Promoting security awareness and commitment

Phil Spurling

Alcoa encourages people to be honest

Introduction

When we talk about promoting computer security awareness and building commitment to computer security, we tend to think about security awareness campaigns, advertising, videos, posters, stickers, booklets, etc. All these things are important and have their place in promoting awareness, but in reality they are only part of the whole process. I believe that if you want to gain long-term commitment you will need to do a lot more than print booklets or put posters all over the place. A commitment to security involves providing a process which fits in with the culture of the organization and it means ensuring that you provide a high quality product and service.

Work at Alcoa has been based around the following three principles:

(1) It is difficult to promote a bad product so do whatever you can to make sure you have the right product.

(2) It is easier to get commitment if the people are involved.

(3) You need to keep the issues in front of everyone constantly.

These are the principles which will be discussed in this article and this will be done by describing some of the experiences at Alcoa. At Alcoa, there is still a long way to go to achieve the level of commitment which would be liked, but it is believed that in the past few years a significant increase in interest has been achieved and even if we have not got all the support to do what we want, we have managed to get recognition of the problems and support to do something about them.

Alcoa

Alcoa of Australia is 60 per cent owned by the world's biggest aluminium company, the Aluminum Company of America, and 39.25 per cent by Western Mining. In Western Australia bauxite from the Darling Range south of Perth is mixed and refined into alumina at Alcoa's three refineries. The alumina is then shipped to smelters in Victoria and many other locations around the world. In Western Australia we produce over 15 per cent of the world's smelter grade alumina.

In Western Australia, Alcoa has a central mainframe providing more of a database server role to its other systems. At each of its seven locations, there is a large Local Area Network connected to others by the Wide Area Network and running LAN Manager, Windows NT, Mail, UNIX systems and a number of VAX Process Control and CAD systems. There are nearly 2,000 PC workstations connected to the LANs. Alcoa also has a connection to its Victoria Operations and Melbourne Corporate office where they run IBM LAN Manager.

From about two or three years ago, Alcoa has had an increasing interface with its parent company in Pittsburgh, both on a people level and in its computer systems. It now has a direct communication link direct to the USA and consequently the rest of the worldwide organization. This has been particularly promoted through what is called the "coalition team" which is attempting to apply some common standards and enterprise-wide systems across the worldwide Aluminum Company organization. In addition, Alcoa is also connected by various means to a number of external organizations and business partners.

Alcoa encourages people to be innovative, to excel in their work, and to work across organizational boundaries. Looking at its user base, it tends to have a lot of task-oriented people who just want to get the job done and perhaps see controls and restrictions as unnecessary bureaucracy. Some of these people are in senior positions in the organization. Alcoa also has a large number of

Information Management & Computer Security, Vol. 3 No. 2, 1995, pp. 20-26

This article was previously presented as a paper at the IIR IT Security Conference held in Canberra, Australia on 10-11 April 1995.

users who only use the systems now and again – perhaps to register their leave, and do not have the time or need to understand the processes involved in getting access. It is also true to say that despite the company's American parentage, it is very much an Australian company with a typical Australian culture which does not suffer excessive bureaucracy and control. If controls get in the way, then ways will be found around them or pressure brought to bear to change. In the context of the very complex network which has been developed at Alcoa, and with the limited resources available to IT security, it is vital that the support of the entire organization is gained. After all, the company gives the keys of its system to each user in the form of their log-on ID and password, so it relies heavily on their support.

Alcoa also has a company value that says its employees will be honest and responsible. This value has generated the attitude that "if we are honest and responsible why am I being prevented from using this system?" or "why do I need to get approval to access these data?"

History of computer security at Alcoa

In 1980 Alcoa installed ACF2 as its mainframe security system. Its security standards were therefore developed based on the philosophy and limitations of this product, which provided a fairly controlled environment. Where it was desired to handle security in ways not suited to ACF2, various application systems had their own security facility built in. After a while, it tended to be normal to provide additional security inside application systems. Some of these may be a basic registration requirement but others developed into very complex security systems. Today, of course, most client/server systems and other packages bought seem to come with their own security systems.

In the early days, there were various process control systems at each plant and a number of standalone VAX systems. These systems have now been connected to the network due to a need to talk to one another and for users to use more than one of these systems.

With the introduction of the Workstations, Local Area Networks, E-mail, Client Server, UNIX – the environment has grown to a very complex network with most of the company's users accessing many different systems. There is also a demand to access more external systems and for external organizations to access Alcoa's systems.

Unfortunately, although the company's systems are linked, the security systems generally do not talk to one another. The result is that most users have to be registered in many different places and by many different people. Even though the company has tried to standardize log-on IDs, they still have to log-on many times and to maintain passwords in different systems to get to the applications they need.

Identifying the problems

It was obvious from the hassles which were experienced with the administration of security and the comments received that the security processes were not meeting the challenges of the new environment. The company knew of various abuses and practices which tried to bypass its security controls. It was obvious that the problem was not just a user problem, but that the very security process needed to change.

Alcoa needed to make sure that the product and services it provided fitted into the culture of the organization, and satisfied the needs of both management and users. It knew from the problems it was having and the complaints received that it was not meeting those needs. Thus, recognizing that as it went further down the open systems route, these problems were going to get a lot worse, Alcoa commissioned a review of its security systems.

In fact, the company established two projects: an internal review, and as a result of that, a project with a firm of external consultants.

In both projects Alcoa tried to involve as many of its customers as it possibly could, which was an important part of the whole process. Both projects came up with a similar list of problems and issues which customers experienced with the company's implementation and application of security. The first project tried to identify the key elements of the "ideal security system", and the second project tried to identify where Alcoa was in relation to the rest of the world and what products were available to assist it to achieve this ideal system. The second project also identified the computing environment which the company was moving towards, what sort of issues it would face, and what products were available today to help it support the security environment. Unfortunately most of the products did not really meet the requirements, turned out to be vapourware, only partially available, or on the "bleeding edge" of technology.

Another important component of the second project was a risk analysis whereby the company was able to identify the real areas that needed to be protected, and help direct its efforts where they would be of most use to the company.

There were three major benefits from this process:

(1) The real problems were identified as were the issues that were going to affect the customers commitment to security. Without that commitment

Alcoa could not be successful. After all, these are the very people to whom it gives the keys.

(2) Alcoa was able to develop an understanding of its customers' part of the problems and issues and why it needed security. The process used gave them the opportunity to think about the issues, and identify weak links. Their participation in itself helped develop a commitment to solving the problems and building an environment which met the needs of the organization and security.

(3) The company was able to redirect its efforts where they would have most impact, and where the real risks were.

The problems identified were:

- too many log-on IDs and passwords to maintain;
- too many people involved in administering security;
- people did not know who to go to to get the access they needed;
- security administrators did not know who to go to;
- it often took weeks for a user to get all the access needed;
- users did not understand the terminology or how to find out what it was they needed to ask for, and Alcoa often did not understand them;
- although it was OK in 1980, the log-on ID structure itself was not suitable for today's environment. The log-on ID has meaning and that meaning no longer reflects how the organization operates which means it has to establish a lot of individual access rules;
- security administration was often unable to determine all the access any particular user or group of users had, so if Alcoa had to set someone up the same as another user, it could not;
- when people changed departments, they had to get a new log-on ID and generally it meant they lost a lot of the access they needed and had to start all over again;
- a lot of people used the system most of the time to look at data which were not considered particularly sensitive;
- many users had to log-on with their password many times; this in particular was a problem which Alcoa could see getting worse as each new client server system or platform installed seemed to have its own log-on ID/password requirement;
- users had to maintain many passwords across different systems;
- some of the administrative processes, such as an annual clean-up, caused far more opposition than the benefits they achieved.

Building commitment

Obviously, having just identified the problems and issues working against it, if the company was serious about building some sort of commitment, the first place to start would be to rectify the problems. Sounds easy doesn't it? Truth is, the task seemed to be too huge, expensive, risky, and a lot of the effort would have to be directed at old systems. Alcoa recognized the problems, and acknowledged the fact that it needed to do something about them, but what? And what resources could it use?

The second project produced a detailed plan of some things the company needed to do, but one of the major steps – changing the log-on ID structure – proved to be a bottleneck which no one wanted to address and Alcoa pondered over this issue for quite a while.

Behind the scenes life went on and the company was able to develop some useful tools to get around some of the problems, and it continued to develop its plans. It was also able to make use of the contacts it had made in the user community to bounce ideas off, and to promote security as issues arose.

It is believed that the two projects were vital factors in gaining recognition from management of the issues faced in security. The first project identified the issues, and by using external consultants and involving management in the second project, they were able to get a better idea of the size and significance of the work required. The effort, the feedback from customers, the stir it caused, the authority of recognized external consultants, and the cost – both of the projects and potential cost of solutions, certainly worked well in gaining management's attention.

Although management was wary about implementing the whole solution at once, security did get permission to proceed one step at a time and that is just what it is now working on. The first step taken was to develop and ratify the security philosophy, vision, and policies.

Philosophy

The chief executive officer of the parent company, the Aluminum Company of America, made a statement that has had a major impact on the company's attitude to information security. At first glance this statement appears to be against all Alcoa had been doing in computer security. However, for the first time it had a clear direction around which it could base its security policies, practices, and procedures. It was a challenge, but as the company got used to it, it soon discovered it was being led into an environment which would simplify security and help Alcoa to focus on what was important.

The CEO said, "Our objective of giving every Alcoan the information required to excel in his/her work will require a common language and a high degree of interconnected

capability across the company to enable communication and the sharing of knowledge…" …people need much more information than we have typically shared with them. Our habit has been to limit the sharing of information on the grounds that we did not want it to fall into the hands of the competition…I believe that for people to work energetically towards a higher level of performance, they need a fact-based understanding of what is possible. Therefore, we must institute a process for sharing information and knowledge so that everyone will understand what their process is capable of achieving."

Out of this statement, Alcoa developed a philosophy for IT security which said "we will open up access as far as we can within the constraints of good business practice, legal requirements and our obligations to other organizations and people we deal with".

This now enabled the company to focus our security on those things which really needed to be secured and not waste valuable time chasing violations or giving access to things which did not matter. In today's complex computing environment, Alcoa does not have the time or resources to spend on things which do not matter.

Vision

It was critical to the success of security that the company was able to show its customers that it had listened to their feedback, and that it was serious about getting something done. The first step was to develop a vision which could be published and which fitted in with the criteria considered important by the customers.

Alcoa's vision for IT security administration based on the new philosophy and the ideal security system it had developed from its internal security project was therefore: "The security system will appear as though we have just one security system in Alcoa of Australia, irrespective of which platform or application is being accessed or where it is located. Users will have one log-on ID, one password, and normally be required to only log-on once. Basic access will automatically be established and an online access request system will enable additional access to be set up quickly, automatically routeing the request for approval and administration. Complete and easy to interpret audit and violation reports will be readily available".

Security policies

With the new philosophy and vision in mind, Alcoa redeveloped a new computer security policy. The policy has now been issued to all users in a security booklet, which is the first time most of them would have seen a security policy.

The philosophy was readily accepted and, after some negotiation and rework, the company had its security policy accepted by management. Actually, it had been urged by management to soften up the policy in some specific areas, but it then discovered that it had to replace them as various issues arose and apply even tougher policies in some specific areas such as totally banning games on company computer systems.

The exercise of revisiting the security philosophy, vision, and policies required much management input and consequently has helped in raising its interest.

Single log-on and password

Single log-on can mean one of two different things. It can mean everyone will only have one log-on ID, or it can mean that people will only need to log-on once, no matter what it is they wish to access or where it is stored. The company strongly tries to maintain the principle that people will only have one log-on ID, but it also has the goal that people will only have to log-on once.

Unfortunately, Alcoa does not believe the facilities are ready yet for it to achieve this goal. It has, however, developed a method so that users can synchronize their passwords across different platforms, and it insists that all systems use the same log-on ID so it is easier for users to manage their passwords.

The single log-on concept (or log-on once) has now been accepted by the parent company as a requirement for the common infrastructure initiative project.

Standardization

Over the past two years and in particular the past 12 months, a lot of progress has been made in standardizing security across the different platforms and across sites within platforms. Although the administrators of these systems had the same overall standards, Alcoa found that the application of these standards varied. A number of teams have now standardized security profiles, and work is continuing on finding ways to ensure standards are maintained.

Improved administration tools

The company is currently attempting to rationalize its implementation of ACF2, developing user profiles, opening access to inquiry transactions where possible, revising how it groups access rules, using flags in ACF2 to record information about other platforms, and redeveloping the UID structure. This requires a lot of effort, especially as it is trying to apply it behind the scenes so users will not lose access during the process.

A lot of the administration tasks have been centralized, removing unnecessary bottlenecks, although the company still has far too many administrators around. It has tried to change the process so that the requests for access flow through better, the biggest problem here being to find out who administers what. Alcoa has

employed a contractor to automate and redevelop the security administration tasks.

The company has designed and is now in the process of building an online access request system which will be used for anyone requiring access to any computer system. In the meantime, it has tried to improve the process of requesting access by allowing whatever means the user can use (E-mail, scraps of paper, official forms, etc.), so long as it contains the information and authorization needed, and can be filed for auditing.

Alcoa is also looking at the interfaces with its human resource systems, the idea being to grant access automatically based on the job requirements when a user joins the company or is transferred. This is going to take time to implement although ways to improve the use of the human resource systems have been found.

Using management to assist

The first step in gaining management support is to get a sponsor or champion. This person needs to be as high up in the organization as possible and have the ear of both those who make the management decisions for the general running of the organization and also be able to have a real influence on the IT management team. The security team was fortunate to find such a sponsor who has helped it promote security issues and get the approval it needs for its policies and expenses. He was also the representative in the Aluminum Company of America's Coalition team. Unfortunately, this person is now moving on to other pastures so the team is now seeking another sponsor who hopefully will be in an even better position to influence the executive board.

In order to maintain management commitment to security, one should try to make sure they are kept involved. In the early days, the team used to try and take on all the responsibility for security. Now, it just makes sure management is aware of the issues and lets them make a business decision whether or not to accept the risks. That is what they are employed for, and it is much easier on the team.

Management is also involved when there is a problem. The security team is not always aware of other issues which may affect how a problem should be addressed so it works with the relevant manager. For instance, whenever a problem has occurred, or violations indicating a particular problem from a small group of users, the team has always gone through the local management to resolve the issue. It also helps to gauge the commitment of management and to provide authority to security's voice. As an example, recently there was a problem where a contractor was trying to access something which had nothing to do with his job, and would, to most people (except this contractor), be highly suspicious activity. In fact, the parent company picked it up and asked the security team to find out what was going on. Before the team took it up with him, they went to his manager and sought his permission to discuss with the contractor to find out what he was trying to achieve, and also got the manager to follow up afterwards.

Employing external consultants on the security project who have a reputation respected by management, and involving management in the risk analysis and research on the problems with security have had a tremendous effect on getting their support. Security is now finding management making decisions about technology based on the security risks, and seeking the team's assistance and advice, so it has obviously had some effect.

Log-on ID

One of the biggest problems is with the structure of the log-on ID. As already mentioned, the solution for this proved to be a major obstacle to getting management approval for the work the team wanted to do.

There are limitations to the log-on ID because it has meaning in the different fields, and whenever someone changes department or location they need a new one. The structure was designed to suit an environment which no longer exists. The organization is far more flexible than before and people work across and are frequently moved across organizational boundaries.

Unfortunately, the log-on ID has been used by most application systems so any changes need those modifications to be made in a number of old systems. It is the work involved in fixing up these systems which caused management to squirm. Just the task of finding out how much work would be involved was going to be too expensive and difficult. How many systems would need changing? How many different programs used the log-on ID? Was the source code still the same?

Eventually, the decision was made to put this one on hold but to recognize that sooner or later the security team would probably have to go ahead. Maybe it could find an alternative, or maybe it could reduce the workload by other options and seeing if it could do something about the restrictions which were causing problems with the log-on ID.

Over the past year or so, work has progressed to try to remove some of these restrictions. From February this year, the need to change log-on ID for most users no longer exists, unless they work in a particularly sensitive area (such as the personnel department). Hopefully, this restriction should be minimized by the end of the year. Other limitations have also been removed, so a lot of the issues which put pressure to change it have been removed.

Even so, the log-on ID does not conform to Alcoa's Coalition Team standards and, with enterprise-wide systems being introduced, this does present an area of concern as new systems will need to use the new structure. It is likely that Alcoa will use the new standard which will be applied for access to new systems. To ensure users only have to know one log-on ID, wherever possible existing platforms will be changed, except the mainframe where a conversion programme will need to be used to avoid the necessity of changing hundreds of application system programs.

Security awareness initiatives

A lot of time has been spent discussing how Alcoa is trying to improve its security product and services because this is believed to be vital to the whole security awareness programme. The process Alcoa went through has certainly had a major role in building both management and user commitment. Now the initiatives taken will be discussed, which can be described as promotional activities or awareness initiatives.

As already explained, Alcoa has at all times in this process tried to involve as many employees as possible, and to keep them informed as much as possible. It also initiated a number of security awareness ideas to keep the general Alcoa workforce aware of the issues and their responsibilities. These have included presentations, training, booklets, newsletter articles, an electronic newsletter, stickers, MS mail and any other means possible.

Presentations and cheerleaders

Alcoa has tried to get out as much as it can to give presentations on security issues to its user force. It gives regular presentations on what it is doing, security risks, virus control, security procedures, etc. to small groups around the organization and at all locations.

The IT department has deployed a number of information systems consultants at each location and identified a number of key users called "area computing reps". Their main function is to act as interface between the IT department and the general user community, to bring user issues to the department and to help promote its facilities to them. The department regularly reports to them, giving them presentations on a number of security topics.

A lot of the emphasis in the presentations is to show the people what the IT department is, and to show that it understands the issues. It tries to present these in a way that will enable them to give feedback if it had missed the target. An advantage of this process is that, having told them what the department wants to do and got their support for it, they also expect it to do it. So they help keep it on its toes to make sure it does what it says.

It has also been possible to identify a number of managers and system owner representatives around the organization and along with the ACRs, and the IT department's own ISCs, they are called cheerleaders. These people are encouraged, fed information about security and what is being done, listened to in order to have ideas bounced off them, and generally are given some extra support in the hope that they will continue to promote security to their work groups.

There is also an annual IT seminar, at which security presentations or videos are shown.

Training

For some time now, computer security has been included in both in-house computer courses and local induction training. Although these are given by different people, the training is based either on a section of the training manual prepared by the IT department, or through its security booklet which is now given to every new recruit.

Training is also provided by local IS staff on a one-to-one basis where required. To facilitate the training and presentations, some of the commercially available videos have been used. The best thing to say about them is that they are useful when you need a different medium for a change.

Work instructions

At Alcoa, there are what are called work instructions for explaining how to do a particular job or task. Work instructions have been developed and are continuing to be developed on security issues, such as how to prevent and remove viruses. This particular work instruction was produced with the help of some of the users and it was interesting to see the change in their attitude as they pondered the risks and possible solutions. The work instructions are now available online through the LAN.

The IT department has also produced instructions to help users understand how to get access, what to do if they change departments, etc.

Booklets

One of the biggest successes in promoting security at Alcoa has been with a booklet published last year. It has been circulated around the entire Alcoa of Australia organization, and is currently under consideration by the USA for publication worldwide.

So far, the IT department has produced two booklets on security-related issues. There are also a number of booklets published by others which included security, or which are on related issues. The two booklets Alcoa has published are *Copyright*, and *Protecting Company*

Computer Systems. Both booklets have been issued with the help of Alcoa's public relations department.

Protecting Company Computer Systems is a light-hearted look at computer security illustrated by an artist who used to work for Walt Disney. This booklet includes sections on log-on IDs and passwords, virus prevention, software licences, copyright, backups, the need for security, corporate vs. personal computers, and includes a copy of the computer security policy.

The copyright booklet focuses on copyright and is supplemented by copyright warning stickers on publications and near photocopiers, and messages as each user log-ons.

Newsletters

The IT department also utilizes its own IT newsletter and the company newsletters to promote areas of concern or a particular security issue. These newsletters are distributed to all staff who often take them home, so it probably reaches people the department is unable to reach by other means. As an example, the department seemed to be having problems with a particular virus which kept reappearing so it used the newsletter (as well as site personnel) to get the message across to everyone. It has also put in articles about log-on IDs and passwords, security policies, copyright, software licences, etc.

The secret is to aim the article at a level which gets the message across without creating panic.

Multi-media newsletter

A new facility has been developed for Alcoa's public relations department which is called BEN – the Booragoon Electronic Newsletter. This system, which runs on the LAN under Windows, can present information using video pictures, sound, text, and graphics. Security awareness has been included in the initial trial in the form of an animated presentation on viruses based on the security booklet.

E-mail

E-mail is used either when there is a need to communicate to a small group, or when there is an urgent need to encourage everyone to do something. A good example of the use of E-mail is when the department hears of a particular virus (i.e. the Michelangelo scare of a few years ago). Again the department aims to keep it light, as can be seen from our security booklet where we employed a cartoonist to illustrate it.

E-mail is useful in keeping management informed of issues and in getting their support.

Screen savers

The department is also developing a series of screen savers and Windows wallpaper based on the cartoon characters, each with its own simple message.

Problem management

Alcoa's attempts to include management in dealing with any problems that arise have already been mentioned. Sometimes it pays to over-react in order to ensure that the problem gets resolved properly. This has been done with a couple of virus problems. As long as you do not always over-react (i.e. "cry wolf"), it can be an effective tool to promote a particular security procedure such as checking for viruses. It can also help in getting management support for improving the facilities or process.

All problems are reported to Alcoa's "Help desk" and the IT department is informed of security problems (but checks their log just in case something gets missed).

Finally

In summarizing, the need to make sure that you have a product which meets the needs of the organization should be emphasized. Keep people informed, involved, and listen to their problems. Keep the promotion light in content but keep the issues constantly in front of people.

As mentioned at the start of this article, Alcoa has achieved a great deal over the past couple of years but it still has a long way to go. There is excitement about the future – there is so much scope for improvement, so many challenges, opportunities to really do something. Already, people throughout the organization are beginning to help and implement security.

A few years ago, there was some very pessimistic feeling about the IT department, but today people see a great future and look forward to seeing the achievements that will happen over the next few years.

Phil Spurling is IT Security and Business Continuity Co-ordinator, Alcoa of Australia, Western Australia Operations.

This article has been cited by:

1. Ali Farooq, Johanna Isoaho, Seppo Virtanen, Jouni IsoahoInformation Security Awareness in Educational Institution: An Analysis of Students' Individual Factors 352-359. [CrossRef]
2. Jahyun Goo, Myung-Seong Yim, Dan J. Kim. 2014. A Path to Successful Management of Employee Security Compliance: An Empirical Study of Information Security Climate. *IEEE Transactions on Professional Communication* **57**:4, 286-308. [CrossRef]
3. Manmohan Chaturvedi Ansal University, Gurgaon, India Abhishek Narain Singh IIT Delhi, New Delhi, India Manmohan Prasad Gupta IIT Delhi, New Delhi, India Jaijit Bhattacharya IIT Delhi, New Delhi, India . 2014. Analyses of issues of information security in Indian context. *Transforming Government: People, Process and Policy* **8**:3, 374-397. [Abstract] [Full Text] [PDF]
4. Ali Farooq, Syed Rameez Ullah KakakhelInformation Security Awareness: Comparing perceptions and training preferences 53-57. [CrossRef]
5. Shuhaili Talib, Nathan L. Clarke, Steven M. Furnell. 2013. Establishing A Personalized Information Security Culture. *International Journal of Mobile Computing and Multimedia Communications* **3**:1, 63-79. [CrossRef]
6. Guido NassimbeniUniversity of Udine, Udine, Italy Marco SartorUniversity of Udine, Udine, Italy Daiana DusCASSCC, University of Torino, Torino, Italy. 2012. Security risks in service offshoring and outsourcing. *Industrial Management & Data Systems* **112**:3, 405-440. [Abstract] [Full Text] [PDF]
7. Nigel Martin, John Rice. 2011. Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security* **30**:8, 803-814. [CrossRef]
8. Rashad Yazdanifard, Mohammed G. Musa, Tshepo MolamuThe Basics Issues on the Security Information Management Practices in Organizational Environment 1-4. [CrossRef]
9. Ryan T. Wright, Kent Marett. 2010. The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal of Management Information Systems* **27**:1, 273-303. [CrossRef]
10. Caroline Chipperfield, Steven Furnell. 2010. From security policy to practice: Sending the right messages. *Computer Fraud & Security* **2010**:3, 13-19. [CrossRef]
11. Shuhaili Talib, Nathan L. Clarke, Steven M. FurnellAn Analysis of Information Security Awareness within Home and Work Environments 196-203. [CrossRef]
12. Aggeliki Tsohou, Spyros Kokolakis, Maria Karyda, Evangelos Kiountouzis. 2008. Investigating Information Security Awareness: Research and Practice Gaps. *Information Security Journal: A Global Perspective* **17**:5-6, 207-227. [CrossRef]
13. Namjoo ChoiInformatics, State University of New York at Albany, Albany, New York, USA Dan KimComputer Information Systems, University of Houston-Clear Lake, Houston, Texas, USA Jahyun GooInformation Technology and Operations Management, Florida Atlantic University, Boca Raton, Florida, USA Andrew WhitmoreInformatics, State University of New York at Albany, Albany, New York, USA. 2008. Knowing is doing. *Information Management & Computer Security* **16**:5, 484-501. [Abstract] [Full Text] [PDF]
14. Aggeliki TsohouDepartment of Information and Communication Systems Engineering, University of the Aegean, Karlovasi, Samos, Greece Spyros KokolakisDepartment of Information and Communication Systems Engineering, University of the Aegean, Karlovasi, Samos, Greece Maria KarydaDepartment of Information and Communication Systems Engineering, University of the Aegean, Karlovasi, Samos, Greece Evangelos KiountouzisDepartment of Informatics, Athens University of Economics and Business, Athens, Greece. 2008. Process-variance models in information security awareness research. *Information Management & Computer Security* **16**:3, 271-287. [Abstract] [Full Text] [PDF]
15. Seppo Pahnila, Mikko Siponen, Adam MahmoodEmployees' Behavior towards IS Security Policy Compliance 156b-156b. [CrossRef]
16. Robert Willison, James Backhouse. 2006. Opportunities for computer crime: considering systems risk from a criminological perspective. *European Journal of Information Systems* **15**:4, 403-414. [CrossRef]
17. H.A. Kruger, W.D. Kearney. 2006. A prototype for assessing information security awareness. *Computers & Security* **25**:4, 289-296. [CrossRef]
18. Jeffrey M. Stanton, Kathryn R. Stam, Paul Mastrangelo, Jeffrey Jolton. 2005. Analysis of end user security behaviors. *Computers & Security* **24**:2, 124-133. [CrossRef]
19. Mikko T. SiponenUniversity of Oulu, Department of Information Processing Science, Finland. 2000. Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice. *Information Management & Computer Security* **8**:5, 197-209. [Abstract] [Full Text] [PDF]
20. Mikko T. SiponenUniversity of Oulu, Department of Information Processing Science, Finland. 2000. A conceptual foundation for organizational information security awareness. *Information Management & Computer Security* **8**:1, 31-41. [Abstract] [Full Text] [PDF]

21. Shuhaili Talib, Nathan L. Clarke, Steven M. FurnellEstablishing a Personalized Information Security Culture 53-69. [CrossRef]
22. Daniel Oost, Eng K. ChewInvestigating the Concept of Information Security Culture 1-12. [CrossRef]
23. J.M. Stanton, K.R. Stam, I. Guzman, C. CaledraExamining the linkage between organizational commitment and information security 2501-2506. [CrossRef]
24. S.J. Marcinkowski, J.M. StantonMotivational aspects of information security policies 2527-2532. [CrossRef]