CHAPTER 3: THE HUMAN FACTOR: THE UNDERRATED THREAT

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology. (Bruce Schneier, Secrets and Lies, *2000)*

Are people the problem?

There is a vast selection of available security tools, including firewalls, intrusion detection systems, anti-virus solutions, and so much more. Each tool is designed to perform a very specific function, and using these tools provides one layer of protection for information systems. However, even the very best tools using the most advanced technology and the most secure algorithms cannot guarantee 100% system security. So, what is the weakest link in the security chain? The answer: people.

People are involved in the development and implementation of security tools, they use the information infrastructure, and they develop and field the applications used to manage their tasks. And people make mistakes. Consequently, people, a major element of any information system, are always going to be the weak point in that same system.

The human factor is the primary reason why so many attacks on computers and information systems are successful. There's almost always a person or process flaw at the source of any security incident. The gap between a desired level of security and that which actually exists is

most likely due to either a transgression of security rules, whether intentionally or through negligence, or a violation of security policies.

Recent high-profile breaches of systems that really should be well protected, such as those at RSA and at some of the US Energy Department's national laboratories, demonstrate the fact that humans are often the weak link in cybersecurity by using social engineering to bypass perimeter protections. Even the sophisticated Stuxnet[1] worm apparently was delivered to its target by a USB device that an individual, intentionally or not, had to manually insert into an information system's USB port.

Many users see their computer as a sort of magic box; they don't understand how it works, and in truth, they probably don't want to learn. They want to use their information system in the same way as a toaster, a refrigerator, or any other household appliance. They certainly do not want to understand how it performs its function. Many other users think that viruses, hackers, and other cyber threats are simply events that happen to other people.

Another component of the problem is that organizations remain focused on external threats, such as hackers and viruses, at the same time consistently underemphasizing internal threats. Organizations looking for a security 'silver bullet' are often more likely to spend money on technology such as firewalls and virus protection than provide resources to properly prepare and educate their employees.

[1] Stuxnet was a malware discovered in June 2010 allegedly created by United States and Israel agencies to attack Iran's nuclear facilities.

It was not until recent years that the security community really started to acknowledge that user behavior often contributes to many security failures, and thus, began considering the effects of human factors on security. Some of the researchers that have been at the forefront of investigating this human component include Martina Sasse, Dirk Weirich, and Helen James.

Further Reading:
James, H. (1996) *Managing Information Systems Security: A Soft Approach*. Proceedings of the Information Systems Conference of New Zealand, Oct 30–31, 1996, pp. 10–20.
Sasse, M. and Weirich, D. (2001) *Pretty Good Persuasion: A First Step Towards Effective Password Security in the Real World.* Proceedings of the 2001 workshop on New Security Paradigms, Cloudcroft, New Mexico, pp. 137–149.

Who are the attackers?

Many think of attackers as highly technical computer experts. This is one end of the spectrum. At the opposite end of the attack spectrum are less knowledgeable, novice hackers, often referred to as script kiddies. In order to defend against an attacker, it is important to understand their motivations and capabilities. By understanding an attacker's motivations, an organization can more effectively allocate resources to those portions of a system most likely to be attacked. Knowledge of an attacker's capabilities allows an organization to align resources based on the likelihood of an attack's success. The next section describes the range and nature of attackers.

Once upon a time, attackers needed years of learning and experience in order to read and write complex software programs or code. Occasionally, an attacker might find a vulnerability or bug, but would then have to spend many weeks of effort developing an exploitation to take advantage of the weakness and allow unauthorized entry into an information system. Today it is much simpler. Even an unskilled attacker, such as a script kiddie, is able to search the Web for a pre-written set of codes that can be easily tailored to address specific targets.

Some of the more technologically savvy attackers have developed programs that automatically scan various sites to find new vulnerabilities as soon as they are announced by Microsoft®, national Computer Emergency Response Teams, or other organizations. They can then quickly spring into action, either developing their own code or modifying pre-written code to execute new exploits. Often, within hours, new attack codes are developed, tested, and widely distributed. Occasionally, a cyber attack takes on a robot-like life of its own, aimlessly roaming cyber space seeking its next victim. One example is the Code Red virus, which was originally launched in July 2000, but which still activates regularly, and then searches for and attacks unpatched computers.

Types of attackers

Two basic characteristics are used to differentiate between attackers based on their knowledge and desire to do harm:

1. Sophistication of technical knowledge. The level ranges from highly proficient programmers who develop attacks to novices, or script kiddies, who rely on attack

scripts designed and distributed by others. It is important to distinguish between the sophistication of the attacker and the sophistication of the attack. Persons with very limited technical ability can now launch very sophisticated attacks thanks to the availability of highly-sophisticated, point-and-click attack tools.

2. Desire and/or ability to cause harm. The spectrum spans those able to determine and execute actions causing significant harm to those for whom gaining entry (and potentially some notoriety) is the sole purpose for the attack.

These characteristics are shared by cyber attackers regardless of their origin. Between inexperienced script kiddies and experienced, well-resourced attackers there lies a wide spectrum of attackers representing a wide variety of skill levels and motivations.

Which brings us to the question – why attack information systems at all? Let's look at some of the motivations.

Motivations for attack

The motivation of malicious intruders for breaking and entering into computer networks goes far beyond destruction of the system or information theft. In fact, many security breaches go unnoticed because the attacker wants to remain hidden and purposefully masks their presence in the information system for as long as possible. An attacker doesn't always choose to 'hit and run'. In order to prevent long-term hacking and abuse of a company's systems and networks, insight into the mind of a malicious intruder and their motivations is essential.

Attackers may have many motivations. So, what are some of the primary motivations for attack?

- The attacker wants something that is on the target system.
- The attacker wants to use or control the system for a particular purpose.
- The attacker wants to execute a denial of service against the system.
- The attacker may want to destroy information on the system or the system itself.

Most likely forms of attack

The Insider

2012 and 2013 may well be remembered as the years when the discussion of Insider Threat became real. The threat of trusted insiders is certainly not new, but until recently, it had received relatively little attention in the media. Recent high-profile cases, such as Bradley Manning and Edward Snowden, have propelled the discussion into the public eye.

Carnegie Mellon University has been engaged in studying insider threat for almost a decade. But despite research indicating significant damage from insiders to private and public organizations, this threat has remained under-addressed until recently.

Insiders have more access to an organization's critical information and information systems since their knowledge is based on legitimate access to sensitive assets. A recent study by PwC indicated that 24% of organizations studied were unable to identify the consequences of an insider attack and 33% had no insider threat processes or plans

although 34% of organizations identified attacks from insiders as causing more damage than external attackers.

When talking about insider threat, however, it's important not to limit focus on the intentional threat. Research organizations, such as Carnegie Mellon, have conducted extensive examination of the intentional insider threat. Carnegie Mellon has defined the intentional insider threat as:

(1) a current or former employee, contractor, or business partner (2) who has or had authorized access to an organization's network, system, or data and who, (3) through action or inaction without malicious intent, (4) causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems.[2]

Carnegie Mellon researchers identified four primary threat vectors for the unintentional insider threat:

1. Accidental disclosure
2. Intentional disclosure or susceptibility to malicious attack
3. Loss or improper disposal of information
4. Loss of equipment; e.g., computer equipment, smart phones, or other devices with internal storage

Looking at these four threat vectors, it is clear that the primary reason for the unintentional insider threat is human

[2] Carnegie Mellon. (August 2013) *Unintentional Insider Threats: A Foundational Study*, p. ix. Retrieved from The CERT Insider Threat Center at www.cert.org/insider_threat/.

error, which is often the symptomatic of other issues within an organization. Initial and refresher training, ongoing education, and – most importantly – observation of leader actions are most frequently how individuals in an organization internalize behaviors.

Organizational cybersecurity policies, practices, processes, and written values inform and shape acceptable organizational security. Organizations use these mechanisms to provide guidance on what behaviors are deemed appropriate and to establish expectations for their personnel.

Armed with knowledge of the unique organizational approach to cybersecurity, an employee observes and participates in the daily operations of the organization. And it is not out of the realm of the possible that an employee might observe that peers and even managers may not practice the cybersecurity measures put forth by the organization's policies. An observed lack of cybersecurity awareness and compliance can lead employees to becoming less observant and compliant themselves.

So how can organizations effectively address the unintentional insider? They can focus on proactive mitigation strategies that include improvements in work processes to relieve time and workload pressures, effective management practices to avoid overburdening their staff, training to increase awareness and motivation, overcoming user errors and negligence, and ensuring that employees understand the value of demonstrating good cybersecurity behaviors.

Reference

PwC. (June 2013) *Key Findings from the 2013 US State of Cybercrime Survey*. Retrieved from www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/us-state-of-cybercrime.pdf.

Further Reading:
Carnegie Mellon. (August 2013) *Unintentional Insider Threats: A Foundational Study*. Retrieved from The CERT Insider Threat Center at www.cert.org/insider_threat/.

Distributed Denial of Service (DDoS) attacks

A Distributed Denial of Service (DDoS) is defined as an intentional attack with the explicit intent of denying authorized users their legitimate use of an information system or information service. It is likely that DDoS attacks against high value targets (political and economic) will escalate, particularly as a component of cyberwarfare or cyberterrorism. Defending against these attacks is also a formidable task.

DDoS attacks can be executed in several ways. Attacks can be broken down into five general categories, any of which could be initiated with executable malware:

1. disruption of configuration information, such as data routing information.
2. excessive consumption of system resources, such as disk space or bandwidth.
3. interference with state information, such as resetting of TCP sessions.
4. disruption of physical network components.

5. obstruction of one or more communication paths between authorized users so that they can no longer communicate adequately.

DDoS attacks are generally directed against an array of targets, but disastrous consequences could result from a coordinated attack on significant national resources, such as financial, government, or communications targets. The primary advantage of a DDoS attack is that multiple systems are able to generate more attack traffic than a single information system; multiple attacks emanating from distributed systems are harder to defend against than a single attack system, and the behavior of each individual system can be made stealthier, making it much more difficult to track and shut down.

Events, such as the attacks of September 11, 2001 and Hurricane Katrina in August 2005, demonstrate that DDoS attacks against critical communication nodes could be particularly harmful, especially during an unrelated natural or man-induced disaster. In the hours after the attacks in New York, when the phone circuits were overloaded, the Internet and its communication options, such as e-mail and chat channels, were the only means for many people to communicate. Potential targets for DDoS attacks are chat and mail servers, government websites, high volume sites such as search engines, e-commerce sites, and news services. As demonstrated in the Kosovo conflict, military websites and communication systems are especially likely to receive DDoS attack variants.

Domain Name Service (DNS) attacks

Computers connected to the Internet communicate with one another using numerical IP addresses. Domain name

servers (DNS) are the 'Yellow Pages' that computers consult in order to obtain the mapping between the name of a system (or website) and the numerical address of that system. For example, when a user wants to connect to the CNN website (*www.cnn.com*), the user's system queries a DNS server for the numerical address of the system on which the CNN web server runs (64.12.50.153). In this example, if the DNS server provided an incorrect numerical address for the CNN website, the user's system would connect to the incorrect server. Making matters worse, this counterfeit connection would likely be completed without arousing the user's suspicion. The result would be that the user is presented with a web page that he believes is on the CNN web server but, in reality, is on the attacker's server. An attacker could disseminate false information with a successful attack on a select DNS server (or group of servers), bypassing the need to break into the actual web servers themselves. Moreover, a DNS attack would prevent access to the original website, depriving the site of traffic.

The system of domain name servers on the Internet is hierarchical. Local DNS servers maintain up-to-date, authoritative information about their own zones only and rely on communication with other DNS servers for information about remote zones. At the top of the hierarchy are root name servers that maintain authoritative information about which server is responsible for each local zone. Historically, successful DNS server attacks have been perpetrated against local DNS servers, causing traffic to selected sites to be redirected or lost. However, the potential exists for attacks on the root DNS servers, and the likelihood of an attack of this kind occurring may increase during the war on terrorism.

Web defacements and semantic attacks

As the case studies portend, politically motivated website defacements will probably continue to escalate as the war on terrorism is fought. Minor intrusions could result in defacements or pro-terrorist propaganda. The most serious consequences of web defacements would involve semantic attacks. Such attacks entail changing the content of a web page subtly, thus disseminating false information. A semantic attack on a news site or government agency site, causing its web servers to provide false information at a critical juncture, could have a significant impact. Potential targets for web defacements and semantic hacks are government or military websites, high volume sites such as search engines, e-commerce sites, and news services.

Viruses, worms and Trojans

Malicious code, such as Trojans[3], viruses[4], and worms[5] are perhaps the most well-known and most discussed forms of information attack. While they do cause a certain degree of damage, it is often mostly in terms of time, resources, and

[3] A Trojan is a destructive program that masquerades as a benign application. Unlike viruses or worms, a Trojan cannot replicate itself. Once activated on a system, its effects can range from irritating to highly damaging. More critically, Trojans can be used to open up a back door into a system, allowing unauthorized intruders to enter a system without the owner's knowledge.

[4] Viruses are a more virulent form of malicious code. They usually take the form of a piece of code attached to another program or file, such as an email, that may be loaded onto the computer without the user's knowledge and execute itself. Viruses are capable of replication, but require some level of human action to spread (such as reading an e-mail or visiting a website). Their effect can vary widely in severity from mildly annoying to damaging software, hardware, and files.

[5] A worm can also replicate from computer to computer, but unlike a virus, it can do so without direct human intervention.

reputation. In fact, the Computer Security Institute's Annual Report (2007) reported that losses due to viruses, worms, and Trojans, which had been the leading cause of loss since 2001, had fallen to second place.

Nonetheless, Trojans, viruses and worms can still cause significant denial of service events, largely due to an increased load on servers, network traffic, and infrastructure-related resources, such as support staff. Critical operations may be halted to determine damage and to conduct repairs.

Despite the reported decrease in losses, hardly a week goes by without some form of scare involving malicious code.

In recent years, we have witnessed an unprecedented number of prolific worms (e.g., Code Red, Ramen, Lion), some of which are suspected of being created in response to political events. The vulnerabilities that worms exploit are usually widely known to system administrators and easily remedied, but often go unpatched on many systems which can cause major problems in the information infrastructure. Analysis of recent worm code by Institute of Security Technology Studies (ISTS) scientists at Dartmouth, and discussion of high profile worms by experts in the computer security community, resulted in the consensus that these intelligent software agents did not carry destructive payloads. A worm similar to Code Red could do much more serious damage with only minor design modifications. This analysis highlights the fact that if maximum destruction is a hostile adversary's goal, worms are a cost-effective way to significantly disrupt a national information infrastructure. New worms may contain a sleep phase, in which the worm will infect as many hosts as

possible, before activating its destructive payload perhaps in order to co-ordinate with a conventional terrorist attack.

Some researchers have predicted the emergence of new classes of worms (Warhol worms, flash worms) which could spread in minutes or even seconds, leaving little or no time for system administrators to react. It is reasonable to expect that new variants of old worms will appear and be renamed to allude to the terror attacks in New York and Washington.

Hybrid worms that combine a series of historically successful exploits to maximize effectiveness are certain to appear in the near future. Inevitably, there will be new worms based on vulnerabilities that are not yet known, and therefore, not immediately patchable. Worms employing such zero-day exploits could leave the custodians of information systems with no choice but to shut down services until patches are available, effectively resulting in a physical denial of service. Recent worms examined by computer security experts have been relatively crude in technological construction, perhaps aimed at easy targets to attract significant media attention. These worms may be used to shield more sophisticated and malicious worms, operating alongside their noisier cousins and targeting critical infrastructure systems.

One of the more recent attacks represents the type of attack likely in the future – a combined attack. In the summer of 2007, the Storm Worm Trojan initially appeared in e-mail messages claiming to contain a warning message about weather danger in Europe. The US-CERT then observed an evolving transformation in the tactics used by the Storm Worm to deceive and infect users. Earlier variants arrived as e-mail attachments or links that, once executed,

downloaded the malware to a user's system. These were expanded to include propagation techniques asking for credential confirmation for membership-based sites and links to adult pictures. Most recently, the Storm Worm Trojan appeared in e-mails claiming that the user featured in a new video on *YouTube.com*. The e-mails contained fake links that directed the user to malicious websites; these sites attempted to download the Storm Worm Trojan by exploiting a variety of browser and application vulnerabilities. Each of these variants took advantage of social engineering[6] by providing tempting topics that induced users to take actions that spread the worm. The most insidious component of this particular worm is that the Storm Worm infection linked the user's information system into a 'robot network' or botnet.

Botnets

Botnets have been one of the more recent occurrences on the information attack scene. The US-CERT at Carnegie Mellon University's Software Engineering Institute defines botnets:

…networks of computer systems that have been compromised by malicious programs so that they can be remotely controlled to send spam, participate in Distributed Denial-of-Service (DDoS) attacks, and perform other malicious actions. The compromised systems are

[6] Social engineering is a technique used by potential attackers to obtain information from unsuspecting victims that will facilitate the attack (whether in the physical space or using information systems). The strategy takes advantage of simple human curiosity and our desire for the quick return to manipulate individuals into performing actions or revealing information they normally would not reveal.

managed remotely through a command and control channel where the botnet's originator, sometimes called the 'bot herder', can operate and unite them with other infected systems to increase their effectiveness and redundancy.[7]

In the case of the Storm Worm, infection resulted in the victim's system being added to a botnet that could then be remotely controlled by an attacker.

Advanced Persistent Threats

Advanced persistent threats are among the most insidious of attacks, largely because they remain 'under the radar.' In an advanced persistent threat (APT) attack, an unauthorized individual uses low resolution attacks to gain access to an information network and tries to remain undetected for a long period of time. The goal of an APT attack is to steal high-value information, such as corporate intellectual property or sensitive government information, rather than to damage the network or organization. APTs focus their attacks on specific target organizations in sectors with high-value information, such as national defense, manufacturing and the financial industry.

Although APT attacks are more difficult to identify than more obvious attacks, the act of stealing large amounts of data is not completely invisible. The best way for an administrator to discover an APT is by looking for anomalies in outbound data, such as large amounts of data leaving the network at unusual times of the day.

---

[7] US CERT (September 2007) *Quarterly Trends and Analysis Report.* Vol. 2, Issue 3.

Many cybersecurity experts have stated that China is the most active and capable adversary in placing APTs in critical organizations. In October of 2011, US Representative Mike Rogers stated publicly:

> *China's economic espionage has reached an intolerable level and I believe that the United States and our allies in Europe and Asia have an obligation to confront Beijing and demand that they put a stop to this piracy. Beijing is waging a massive trade war on us all, and we should band together to pressure them to stop. Combined, the United States and our allies in Europe and Asia have significant diplomatic and economic leverage over China, and we should use this to our advantage to put an end to this scourge.*[8]

Phishing

'Phishing[9]' refers to a form of scam that involves fraudulently obtaining and using an individual's captured personal or financial information. This is how phishing typically works:

- An individual receives an e-mail which appears to originate from a known individual, a legitimate financial institution, government agency, or other well-known/reputable entity.

[8] SC Magazine Online Video available at *http://outsidelens.scmagazine.com/video/US-Lawmaker-Calls-Chinas-Corpor;search%3Atag%3A%22espionage%22*.

[9] The term phishing is a variation on 'fishing,' the concept being that digital bait is thrown out with the hopes that while most will ignore the bait, enough will be tempted into biting to make it worth the effort.

- The message describes an urgent reason personal or confidential information must be 're-verified' or 're-submitted' by clicking on a link embedded in the message or offers something the individual is unlikely to resist (e.g., 'watch the cat playing the piano').
- The provided link appears to be the legitimate website of the financial institution, government agency or other well-known/reputable entity or a link, but in 'phishing' scams, the website belongs to the fraudster/scammer.
- Once inside the fraudulent website, the individual may be asked to provide Social Security numbers, account numbers, passwords or other information used to identify the consumer, such as the maiden name of the consumer's mother or the consumer's place of birth. In some cases, just clicking on the link exposes the individual's information system to attack.
- When the consumer provides the information or allows access to their information system, those perpetrating the fraud can begin to access consumer accounts or assume the person's identity.

Phishing is the 'granddad' of attacks based on deception, and it has spawned a number of other types of attacks using deceptive messages to prompt users to take actions resulting in opening their system or mobile device to attack. Here are some brief descriptions:

- *Spear Phishing* – Spear phishing is a more directed type of phishing attack that focuses on a specific user or department within an organization, usually directed at someone within the company in a position of trust, requesting information such as login IDs and passwords. Once an attacker has obtained access, they often use it to gain entry into multiple locations on secured networks.

- *Pharming* – Pharming is similar in nature to phishing in that it seeks to obtain personal or private information (usually financially related). Instead of the user being spammed with legitimate-appearing e-mail requests to visit websites, pharming 'poisons' a Domain Name Server (DNS) server by implanting false information into the server, causing the user's request to be redirected to a false site. The browser, however, will still seem to be showing the correct website, which makes pharming serious and difficult to detect. Pharming allows the scammers to target large groups of people at one time through domain spoofing.
- *Twishing* – Twishing is the act of sending a legitimate-appearing message to a Twitter[10] user in an effort to obtain the user's name and password. The message may direct the recipient to visit a website and ask them to log in. The website, however, is counterfeit and designed only to steal the user's information. Twishing takes advantage of the every-growing number of Twitter users.

Infrastructure attacks

Serious cyber attacks against infrastructures, through unauthorized intrusions, DDoS attacks, worms, Trojan horse programs, or malicious insiders, have been the subject of speculation for several years. Vulnerabilities in America's power distribution grid were first exposed during the Joint Chiefs of Staff exercise 'Eligible Receiver'. Pentagon

[10] Twitter is a free online social networking service that enables users to send and read 'tweets', which are short text messages limited to 140 characters.

spokesperson, Mr Kenneth Bacon, stated, 'we did learn that computer hackers could have a dramatic impact on the nation's infrastructure, including the electrical power grid.' This vulnerability was exploited for real in June 2001, when computer hackers, routed through networks operated by China Telecom, penetrated the defenses of a practice network of the California Independent Systems Operator (Cal-ISO) for 17 days. The scenario of an unanticipated and massive attack on critical infrastructures which disables core functions such as telecommunications, electrical power systems, gas and oil, banking and finance, transportation, water supply systems, government services, and emergency services, has been raised in a number of reports on national security. The degree to which these infrastructures are dependent on information systems, and interrelated to one another, are still not well understood. Neither is the extent to which these information systems are exposed to outside entry from the Internet.

Information systems associated with these critical infrastructures must be considered likely targets for terrorists, nation-states, and hackers in the age of asymmetrical warfare. Some examples:

- Banking and financial institutions utilize infrastructures that are vulnerable to cyber attack due to their dependence on networks. However, this sector still operates largely private networks and intranets with very limited external access, thus affording some protection from external cyber attack.
- Voice communication systems are vulnerable to proprietary software attacks from insiders familiar with the technical details of the system. This includes emergency services telephone exchanges.

- Electrical infrastructures have sensors that assist engineers in shutting down components of the national grid in times of natural disaster, which could become vulnerable to cyber manipulation, potentially resulting in power outages.
- Water resources and the management of water levels are often controlled by sensors and remote means. Physical security, in addition to heightened cybersecurity awareness, must be followed for any impending conflict.
- Oil and gas infrastructures widely rely on the use of computerized Supervisory Control and Data Acquisition (SCADA) and Energy Management Systems (EMS). These systems could be vulnerable to cyber attack with the potential to affect numerous economic sectors, such as manufacturing and transportation.

Malicious insiders are the greatest threat to critical national infrastructures. Insiders armed with specialized knowledge of systems and privileged access are capable of doing great harm.

Compound attacks

Individually, any one of the scenarios discussed here could have serious consequences. However, a multi-faceted attack employing some or all of the attack scenarios could be devastating if governments and organizations remain unprepared.

A compound cyber attack could have disastrous effects on infrastructure systems, potentially resulting in human casualties. Such attacks could also be coordinated to coincide with physical terrorist attacks, in order to maximize the impact of both.

Further Reading:

Anonymous (2003) *Maximum Security: A Hacker's Guide to Protecting Your Computer Systems and Network*. 4th Edition. Indianapolis, Indiana: Sams Publishing.

Gregory, Peter. (2013) Advanced Persistent Threat for Dummies. Available as an e-book from Seculert at *http://info.seculert.com/apt-protection-for-dummies-ebook-lp*.

Krone, T. (2005) *Hacking Motives* in *High Tech Crime Brief*. Australian High Tech Crime Centre, June 2005. Available at: *www.aic.gov.au/publications/current%20series/htcb/1-20/htcb006.html*.

Lakhani, Karim R. and Wolf, R. G. (2005) *Why Hackers Do What They Do: Understanding Motivation and Effort in Free/Open Source Software Projects*, in Perspectives on Free and Open Source Software. Cambridge, MA: MIT Press. Available at *http://ocw.mit.edu/courses/sloan-school-of-management/15-352-managing-innovation-emerging-trends-spring-2005/readings/lakhaniwolf.pdf*.

Thomas, D. (2002) *Hacker Culture.* Minneapolis, MO: University of Minnesota Press.

Sometimes it's just human error

Recently in the news…

On 21 November 2007, the British Government made an embarrassing admission that two computer disks containing the personal information of approximately 25 million individuals had been lost while being transported by a junior-level courier between two government departments. The personal information included names, addresses, and dates of birth, **national insurance numbers, and banking record details.** *The loss was the*

result of a lack of compliance with existing policy requiring media with personal information to be encrypted (these were not) and tracked (also not done).[11]

In 2006, the US Veterans Affairs (VA) Department reported the loss of information on over 26 million US military veterans. Against agency policy, a VA employee went home with a laptop and media containing personal information, such as names, addresses, and social security numbers. The laptop was then stolen from the employee's home.

Humans are fallible. Despite some of the best intentions, humans do make mistakes – and these can be costly to an organization's information systems. Some of the most widespread and devastating recent incidents are more readily attributable to mistakes, rather than intent to cause harm. Many could have been prevented with the implementation of proper processes, or equally, through compliance with existing processes.

People can also be the solution!

It is disingenuous to think that people are only the root of the problems in information systems security. At the same time as we consider the human factor a weak link in security, we also must look at people as the best avenue for establishing an effective cybersecurity program. On initial view, cybersecurity is often assumed to be purely technical: it is often perceived only as protecting IT from viruses,

[11] SC Magazine Online, November 2007.

malware and other threats that just keep expanding in the digital age.

The real source of some of the most frequent and most serious security incidents often lies in process errors, such as ignoring security as a critical component in the strategic goals of the company, not including security considerations from the initiation of a project, over-reliance on security tools, lack of or insufficient security training and education, lack of staff motivation as a result of weak values in corporate culture, insufficiently defined security goals, deficient structures, an absence of security processes, rules and procedures, and diluted responsibility. To put it simply – there is no information systems security without the human factor.

Several significant events over the last decade have demonstrated that technology alone is not the solution to organizational issues where security processes need to be developed and implemented. In fact, relying only on technology to solve cybersecurity problems can actually cause more vulnerability. Thucydide, a Greek historian from the 5th century BC, stated this most clearly: 'The thickness of a wall is less important than the will to defend it.'

Educating users is one of the primary means of achieving better levels of cybersecurity within an organization. Another measure is to increase the cybersecurity workforce, however, this has not been without its own challenges. When you consider the explosive growth of malware, the threat of a multitude of cyber attacks, and the fact that even major players like RSA or the US FBI are successfully attacked from time to time, it would appear clear that cyber security is a growing job market. But our most plugged-in generation,

known as the Millennials seem – if not totally uninterested – then at least inconsistent about protecting their own digital lifestyles, much less looking at cybersecurity as a possible career field.

So while billions of dollars continue to be spent on new cybersecurity technologies, it is only the people with the right knowledge, skills, and abilities to implement those technologies who will determine success. Although it appears difficult to entice sufficient new staff to fill the growing number of cybersecurity positions, it is possible to train and educate current employees to fill those gaps.

Here's the bottom line: a wide-ranging perspective that encompasses the critical aspects of people, process and technology is essential to attain and maintain a state of resilient cyber readiness.