as: Jones A, How do you make information security user friendly?, Inform. Secur. Tech. Rep. (2010), doi:10.1016/j.istr.2010.04.001