GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

Computer Security Education – The Tool for Today

GCIH – Gold Certification

Author: Ian R. J. Burke, iburke@headwallsecurity.com

Adviser: Jeff Turner

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Outline:

1. **Abstract**:.....3
2. **Introduction**:.....4
3. **The First Steps to Incident Handling**:.....5
4. **NIST's Approach to Education**:.....8
5. **Financial Regulations and the Need for Education**:.....11
6. **HIPAA and the Need for Education**:.....18
7. **Breach Laws and the Need for Education**:.....22
8. **Federal Rules of Civil Procedure**:.....26
9. **ISO Standards and Requirements for Education**:.....29
10. **Conclusion**:.....32
11. **References**:.....35

© SANS Institute 2007, Author retains full rights

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

1. Abstract:

Security education, for a long time, has been seen as a thing reserved for security professionals. The Computer Security Act of 1987 put forward for the National Institute of Standards and Technology to create standards and guides for security awareness and training. This act was the first of a string of legislation that would place mandates around security education for non-security professionals. This trend illustrated newfound awareness in the community and in the world around computer security.

People are incorporating computer security into all aspects of their lives, from the secure web sites where they are making their online purchases to the biometric authentication that has been incorporated into their laptops and PDA's. More employers are incorporating single sign-on solutions and multi-authentication methods to get into critical applications. Many corporations are filtering content on their networks and monitoring which web sites their employee's visit. With all of these changes are we taking the time to explain to people the why behind all of this technology and security?

In the news on almost any given day you can find a story about some corporation, government agency, school, or organization that has lost confidential data due to a security breach; a firewall was left off line, a laptop was stolen, or a hard drive was lost. You can also find frequent stories about new government rules and laws, both at the state and federal level, tightening computer security. These laws are driving development in new tools for defense and new techniques in incident handling.

All the while the masses of employees in these companies come to work, turn on their computers and promptly check the

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

news, log onto Yahoo to check their mail, or go to their favorite weather site to find out if it is going to rain. The more adventuresome go to check their bids at eBay or to buy a ticket from their favorite discount travel agent. How do we get this mass of users to switch from being a hole in the wall of security to being a tool for security? How do we get them to understand all of those news articles and to understand all of the technology that their information technology departments have put into place? In 1987 NIST was charged with helping to create standards to answer that question. There have been many laws in the time that has past since that call for computer education. Today, more than ever, there is a need for organizations to employ security education as a tool in their arsenal against the many threats facing their data and infrastructure.

2. Introduction:

Compliance has become the yardstick by which many organizations gage their security incident preparedness. Every day we ask our employees to keep our companies, hospitals, banks and organizations in compliance with the laws and standards that govern our commerce. Every day these laws and standards become more stringent; both in an effort to protect the people of our country but also to encourage organizations to protect themselves against the increasing number of threats facing our digital assets. Users need to be able to identify threats like viruses, policy violations, HIPAA violations, and other security breaches. Security administrators need to know how to contain and handle DoS attacks, Smurf attacks and other security events. They need to know how to protect against them with the new technologies being introduced every day. When we put together

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

our information technology budgets, compliance is always in the front of our minds. Empowering your employees with the knowledge they need to stay in compliance may be the cheapest investment you can make toward compliance, but more importantly toward incident preparedness. If we are unable to meet these goals are we going to be able to respond to a security event when it occurs?

3. The First Steps to Incident Handling:

Incident handling is an involved and ongoing process. This process starts with a continuous preparation. This involves knowing the laws impacting your environment. It means that you need to be aware of what is going on across your infrastructure. There needs to be an understanding of the stresses and impacts on the infrastructure. There also needs to be a continued effort to educate the user base on these same issues so that they can contribute to the preparation effort and be a part of the second step, identification.

But the preparation process is involved and multifaceted. Penetration tests, vulnerability assessments and risk analysis need to be done on both systems and processes routinely. A well-educated user base will be able to contribute to these tasks and help to enrich them.

When doing a PEN-test one of the first weaknesses that an ethical hacker goes after is the password. Educated users will know how to follow the password policy that the organization has put into place making sure that if the PEN-test is able to crack the password it is showing a weakness in the policy not in the user.

The educated user can contribute to a vulnerability test and risk assessment as well. If they have been trained on the

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

policies and systems and they are aware of the laws and standards that govern their processes and systems, they will be able to help the security team and incident handling team identify potential weaknesses in their processes that the security team may not be familiar with.

All of this is the preparation process as the incident handling process loops through a preventative cycle. In the event that there is a security event the handling process moves past preparation and into identification. The faster that a breach or security incident is identified the faster it can be contained and the damage can be stopped. If the user population has been educated in the preparation phase then they can help to identify the incident and bring a quick notification for a quick containment.

If you have a user that has not had the proper education and has not joined the security effort they may find themselves in a situation similar to the following. The user may be surfing the Internet and hit an anonymous website with several pop-up advertisements. One of those pop-up windows is loaded with a script that executes a directory traversal and scan, looking for any vulnerability it can find on the user's system. Anything it finds it sends back to a bot net or host for a later attack. The educated user would either have known to avoid the site from the start or would have been able to spot the vulnerability and notify the incident handler when they spotted the pop-ups on their system. This uneducated user did not make notification. The incident handler did not notice the problem until the issue was spotted on their intrusion detection equipment. Again there needs to have been education for the security team here. If they did not receive the training on the IDS equipment they may not even spot the vulnerability at this level and the issue may slip by as a call to the helpdesk as a slow computer. Without

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

training this event may still leave a backdoor for that remote host to come back in even after this system is repaired by the helpdesk as some of the vulnerabilities that the website initially found may still exist. Proper education of both the user and the security team would have made the incident handling process of this security event easier and more effective.

Whether the event is spotted by the security administrator or by the helpdesk, the event needs to be contained in some fashion. If we provide education for this security team, an event like this one is often spotted by an IDS allowing for the incident handling process to work in advance of a major breach. In this event the security team may have been able to notify the helpdesk before the user even noticed the issue with their system. This could have provided the opportunity to contain the breach to the one isolated system. From here the security team could work with the policies established for their organization, and as appropriate for the system, to contain the system and to eradicate the issue. If the helpdesk is provided the appropriate training, they can work with the security team to provide many of the containment and eradication services for non-critical systems where chain of custody may not be essential. On more critical systems that contain protected information or where litigation may be involved, the incident handling team would need to take possession of the system and secure the evidence in accordance with the organizations retention and chain of custody policies.

In our simple scenario here, the security administrator would continue to work with the helpdesk or other involved parties to see that the intrusion was removed and that the vulnerability was removed from the system. Once these steps are complete the system would be restored and placed back into production. But the process is not over. What good would this

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

process be if the user did not learn anything? How would things improve if we did not question all systems for this same vulnerability? As we move systems back into production a learning process must begin; not just for the security team but for all those involved with the event.

4. NIST's Approach to Education:

Many CIO's and CSO's today depend on the work generated by the National Institute of Standards and Technology. They produce crib sheets, standards documents, white papers, and sample plans that information technology security departments around the world have turned to as templates and doctrine. The Computer Security Act of 1987 helped to found NIST in its current form and with its formation issued a mandate for computer education. In 1998 NIST published a document, 800-16, *Information Technology Security Training Requirements: A role- and Performance- Based Model*. This document not only outlines methods for training and the need for training in government agencies, but also, as is the mission for NIST, expands its scope to the private sector.

800-16 outlines three levels of training that are essential for any organization, "Awareness", "Training", and "Education". With this model it is clear to see how a training model can be applied to any organization. The awareness level, as prescribed by NIST, applies to every employee in an organization. "Awareness" suggests that there should be some level of understanding that there is confidential information and what the security expectations are for the organization. This is a more passive information sharing approach with an organization's staff: bulletin boards, fliers, marketing efforts by the security team.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

"Training" is more directed and interactive. "Training" is provided to every person that has interaction with technology or the standards. Employees that work with the data need to know what is expected of them to protect the data. "Training" is not intended to make every employee a security expert but rather to make them aware of HIPAA regulations if they are a healthcare worker, or how your organization has chosen to comply with Sarbanes-Oxley if they work with insurance or financial information. "Training" is giving the majority of the employees the tools that they will need to stay in compliance with the organization's security policies, and to help the organization stay in compliance with federal regulations.

Users are the experts of their data and their systems. When they have the training they need they are able to help the security experts with all levels of the incident handling process. By providing "Training" and ensuring that users are experts of their systems and have an awareness of how their systems interplay with other systems and the security process users become valuable assets in containing and eradicating events. They now poses the knowledge to identify what processes belong in a system and which ones could possibly be foreign. They also now have the knowledge to help provide the quality checks when bringing a system back on line in the repair process. They can watch for events that are not part of a normal working environment as they are not only aware of their own daily routine but they have awareness outside of their bubble.

"Education" is in reference to formal training given to the staff in charge of the security of your data and networking infrastructure. This would include formal classes, seminars, labs, and professional groups as well as other resources that could help to strengthen the security team's knowledge base. "Education is not intended for the general staff or for the

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

average user but rather for the professional security expert. This is what differentiates the security professional from the other users of the information infrastructure. A security professional today is not an expert on the applications they support, that is left to the trained user, but rather is an expert on the methods that a hacker will use to gain access to the organizations systems. The security professional knows the laws that govern their organization so that they can guide the organization both into compliance and away from incidental exposures. Security professionals today are experts in eradication and recovery techniques. This requires them to be experts at digital forensics. Perhaps above all, they need to be educators and students at the same time.

This NIST model is built for a sound preparation model. It ensures that every member of your organization has some awareness level so that they do not add to the threat risk. It provides training to your user base so that they can contribute to the identification process. And provides the skill set to your security team so that they can contain, eradicate, recover, and review the incident.

By providing for an understanding of the security issues at all levels of the organization, it makes it possible to bring every player in the organization into play when working on processes such as disaster planning or reviewing from a security event. A major security incident affects the entire organization, from the non-computer user in housekeeping to the programmer in development. Whether preparing for an event at a tabletop drill with members of management or reviewing an event with members of your incident handling team, every member of the organization needs to be involved. If they are going to be involved in the process they need to be educated on the issues that come into play as well as the tools and systems that are involved in both

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

the event and the remediation. While a housekeeper may not need to know about a firewall, they will need to know why there requisitions are not getting through and why their staff is now locked out of the west wing of the building. If they are part of the incident handling team because they manage facilities, they need to have some understanding of what it is that the technical security people are talking about. While a network administrator may not need to know about Halon systems they do need to know that there is appropriate fire suppression in their server room and to be able to understand how that system works so that they can explain that to the incident handling team in both table-top drills and in event reviews.

These three core education levels from NIST 800-16 are abstracted into an entire methodology for security training that was continued into NIST's document 800-50, *Building an Information Technology Security Awareness and Training Program.* Not only does this plan echo the "Awareness", "Training", and "Education" classes, but it goes on to say that, "Security training and awareness should be focused on the organization's entire user population." (pg7) 800-50 points out that there are many requirements in the information security arena and that the "Training" and "Awareness" components of education are the avenues to communicate these requirements across all levels of the organization. We are all familiar with writing policies. We are also all familiar with directories filled with policies that are unmanageable. 800-50 suggests that education is the mechanism by which the user population will come to know and understand these policies.

5. Financial Regulations and the Need for Education:

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

For many organizations the new policies being written today are being driven by the Sarbanes-Oxley Act and the Gramm-Leach-Bliley Act. These two pieces of legislation, along with the Payment Card Industry standards, have generated a bustle of activity in the information security community. Policies and procedures as well as new technologies have been introduced throughout most industries. Practices that use to be commonplace are now being called into question. But how does the average user know about this? Do they know that they can no longer email that confidential file out to their old distribution list, which might contain internal and external email addresses? A large number of users today still come from backgrounds where they may not have much exposure to computers outside of work. Understanding the reasoning behind screen locks, strong passwords, and multi-authenticated logons could take some explaining. There was a day when we saved all of our files on our local systems. For a user that has been working as an administrative assistant for fifteen years, having to now change to saving these files to an encrypted network share with limited access may seem strange. For a housekeeper that never uses a computer and has had free reign of the facility for the past five years, suddenly having doors locked and keys taken away may require some education on new security issues.

Applying the NIST model to these situations it is easy to see how organizations could benefit from a security education plan as they move through these transitions with the GLBA and SOX regulations. With these stringent regulations there are new organizations offering training and services to assist the security professional with the policy, intrusion prevention, data retention, and encryption requirements that they are now facing. With this there is a need for education in these new regulations; a need for education by the security professional

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

and education by the general user population. But, this goes beyond just bringing these users into compliance with the laws. A solid education program will also help to shift these users from being potential security risks to being a part of the incident handling team. It also empowers the user to contribute to the entire incident handling process as they now are able to contribute to the containment process with their knowledge of the systems of which they are owners and experts. It allows them to help with the eradication of the intrusion by helping to differentiate between normal processes and those that could be placed by unwanted hosts. The educated user now has the skill set to help with restoration of an infected system as they have the knowledge to provide the quality checks as the data is restored or the system is brought back on line. This involved user is now an integral part of the review process at the end of every incident handling process as they have now been both a contributor and a witness to every step of the engagement. To maintain this involvement, the user needs to be educated on new technologies that are injected into the infrastructure to satisfy the demands of SOX as well as the reasons behind the technology.

An executive on a business trip today often takes a laptop full of business and personal information. The opportunities for that system to become a security incident are everywhere on that trip. If that executive has joined the security team, as they move through there business they will work to secure their data: encrypting their hard drive, ensuring their system is not left unattended, password protecting the system and files. At the same time it is important to ensure that this person is aware of the laws and policies governing them so that they know what to do both to protect their data and in the event that something does happen. Only with this knowledge will they be able to stay

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

in compliance and to be the eyes for the security team. Without this knowledge that very executive, who is working to help protect the data, may not know what to do in the event that they do lose a thumb drive or misplace a CD-Rom.

One of the primary focuses of Sarbanes-Oxley is privacy. This piece of legislation, like many of these laws, does not dictate technology. What it does is create guides for how information is handled. It outlines classifications of information. The security expert needs to understand the technical ramifications of these classifications and how this will impact the security policy and plan. The user needs to know generally about the information itself so that they handle their data correctly, and in compliance with the security policy that was created to comply with the law.

A big part of the preparation in any incident handling process is writing and implementing policy. To write effective policies understanding data classifications and the different types of data on the network is essential for the security team. Proper education on both SOX and other laws and standards that influence data classifications is important for this process. Once classified, the user populations needs to understand where their data fits into the different classifications so that in the event of an incident they can let the security team know what type of data may have been breached. This helps with the containment process. If you have had a general data breached one type of response may happen while critical, confidential data may result in a different response for containment.

While the Payment Card Industry standards, PCI, are much more technical and specific than some of the Federal regulations, again these standards require two levels of understanding. The security professional needs education on the technology, policies, and systems that they will need to implement into

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

their security policy and infrastructure. The security professional will need to be familiar with systems such as IDS and IPS solutions. The standard has a requirement for scanning of IP interfaces. This requirement requires the security professional to have the training to use vulnerability assessment tools. The standard identifies DoS and Buffer overflow events as scans that are not permissible. As such not only does the security team have to be able to know what to avoid in their scans, but they need to be able to identify these in their identification stage of their incident handling process. They also need to know how to contain an event of this sort. With out this training, not only would an attack of this sort do damage to their network, it would be outside of the compliance of this standard. Security teams need to have broad training. When looking at a PCI scan for standard accreditation, or after a breach, systems as cross-platform as web servers and applications, scripts, databases and servers, mail servers, firewalls, routers, and wireless access points all are systems that should be checked for vulnerabilities. The security professional is not expected to be an expert of each of these systems but on the incident handling team you need to have the knowledge base to administer all of these systems. Collectively the team should be able to identify the vulnerability and contain it, eradicate the threat and repair the system. Once the system is back on line it is this combined team that will review the event.

These new financial regulation and standards, reach into all industries. They are not limited to the banking and insurance companies but extend to hospitals, resorts, restaurants, companies with 401k plans and all firms that have financial transactions. These new laws are not intended for the security professional as a method of ensuring that they have

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

their systems in line but rather are targeted at the organization in hopes of systemic change across the corporate fabric. This will not happen if the entire user population is not educated both in the new regulations and in the new processes being implemented to meet those regulations.

One security solution commonly being employed by businesses today is cryptography. The security professional needs to understand how to implement SSL on the web server or the web based mail server. They also need to know how to configure the key management for disk encryption or file encryption if their organization is implementing those services. Failure to understand these processes and configure them correctly could not only lead to vulnerabilities but could also lead to difficulty in identifying and containing a breach if one should occur.

The user base needs to have an understanding of key management as well. If a user has a PDA that they synch with the web-mail server, they may need to maintain a certificate or key on their PDA. Users need to understand the keys that they pull across the web to their browser. Being able to identify a bad, corrupt, or invalid certificate could help to identify a potential breach before it occurs. At a higher level, basic training of the user population will help them to identify if they are on a secure HTTPS web site when making SSL communications.

If organizations make the sweeping changes needed for these laws and maintain their systems in compliance with these laws there will be an ongoing cycle of preparation and preparedness. The preparation will include corporate wide training that is refreshed on a regular basis and updated with changes to systems and changes to laws or standards. A well-designed system would go beyond this to draw in the user base to build a sense of

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

ownership of the security risk making them a part of the security team. This continuous preparation, this systemic overhaul that these laws are encouraging, builds for companies to be well seated at the top of the incident handling process.

Users really are the key to identifying what has been contaminated. When looking at SOX the well trained user understands that they need to be aware of not only what it is they do but how it interacts with the systems around them. If a user understands how their data travels and where it goes, they will be better able to prevent a data loss. In the event of a security event, they will be able to work with the security team to help them identify those systems that have been affected. An incident handler may never work with the actual applications that have been compromised in a breach. They will rely on the user to help the user population to identify all of the systems that have been compromised. The incident handler needs the user to be well educated in the systems they are working with, the relationships those systems have with the rest of the data repositories in the organization, as well as an understanding of the laws and policies that govern those systems. A user with this understanding will be able to help identify what systems have been compromised and how.

Once the violated systems have been identified the incident handler needs to know how to isolate the issue. In some cases this can be as simple as removing a problem workstation or pc. At other times there may be a critical database that has been called into question. This scale of an event would fall into a class governed by SOX. A financial records database that has been compromised would need to have recovery plans and safeguards in place that were prescribed by these financial regulations. How you would proceed on an event like this should have been predefined in your policies that were prepared in

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

response to SOX or GLBA. Events like this require the team work of both a security specialist that understands the implications of the security event at a level where they can not only eradicate the issue but can also explain it to other incident handler team members. It also requires the skill of system administrators and or database administrators that can navigate the intricacies of database maintenance and outages. All of these team members need to have the training and skills to work with each other and understand what the other team members are bringing to the table. They also have to have the knowledge offered by the user base of what data may have been compromised.

6. HIPAA and the Need for Education:

HIPAA, the Health Information Portability and Accountability Act, is perhaps one of the best known pieces of legislation to come across the security infrastructure in recent history. In 1996 Congress passed sweeping legislation to both protect the health information of individuals and to increase the ease with which that information was transferred between providers and financial institutions. This second part of the act is an important but often forgotten component of HIPAA, portability. Many of the privacy and security components and certainly the transaction code sets pertain to the portability of information. So often the thought is around the restrictive aspect of the law but many of the subtle components of HIPAA are around how to get data from one provider to another.

While there are many components to this law, Security and Privacy are key components that drive a training program in healthcare organizations. Section 164.306 of the HIPAA Privacy rule mandates that organizations subject to HIPAA must provide a “security awareness and training program”. The privacy rule goes

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

on to require that there must be training specifically on what HIPAA has defined as " protected health information" (PHI). In short the law is saying that you must meet both of NIST "Awareness" and "Training" levels of training. In the actual HIPAA Statute Section 1174(b).(1)(A)(iii) it again calls for training for any person that has access to health information.

Like many of these laws HIPAA has created many opportunities for organizations to have security breaches that are different than that of which we traditionally think. A nurse leaving a patient record visible on a computer screen is now a potential security breach. A lab report printing to the wrong printer on the network is now a security breach. With the introduction of HIPAA, events like these have become security breaches. Initially these events were thought of as privacy breaches but more and more Health and Human Services is pointing out that behind this lies the security rule and that it is enforceable and that while there is a privacy breach in play the underlying issue is a security issue that needs to be addressed. By HIPAA statute the organization is liable on both fronts.

In this instance, identifying the breach of the lab report being sent to the wrong printer truly can lead to identifying an issue along the scope of a flaw in an application. This becomes the containment envelope. Eradicating this and building your incident handling team now may involve programmers and rewriting code in an effort to fix the way the application disperses the lab reports. Once the error is repaired and the new code is tested, the fix needs to be put into production and the repaired system needs to be verified to ensure that the breach will not re-occur. The review of this process should include a review of the initial quality check process for the application install and writing. As well as how these processes work organization wide.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Users need to be educated on the HIPAA statute not just on what PHI is and how not to expose it but beyond that on the systems and how to identify when they are not working so that when a lab report prints in the wrong location they can notify the correct people and can help resolve the problem.

HIPAA has brought forward the prospects for so many different threats and the idea that we must protect against all of them. Identifying a threat is a skill that any incident handler must accomplish if they are going to have success in eradicating a problem. Certainly one of the biggest threats facing any organization today is the internal threat. These range from user error to internal espionage. In the HIPAA world massive efforts have been made to try to prevent many of these security breaches of PHI. Where the effort has fallen short is that they educate about the health record they do not educate about the security risk. Users still surf the web the same way they used to. They still email data without regard to security. But what of the other threats? More and more security professionals are starting to shift their focus away from the PHI center they have been on and back to the worms, SQL injections, and spoofed IP addresses of the hardcore hacker. The security professionals today are realizing that these alerts coming from their IDS equipment actually mean something, and they do not know what to do with them. More and more the security team is seeking out the training on the more technical attacks as they recognize that they are also threats to the PHI. Now along with the disaster plan that they are still completing and the physical security changes they are reviewing from the first rollout of HIPAA preparedness, these professionals are now seeking the training and skill set to know how to identify and stop all of these technical attacks.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Identifying and containing many of these problems in HIPAA can range from calling a person and providing education on an issue, to shutting down entire systems until a programming issue has been resolved. At the same time, the user base needs to be educated in systems such as encryption systems while the security team is educated in sniffers and IDS systems. The end goal is to ensure that PHI is not leaving the organization in unsecured formats and to unauthorized locations.

The difficult part with HIPAA is that the law is trying to accomplish two tasks. It recognizes and supports that the medical field is a dispersed process. Often providers are separate entities. Data that belongs to one organization must be sent to another for the continuation of care. At the same time the data must be protected and only the providing parties should have access to the medical record. As a security professional, considerations such as man-in-the-middle attacks and wire taps need to be considered as well as more blatant issues such as incorrect email addresses and viruses. Getting the users to understand these issues happens at a different level. They have no need to understand the technical threat. They need to understand the theoretical risk. If the user base understands that there is a risk in how they manage their data then there will be a better engagement with the security process. If the security team has a strong understanding of the technical aspects of the risks facing the infrastructure then they will have a better grasp of how to implement tools such as honey pots, IDS and IPS solutions, and NAC solutions.

Over the last few years there has been a flood of new technologies and increased understanding about how to keep this information from being disclosed across this dispersed and dynamic environment. With these new technologies, standards and information comes a need for new training. The user base has

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

needs beyond the traditional web session on PHI. They now need to understand the how, when and why behind encrypting the medical record they are sending to the insurance company. They need to understand the reasons behind the new policy that prohibits them from password zipping the radiology image and sending it across their web based mail account. A strong education program can develop ownership by the user population and then they can become a part of the incident handling team and not a potential threat. At the same time, the security team needs to learn the new tools so that they can use them effectively at all stages of the incident handling process.

7. Breach Laws and the Need for Education:

So you have the policy but never provided the training. A user emailed financial records for fifty thousand clients across the web and now it is out in the wild. This user became your incident. Now you have to assess your liability. In many states that liability is changing. Can you account for which records have been violated, and can you contain the damage? Can you do this before you legal department notifies the state and before the media is knocking on your door?

In February of 2002, California led the way by drafting one of the most comprehensive breach laws in the country. Simply stated the law requires that any organization with data containing personal information of another party, which has been breached, provide notification of the breach in a timely fashion. While there were exceptions made for delays for law enforcement, the law is fairly simple and clear. Many other states now have similar laws.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

These laws have changed the approach that many organizations are taking when they are breached. The attitude of contain and conceal is no longer acceptable. Now organizations must have a swift and efficient method of dealing with a breach. Users must be well trained and versed on how to respond when they detect a breach and they must know what to look for in a breach, as they are the front line for the security department.

Once a breach is detected the clock is now ticking for the security team to identify and contain the breach and to do any forensics that they wish to complete in a sterile environment. The incident handling team wants to have systems in place during the preparation process that are capturing data and looking for clues to help identify any event. Systems like IDS and IPS and sniffers. All of these devices will both provide logs to go back to should an event occur and also to help identify the event and the containment envelope. These systems, the affected systems' logs and data stores, and the users involved are the limited resources that the security team will have to turn to in their initial assessment. Often they will be asked to quickly decide if notification of a breach is required. At that point the process involves legal counsel and then a political and legal process may take hold of the breached environment and compromise the forensic envelope.

Training the user population on how to identify a breach as well as how to respond to a breach will shorten the response time and will maximize the time that a security team has to work on an environment. It will also help to reduce the amount of damage that a breach may cause. If the user population is educated on how to identify a breach then they will be less likely to damage any of the evidence; allowing for the security team to get a quick clean picture of the event. This often makes it easier for them to capture the event.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

In the containment stage of the incident handling process, the incident handlers managing the systems need to check several things with respect to the data. First they need to check to see if any confidential data was transferred. Second they need to look to see if in the breach any backdoors have been placed for continued or future access. They also need to see if any other systems or accounts might have been compromised so that those systems can be reset and or changed to restore security. In the event of a trojan that plants a back door such as netcat; the incident handler may spot the trojan. But if they were not familiar with the virus they may miss the payload. This is the opportunity that the incident handler will have to verify logs for tampering and cleaning. If the initial incident was web based, the handler will need to use this opportunity to check logs on sniffers and IDS equipment for signs of scripts; using ngrep to search for wget commands and account harvesting. Or, check the IDS for alerts on cross-site script signatures. This is the incident handlers opportunity to scour the system for any evidence they can find.

From a business standpoint the desire is always to avoid notification and the "black eye" of public awareness of your breach. An educated user base can help with that as they cannot only help with quick identification, but they can help identify the data set and therefore the containment envelope. This will help lead to a quick containment and therefore lead to a smaller number of breached records.

But the incident handling does not stop there and the incident handling team needs to have the education to give them the skill set to not just contain the threat but to stop the threat. Stopping an attack requires knowing how the attacker managed to gain access to your system. The NIST Model talks about the "Education" that the security professional should

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

receive. One of the best tools that a security professional has in their toolbox is the ability to train the user base. Most of the threats facing the organization today are internal threats. If the security professional can work with the organization to provide the “Training” to the user base so that they take ownership of the infrastructure then the number of internal incidents should drop.

Beyond that the security professional needs to be educated in all forms of attack so that they can eradicate an attack effectively. While an attacker may have used a trojan to make an initial attack; through that attack they may have discovered a vulnerability in the web site on the IIS server. The educated security administrator, having found the Trojan on the web server, would know to work with the web administrator to check the server for vulnerabilities and make sure that the server was patched. Running a vulnerability scan such as Nessus against the server would be a technique that both the hacker and the incident handler might want to use. Knowing how to identify these threats and also knowing how to pull in the educated administrator to form an incident handling team qualified to eradicate the threat is paramount to the process.

Hackers do not want to be found. A strong security administrator will know how to look for vulnerabilities and to look for threats. They also will know how to work with the system administrators to look for changes in the system, system logs, and system parameters to see if anyone has modified the server. Working as a team allows for the incident handling process to bring together those players which posses the best knowledge base for the situation. The NIST model allows that there is education across the entire organization. It does not specify that the training must be specific to a technology. As we see with the Federal Rules of Civil Procedure, the legal

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

staff of an organization will need training at the NIST "Education" level on these Federal Rules if they are going to be able to adequately support the security team in the incident handling process. Likewise the members of the staff that work with and administer the financial software will need to be experts both with their software and with SOX if they are going to be able to help troubleshoot a buffer overflow attack that loaded a back door onto the web server that hosts the front-end to their software. Only the people who have been educated on the systems and the laws governing those systems will be able to help the incident handler navigate the labyrinth of issues around each security event facing an organization.

8. Federal Rules of Civil Procedure:

With all of these laws it fits that there comes new rules about how to handle electronic evidence. The process by which information is passed between parties in court is managed by the Federal Rules of Civil Procedure (FRCP). Rule 16, Rule 26, Rule 34, and Rule 37. All govern how electronic media is managed in this respect. These rules cover topics ranging from retention to the format that the data must be produced when presented to the opposing party.

In 2006 the standing rules were amended to more thoroughly encompass electronic data as it is embodied today. Like most federal laws, these amendments do not dictate technologies or specific rules but rather specify expectations that will influence business practices. In the amendment to Rule 34, Subdivision (b) the authors provided that all electronic material will be provided in the same fashion that it is usually stored. While in the amendments to Rule 26 it is stated that

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

parties would negotiate what format the materials would be provided in and that all electronic material would be provided in a tangible format. In Rule 26 and Rule 33 it is stated that material does not need to be presented if it poses an undo burden but that the proof of burden is on the bearer and that the material may have to be presented to the court at a minimum.

The message that is taken from these amendments is that corporate standards, policies, and procedures need to be in place long before litigation becomes an issue. With these policies there needs to be training. This could be called to task. A good training program on your retention program is essential to ensure that your policies are being followed. Also, a firm understanding of the new FRCP by your security team and legal counsel will go along way in protecting your firm in the event of litigation. As prescribed by NIST, the training for the FRCP can again be layered. There needs to be an awareness of the Rules throughout an organization. Without an understanding of an organization's retention policies on email it is easy for an individual to either maintain an archive of deleted mail or to delete mail that could be needed in litigation.

Likewise, there should be training for both legal counsel and information technology staff on the actual rules and how they impact the organization so that they can collectively develop new policies and methods to ensure that the data infrastructure is prepared in the event of litigation. This training is part of the continuous preparation that is done in any incident handling cycle.

One of the pieces that the security team and legal counsel will need to establish will be retention policies for data. These will affect forensics, containment, eradication and repair during and incident. The user population needs to be well trained on these policies as well so that practices are

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

consistent through out the organization. In the event that there is a security event, there is always the chance for litigation. All data and evidence needs to be retained to some standard. That standard needs to have been established in advance. Not only do these standards need to have been established but they need to have been tested. If a process of assessments is in place reviewing policies and procedures and evaluating the incident handling process for the organization and the education standard for the user population, the organization stands a better chance of withstanding litigation and critique. Again, you can look at the NIST model here and apply it to incident handling. If you provide “Awareness” for the general population and “Training” for the computer population and “Education” for the security team or people who work directly with the technology or law, you will have an incident handling team that will be prepared to work with each security event and to ride out the storms of litigation, oversight, and regulation.

In the event of a breach a user needs to know what to do to preserve the evidence and process that evidence in a contained fashion to the incident handler so that an appropriate evidence trail is established. The incident handler is concerned about chain of custody. Not only will they need this if they need to hand information over to authorities, but in the event of litigation, properly established chain of custody will help when establishing a case under a Federal Rules of Civil Procedure claim or under a state breach claim.

If a user found that their computer in a chemistry lab had been tampered with, as the owner of that system, they would need to be trained in the incident handling process. They would need to know first who to notify and what to or not to touch. Second, they would need to be able to help the incident handler identify all the affected evidence so that it could be properly contained

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

and documented. As a part of that documentation, the user would need to be able to identify every one that had come in contact with the evidence, either directly or remotely, from the time that they identified the breach. They also would want to help identify everyone that might have had contact with the evidence since the last time they had been in possession of the system. Being well trained in the processes, laws, and policies governing there environment and also being well trained in the aspects of the incident handling processes that affect them will help this user process evidence on to the incident handler.

Documenting everything they do, and where possible having a witness to their work, the incident handler wants to make a bit level copy of all data using an application, such as DD, which will not modify the original data. This will allow them to do future forensics from this copy. The incident handler wants to lock all original evidence in a location where no parties will be able to tamper with it until such time as all legal claims have been settled and the data retention policies have been met. In the event that evidence needs to be handed over to police or other authorities it is best to give them copies of evidence if they will accept them. When all claims against the evidence have expired it can be signed back into production or destroyed as prescribed by the organizations policy.

9. ISO Standards and Requirements for Education:

It is not just legislation that is driving the need for education. Many firms are tuning to standards organizations such as the International Organization of Standards, ISO, for ways to meet compliance with the new laws that are governing their industries. They are also finding many of the new standards that

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

are being put forth as a solid platform from which to sell their products. Many of these standards have education components and those that do not outright require education soundly justify a good education program.

ISO-17799 is an established standard for information technology security. SANS established a comprehensive 17799 checklist that covers such a broad cross section of any organization that the burden of completing the checklist may seem daunting. A closer look at the list and it becomes clear that the task is not intended for a single security administrator, or even a security department, to accomplish. ISO-17799, and the SANS checklist are intended to be a corporate wide overhaul.

The standard talks about processes such as incident management, external facilities management, capacity planning, and information handling procedures, compliance with legal requirements, business continuity, and outsourcing. Any one of these topics will require the joint efforts of multiple players in an organization and will require new processes that training will be required for. Whenever a new system is established new education systems must be established. New standards need to be maintained and training is a sound way to keep that standard level.

With all of these laws we have talked about the different aspects of the incident handling process that are integrated into them and how education of the different levels of the user population will aid in the incident handling process. ISO-17799 is perhaps the most complete statement about this process. It has statements about every aspect of the organization and every aspect of the incident handling process. One of the components that this standard touches on is the process of repairing a system after it has gone through the other stages of incident

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

handling. Repairing a system back to its normal running state after an event has been eradicated is not just a matter of restoring a tape backup. Security administrators need to work with the experts on the affected systems to ensure that the systems are restored to their normal state, and that the vulnerabilities are not restored. Security administrators may introduce new security measures such as a honey pot to watch for a return of the hacker while system administrators may install new patches and updates to ensure that old vulnerabilities have been removed. ISO-17799 provides for measures to verify systems both from the vulnerability assessment side and from the security measures perspective. A strong standards check list can be applied by a trained incident handler both at a systemic level to the entire organization but also to an individual incident as they insure that each process is secure.

ISO-15446 was written in 2004 as a standard for managing information technology security around focused areas. It identifies key components such as “Protection Profiles”, “Target of Evaluation”, and “Security Targets”. This standard is particularly focused on more directed security environments but provides a framework that can be extrapolated to any environment that has heavily regulated or confidential assets.

As an organization adopts some of the standards identified in ISO-15446 practices will develop in the organization that will need to be transferred from the Information Technology department across the user population of the rest of the organization. This will require some form of training on these new standards. Full adoption of ISO-15446 would mandate some form of an education program. The standard in different sections, such as section 9.3, identifies objectives that are non-technical and need to be accomplished by the organization. One

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

of these is education on the processes implemented to secure the security focus.

In ISO-15446 there is a security focus that the paper talks about protecting. The security team in any organization has a focus, a core of data or infrastructure that they focus on protecting. A hacker may not start on that central core, but rather on the edge, looking for vulnerabilities: scanning with Enum for account information on the system that can then be run against John the Ripper, A Nessus scan in search of an un-patched system with easy exploits. Once a hacker has managed to find one system they will use that system to move to another, perhaps leaving a back door on the first but cleaning their tracks as they go. The hacker's goal is that central security target that the security team is protecting but by working from the outside in they hope to avoid detection and to leave multiple reentry points should they have to leave quickly. As the security team is focusing on the core, they need systems in place to watch the edge or other system. Today we have host based IPS and anti-virus software that help, but we also need educated users to be aware of their systems and the changes that happen on them. 15446's mandate for education helps with this process strengthening the protection out from the security target.

10. Conclusion:

Every incident handling process ends with a review. This should not only be a documentation process but a process that pulls all of the key players back together to review the incident for an opportunity to learn from the event for future preparation. The core of this very concept drives to the heart of the idea that incident handling is enhanced if not dependant

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

on education. Incident handling is a cycle where the top of the process is the bottom of the process. When you finish an incident you conclude every event by preparing for the next by learning from what just occurred. The top of the incident handling process includes education as a form of preparation against future events. Two key parts of that preparation are knowing the governing laws and providing the education that the staff will need. Many organizations are adopting new stringent standards from organizations such as ISO or from hardware manufacturers in an effort to find compliance with the many new laws that are coming in to play in their respective industries. Sarbanes-Oxley and Gramm-Leach-Bliley both have brought sweeping changes over how the financial industry and most corporations deal with confidential information. Their rules around information transfer and communication restrictions have affected not only how information technology departments are managing their systems but how companies are managing their data. Users need to be trained on new encryption software, privacy policies, and other rules and methods for how they interact with their systems and data.

Other rules have changed the way we interact with and how we manage our data. The Federal Rules of Civil Procedure and HIPAA both have broad impact on the users. Both will require training. HIPAA has a direct mandate for it. The FRCP will need the training and involvement of legal, technical, and other staff. If people are not trained on these laws, not only will organizations fall out of compliance and be open to sanctions but the risk to vulnerability will increase.

These laws and standards are designed to improve security for the user, public, and the company. The security team needs the user population to be a component of the incident handling team. They provide the first opportunity to prevent and spot

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

security breaches. They also possess the broadest knowledge of the data set. Their contribution will allow the security team to do a better job with preparation. The security team also needs to be well versed in the potential vulnerabilities, whether violations of the law or policies by users or intrusions and violations by Trojans, bots, and other methods of infiltration.

A strong education program is the best tool to turn the user base from a security risk to a part of the incident handling team. Education is a fundamental part of preparation, the first step in the incident handling process. A well-educated user base will be able to help with identifying security issues so that the security team can contain the event in a quick and effective fashion.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

11. References:

1: 104th United States Congress. (1996). *Health Information Portability and Accountability Act of 1996.* Washington, D.C.: http://aspe.hhs.gov/admnsimp/pl104191.htm.

2: 107th United States Congress. (2002). *Sarbanes-Oxley Act of 2002.* Washington, D.C.: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.txt.pdf.

3: California State Senate. (2002). *SB*-1386. Sacramento, CA.: http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html.

4: Committee of The Judiciary, House of Representatives. (2006). *Federal Rules of Civil Procedure.* Washington, D.C.: U.S. Government Printing Office.

5: International Organization of Standards. (2004). *15446 – Information Technology – Security Guidelines – Guide for the production of Protection Profiles and Security Targets.* Geneva, Switzerland.

6: National Institute of Standards and Technology. (1987). *Computer Security Act of 1987.* Washington, D.C.: http://csrc.nist.gov/ispab/csa_87.txt.

7: National Institute of Standards and Technology. (1998). *800-16 – Information Technology Security Training Requirements: A Role- and Performance- based Model.* Washington, D.C.: http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

8: National Institute of Standards and Technology. (2003). *800-50 – Building an Information Technology Security Awareness and Training Program.* Washington, D.C.: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

9: National Institute of Standards and Technology. (2004). *800-61 – Computer Security Incident Handling Guide*. Washington, D.C. http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf.

10: PCI Security Standards Council. (2006). *Payment Card Industry Data Security Standards*. https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf.

11: Senate Banking Committee. (1999). *Gramm-Leach-Bliley Bill*. Washington, D.C.: http://banking.senate.gov/conf/confrpt.htm.

12: Symantec. (2007). *CIO's Guide to New Federal Rules of Civil Procedure: Assessing the IT Impact of Email/file Retention on Discovery Requirements.* Mountain View, CA.: Contoural.

13: Val Thiagarajan, B. E. (2006). *Information Security Management BS ISO/ IEC 17799:2005(BS ISO/ IEC 27001:2005)BS 7799-1:2005, BS 7799-2:2005*. August 20, 2007, http://www.sans.org/score/checklists/ISO_17799_2005.pdf.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.