

INFORMATION SECURITY FOR HUMANS



**Improve Information Security and Save Resources by
Maximizing the Human Side of the Security Equation**

John Davis, CISSP

Risk Management Engineer



Have you ever heard the adage “security is a human problem, not a technological problem”? While this is still true in many ways, to organizations that depend on information processing systems to do business, (and what organization doesn't rely on information processing systems to keep their business running efficiently and competitively nowadays?), technology really *is* a part of the problem. And consequently, it also must be part of the solution. But it certainly isn't the entire problem. Currently, the security equation reads: Technological Security Measures + Human Security Measures = Security. But are we applying too many resources on the technological side of the equation while largely ignoring the human side? I say yes!

In the early 90's, just as the Internet and server-based computer systems were becoming really user friendly and powerful, people started to hack into them and wreak all kinds of havoc. After all, these systems were never meant to restrict and secure the flow of information. They were built to maximize the flow of information! And the way these people hacked into computer systems was by the use of technology. They took advantage of how the information was packaged, how one computer established communications with another, how the information flowed across the telecommunication wires, how the software was written, all kinds of different methods, but almost universally these methods were technological in nature.

So how were we going to address this new problem? We couldn't start over from scratch with a totally new, more secure system. The old system was already established. People were used to it already, and what is more, large amounts of money had already been spent on infrastructure, hardware and software by everyone from individuals to large corporations. The answer is that we started to throw technological fixes at these technological problems, of course! Firewalls! Intruder detection systems! Encryption systems! Anti-virus software! These were going to be the answer to everything!

Throwing Dollars at the Problem

We bit the bullet and spent *lots* of money. We *bought* the new equipment, *hired* additional employees and *used* the managed security services. And what was the result? Our systems and information were still being compromised! In fact it is getting worse all the time. Today, there is more identity theft and other kinds of information compromise than ever before!



So why was this happening? Why didn't the great new machines and software keep our information safe? There are really several reasons. One reason is that computers and the applications that run on them change so *fast!* Seemingly every day someone comes out with a new application, operating system or machine that revolutionizes the way we do business and communicate with each other. And lots of these new machines and software packages end up having some kind of new security flaw that can be exploited!

Another reason is that the machines and applications that help us secure our information are not very user friendly. Let's take firewalls and intrusion detection systems (IDS) as examples. First, they are all very expensive, and the more they do, the more expensive they are. Second, they are extremely difficult to administer correctly. If they aren't configured correctly, they can let in the very exploits that they were designed to keep out. Also, they give you so much information that it would take an entire staff of employees just to keep on top of the logs they generate. Third, the better they are and the more types of things they look at, the slower information flows through them. So, organizations that computerized themselves in the first place in order to increase the speed and efficiency in which they handle information start experiencing slow downs and increased expenses instead! In fact firewalls and IDS are so notoriously difficult to set up and administer that smaller organizations most often hire service providers to do it for them.

Another reason is that the people that hack the machines are adapting their techniques to the new, higher security equipment and software that is on the market today. Instead of attacking the new machines and software directly, today's hackers are using social engineering techniques and outright physical theft to get the credentials they need to indirectly gain access to our computer systems. In other words, modern attackers are exploiting the *human* side of the security equation.

The Central Issue

Which brings us to the central questions posed by this paper: since technological solutions alone don't seem to be getting the job done, and the hackers seem to be using human security weaknesses to worm their way past the technology, why not turn the situation around and use more human-based information security techniques to help solve the problem? It's less expensive, and ultimately can help your organization run more smoothly and efficiently.

How is an organization supposed to go about doing this, then? Should we just forget about all the security technology? No, unfortunately the basic technology is still needed. An organization still must have a firewall and run anti-virus software. An organization still should have basic IDS and encrypt sensitive information for transmission and storage. But do we have to have the most expensive models and the latest equipment? Probably not. Do we have to use all of the managed services to look after our security equipment for us? Again, probably not.

What is needed is a comprehensive information security program that is incorporated naturally into every aspect of the day to day running of the business, and a work force that keeps information security constantly in mind as they perform each task during the day. I know that must sound like a bit of a utopian ideal, but it really can be achieved to a large degree, and in surprisingly little time. I have experienced this myself in a military intelligence and information security setting.

To actually instill this kind of mindset in an organization, there are a few things you have to put in place. Number one is that you must have the enthusiastic support of management within the organization; the more senior the manager, the more enthusiastic they should be. Management must also be seen to be actively participating in the program. Without this support, you might as well forget the rest of what follows; the program will surely fail.



Awareness Counts

That brings up the second point: security awareness must be put in front of the entire workforce on a constant basis. Personnel must be made aware of a few basic points of information security to start with:

- 1.No security system is perfect. Clever and determined people have compromised almost every type of security system ever devised. Why should it be any different now?
- 2.Good information security is all about noticing and acting on the little things. Personnel must realize the importance of noticing and reporting little strange events such as odd phone calls coming in, or repairmen showing up unannounced, or their PCs performing strange functions without any input from them; the list is endless!
3. Personnel must be schooled against their natural tendency to be helpful and accommodating. I'm not saying that your personnel should be rudely suspicious or unfriendly or anything like that. Only, when repairmen do show up, call their company or your supervisor to make sure their visit is legitimate. Don't go to get coffee and leave the service provider you are escorting alone in a sensitive area. Don't give out a password over the phone because of the pleas of a frantic spouse! Believe me; people will cave in to these sorts of "social engineering techniques" nine out of ten times unless they are properly schooled.
4. Personnel must be made aware of the importance of following security procedures every single time. Many times security breaks down simply because people get busy or bored or complacent or something and simply stop following the established procedures. Check lists are a very good way to fight this tendency. Also, management must be seen to be checking on whether or not personnel are performing their information security duties.
5. And, of course, personnel must be kept up to date on the kinds of threats they are currently likely to encounter. Members of the organization must keep tabs on the latest and most prevalent types of security compromises and make sure this information is communicated to all.

The last thing an organization needs to do is review and update their information security program on a regular basis. This is very much analogous to keeping your house clean. We all know that once you have your house all in order, it is pretty easy to keep it that way as long as you don't start putting things off. If you rinse the dishes and stick them in the dishwasher right after a meal, for example, you're fine. But, if you let the food dry on them over night, you are in for ten times the work! It is the same thing with an information security program. If you keep on top of it and every time you change a software application or add a new server, you also update all the pertinent parts of the plan, things will run smoothly. If you don't, confusion comes into play and mistakes start to happen.

Now I know that you are probably thinking that this is a lot to do! And you are right. You are also probably wondering how adding all this training and extra duty can help the business save money and run more smoothly? Well, there are several answers to that that may not be readily apparent.

The Hidden Helpers

One answer is efficiency. If everything is written down, if everyone is well trained and aware, and if everything is tested or practiced on occasion, then personnel are more comfortable and liable to be less confused when it counts. The business runs smoothly. Also, you don't get personnel working redundantly or at cross purposes as much. And the more efficiently your organization runs, the more you can streamline your workforce. And a few less people on the payroll translate into a big savings!

Another answer is that you may be able to cut your technology bill considerably. A workforce that is well motivated and educated in information security may be able to come up with simple techniques that will provide the same amount of information security or more than an expensive machine or software package can offer. For example, a simple telephone call or having a photograph of a service provider could provide better authentication than a brand new server. If your workforce is motivated properly, they can help show you where you need to apply technological solutions and where you can achieve the same results some other way. Once again, no one knows the job better than the people that do it every day. Also, if your system administrators are knowledgeable about system threats and vulnerabilities, they may be able to show you a way to simply shut down a service or do one little thing manually that keeps you from having to replace or augment a whole operating system!

And how about third party service providers? If you are doing more of your own set up, monitoring and such in-house, won't you be able to get by with less hosted services? Won't you be able to apply older, less complex and expensive hardware and software systems and make them work for a longer period of time? If you can add a year or two to your equipment and software life cycle, wouldn't that save considerable expense?

Also, if your information security program is well set up and viewed as a whole, couldn't the organization streamline and combine parts of the program testing schedule? If all personnel are well schooled in the information security program, then why not test the incident response program at the same time you are doing your business continuity exercise? And isn't while all this is fresh in your mind the right time to update your policies and procedures?

Lastly, having a good written and practiced information security program in place can save your organization from a lot of reputational damage and regulatory involvement. For one thing, you are much more likely to notice and catch an information security problem if you have a well trained workforce and good program than if you have the best technology in the world. That means that the incident may never happen in the first place, which certainly helps keep your reputation intact! And if your organization does sustain a compromise of its information, won't the regulators be less likely to impose fines or sanctions if you can show them documented proof that you have had good information security program the whole time and it is not negligence on your part?

In closing, let me go back to the adage that began this paper: "security is a human problem, not a technological one." While it has been shown that this is not strictly true, I hope the reader can see how the human side of the security equation has been neglected over the last two decades and why we should emphasize that role more now and in the future!