Constructing Positive Influences for User Security Decisions to Counter Corporate or State Sponsored Computer Espionage Threats

Martyn Styles

University of South Wales Pontypridd, Glamorgan, CF37 1DL, UK
03157210@glam.ac.uk, martyn.styles@ntlworld.com

Abstract. This paper presents an analysis of employees' security behavior, which focuses upon improving user awareness to counter computer espionage attempts by corporate or state sponsored activity. The author examines existing literature, presents the results from initial experiments in security awareness and proposes further work.

Keywords: Security awareness, user behavior, APT, corporate espionage, employee psychology, social engineering.

1 Introduction

Already, 2013 is shaping up to be another significant year for computer security breaches. Apple, Microsoft, Facebook, The New York Times, NBC and Evernote have all succumbed to computer hacking in the first months of this year. Almost universally, they appear to be the result of weaknesses in employee security behavior. Since 2007, the perceived rise in state or corporate espionage (as designated by the modern term 'Advanced Persistent Threats' or APTs) has caused many firms to consider the type of activities they are engaged in and the likelihood of them being a target for long-term malicious activity. A significant proportion of current academic literature ignores the psychological aspects of computer security. This research paper has been undertaken in part to address this shortfall with the aim of reducing the risks of corporate espionage. Why is it that most computer users feel an overwhelming urge to open suspicious email, access a URL sent to them by an unknown 'friend', open the attachment that they were not expecting but which appealed to their curiosity, or to click on a pop-up message telling them to "Update your anti-virus software now!" when they open a web page? Research into this kind of human 'herd mentality' has been clearly shown to affect social networks (Onnela and Reed-Tsochas, 2010). Onnela and Reed Tsochas analyzed Facebook applications from 2007 during a period when the site allowed friends to alert each other when they installed an application. Their research clearly highlighted a pattern of social influence that compelled users to follow their friends in tendency of installing common applications. When a Facebook

L. Marinos and I. Askoxylakis (Eds.): HAS/HCII 2013, LNCS 8030, pp. 197–206, 2013.

user generated an alert to their friends by installing an application, there was an implied endorsement of the application's features and benefits which tended to lead recipients of the alert to install the application themselves; even though their friend may have already uninstalled the application after finding it unsuitable or worthless. Similarly, computer hackers have begun utilizing methods that imply recommendation from others to persuade targets to install rogue software such as malicious imitation anti-virus programs (FakeAV), which attempt to fool users into fraudulent purchases. Cognitive dissonance causes the subjects confusion when faced with on-screen choices that imply required obedience, by the implication that installing an application is mandatory behavior that is expected of them. Obedience and a willingness to conform help to re-enforce that behavior to the benefit of the criminals who manufactured the fake software.

Corporate security officers may rely on technology to secure their network infrastructure, but this ignores the fundamental issue of human vulnerabilities, which exist in every organization. The focus of this research on analyzing end-user security behavior in order to address the growing number of corporate or state sponsored computer espionage threats. The U.K government office of the Centre for Protection of National Infrastructure (CPNI), a commercial subset of the intelligence service M.I.5, has recently provided advice to professional services firms for recognizing APT-type behavior since they recognize that these businesses are increasingly likely targets of state sponsored espionage. This is because it is recognized that finance and government organizations generally spend large amounts of budget on security measures, whereas professional services firms may be lacking the necessary resources and inclination for comprehensive security controls. The author of this research paper is employed by an international law firm, as an information security professional. Both in the U.S and in U.K, since 2011, there have been regular meetings with InfoSec representatives from all the major law firms together with security professionals from financial and international corporate organizations, in response to the rise in global corporate hacks. This is an attempt to address the human weaknesses in corporate data security.

2 Research Hypothesis

The proposition of this research is that through critical analysis and modeling of employee computer security behavior, security professionals will be able to identify and positively influence user security decisions to counter the threats of corporate or state sponsored computer espionage.

Do end-users really care about information security? In most industries, end-users often subscribe to the view that information security is 'someone else's problem'. This can lead to somewhat reckless behaviour – for example when surfing the Internet. The information security industry needs to understand its users much more if they are ever going to be in a position to dramatically reduce human-aspect security incidents. Examining corporate or state sponsored computer espionage is a challenge to researchers because proving the hacker's origin and motivation is inherently difficult. Hackers commonly utilise multiple jump-box hosts and encrypted VPN tunnels (such as the notorious Tor network) to hide their geo-location. Hackers may work alone or with others and may be motivated by money, a quest for fame or allegiance to a business or country. This research project examines hacker activity through the analysis of employee workstations that have been subject to attack and by investigations of infection patterns through corporate anti-malware technologies. Contacts with other corporate information security officers will enable comparisons to be made across industries and co-operative research with a major anti-malware vendor is planned. Global firms with international offices in Russia, China and France have the potential, according to meetings held with the U.S & U.K security services, to be compromised by state or corporate sponsored espionage.

3 Psychological Factors Influencing User Security Behavior

People often believe that they are in full control of the computer that sits in front of them. However, although the computer system may appear to function at the behest of the user, many aspects of computer activity may be beyond the user's control or cognitive understanding. Current research into computer user behaviour, particularly by Eirik Albrechtsen (Albrechtsen, 2007) and Jeffrey Stanton (Stanton et al., 2005), indicates that there is still a long way to go to improve end user security behaviour. Corporate or state sponsored criminal activity is extremely difficult to detect if users are not motivated to identify and stop it. This is because technological protections are quite often far too restrictive towards genuine business activity, leading to a condition in which security systems, which may have been used to prevent data egress, are simply either turned off or put into audit or monitor-only mode. Security managers, across different business sectors, have confirmed that installed Data Loss Prevention (DLP) systems are often not used, because to do so would prevent essential routine file movements inside and out of the organisation. Other security managers stated that their DLP systems are permanently set for Data Loss Detection i.e. audit only mode rather than blocking. David Lacey (Lacey, 2009) analysed the security structures of corporate enterprises and found them to be severely lacking in sophistication and effectiveness.

- **Motivation.** Employee motivation towards information security is a key factor in helping to protect corporate assets. Psychological homeostasis, which is when a state of mind is reached where the subject feels that they have attained equilibrium, can also be applied to user security behavior. A lack of homeostasis can cause people to feel be disillusioned if they feel that they are not motivated enough, and in terms of behavior they may feel that security is of no interest to them because they are divorced from the effects of any negligent or naive behavior which may lead to security incidents. Research into computer user behavior by Albrechtsen (Albrechtsen, 2007), (Albrechtsen and Hovden, 2009) and Kruger (Kruger and Kearney, 2006) has stimulated thought on some of the motivational aspects of security awareness. Indeed, Albrechtsen asserts that most 'users consider other work demands as more important than information security tasks in the day-to-day operation of the organization'(Albrechtsen and Hovden, 2009). Other researchers, among them Jeffrey Stanton (Stanton et al., 2005) (Stanton and Stam, 2006) and Donn Parker (Parker, 2002), also consider the motivation of users for computer security through empirical research amongst the information security community. Parker is particularly interested in the relative inequalities of the resources and motivation of hackers, compared with security managers, in the 'cat and mouse' war of control over an organization's information assets. Articles by Angela Sasse et al. (M A Sasse, 2001) (M. Angela Sasse, 2007) (Inglesant, 2010) argue that user motivation for the typical password based security mechanisms that most organizations use for authenticating users to systems needs to be improved because social engineers like Kevin Mitnick (Mitnick and Simon, 2002) commonly exploit user preferences for simplistic password choice.

- **Obedience.** Most organizations define acceptable use policies and best practice guidance to ensure that employees do not abuse the privileges they enjoy when using company equipment. Just how obediently employees follow these rules and regulations is an interesting area for investigation. A number of experiments in the 1960's and 1970's investigated the obedience traits in humans. These experiments provide us with an insight into the way people react to orders, and how in the area of computer security, we can begin to understand why users may cause security incidents through negligent actions. The Milgram experiments (Milgram, 1974) demonstrated that participants willingly administer apparently painful electric shocks to fellow participants if they believe that compliance is required through an order issued by a figure of authority. Similar to Milgram's experiments, the Hofling experiment (Hofling, 1966) studied the effects of authority (an impatient doctor) on nurses in charge of patient drug administration. It was found that 95 percent of nurses would administer dangerous doses of medication when demanded by a doctor. These two sets of experiments emphasize the lengths to which humans may go in order to comply with perceived authority. This also seems to be the case with the example of 'The Third Wave' experiment. In this experiment, school children were inducted into a neo-Nazi movement by their history teacher, as a means of explaining the apparent willingness of the German populace to participate in Nazi atrocities. Although this experiment was performed on school children and was poorly documented (Leler, 1967), it is a valuable commentary on obedience. The six day 1974 Stanford Prison Experiment (SPE) (Zimbardo, 2007) and the BBC Prison Study (Reicher, 2006) showed that group behavior bordering on sadism could be produced by simply arbitrarily designating 'prison guards' and 'prisoners'. The key to understanding computer security behavior may lie in user attitudes to obedience; Do employees willfully open malicious email attachments as a way of defying the obedience required by the organizations IT policies?
- **Cognitive Dissonance.** The theory of cognitive dissonance, which states that the mind becomes confused when trying to assess conflicting ideas, was defined by the psychologist Leon Festinger (Festinger, 1957). Cognitive dissonance can used by social engineers (Hadnagy, 2011) to their advantage and malware writers can

use it to cause target employees confusion and uncertainty which leads to them unwittingly installing malicious software on company computers. This phenomena has been witnessed many times in many organizations when users receive emails which claim to come from genuine individuals or companies, but which turn out to be counterfeit and contain either malware or links to malicious websites. Recipients tend to believe the messages unless the forgery is particularly poor and will execute the attachments and install the malware. Because such messages often zero day executable code, which is unrecognized by anti-virus vendors, the only way to stop them reaching their intended targets is to block all messages containing executable code. Malware analysis websites such as VirusTotal.com and ThreatExpert.com can be used to evaluate unknown code – in the same way as the malware writers, who use these websites to see if AV vendors recognize their code as malicious! Cognitive dissonance, which results from the receipt of a malicious email that claims to contain a genuine security update, is difficult for end users to resolve. Unfortunately, the action of blocking all incoming executable code can have a business impact because genuine emails are also stopped.

- **Automatic Social Behavior.** Automatic social behavior is a relatively new area of psychology that explores the influences that compel individuals to exhibit behaviour that verges on automaton-like actions, through peer pressure inferred by online friends or acquaintances. A number of papers, particularly by John Bargh (Bargh, 1989) (John A. Bargh, 1996) and Ap Dijksterhuis (Dijksterhuis, 2000, Ap Dijksterhuis, 2001) together with Joseph Cesario (Cesario et al., 2006), have established this phenomenon as a valid area of psychological research. Researchers argue that humans use inaccurate mechanisms to justify their self knowledge and identified the presence of automatic behaviour in the misattribution of decisions which would lead them towards a particular objective (Bar-Anan et al., 2010). This is an interesting theory because it is recognised that sometimes users will give inconsistent reasons for errant security behaviour based on their perceived objective. For example, an employee who forwarded confidential information onto a gossip website may justify their actions by claiming that the information is already common knowledge amongst their peers both inside and outside the company rather than admitting that they had done any wrong, even though the document was marked ‘Company confidential - Do not forward outside’. The temptation to automatically forward confidential information to personal email accounts, webmail accounts or file-sharing sites is often too much for staff to resist.
- **Probability Neglect.** Jonathan Baron (Baron, 2008) and Cass Sustein (Sunstein, 2002), (Sunstein, 2009) delve into the phenomena exhibited by the human trait of probability neglect which leads individuals to make irrational decisions based on an inability to believe that a series of events will result in a particular outcome, either negative or positive. This is particularly interesting for information security when the number of security incidents is a growing trend – this may explain why users ignore the warning signs leading up to a security incident because they feel immune from security issues. Users may cite a naive “It will never happen here,” or “It’s someone else’s problem” in response to appeals for security vigilance.

- **Risk.** Risk homeostasis (Wilde, 1982), could help to explain the reason for naive or negligent computer security behaviour. Risk homeostasis would apply because users feel they are protected from Internet threats through the organization's security defences, and therefore will take risks such as visiting potentially dangerous parts of the web or wilfully clicking on obviously unsafe website elements. Risk management is a key topic in the information security industry. CISO's and information security officers are increasingly asked to provide management with tangible evidence of security vulnerabilities and capable threat agents before budgets for security solutions are released (Gerber and Vonsolms, 2005).
- **Mistake.** People make mistakes. A number of information security managers and CIO's that were approached agree that a commonly held belief in the fallibility of IT users is expected and that employees are bound to make mistakes that lead to security incidents. Travis and Aronson's book (Tavris, 2007) provides insight into the paradox that users face when accused of mistakes at work. This is a particularly interesting area for information security research because of the link between simple mistakes and security incidents. An unintentional confidential email sent by mistake to an unauthorized third party being a prime example. In April 2010, Gwent police sent a plain text Excel spreadsheet containing over ten thousand names and addresses from a confidential Criminal Records Bureau (CRB) disclosure, which included 863 people who had been in trouble with the police, to the technology website 'The Register' (Williams, 2010). The email address of The Register had been saved in the sender's email address list after The Register had previously been in contact with Gwent police over a Freedom of Information request. In September 2011, an article in WIRED online magazine (Vetter, 2011) indicated that two researchers managed to capture 20 gigabytes of misdirected data via doppelgänger Fortune 500 domain registrations - users had simply mistyped the real domain names and forwarded confidential data to the doppelgänger domains! Clearly, something has to be done to reduce end user mistakes such as these.
- **Self-Control Reserve Depletion.** Preserving an element of self-control is required by employees to counter the conflicting information that they may experience, for example, following the receipt of a malicious email or perhaps the compromise of their work computer by Fake Antivirus infection. Cognitive resource depletion may be experienced by employees as a result of the bombardment of inaccurate information from malicious sources leading to perception corruption and the inability of users to make rational security decisions. In these instances, infiltration of an enterprise by Advanced Persistent Threats is possible. If the method of infection is designed in such a way that recipients are not alerted, and the Trojan code is utilized in a stealth manner, the infiltration of an organization can go unnoticed for months if not years. The 2011 Google (Operation Aurora), Sony PlayStation and RSA hacks were perpetrated through the compromise of the computers of low privilege users. The hackers slowly escalated their privileges through the infection of subsequent computers and user accounts throughout the organizations own internal networks. Those low privilege computer users were targeted as a doorway into a fortified network protected by multiple technological defense systems.

4 Neuro Linguistic Programming and Social Engineering Defense

Neuro Linguistic Programming (NLP), credited to Richard Bandler and John Grinder (Bandler et al., 1990) and based on earlier work by Milton H. Erickson, has been used by some recent authors to explain the uncanny ability of some social engineers to elicit confidential information from targets. Mann (Mann, 2008) and also Brown (Brown, 2006) identify how NLP may be used by talented social engineers to compromise security. It is an interesting challenge to educate employees, particularly reception staff, about the possible use of NLP in the perpetration of social engineering attacks. Few academic and commercial articles currently address social engineering defense strategies, most simply exist to glamorize the life of a social engineer, with Kevin Mitnick (Mitnick and Simon, 2002) and Frank Abagnale Jr. (Abagnale and Redding, 1980) being the most notorious examples. Recent publications by Mann (Mann, 2008) and Hadnagy (Hadnagy, 2011), however, have a number of interesting ideas including sections on interpreting and rejecting attempts by social engineers to use NLP-type techniques on unsuspecting targets.

5 Method and Metrics

Measurements will be made through a combination of online surveys, social engineering experiments and observed end-user behavior (monitored at user workstations and through Internet gateway traffic analysis). Measurements of existing technical solutions will be performed through statistical analysis of data gathered from enterprise anti-malware systems, together with APT analysis through code sandboxing and Command and Control ‘phone home’ monitoring. The number of virus and Trojan horse infections on machines within a global corporate enterprise are a key metric compared with the number of malicious files received through email and web channels. These statistics help to identify the number of compromised machines on the network.

6 Security Awareness Experiments

Security Questionnaire. As part of an initial experiment, a Survey Monkey (www.surveymonkey.com) questionnaire was designed according to the standards set by the Social Psychology Network (www.socialphychology.org), which is available as an academic resource for online psychological testing. Participants were sought through professional LinkedIn contacts (www.linkedin.com) and links to the survey were published via the Social Psychology Network website and Twitter (www.twitter.com). Over the two-month period that the survey was open, a sample of 73 people started the survey and 49 (67.1%) completed all the questions. All the answers were anonymous and only a log of IP addressed of responds was retained. The participants were mostly a purposeful self-selection biased sample because it was determined that there was a need to test out some of the question formats and the questionnaire design, on a reasonably mature and co-operative audience. The demographic of participants were a cross-section drawn from both senior staff and professional level members of society, together with those participants who arrived at the survey via the Social Psychology Network website and who were interested in taking psychological surveys. An experiment was designed using an online survey website to evaluate user attitudes in relation to some of the security behaviors under investigation. Subject areas investigated included some of the topics identified as areas of interest: Automatic Social Behavior, Motivation for security objectives, Mistake and Cognitive Dissonance. Extensive questionnaires and spear phishing experiments are planned for 2013 to build on the results of the initial test.

Tiger Team Social Engineering Exercise & Results. Given the current industry focus on Advanced Persistent Threats it was decided that an evaluation of employee reaction to unknown/untrusted USB devices was necessary. Tiger (or Red) Team exercises attempt to test the security of an organization by breaching physical barriers through social engineering and other such methods of entry. Custom benign malware was developed which would initiate a ‘phone home’ event when a USB memory stick was plugged into a corporate workstation. Devices were also posted to staff working in the UK, France and Morocco, along with bogus letters, using office contact details found during Internet reconnaissance. The consultant retrieved target contact details though a fake LinkedIn account linked to the company name. Within days, 17 employees confirmed a connection with the fake id, which demonstrates that people do not routinely check the legitimacy of online curriculum vitaes. The professional social engineer, dressed in business attire, successfully infiltrated the corporate office building and dropped compromised devices in high footfall areas of the building. Three days later, several USB devices containing the custom malware were handed in to the security department as suspicious items. Investigations through the centralized USB device management console reports showed that six employees had attempted to execute the malicious content on the USB sticks, but had been blocked from doing so by the corporate USB device policy which prevents executable code from running from USB. The results of the exercise were reported to the company Risk Committee and actions were planned to improve employee security awareness when dealing with suspicious USB memory sticks.

7 Conclusion

Research carried out to date has demonstrated that there is a clear need for further work in the field of end user security behaviors. Analysis of the current literature available on the security behavior of users has established that there is still much work to be done to reduce the impact of negligent or compromised user activity. The experiments conducted this year have demonstrated that even users who have been schooled in good security behavior may still act in negligent ways, which potentially increase the risks to the organization. There is still much work to be done in the area of user security awareness - since 2010 multiple corporate businesses began identifying long-term and extensive hacking incidents. Technology alone cannot protect organizations because in order to function as a business there is a need for users to maintain some autonomy in the actions they perform on information systems. New and flexible ways of working, including mobile communications, Bring Your Own Computer/Device (BYOC/BYOD) and Cloud applications/data management will undoubtedly require even more considered and appropriate user behavior if information is to be kept confidential. Security-educated employees should be motivated, able to recognize computer espionage attempts, and capable of alerting the presence of anomalous computer activity to their in-house information security or incident response team. This will consequently reduce the possibility of corporate cyber-crime success.

References

1. Abagnale, F.W., Redding, S.: Catch Me If You Can: The Amazing True Story of the Most Extraordinary Liar in the History of Fun and Profit. Edinburgh, Mainstream (1980, 2003)
2. Albrechtsen, E.: A Qualitative Study of Users' View on Information Security. Computers & Security 26, 276–289 (2007)
3. Albrechtsen, E., Hovden, J.: The Information Security Digital Divide Between Information Security Managers and Users. Computers & Security 28, 476–490 (2009)
4. Ap Dijksterhuis, J.A.B.: The Perception-Behavior Expressway: Automatic Effects of Social Perception on Social Behavior. Advances in Experimental Social Psychology 33, 1–40 (2001)
5. Bandler, R., Grinder, J., Andreas, S.: Frogs Into Princes: The Introduction to Neuro-Linguistic Programming. Enfield, Eden Grove (1990)
6. Bar-Anan, Y., Wilson, T.D., Hassin, R.R.: Inaccurate Self-Knowledge Formation as A Result of Automatic Behavior. Journal of Experimental Social Psychology 46, 884–894 (2010)
7. Bargh, J. A.: Conditional Automaticity (1989), http://Books.Google.Com/Books?Id=Ht6ddclz6eac&Lpg=Pa3&Ots=Db9yj_Q5ai&Dq=CognitionAttention&Lr&Pg=Pr4V=Onepage&Q=Cognition%20attention&F=False
8. Baron, J.: Thinking and Deciding. Cambridge University Press, Cambridge (2008)
9. Brown, D.: Tricks of the Mind. Channel 4 Books, London (2006)
10. Cesario, J., Plaks, J.E., Higgins, E.T.: Automatic Social Behavior as Motivated Preparation to Interact. J. Pers. Soc. Psychol. 90, 893–910 (2006)
11. Dijksterhuis, A.: On The Relation Between Associative Strength and Automatic Behavior. Journal of Experimental Social Psychology 36, 531–544 (2000)
12. Festinger, L.: A Theory of Cognitive Dissonance. Evenston, Row Peterson (1957)
13. Gerber, M., Vonsolms, R.: Management of Risk in the Information Age. Computers & Security 24, 16–30 (2005)
14. Hadnagy, C.: Social Engineering: The Art of Human Hacking. Wiley (2011)
15. Hofling, C.: An Experimental Study of Nurse-Physician Relationships. Journal of Nervous and Mental Disease, 171–180 (1966)
16. Inglesant, P.S., Angela, M.: The True Cost of Unusable Password Policies (2010)

17. John, A., Bargh, M.C., Burrows, L.: Automaticity of Social Behavior: Direct Effects of Trait Construct and Stereotype Activation on Action. Journal of Personality and Social Psychology 71, 230–244 (1996)
18. Kruger, H., Kearney, W.: A Prototype for Assessing Information Security Awareness. Computers & Security 25, 289–296 (2006)
19. Lacey, D.: Managing the Human Factor in Information Security. John Wiley and Sons, Ltd. (2009)
20. Leler, R., Bernice, S.: Through the Tiger's Eye. The Catamount 11, 2 (1967)
21. Sasse, M.A., Brostoff, S., Weirich, D.: Transforming the 'Weakest Link' — A Human/Computer Interaction Approach to Usable and Effective Security. Bt. Technol. J. 19(3), 122–131 (2001)
22. Angela Sasse, M., Ashenden, D.: Human Vulnerabilities in Security Systems. Cyber Security Ktn White Paper (2007)
23. Mann, I.: Hacking The Human: Social Engineering Techniques and Security Countermeasures. Aldershot, Gower (2008)
24. Milgram, S.: Obedience to Authority: An Experimental View. Pinter & Martin, London (1974, 1997)
25. Mitnick, K., Simon, W.L.: The Art of Deception: Controlling the Human Element of Security. Wiley, New York (2002)
26. Onnela, J.P., Reed-Tsochas, F.: Spontaneous Emergence of Social Influenc in Online Systems. Proceedings of the National Academy of Sciences (2010)
27. Parker, D.B.: Motivating The Workforce to Support Security Objectives: A Long Term View (2002)
28. Reicher, S.D., Haslam, S.A.: Rethinking The Psychology of Tyranny: The Bbc Prison Study. British Journal of Social Psychology, 1–40 (2006)
29. Stanton, J., Stam, K., Mastrangelo, P., Jolton, J.: Analysis of End User Security Behaviors. Computers & Security 24, 124–133 (2005)
30. Stanton, J.M., Stam, K.R.: The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets-Without Compromising Employee Privacy or Trust. Information Today, Medford (2006)
31. Styles, M., Tryfonas, T.: Using Penetration Testing Feedback to Cultivate An Atmosphere of Proactive Security Amongst End-Users. Information Management & Computer Security 17, 44–52 (2009)
32. Sunstein, C.R.: Probability Neglect: Emotions, Worst Cases and Law (2002)
33. Sunstein, C.R., Richard, A.Z.: Dreadful Possibilities, Neglected Probabilities (2009)
34. Tavris, C., Elliot, A.: Mistakes Were Made (But Not By Me): Why We Justify Foolish Beliefs, Bad Decisions, and Hurtful Acts. Harcourt, Orlando (2007)
35. Vetter, K.: E-Mail Typos Result in 20gb of Stolen Data. Wired (2011) `http://Edition.Cnn.Com/2011/Tech/Web/09/09/Email.Typos.Stolen.Data.Wired/Index.html` (accessed September 9, 2011)
36. Wilde, G.: The Theory of Risk Homeostasis: Implications for Safety and Health. Risk Analysis 2, 209–225 (1982)
37. Williams, C.: Police Send Reg Hack Crb Check Database - Massive Security Breach Prompts Investigation. The Register (2010), `http://www.Theregister.Co.Uk/2010/04/16/Gwent_Police_Data/` (accessed September 2011)
38. Zimbardo, P.G.: The Lucifer Effect: How Good People Turn Evil. Rider, London (2007)