People – the weak link in Security

Steven Thomason

East Carolina University

Abstract
People – the weak link in Security

The weakest link in any security plan or implementation is a human. The weak links include everyone from the hourly paid end user to the owner of the company. Even many of today's security professionals may not have the time or ability to perform their current duties and keep up with an ever-growing number of threats. If someone is not aware of a threat then they are going to behave as if there were none. The job of the security professional is to change this behavior. It involves using a combination of technology and education to help users understand and follow security requirements. Everyone needs to understand why we need to have security policies and why they need to be followed.

Security personnel are facing tougher opponents in the fight to keep business assets secure and safe from intrusion. Attacks are becoming more sophisticated and there are more entryways to get access to a company's network and data. In the past not everyone had Internet access and if they did the access speed was not very fast. Almost every business has to have some Internet presence. Today virtually everyone has access to high speed Internet, probably a smartphone, and maybe a tablet as well. All of these devices are finding there way into the corporate world whether the IT department wants it not. Many non-IT personnel don't have any idea of the risk that they are putting the business in. As many if not most of the intrusions into corporate networks and data are caused by human error and IT practices to mitigate threats can't stop everything, users need to become accountable for their actions.

Before anyone in the company can be held accountable for breaching security policies they need to know what they are. Here is where the company needs to have a computer security policy in place. The policy should state what the company goals are and put forward information that allows the user to understand what is expected of them. Also along with the processes and requirements of the policy statements there needs to be a way to enforce the policy. If the policy is not clearly spelled out then the user will either not understand what is required of them or will simply ignore the rules or guidelines?

To quote an article from Terry Corbitt[i], "We can never be sure that data files are totally safe from hackers but the truth is that the greatest threat to computer security comes from within our organizations." Accordingly he states that it is important that a security policy contain four parts: implementation, detection, response, and education.

A security policy needs to be defined with the involvement of the IT department, department managers, executives and especially the Human Resource department. The managers and executive's help to define what the goals of the company are and help rank the importance of the company's processes, applications, and data and what level of risk is acceptable for each component. The IT department can then assess the costs and methods of protecting the company's security profile. After everything has been evaluated a policy needs to be created to define what is required from each employee. If an employee does not have any idea of what they are responsible for or are made aware of the possible risks that they are exposing the company to then they cannot be held liable. For example, several of the sales people with our company had no idea that it was a bad idea to let their children install free games they found on the Internet on their company laptops. One employee had so many viruses on their computer sending traffic to the Internet that the local ISP had to disconnect their access. Users were not educated as to what security procedures should be adhered to and how to do it. Also at the time there was not a computer policy in place.

A security policy at a minimum must have a scope, definition or classification of assets, personal and company responsibilities, and a defined enforcement component. Company risks and requirements, disaster recovery and Internet security need to be part of the policy structure[ii].

A policy should define what is to be covered and to what extent. Levels of responsibilities are defined. Some of the basic procedures[iii] that should be included within a security policy are listed below:

- Employees are not allowed to download or install unauthorized software
- Employees are not allowed to disable any management software such as virus protection
- Employees are not allowed to access prohibited sites on the Internet
- Employees are not allowed to access area servers, software, or data not related to their job function
- Upon termination of an employee all access to the companies systems should be canceled.
- Upon termination of an employee all computer, technology, and access devices should be returned.

The last two points in the list above are dependent on communication between the Human Resource department and the IT department. Here again security is dependent on humans and not on technology.

What is security as far as the computer user is concerned? According to a definition by Simson Garfinkel and Gene Spafford: "A computer is secure if you can depend on it and its software to behave as you expect. [iv]" You expect for users to keep their computers safe and secure. They expect you to keep their computers safe and secure.

While there are many definitions of security a basic premise is that the data is secure if it can only be accessed and changed by the people it is intended for and that the data is available when needed. According to an article by Roger Grimes, simply keeping up with system and software patches could have prevented most of incidents of systems being penetrated. The other major risk occurs when users install applications that they shouldn't such as fake antivirus scanner, disk defragger, or other unapproved software[v]. Many times they are not even aware of what they have installed because either they thought that they were suppose to do what the popup told them to do or they clicked on a link in an email.

Many companies miss the boat by trying to solve all of their security problems with hardware and software. They concentrate their time, money and energy into technology. Vendors want to sell you the latest IDS/IPS systems, firewalls, scanning appliances, and services. Technology cannot protect against every threat. While all of the above devices may and probably are needed it is easy to miss the one area in

security where spending little money can give the greatest return – the end user. End user in this context includes managers, executives, IT personnel, and non-IT or management personnel. If a user understands that it is their responsibility to help keep the company safe and secure from a security standpoint then there will be fewer incidents that need to be addressed. If the user knows not to click on the popup for a "new" update to the virus software then the IT department doesn't need to find, remove, and protect against that program. There will always be new threats but the fewer that make it into the network and onto computers the better. If an educated user can close a door of access, then there will be less for the IT department to worry with.

An educated user can also help in other ways. Do your users have access to the company network through their home computer? Do they access their email from home? Logging into the corporate network from an infected computer can give a criminal the company the person works for along with their user name and password.

The Internet has allowed people to work from almost anywhere. Homes have become virtual offices. Socializing, banking, reading, shopping, and other activities can be done from work or home. Most home computer systems don't have the security infrastructure that is available at work to keep their systems safe.

According to Consumer Reports "State of the Net Survey" released on May 1, 2013 over 58.2 million Americans had a malware infection on their home PC last year and over 9.2 million fell victim to phishing schemes[vi]. These are the computers that employees use to connect to their corporate network.

Frequently only the people tasked with security are even aware of the possible security risks associated with certain behaviors. To see how easily computer users within a company could be faked into clicking on a phishing link a CIO sent out an email with a bogus link to 450 employees[vii]. Out of 450 people 240 opened the email and of these 120 actually clicked on the link. In another test Symantec created a smartphone honeypot that stored simulated corporate data. 50 phones were left behind in a variety of public places. 83% of the monitored phones show attempts to access the data and 49% showed attempts to access remote administrative applications. Data is at risk through the actions of users. Technology does not stop people from clicking on links and does not keep people from losing their phone or computer.

In March of 2013 the average number of spam emails sent out daily reached 117.8 billion[viii]. Android phones are increasingly coming under attack. The blackhole exploit kit use is increasing and spammers are sending more and more legitimate looking emails from sites such as LinkedIn, PayPal, and others. Unless the user really knows what to look for they are likely to click on the link especially if that have an

account with the website. IT processes and systems cannot catch everything and they need the users' help.

According to a survey by CompTIA[ix] the most underestimated component of security intrusions it from end user error. Less that 45% of companies provide security training to their non-IT staff. The loss of thousands of dollars in productivity and systems downtime caused by inadvertent security breaches by users has shown a greater need for more employee training and technology education. With the increase of smart phones, portable computers, tablets, social networking, and other easily accessible services, users are exposed to many new security threats not even imagined several years ago. Back in 1992 Dr. Glenn Boyer said that "Information systems security isn't a computer problem, it is a people problem![x] That is still the case today. People have not changed their habits and still need to be trained.

If the user understands the importance of keeping a system patched and understands the dangers of opening emails from unknown senders then they will keep their own equipment safe, which in turn keeps the company safer.

Why do we need security? What is worth protecting: the company reputation, data, the ability to produce, sell, or manufacture product. Not often considered but companies have to be concerned about their reputation. Denial of service attacks originate from computers infected with botnets. The hacker is not going to attack anyone directly from their computer, they want to use yours. Microsoft and other companies have been the victims of attacks and you don't want the attacks to come from your network because you allowed your internal systems to become infected from human error. There is almost no company around anymore that can continue to exist with the loss or corruption of its data. If it is electronic and we don't want anyone else to have it then it is worth protecting.

There are multiple ways to keep your data safe. It is fairly common knowledge that you need a firewall and virus protection but that is where most people stop.
I believe that there are three basic groups of people that need to be targeted to increase security awareness. First of all there is top level management, which includes owners, CEOs, vice presidents, and department heads (of what ever title). Next there is the IT community itself, which consists of programmers, business analysts, and technical people responsible for running the network, storage, and server infrastructure that make up the IT department. Finally there is the non-technical user group that needs to access data at various levels affecting everything within the business including production, sales, inventory, payroll, and other vital operations of the business.

Top Level Management
Now where does management fall short? Many company owners, especially those that are SMB still believe that they are too small a target and do not put security as a priority or don't realize the risk unauthorized access can have to the business and

its continued operation. Often the CEO is so busy running the entire business that security gets lost in the day-to-day operations. They have heard of other companies getting hacked or losing data but they are much bigger companies and ours in probably not a target. CIOs are tasked with running the IT department but usually have to worry more about keeping costs down then spending money that doesn't show a hard return. People and equipment are hard dollars that are easier to justify and if the rest of the management is not concerned with security than it will not become a priority for IT management either.

Marketing should be concerned that their trademarks and marketing materials are protected. They don't want the competition to know what they are planning. Manufacturing needs to know that their formulas and production methods are safe so that other companies start making the same product and sell it at a lower cost. The CFO definitely wants to know that banking with its associated wire transfers are safe. And the list goes on. Each department believes that their data is secure but never looks any further. Everyone just assumes that the data is safe or that policies, procedures, and responsibility resides elsewhere and they don't need to get involved.

HR, which is usually very aware of the need for keeping data safe and confidential, is not fully aware of the risks involved in keeping data safe. Frequently you hear about people having their social security numbers and other important information stolen from a lost laptop that wasn't encrypted.

IT Department

The CIO in change of the IT department is not always an advocate for increasing security. The more security procedures you put into place, the more the end use community complains so often the process are scaled back so much that they are all but useless. IT just puts the minimal amount of security in place and hopes for the best. The full IT community needs to be fully on board with security policies and procedures. These should be based on the policies that were defined and agreed upon by upper management.

Programmers need to understand how to write secure programs and program to design best practices. Business analysts need to understand data flow and how to keep it safe. The most venerable part of any firewall implementation is human error so the security engineer needs to fully understand the result of any rule or change. Those in charge on the infrastructure itself need to understand the importance of keeping these devices patched and up-to-date.

End User Support is tasked with getting equipment purchased, software installed, and distributed to the end user as fast as possible. Often fully patching a system before it goes to the end user is neglected. Even if a fully patched image is used it is often not updated as frequently as needed and patches gets outdated. Ease of management also contributes to lower security. It is much easier to remember the local administrator password for all of the computers if they are the same on every

computer. That also means that if only one computer out of hundreds is compromised then they all are. The hacker only needs to break one password or utilize one hash.

IT personnel like to think that they solve every problem with faster hardware and newer software. A common thought is to not trust the end user because they are the enemy and the cause of all problems. So one common way to secure systems is to require harder and more complex passwords. Many times what this does is actually reduce the security of the system. The can actually cause "password overload[xi]" causing more risky behaviors instead of reducing them. For example, one drug company had a user that had to enter 8 complex passwords every time that they logged in and the passwords are required to be changed every three months. How does she remember them? She looks at the post-it note on the computer screen. IT must work with users and explain why passwords need to be complex and at the same time make it easier to use the systems. For example they could still require complex passwords but only require them to be changed once a year or at most once every 6 months. Allen Guinn stated that it is "Better to have a password that's two years old that someone can remember than a password that's just been changed that's been written down that somebody can find,

Security requires teamwork. All areas within a business need to understand the importance of security to the well being of the company and its continued success. What are some of the problems that could occur if end user security is ignored?

Examples

One website that offered cooking classes required you to pay for the class in advance. The website advertised that any data you put on their website was safely transmitted to the credit card company. This was true. What they didn't do was give the end user a safe connection to their website and anyone watching the site could see everything you type is in clear text. The owner of site was unaware of the risk. The company setting up the site was unaware of the risk or just incompetent and the end user was told that there wasn't any risk. In this situation if the person browsing the site knew to look at the key or lack of a key they would have know that it was not a secure connection. They would have also seen that their connection was http and not https. Unfortunately many people don't know the difference. Education would solve that.

In another situation, several executives had their passwords stolen and after the company could not finding any leads halted investigation ignoring any possible problems. The company's upper management ignored the possible ramification of their being a compromise of their network and even ignored the advice of their security staff. The lack of understanding of what occurred caused this company to go bankrupt. The company was Nortel[xii]. People at all levels need to understand the cost of loose security practices.

Security companies are not immune to attacks either. A security company had their network compromised not through a technological attack but through social engineering. A 15-year-old girl convinced a system administrator to drop security through a series of emails whereby the girl claimed to be the company CEO. She was then able to download a large part of the company's database and post it on the web[x].

There are many more examples of technology working but people failing. All it tasks is a search of the Internet and you can find many examples where the weak link was a human. According to Frank Hayes[xiii] while you can "up the security ante - pile on the encryption and biometrie authentication and lots of other cutting-edge security technology - won't fly. They're too expensive, and besides, the weak links are almost always people, not technologies."

There are different ways to keep employees up-to-date on security procedures. Newly hired employees can be required to take a training class on security. This can be in whatever form works best for the level of user being hired. It can be a written document, a series of power point slides, one-on-one training, or someone actually teaching a class. Some software companies even offer videos that the company can use for training[xiv].

Some of the tips for educating users include the following[xv]:

- As threats and technologies change security procedures should be reevaluated and retested on a quarterly basis.
- Have users bookmark important sites, especially financial so that fake sites cannot fool them. Use your bookmark and not the link in an email.
- Train users in the proper way to create and use passwords.
- Don't click on unknown links
- Don't answer surveys. Do you really know who is calling?
- Develop procedures so that someone cannot use social engineering techniques to gain information needed for access.
- Develop methods for authenticating a user calling in for help or information.

Educating everyone on the need for security and what the risks are for ignoring this is one of the most important and cost effective ways to increase a company security profile. This training should include everyone, including people in the IT department. Writing a poorly designed web interface can be just as damaging as a user inadvertently installing a Trojan on their computer. Training should be customized to addresses to the level of access the group has. It doesn't make one bit of difference how secure your firewall is or how strict your rules are if everyone gives out their password or clicks on every link in an email. Technology can never overcome stupid. Training and education have a much better chance.

When management understands how much of a risk they have and what needs to be done to create a more secure environment it will be become easier for a security

profession to do their job and get funding. People at all levels need to have security training. Everyone from the top-level executives, to the non-IT personnel, to the people in charge of security have something to learn. Having everyone on board and understanding the critical nature of security and how carelessness can do damage to the business and their jobs will make for a more stable and secure company.

The better educated everyone is concerning best security practices then greater your chance of being secure is and the less of a chance you have of losing data or suffering a breach. Security losses cause money and jobs. Educating people is one of the least expensive and cost effective things you can do to fortify your network and systems. While you can't fully eliminate human errors but you can reduce problems caused by ignorance and lack of knowledge. Fewer problems equates to money saved.

[i] Corbitt, T. (2002). Protect your computer system with a security policy. *Management*

[ii] Forcht, K. A., & Ayers, W. C. (2001). Developing a computer security policy for organizational use and implementation. *The Journal of Computer Information Systems, 41*(2), 52. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/232578275?accountid=10639

iii Essential Security Policies for Human Resources. (May 19, 2010) Retrieved from http://www.computer-network-security-training.com/essential-security-policies-for-human-resources/

iv Ross, Seth T. Excerpt from Unix System Security Tools. Computer Security: A practical definition. July 2, 2013. http://www.infoworld.com/d/security/your-guide-becoming-true-security-hero-219313?source=IFWNLE_nlt_daily_am_2013-05-28

v Your guide to becoming a true security hero. (May 28, 2013) Retrieved from http://www.infoworld.com/d/security/your-guide-becoming-true-security-hero-219313?source=IFWNLE_nlt_daily_am_2013-05-28

vi Consumer Reports: 58.2 Million Americans Had a Malware Infection on Their Home Pc Last Year. (05/01/2013) Retrieved from http://pressroom.consumerreports.org/pressroom/2013/05/my-entry.html

vii CTO of media company faked-out employees with "phishing" emails. (July 3, 2013) Retrieved from http://www.scmagazine.com//cto-of-media-company-faked-out-employees-with-phishing-emails/article/301603/

viii Internet Threats Trend Report April 2013. (April 2013) Retrieved from http://www.commtouch.com/uploads/2013/04/Commtouch-Internet-Threats-Trend-Report-2013-April.pdf

ix Lack of End User Training is a Large and Growing Threat to IT Security, CompTIA Study Finds
Lack of end user training is a large and growing threat to IT security, CompTIA study finds. (2009, Mar 10). Business Wire. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/444214389?accountid=10639

[x] Boyer, G. L. (1992). Information systems security isn't a computer problem, it is a people problem! *SuperVision, 53*(11), 7. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/195587894?accountid=10639

xi RSA Security Survey Reveals Multiple Passwords Creating Security Risks and End User Frustration
RSA security survey reveals multiple passwords creating security risks and end user frustration. (2005, Sep 27). PR Newswire. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/451364926?accountid=10639

xii Nortel hacked for years but failed to protect itself, report says (February 14, 2012) Retrieved from http://news.cnet.com/8301-1009_3-57377280-83/nortel-hacked-for-years-but-failed-to-protect-itself-report-says/

[xiii] Hayes, F. (2011). It's not funny when security becomes a joke. *Computerworld, 45*(7), 36. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/861496915?accountid=10639

[xiv] WatchGuard helps strengthen "weakest link" in network security with new end user training tool; launches SecurityWise sessions as part of LiveSecurity service. (2006, Feb 28). *Business Wire*. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/445274099?accountid=10639

[xv] Herbka, P. (2010). What to look for in IT security. *Bank News, 110*(11), 10-12. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/763605073?accountid=10639