Cyber Security

Knowledge Transfer Network

Knowledge Transfer Networks
A DTI business support solution
Delivered through the Technology Programme

HUMAN FACTORS WORKING GROUP COMPLEMENTARY WHITE PAPER

To Err is Human, to Design-Out Divine

Reducing Human Error as a Cause of Cyber Security Breaches

Costis Koumpis, Graham Farrell, Andrew May, Jen Mailley, Martin Maguire, Vaia Sdralia

Contents

Abstract

This paper is presented as a complement to the White Paper 'Human Vulnerabilities in Network Security'. We focus upon ways of reducing the potential for human behaviours that play a role in breaches of cyber security. The paper begins by outlining types of human error and the various forms of cyber security breaches relating to human error. We present the 25 techniques of situational crime prevention, a cornerstone of the fields of security and crime prevention, as a heuristic device that assists the understanding of the mechanisms by which cyber crime can be prevented or its damage reduced. Three case studies of areas where human error plays a role in breaches of cyber security are analysed and modelled. These are a) fraudulent 'social engineering' whereby confidence tricksters gain access to critical security information, b) phishing attacks in e-commerce, and c) 'accidental' data disclosure by employees. In each instance, an effort is made to link the discussion to the framework of situational crime prevention. A section discussing ways of improving the implementation and increasing the adoption of cyber security follows. The paper concludes with suggestions for further research.

1. Introduction

Cyberspace is the metaphorical space of computer systems and networks. It started off as a place for electronic data storage and online communication for scientists but it is now being accessed by over a billion users worldwide. In the early days of cyberspace, far fewer users were attempting to exploit the gaps in technology and social trust. However, the rapid growth in the number of users, hosts, web sites and means of connectivity as well as the increasing role that cyberspace is playing in everyday life (personal, technical and financial) has made such exploits much more lucrative. While some users may passively or actively accept the requirement for security, others actively seek to close or circumvent it where it reduces performance (inconvenient security). One of the reasons is that many have not yet adjusted their perception of non-traditional security threats. Security risks can be generated by accidental, inadvertent or deliberate misuse by users, which is distinct from (though related to) the threat generated by overt attacks. Interestingly, as technologies are maturing (e.g. cryptographic algorithms), these are becoming less of a target. Instead, users are considered as the weakest link[1] and have become a primary factor in cyber breaches.

Security risks can be generated by accidental, inadvertent or deliberate misuse by users, which is distinct from (though related to) the threat generated by overt attacks.

There are many permutations of circumstances and conditions under which humans can make erroneous decisions that lead to breaches of cyber security. Several types of human error have been identified and studied. Errors can be caused as a result of ignorance, lack of knowledge and experience, but humans with

1 B. Schneier. Secrets and Lies. John Wiley and Sons, 2000.

knowledge can also make poor and incorrect decisions. While creativity, adaptability, and flexibility are human strengths, constant alertness and precision in action or memory are our weaknesses.[2] Conditions that increase the likelihood of error can be specified in advance and include cases when humans are idle, tired, uncaring, and apathetic. Humans can also be distracted, fooled, persuaded, manipulated, bribed and blackmailed. The natural tendency to interpret partial and noisy information — although often our prime virtue linked to creativity and robustness — can lead users to produce errors.

There are two main approaches for strengthening the user link: a) teach the user how to do the right thing and b) prevent the user from doing the wrong thing. Both approaches have an important role to play, but also have their limitations. The education and training of humans will always remain a critical component of data management because if they are unaware of security issues, they might inadvertently undermine available protection. Usability experts have argued though against relying too much on user education.[3] In their view, it wrongly places the burden on the user, since the problem originates from the technical layer. User education should be seen as a last resort for existing secure applications with poor usability that are mission-critical (e.g. for military systems). However, one should not expect a home user to have received previous training or be willing to do so.

There are two main approaches for strengthening the user link: a) teach the user how to do the right thing and b) prevent the user from doing the wrong thing.

Preventing the potential for human error can be achieved by designing it out earlier, ideally at the system design phase. Behavioural psychologists have a useful aphorism: 'It is easier to act yourself into a new way of thinking, than to think yourself into a new way of acting'. Design features that eliminate or minimise human error lead, in turn, to further good practice. This approach underpins many efforts in ergonomics where design can significantly influence human behaviour (office chairs which encourage good posture may lead, in turn, to users seeking good posture more generally) or accident prevention (speed bumps create a more general awareness of the risks of speeding in residential areas). Designing-out human error can also reduce risks due to deliberate deception. For instance, administrator-only modification and execution of critical software components, and cut down versions of operating systems can help minimise security breaches.[4] At one time it was necessary for humans to actively load anti-virus software and updates. These security practices are now typically automated, thus designing-out the many possible routes for human error to introduce risk into the system.

2 D. A Norman. Design rules based on analyses of human error. Communications of the ACM, Vol. 4, pp. 254-258, 1983.
3 J. Nielsen. User education is not the answer to security problems. Alertbox, 2004.
4 B. Cheswick's keynote at the 1st Symposium on Usable Privacy and Security (SOUPS 2005) proposed 'Windows OK': a stripped down version of the operating system to suit the large number of computer who just need basic Internet access.

2. Types of Human Error

The study of human decisions in the event chains resulting in industrial accidents provides a useful framework for considering those decisions which result in cyber security breaches. This section draws upon the typology developed by James Reason which makes the distinction between errors and mistakes.[5] Errors are, in essence, a failure to follow a plan. The two types of error are slips and lapses. Slips are defined by execution failure such as, for example, being distracted and attaching the wrong document to an email. Lapses result from human memory storage failure such as, for example, forgetting to log-off a computer over lunch which facilitates its misuse. Mistakes result when the plan is followed but the plan is inadequate, such as responding to an email that appears to come from a legitimate source.

Jens Rasmussen's Generic Error Modelling System (GEMS) classification, which attempts to understand the origins of human error, is applied later in the paper to specific areas of cyber security breaches.[6] The different error types relate to levels of human performance:

- Skill-based: familiar, automatic procedural or subconscious tasks, e.g. typing a password.
- Rule-based: tasks approached by pattern matching from a set of internal problem-solving rules e.g. “If my bank sends me a message I will respond.”
- Knowledge-based: tasks approached by reasoning from first principles, when rules and experience do not apply, e.g. sending sensitive data to a home email address, not realising that the network connection was less secure than the corporate network.

Since it takes relatively few forms, human error is arguably predictable.

Since it takes relatively few forms, human error is arguably predictable. Reason argues that the ‘fallible machine’ or human brain consists of the working memory and the knowledge base. Although the knowledge base can be increased to some extent by training and practice, working memory can not be. Instead, the sensible approach is to acknowledge that storage failure will occur, and mechanisms should be designed-in to both lessen the frequency of harmful decisions being allowed to continue, and lessen the impact of those which can not be avoided.

If cyber security breaches are the results of an event chain, then the application of Reason’s argument would imply that the resultant adverse event is due in most instances to a combination of an active error or mistake by the user, and latent conditions within the system or procedures involved. Crime occurs when a likely offender interacts with a suitable target in the absence of a capable guardian. It is very difficult to influence the motivation of offenders, but it is possible to influence both the suitability and frequency of targets as well as

5 J. Reason. Human Error. Cambridge University Press, Cambridge, UK, 1990.
6 J. Rasmussen. Information Processing and Human-Machine Interaction. North-Holland, New York, 1986.

the capability and frequency of guardianship. Hence crime, including breaches of cyber security, can be reduced by altering the opportunity for, and environment within which, it can occur. Where cyber security breaches result from a combination of active user errors and latent conditions, and if humans are inherently difficult to alter, the most effective solution is to alter the latent conditions which allow the active errors to be performed. Hence a theme and conclusion of this paper is that there should be a preference for solutions that design-out human error, and this is expanded upon in what follows.

3. The Extent and Nature of Cyber Security Breaches

Breaches of cyber security take various forms. There is not, to our knowledge, any single source that definitively measures the extent, nature or impact of the problem. This section briefly covers a key source of information plus significant patterns and trends. Specific empirical data is also presented as part of the case studies analysis that follows.

Where cyber security breaches result from a combination of active user errors and latent conditions, and if humans are inherently difficult to alter, the most effective solution is to alter the latent conditions which allow the active errors to be performed.

The 2006 survey by PriceWaterhouseCoopers for the DTI is a key source on UK corporate information security breaches.[7] Table 1 is adapted from information presented in that report and shows the main broad categories of security breach. Two rankings are shown in the table. The first is the ranking based on the frequency of reporting of each type of breach. The second ranking is based on the extent of the cost or impact of each type of security breach (companies were asked which type of breach was the worst type they faced).

Table 1: Types of Security Breach

Type of Security Breach	Frequency (Rank)	Impact (Rank)
Virus infection and disruptive software	1	1
Systems failure or data corruption	2	2
Staff misuse of information systems	3	3
Unauthorised access by outsiders (incl. hacking attempts)	4	4
Theft or fraud using computers	5	6=
Physical theft of computer equipment	6=	5
Theft or unauthorised disclosure of confidential information	6=	6=
Identity theft or impersonation of the company	6=	7

Note to Table 1: The table is based upon Fig 54 on p.22 and Fig 55 on p. 23 of the 2006 survey.

Like many types of crime, cyber security breaches, including those relating to human error, are highly concentrated. A small proportion of companies experience a disproportionate amount of security breaches. The 2006 DTI survey suggested that earlier viruses and malware were orientated primarily towards overt disruption of users: they 'downed' the user's computer,

7 PriceWaterhouseCoopers. DTI Information Security Breaches Survey 2006, Technical Report. Department of Trade and Industry, 2006.

and the user knew it. More recent attacks have adapted to security responses and are now more typically covert, so the user is less likely to be aware of the attack even if they have inadvertently facilitated the attack. Further, attacks are now more likely to seek to gather data of various forms rather than to simply disrupt the user.

The 2006 DTI survey did not have human error as a particular focus. However, it is clear that virtually all of the types of security breach could, in some instances, be due to human error. The only breach type where human error was reported as a cause was 'System failure and data corruption'. The proportion of these incidents which were directly attributed to human error within this study was only 2%. The real figure is likely to be very much higher — the discrepancy highlighting the difficulties in understanding the human element in system integrity and security. Considering the users' contribution to the data breach, many people will be unaware of the error they committed, for example if malware had covertly loaded onto the system from a trusted website. Others will be aware but unwilling to report or admit to their more culpable actions, for example if they disabled firewalls to speed up their computer. Perhaps more importantly the latent conditions in the system caused by human errors upstream of the users actions — errors of administration, design, process and management - will rarely be unearthed. Only thorough and wide-reaching company investigations into breach causes would include such upstream factors and so capture their existence, nature and extent.

4. A Heuristic Framework: The 25 Techniques of Situational Crime Prevention

The set of 25 techniques of situational crime prevention have been developed over a quarter of a century by Ronald Clarke and are arguably a cornerstone of the disciplines of security and crime prevention.[8] The techniques were recently applied to information and communications technology in a white paper published by the European Telecommunications Standards Institute (ETSI).[9] The present paper is, to our knowledge, their first dedicated application to cyber security. The techniques are grouped into five categories: increasing the effort; increasing the risks; reducing the rewards; reducing provocation, and removing excuses. Traditional perceptions of security often embrace only the first technique of ‘target hardening’. In Table 2 the techniques are applied to activities undertaken to prevent cyber crime. A range of cyber security related prevention efforts

Traditional perceptions of security often embrace only the first technique of ‘target hardening’.

8 Clarke's first version appeared in the British Journal of Criminology in 1981. For the most recent statement see Cornish, D.B. and R.V. Clarke. Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention in M.J. Smith and D.B. Cornish (Eds.) Theory for Practice in Situational Crime Prevention, Vol. 16 of Crime Prevention Studies. Cullopmpton: Willan Publishing,. pp. 41-96, 2003.

9 C. Brookson, G. Farrell, J. Mailley, S. Whitehead, D. Zumerle. ICT Product Proofing Against Crime. ETSI White Paper No. 5. Sophia Antipolis Cedex, France, 2005. (available at www.etsi.org).

are shown while those which reduce opportunities for, or provocations to, human error, are shown in italics.

Table 2: 25 Techniques of Situational Crime Prevention Applied to Cyber Security (adapted from [10])

Increase the effort	Increase the risk	Reduce the rewards	Reduce provocations	Remove excuses
1. Target Harden ● *firewall* ● *phishing filter* ● *encryption* ● *patch management* ● antivirus software ● robust software development	**6. Extend Guardianship** ● remote tracking of use	**11. Conceal targets** ● security policy through trusted connected systems	**16. Reduce frustrations and stress** ● do not overwhelm the user	**21. Set rules** ● *security policy* ● *usage policy and protocols* ● *implement best practice standards*
2. Control access to facilities ● *authentication* ● *monitoring incoming email* ● access control groups	**7. Assist natural surveillance** ● informant email address ● expert or community ratings	**12. Remove targets** ● air-gap sensitive systems	**17. Avoid disputes** ● political mediation ● clear policy on acceptable use	**22. Post instructions** ● security policy ● policies on use of portable data devices
3. Screen exits ● *monitoring systems* ● *monitoring outgoing email and webmail* ● IDS (Intrusion Detection Systems)	**8. Reduce anonymity** ● *authentication* ● *digital identification*	**13. Identify property** ● *digital signatures/certificates* ● Registrar of property (control access to data – audit trails)	**18. Reduce emotional arousal** ● awareness building ● remove provocations	**23. Alert conscience** ● User warnings (ex. IP stamps) ● *awareness campaigns*
4. Deflect offenders ● honeypots	**9. Utilize place managers** ● moderators ● users through awareness building	**14. Disrupt markets** ● *ISPs to provide protection against phishing, viruses and spyware*	**19. Neutralize peer pressure** ● *awareness building*	**24. Assist compliance** ● secure, robust applications
5. Control tools/weapons ● restrictive or authenticated use of IT ● *authentication* ● *digital identification* ● IP address linked to specific User	**10. Strengthen formal surveillance** ● *monitoring systems* ● *publicly portray security accreditation*	**15. Deny benefits** ● *immediately fix vulnerabilities* ● *encryption* ● *back-ups* ● *limit new vulnerability publicity* ● *computer or data 'kill' technology*	**20. Discourage imitation** ● negative publicity for bad practice	**25. Control drugs and alcohol** ● *ban their consumption by personnel in critical posts (e.g. physical or IT security)*

Note to Table 2: Tactics which can reduce human error are shown in italics.

Firewalls and phishing filters reduce the chances and consequences of human error relating to risky computer use. Keeping a backup of data does not make data any more difficult to accidentally delete, steal or otherwise disrupt. Yet backups reduce the damage done when data is accidentally deleted, and they reduce the damage done by more malicious efforts to destroy data. Automated software loading and patch updates reduce human error by removing the requirement that users manually activate that software and load updates. Software that monitors incoming and outgoing email works by different mechanisms. It will reduce general misuse of email and thereby encourage good practice. It will also check sensitive data attachments thus reducing the possibility of human error leading to data disclosure to the wrong recipient. Clear policies and protocols for security policies, in contrast, do not make it harder for employees to commit error, or to misuse or abuse data, but they remove any excuses for so doing and clarify the consequences (the costs to the employee) of negligent actions. As such they will promote good practice which reduces human error. In fact, many existing cyber security efforts contain at

10 R. Verhaaf. Cyberterrorism. Thesis submitted to the Midlands Centre for Criminology and Criminal Justice, Loughborough University. Loughborough, 2006.

least some orientation towards designing-out human error. Some existing tactics work via more than one mechanism. For example, honeypots are known to be used for the detection and tracking of offenders. Yet a key role of honeypots can also be to deflect attacks away from more vulnerable parts of a network, and they are included here under the technique of deflecting offenders.

As with most typologies and taxonomies, the set of techniques is a heuristic device to summarise a great deal of information, to focus and inform thinking about additional security issues. The brief coverage it is given here does not do justice to the value of the framework. Further, if the development of new and innovative security tactics is the aim, the set of techniques should be viewed only as one component of a broader problem-solving approach.

5. Case Studies

In this section we review three case studies, namely personnel security exploits using social engineering, phishing attack in e-commerce and accidental data disclosure by an employee. The case studies illustrate various aspects of the role of human error in cyber security breaches that it is not possible to convey in the more general discussion and frameworks elsewhere in the text.

Social engineering is an extremely difficult type of attack to detect and defend against, because it is largely non-technical.

5.1 Personnel Security Exploits using Social Engineering

Social engineering is defined as gaining sensitive information through deception, manipulation, influence, and persuasion. It involves tricking employees to reveal information about their organisation or their computer systems, or to take certain actions at the request of the attacker. This is an extremely difficult type of attack to detect and defend against, because it is largely non-technical. It relies heavily on human interaction with the skilled social engineer preying on the best qualities of human nature: the tendency to be helpful, polite, a team player, and the desire to get the job done.

Typical social engineering targets include large corporations, financial and banking institutions, military establishments and government agencies. Some social engineers base their success on research abilities which may include mailbox raiding or “dumpster diving” (going through discarded paperwork to find credentials and other useful information). An attacker may develop elaborate schemes claiming to be a new employee, a repair person, or a cleaner to gain initial access, while others do all their work remotely over the telephone or via email and never set foot near the physical site. A determined social engineer may put days or weeks of effort into obtaining credentials to support that identity and gaining the trust of a target employee. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organisation and rely on the information

from the first source to add to his or her credibility. Social engineers do not need to be particularly technically savvy but when their social skills are combined with technical expertise, it becomes easy to breach almost any network.

Case study: Kevin Mitnick and Motorola StarTAC Source Code

Kevin Mitnick is perhaps the most notorious hacker of recent years. Relying heavily on human vulnerabilities, he accessed the computer systems of technology companies including Fujitsu, Motorola, Novell, Nokia and Sun Microsystems as well as various government agencies. The case of stealing the source code of the StarTAC phone from Motorola when it first came out illustrates how effective social engineering can be. Mitnick owned that particular phone and was curious to pull it apart and see if he could gain access to its source code. Source code is proprietary software, considered to be very valuable since it enables many of the features that differentiate a product in the highly competitive mobile phone market.

Walking from his office to his apartment, Mitnick used a prepaid mobile phone registered to a fake name to call Motorola. He pretended to be from corporate R&D and got passed around a lot but finally reached the lead developer's assistant. Within minutes, he had gathered enough information to convince her that her boss — who had just left on vacation for two weeks — was supposed to have sent him the phone's source code. She found the requested files and, with some coaching, tried to upload to an ftp server the address of which Mitnick provided, but could not because of some internal security restrictions.

Before he could protest, she put him on hold while she spoke to security to find a workaround. She then came back with information of a proxy server outside of the company's firewall, which was used to send the source code. It was only after four calls demanding different versions of the source code — which Mitnick said he did just to prove that he could do it — that the con was discovered. The Motorola employee discovered that the extension he had left her was fake when she tried to call him back to inform him that she had to rush off to a meeting.

Sources: US Department of Justice, Herald Tribune

Common social engineering scenarios include the following cases which are subsequently modelled in Figure 1.

- Calling a user and posing as a member of the IT team, who needs the user's password and other information in order to troubleshoot problems with the network or the user's account. *(Human vulnerability: Tendency to a good team player and afraid to ask credentials. Human error: Rule-based).*
- Calling the IT department and posing as a high ranking executive in the company, pretending to have forgotten his/her password and demanding that information immediately because of a compelling business urgency. Often prior to that, attackers have to find the employee name and call the helpdesk to find out what is needed in terms of authentication. Then they abandon these 'research calls' on some pretense and go get what the helpdesk has asked for. *(Human vulnerability: Fear of not complying with superior's request and tendency to be helpful. Human error: Skills-based).*
- Developing a personal relationship with a user or IT team member with the intent of extracting confidential information from that person that can be used to break into the network. *(Human vulnerability: Hoping to benefit from the relationship. Human error: Knowledge-based as rules and experience might not apply).*

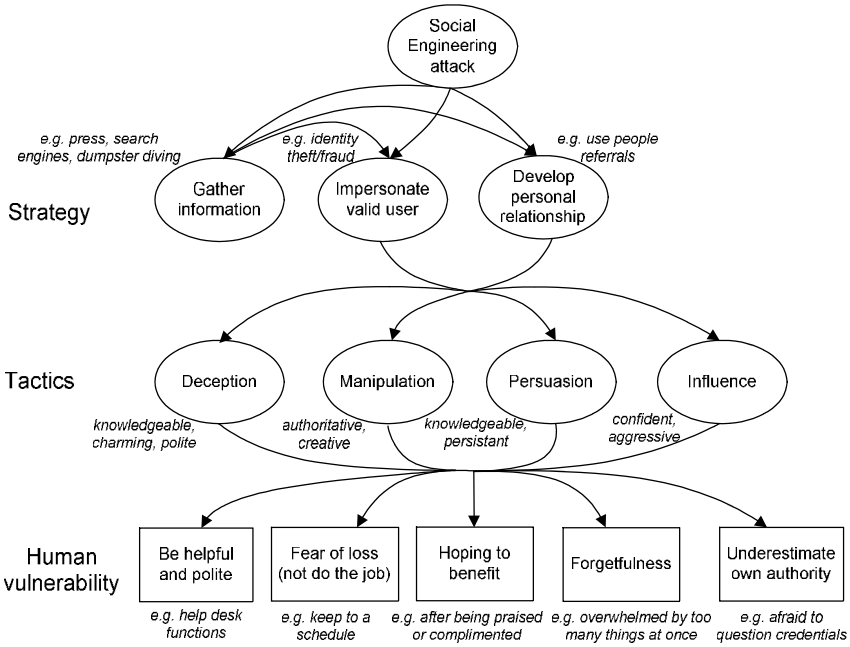

Figure 1 Strategy and tactics in social engineering attack.

Countermeasures

Social engineering is often by far the easiest way for an attacker to gain access to a computer network, and one of the most common. Yet many organisations keep spending large portions of their budgets on defending against technical attacks and do nothing to prevent exploitation of the human factor. The risk of social engineering is also underestimated in employee training programmes or corporate security policies. Establishing policies is the first step in preventing this type of attack. As part of them, organisations should avoid posting managerial charts or lists of key people and shred any documents that are discarded that may contain sensitive data. But perhaps the most important step is an ongoing education of employees to make them aware of the danger of social engineering. The people who fall victims to social engineering attacks are those who have not heard about these scams before. Employees should also be suspicious of unsolicited email messages, phone calls, or visits from individuals asking about employees or other internal information and never be afraid to question the credentials of someone posing to work for their organisation.

5.2 Phishing Attacks in e-Commerce

Phishing is a form of social engineering, where perpetrators attempt to get users to provide personal, financial or computer account information. Phishers attempt to acquire account information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication, typically email or instant messaging. Most phishing scams instruct users to supply information via a form in the body of the message but also prompt users to click a link that appears to lead to a website that belongs to a legitimate, trusted company or by downloading and installing hostile software. According to Gartner, an IT industry analysis firm,

Phishing is a form of social engineering, where perpetrators attempt to get users to provide personal, financial or computer account information.

about 57 million Americans were targeted for phishing in a recent 12-month period, and phishing-related fraud has already reached $1.2 billion annually. The 2005 E-crime Watch survey showed that phishing was reported by 57% of participating companies as the most prevalent attack type, compared to just 31% in 2004[11]. As more and more communications and transactions are taking place online, phishing schemes and other attempts to steal sensitive personal information have become increasingly prevalent and innovative. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, and technical measures. Countermeasures should also be considered for application to mobile products and services which are likely to become a major target for phishing in the future.

Case Study: Evolution of Phishing Attacks

In the past, phishing has primarily relied on scaring or worrying the public into unwittingly disclosing personal information. The most common scenario involves an email telling the recipient that their account has been temporarily frozen, and that to secure that account and restore full access they need to provide certain information. eBay and PayPal are two of the most targeted companies, and online banks are also common targets. If the victim clicks on the link provided in the fraudulent email, they end up at what appears to be an official site, as exemplified by the scam where an imitation of PayPal was hosted at paypai.com. Any personal information they enter is then captured by the identity thief. Since 2004, the success of Phishing has attracted well funded and highly organised crime groups, whose sole objective is to steal online identities and commit fraud.

More recently phishers are bypassing email and counting on search engines to bring them victims. Phishers set up a fake e-commerce site selling popular goods and wait for a search engine to index them. A user types a query into a search engine and ends up at a real-looking site selling those goods. The site allows users to order goods and pay via credit card, but keeps all their personal details and never sends the goods. In another scenario, the fake e-commerce site can contain disguised links that in reality install Trojans on the user's computer. An attacker would then be able to piggyback on a user's session whenever s/he logs into certain websites and make fraudulent transactions thereafter.

A more sophisticated phishing attack methodology known as ‘man-in-the-middle’ was reported for the first time in August 2006. In this scenario the victim received a 'standard' phishing email, where the link directed them to fake URL. There a genuine-looking PayPal login box was displayed, requesting that the user typed in a valid PayPal user name and password. It is believed that the scammer had created a shadow login to the real PayPal site and essentially the victim interacted with genuine content from the legitimate web site — which had been 'imported' — thus allowing the fraudster seamless, invisible and immediate access to specific data. Luckily, F-Secure raised the alarm about this new methodology, before it was widely spread and the appropriate authorities were alerted about the site. Since then, ‘man-in-the-middle’ attacks are known to have been attempted against Amazon and Citibank customers. However while internet users may become familiar with phishing attempts from such well known enterprises, there is now evidence that the number of brands being exploited is growing, thus continuing to catch recipients unawares.

Sources: Anti-Phishing Working Group, CNET News, Phishtank, SC Magazine.

Human Vulnerabilities

Phishing techniques work by taking advantage of predictable human vulnerabilities via *tricks*. The most common phishing

11 Conducted by CSO magazine in cooperation with the US Secret Service and the CERT Coordination Center.

tricks are taking advantage of human vulnerabilities are discussed below and modelled in Figure 2.

- Requesting personal details for innocuous reasons such as a system upgrade or a credit card that has expired. The message is boring, safe and legitimate and appears to be trying to be helpful. *(Human vulnerability: Assuming that normal is safe. The human error type is a Rule-based mistake. Previously, following the rule that the brand or person in question was safe, lead to secure transactions or information exchange.)*
- Inviting the recipient to do something that will benefit them, e.g. join a credit card protection service or to become a 'Power Seller'. Alternatively the message may inform the recipient that they are 'a winner' and request personal information to claim their winnings. *(Human vulnerability: Attraction to possible benefits. The human error here is a Knowledge-based mistake: the victims perform intentional acts, giving their details, in ignorance of or despite knowing the risks)*
- Creating a concern that a person's bank account or card is being targeted and that the customer needs to take action quickly. *(Human vulnerability: Fear of being defrauded. Human error: Rule-based).*
- Using different delivery mechanisms for phishing that are not expected. While people are now becoming more aware of phishing emails arriving they may be less aware of them via instant messaging or VoIP telephone calls. *(Human vulnerability: Lack of knowledge about new media for phishing. Human error: The fact that people respond naturally Instant messages or phone calls with suspicion is a Rule-based error bordering on a Skill-based response).*
- The phishing message containing information that is specific to the recipient such as their name, membership number or other personal information to appear more legitimate. The email may claim that there is a deposit waiting in their account or that they have been outbid in an auction and need to respond. *(Human vulnerability: Assuming that a personal communication is safe and trustworthy. Human error: Rule-based since people typically work on the rule that a personal message can be trusted).*
- Using seasonal or national events to take advantage of peoples' emotions or benevolence e.g. by posing as a charity collector, or claiming that the false organisation has donated money and asking the recipient to contribute. By sending a charity related message, this allays suspicions about the activity being fraudulent. *(Human vulnerability: Appealing to recipient's emotions or benevolence. Human error: Knowledge-based – The recipient is invited to help others which they think about and are willing to comply).*
- Imitating well established brands with huge numbers of potential victims. *(Human vulnerability: people are less*

likely to be on the lookout for frauds and where the total number lacking the technical knowledge to spot phishing attacks is also large. Human error: Rule-based since communications from well established brands are trustworthy, until the targeting of particular brands becomes well known).

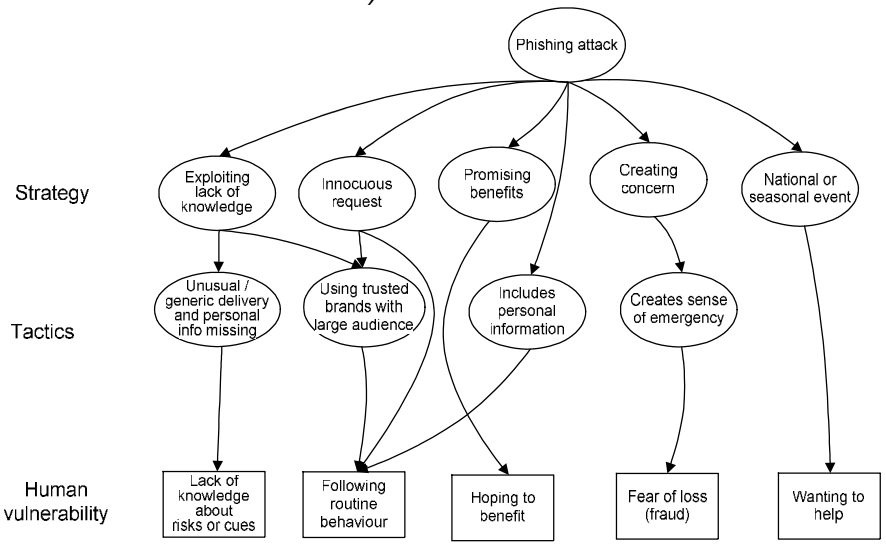

Figure 2 Strategy and tactics in phishing attack.

Countermeasures

Classifying human errors in response to tricks can lead to different kinds of solution to countering the phishing attack. So if an error is made because a person's rule set is inadequate, new rules can be devised, learned and possibly supported with help from the system. If errors are made due to lack of knowledge, the solution may be to educate users and enhance their knowledge. Advice given to those who suspect they have received a phishing communication involves either ignoring it, not following the link (in an email), and not supplying personal or financial information. Other advice is to check credit card and bank statements immediately after receipt and to look for unexpected charges, even small ones. A new approach being adopted by financial institutions involves a two-factor authentication: each time customers wish to log on they need to insert along with a username and password a code generated randomly by a personal security device associated with their account. If personal or financial information is supplied in a phishing attempt, recipients are advised to inform the appropriate institutions immediately e.g. the bank or police. However on a recent ITV programme, 'Tonight', presented by Trevor McDonald (6/4/2007) it was said that there are only 400 cyber crime specialists in the UK police force, far less than the number needed to deal with the size of the problem. The solution which gets rid of one of the latent conditions allowing phishing to be successful is to use software which checks the security of websites visited, thus alerting users if they are on a suspicious site.

5.3 Accidental Data Disclosure by an Employee

Traffic safety experts claim there is no such thing as an accident. They prefer the terms 'crash' or 'incident' to recognise the fact they are virtually all avoidable. The same is true of damaging data disclosure by employees – it is arguable that there are no accidents. Data disclosure is a vital part of business communication but a small fraction may be damaging when sensitive data ends up in the wrong hands. A preferable neutral term might be 'data escape', while a term that locates responsibility with negligent individual or institutional practices would be 'data betrayal'. Here we use the term data escape. Escape can occur during the acquisition, use or analysis, transfer, storage, and destruction of data. It can result from acts of omission or commission. Acts of omission include the absence of adequate institutional policy or procedure. Acts of commission include wilful disclosure, even though it is not intentionally damaging, plus negligent acts involving failure to follow procedure. In this formulation, acts of omission are institutional errors, or latent conditions, and acts of commission are human errors. To reduce human error, the best systems are designed to reduce opportunities, and minimise resultant harms, rather than relying upon humans choosing safe practices.

Data disclosure is a vital part of business communication but a small fraction may be damaging when sensitive data ends up in the wrong hands.

Traffic safety problems are researched to identify geographical hot spots, recurring types of crash and common causes that may help identify 'pinch points' for prevention. The 'whole system' approach to prevention emphasises road design (adequate lane width, clear sightlines, non-adverse cambers), road furniture (roadsigns, markings, barriers), and vehicle safety (lights, turn signals, brakes, proximity sensors) in addition to damage limitation (safety belts, air-bags, crash zones). Law and education guide the elements of driving that require human decision-making, but opportunities for error remain.

There is more than just an analogy with efforts to design-out human error relating to data traffic. Both also take place in the broader context of socio-economic and technological progress that result in faster and more frequent traffic. The media by which data escapes are varied and depicted in Figure 3.

- *Email:* This includes using the incorrect address, attaching the wrong file, or transmission over insecure channels.
- *Loss of portable data devices:* This includes the loss or theft of laptops, USB memory devices, CD-ROMs and DVDs, PDAs and mobile phones.
- *Allowing access to data:* This includes leaving or losing hard copies of sensitive reports, failing to password-protect or log-off a computer, and circumventing or failing to use firewalls or similar.
- *Word of mouth:* This includes indiscretions to friends, family, colleagues or 'others' who are not actively seeking sensitive information.

While there is agreement it is widespread, the precise extent of electronic data escape is debated, and the nature and scope of sources are varied. A 2006 survey by Proofpoint, a messaging and anti-spam software firm, estimated that in the past 12 months, in relation to UK companies: 1 in 5 emails contains risky (legal, financial or regulatory) content; Over half the companies had investigated an email leak of confidential or proprietary information; 1 in 3 had reported negative impact from the exposure of sensitive or embarrassing information; Over a third had sacked an employee for email violations and over 70% had disciplined an employee for improper data-related behaviour. Another survey of UK company staff by Pertemps, a recruitment firm, estimated that 44% of office workers had sent email to the wrong person while 71% had sent an email with the wrong file attached. Websense, a web security firm, reported that 50% of those in possession of a company laptop allowed friends and family to use it for personal use, while Forrester Research, a technology and market research firm, reported that 84% of data leakage in UK companies was generated internally rather than by hackers, viruses or other external entity. Many media reports inform us of the loss and theft of laptops, discs and portable storage media containing sensitive information. The following case study resulted in the largest Financial Services Authority (FSA) fine to date.

Case study: Theft of Laptop Containing Customer Records

In 2006 a longstanding employee of a UK building society downloaded a database to his laptop so he could work at home. The data included 11 million customers' names, addresses and account numbers. The laptop was later stolen from his home. The employee did not notify the company about the data on the laptop until returning from a three week holiday. In total it was three months until the building society informed the relevant customers. They reassured customers that there was no loss of money due to the laptop theft, as PINs, passwords and account balances were not lost. In its investigation, the FSA concluded that the company had failed to assess the risks associated with its customer information, failed to implement procedures and training to manage its risk, and dealt inappropriately with the specific incident. The FSA imposed a fine of just under £1 million.

In this context, the absence of adequate company policy and practice arguably facilitated willful error (perhaps well-meaning circumvention of guidelines) on the part of the employee. Safeguards could have existed at various levels. In terms of prevention these include: Restriction of movement of portable data devices; control of data allowed onto such devices, and logging events where data were downloaded. In terms of damage limitation, data encryption or the use of 'kill' technology to render the computer useless, would minimise the consequences of the loss. The use of satellite system or other tracking of data devices could facilitate offender detection (investment in such technology being worthwhile and in proportion to risk).

The cost of the loss of sensitive business information is difficult to estimate when it relates to product research and development, marketing, or other such information where its loss may have a result akin to industrial espionage.

The costs of data escape can be extensive. The cost of the loss of sensitive business information is difficult to estimate when it relates to product research and development, marketing, or other such information where its loss may have a result akin to industrial espionage. The loss of records on customers could have significant costs to those customers if the information is put to generate financial fraud by abusing customer's identities. Clearly, in such instances, there can be costs in terms of

damage to reputation and the opportunity costs of lost future business. In addition there is also the emotional and psychological cost to any subsequent victims of crime, the costs of police investigation and the criminal justice system, and insurance administration costs.

Countermeasures

At the strategic level, system-based solutions to data escape can be grouped into three categories. In descending order of effectiveness there are data security measures where user compliance:

- to policy and rules is required
- is optional, requiring some effort by the user
- requires proactivity on the part of the user

Where possible, user compliance should be a required part of the system design so that the opportunity for data escape is eliminated without overt circumvention on the part of the user.

Where possible, user compliance should be a required part of the system design so that the opportunity for data escape is eliminated without overt circumvention on the part of the user.

At the tactical level, Gartner present a 'top 5' tactics for a company:[12]

1. *Deploy content monitoring and filtering (CMF) software*. CMF monitors email, webmail and other e-communications, alerting users or blocking communication if preset rules are violated. Simple human e-errors — sending email to an unapproved address, sending a known-sensitive attachment, sending unencrypted data over an insecure channel — can be stopped.
2. *Encrypt backup tapes and mass storage*. This reduces data loss risks.
3. *Secure workstations, restrict home computers, and lock portable devices*. Regulating and shaping the manner in which employees use home computers for work purposes can reduce risks. Restricting the use of sensitive data and/or providing anti-virus, anti-spyware and firewall software to employees can reduce the risk of data escape. The measure has to be reconciled with the growing desire for working on the move with mobile technology.
4. *Encrypt laptops*. Encryption does not necessary reduce data loss, but it reduces the resulting damage if the data cannot be accessed. The analogy is with crumple zones, safety belts and airbags in road safety.
5. *Deploy database activity monitoring*. This can recognise unusual (potentially damaging) network activity. It can also record the location of data so that, if stolen or otherwise leaked, the damage can be confined. Knowing which records have been disclosed can be used to focus damage limitation activity.

12 The Register. Tips to prevent data loss. http://www.theregister.co.uk/2006/08/08/data_loss__prevention_tips/

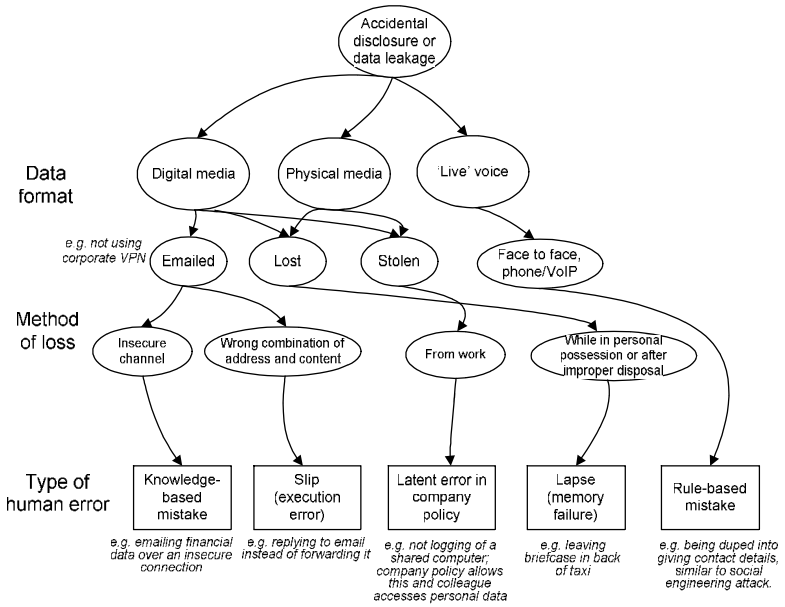

Figure 3 Accidental data disclosure by an employee.

6. The Demand for Cyber Security: An Implementation Issue

Like all forms of security, cyber security is under-provided by the market. This is partly due to imperfect information where customers are uninformed of the risk they take on in purchasing a product – whether a computer, a house, a car or mobile phone. To the customer, the value of purchasing add-on security (an alarm for a house, or software for a computer) is not necessarily intuitively obvious. Many customers prefer to take the risk or hope to free-ride on the purchases and secure practices of others. In the context of cyber security, free-riding occurs by those users who do not purchase anti-virus software in the hope that malicious software and hacking will be deterred by the widespread adoption of anti-virus software by others. Open source business models are a great opportunity to increase the adoption of security practices, e.g. Mozilla Firefox browser. Where a secure solution exists but is not in demand, that is, it is not widely used or adopted, then there is an implementation problem. Implementation is widely acknowledged as one of the biggest stumbling blocks in the field of security and crime prevention.[13] The following case study shows an example of implementation that takes the responsibility from the user and at the same time does not affect productivity by unnecessary interruptions.

Open source business models are a great opportunity to increase the adoption of security practices.

13 N. Tilley and G. Laycock. Implementing Crime Prevention, in M. Tonry and D.P. Farrington (Eds.) Building a Safer Society: Strategic Approaches to Crime Prevention. Chicago: University of Chicago Press, pp. 535-584, 1995.

Case Study: Software Updates with Fewer Reboots

Having the latest versions of programs is advantageous because it makes computers more secure and more robust. Only a few years ago "updating" a program or an operating system meant installing an entirely new version of the software. Then Microsoft and some software vendors started posting "patches" mainly in connection to the Internet related features of Internet Explorer, Outlook Express and the Application Execution Service. Those were, however, difficult to locate and not straightforward to install.

A few Windows versions ago Microsoft introduced Windows Update. It is a service that enables identification, delivery and installation of the missing updates, including security patches, bug fixes, software and certified driver updates, and service packs. This is done without collecting any personally identifiable information from the systems it services. Software vendors followed suit, and it soon become common to have a "Check for Updates" feature in a software package so that you could remain up-to-date.

One of the biggest productivity problems that came with this feature was the "Reboot Required" requirement. This means that users have to save all their work, shut down all running programs, restart the system, and then open their programs, and files all over again. Windows Vista is tackling this problem with a new technology called Restart Manager. Restart Manager looks for all the processes that are using the file that needs to be updated, it shuts down all those processes and after the updates are applied, it restarts those processes.

Sources: eWeek, Microsoft, PC Magazine, OS News.

There are many studies of efforts to encourage or coerce businesses, communities and individuals into adopting more secure equipment, practices, policies and procedures. The means of increasing demand take various forms which fall into the categories of incentives and disincentives. Disincentives include fines and/or negative publicity for insecure or anti-social behaviour. Disincentives can be enforced by law, or less formally by various forms of civil regulation as well as industry-self-regulation via standards. The range of possible incentives is varied.[14] The provision of information about the extent, nature and cost of crime may reduce the degree of imperfect information in the market and cause some customers to purchase security or adopt safe practices. Kitemarks and other forms of approval ('Secure by Design' standards are now widespread) are one popular incentive, as are indices. The Car Theft Index is argued to have significantly stimulated the car industry to improve automotive security, and a mobile phone theft index was recently developed that highlighted the most frequently stolen phone models.[15] Coordinated action by industry can effectively tackle problems that may harm the customer and potentially the market as a whole, as illustrated in the case study of the premium rate numbers that follows. Tax breaks for good practice are one form of increasing the adoption of secure practices. Free provision, whether by government (to those most at risk, or perhaps to those least able to provide for themselves) is one form of increasing the adoption of security. In other instances, particularly those relating to anti-virus and anti-spyware software, the market has encouraged the take-up of their use by providing them as free

Coordinated action by industry can effectively tackle problems that may harm the customer and potentially the market as a whole.

14 For a recent review see: Home Office. Changing Behaviour to Reduce Crime: An Incentives-Based Approach. Online Report 05/06. London: Home Office, 2006. Available from http://www.homeoffice.gov.uk/rds/pdfs06/rdsolr0506.pdf.

15 See G. Laycock. The UK Car Theft Index: An Example of Government Leverage' in M. G. Maxfield and R.V. Clarke (Eds.) Understanding and Preventing Car Theft, Vol. 17 of Crime Prevention Studies. Monsey, NY: Criminal Justice Press pp. 25-44, 2004 and J. R. Mailley, S. Garcia, S. Whitehead and G. Farrell. Phone Theft Index, Security Journal, 2007 (in press).

advertisements for sales of more advanced software. Overall, however, there does not, to our knowledge appear to be a review of the means of increasing demand for cyber security, and this might be a useful area for further study.

Case Study: Collectively Tackling Premium Rate Scams

Premium rate numbers — those starting 09 — were first introduced as a payment system in 1986. They attract higher call charges (ranging from £0.10 to £1.50 a minute) and are used to provide information services such as traffic conditions, weather forecasts, TV votes, and support services. But premium rate lines are also used by scammers to generate large amounts by luring unwary customers via text message prompts into running up huge phone bills by calling these numbers.

As a response, some of the UK's leading telecom companies signed up in May 2005 a Memorandum of Understanding to an early warning system that should help the industry spot scams and take action more swiftly against rogue operators. If they suspect a service provider is acting illegally — by employing expensive premium rate number for rogue diallers or non-existent prize scams — then these companies will swap information and, if necessary, report companies to the watchdog ICSTIS (The Independent Committee for the Supervision of Standards of Telephone Information Services). In early 2007, another regulation was introduced which requires customers to be warned if they spend more than £10 on phone calls in any one day.

Sources: The Register, BBC News On line, This is Money.

7. Conclusions and Suggestions for Further Research

While cyberspace is becoming ubiquitous for users, the crime associated with it can be viewed as a cost that has occurred in the context of overall progress and benefit.

Computer systems and networks have played a significant role in opening new avenues for knowledge and wealth creation, overcoming longstanding barriers to innovation and economic prosperity. While cyberspace is becoming ubiquitous for users, the crime associated with it can be viewed as a cost that has occurred in the context of overall progress and benefit. One of the negative aspects inadequate security brings is that people can lose confidence in on line communications or transactions and feel constrained in using the related technologies with a huge impact on the socio-economic activity. As a relatively new area of research, cyber security should be able to draw upon existing analytic frameworks from the fields of security and crime prevention. The present paper is, to our knowledge, the first to assess cyber security in the context of the 25 techniques of situational crime prevention. As such it is presented as a preliminary scoping of an area that warrants further in-depth exploration. If it serves to stimulate debate about the extent, nature, and effectiveness of crime prevention in this arena, then one of its aims will have been achieved.

Designing-out the potential for human error leading to cyber security breaches is the optimal approach to tackling the problem. If the opportunity for human error does not exist (think of automated rather than user-installed security software upgrades) then it will not occur. Likewise, if rules relating to the use and handling of data are clearly defined, as well as the consequences of breaking those rules, this will induce a deterrent effect that serves to reduce human error. An implicit aim of designing-out human error, therefore, is to minimise the

need for education, training, and a culture relating to security. This is because the best security is that which does not require a particular cooperation on the part of human users, although human awareness of a problem is a useful additional barrier. Where possible, the default option should be security, so that it is only an overt action to circumvent security that leads to a breach. Overt action to overcome security is itself an offence and, by definition, a deliberate act is not an error.

The present paper has scratched the surface of the relationship between human error and cyber security breaches. Further research would appear necessary along the following lines: There would appear to be scope for a comprehensive review of knowledge relating to the extent and nature of cyber security breaches and the role of human error. In addition, a comprehensive review of what is known about the nature and effectiveness of measures to reduce and tackle human error would be informative. These studies would form a platform to build upon with further studies of the role of human error that take both qualitative and quantitative form. Quantitative measures, combining analysis of official records of cyber security breaches (where such are available) could be combined with a more comprehensive survey of the role of human error. Qualitative studies, such as in-depth interviews with individuals who are known to have erred in ways that caused security breaches, as well as with a sample of other computer users in different contexts, could provide useful information about the intricacies of human error, and thus inform the development of security efforts. Interviews with known offenders, including hackers and those known to have committed (perhaps those convicted of) social engineering attacks, would provide information to further cyber security. In addition to this general approach, specific further issues also warrant attention. The fact that cyber security breaches and human errors are likely to be highly concentrated, means that the dimensions of such concentrations should be of particular interest. Stimulating demand for security is an area in which significant amounts of research have been undertaken, an in-depth review of which might inform the further implementation of cyber security. Such a research agenda becomes of even greater importance when considering that in the foreseeable future the cyber and physical spaces, i.e. the worlds of data and things, will merge.

Such a research agenda becomes of even greater importance when considering that in the foreseeable future the cyber and physical spaces, i.e. the worlds of data and things, will merge.

Authors' Contact Details

Costis Koumpis
Vodera Ltd.
koumpis@vodera.com

Graham Farrell
Midlands Centre for Criminology & Criminal Justice, Loughborough University
g.farrell@lboro.ac.uk

Andrew May
Ergonomics & Safety Research Institute, Loughborough University
a.j.may@lboro.ac.uk

Jen Mailley
Midlands Centre for Criminology & Criminal Justice, Loughborough University
j.c.mailley@lboro.ac.uk

Martin Maguire
Ergonomics & Safety Research Institute, Loughborough University
m.c.maguire@lboro.ac.uk

Vaia Sdralia
Vodera Ltd.
sdralia@vodera.com

Acknowledgements

This work has been funded by the DTI supported Cyber Security Knowledge Transfer Network. G. Farrell and J. Mailley also acknowledge funding from the European Commission AGIS Programme to study theft and misuse of electronic services. The paper has benefited from cooperation and discussions with Angela Sasse and comments from other experts in the Human Factors Working Group.

Legal Notice

The findings and conclusions in this paper are those of the authors and do not necessarily reflect the views of the sponsoring organisations. All brand names, product names, or trademarks belong to their respective holders.