An Incident Handling Process for Small and Medium Businesses

GCIH Gold Certification

Author: Mason Pokladnik CISSP, CISA, mason@schwanda.cc

Adviser: Adrien de Beaupre

Accepted

Outline

1 Introduction

If you work for a small to medium size business (SMB) you are well aware that what works for a Fortune 500 company does not always work for yours. Smaller companies are often constrained in areas such as:

- Personnel – Smaller staffs often require that positions that may exist separately in a large company to be combined in smaller ones. This probably means at best you have one or two people dedicated to security and more likely it is only part of the job description for someone and not their "real job."

- Training – Even if you are lucky enough to receive training specifically on security related topics it is unlikely your entire incident team is able to attend. Finding resources that allow you get up and running (like this document) are a great way to augment a team's knowledge and get up and running faster.

- Tools – With staff attention pulled in many directions the best chance at identifying potential incidents is with tools that automate as much of the day to day operations as possible and alert when they need attention. The best of tools can even be justified by their ability to reduce the need to hire new staff. Unfortunately, you do not have a million dollar budget for security software so you will need to buy what you can and improvise with the best of what is available for free.

- Time – The luxury to work on a single project from start to completion is

a much rarer occurrence with smaller staffs. When you have servers and a network to upgrade and maintain, holding a day long committee meeting to discuss may seem like a waste of time, and it probably will be if you do not prepare in advance what you want to get out of it.

For the purposes of this paper I will assume that you have already gotten management buy in for your incident response team, but need to implement it with limited resources. A typical company wanting to apply the incident response process described here would probably have less than 500 total employees and 15 or less total IT staff including operations and programming. If your organization is significantly larger than this, you will likely be better served by another guide that will address the difficulties of dealing with getting access to people and systems spread across a large organization. For the SMBs, I will attempt to address some of the items that are either critical or just nice to have for your team, and on occasion point out some things that might best be left for organizations with more people and money. We will begin our adventure with a discussion of the disadvantages and advantages of SMBs with relevance to setting up an incident handling team. Then continue on with a step through the six incident handling steps (preparation, identification, containment, eradication, recovery, lessons learned) with a special emphasis on the preparation, identification and lessons learned phases as they are the most affected by company size. This second half of the paper is intended as a quick start guide and discussion of the checklist items in Appendix B. It should allow a new incident responder or team to verify that they have considered at least the minimum necessary set of issues in planning a small business incident response capability.

The smaller your organization is the less formal your response probably needs to be. As you read the paper you will notice many topics covered and you will need to decide what is necessary to implement in your organization based on your business's needs. If you are the only person in the IT department then you may not even need to create an incident team. However, you should consider the various issues so that you can decide how you will handle certain situations ahead of time instead of when you encounter them for the first time during an incident.

What this paper is not. It will not address all possible issues involved in the process of setting up an incident response capability in a large organization. There are many other guides and books available including the NIST *Computer Security Incident Handling Guide* and many papers available in the SANS.org reading room. A more comprehensive guide can guide you through the many political, legal, and technical hurdles involved in the process to make sure you do not overlook a major step. This paper's intention is to assist you in getting an incident response capability off the ground in a SMB environment by analyzing some of the constraints of a smaller corporate environment. It will specifically recommend that at the beginning you avoid certain things such as forensics at first in order to get a team organized and then add capabilities over time as you see the need for them.

2 Personnel Differences

Obviously, a smaller company means smaller IT staff sizes. This has many implications to explore for incident handling. On the positive side, your help desk

personnel probably know most of the companies' employees so social engineering risks may have been reduced significantly from the IT side of things. Also, job functions that might be separate in a larger organization are probably combined in a smaller one; therefore, I assume your IT department is not so large that you would have no idea whom to ask about a particular system you might have a question about.

Possible negatives may include the fact that some positions may not exist at all, such as in house legal counsel. This situation is not as big a problem as it may seem at first glance for a couple of reasons. First, the larger your company, the more politics are involved. What should be a relatively simple task such as securing access to systems to check for signs of an intrusion can be a major undertaking in a highly decentralized organization. In a smaller firm your goal should be to make sure you have a system administrator on your team accomplishing the dual goals of access and having the needed expertise and knowledge of the systems under attack to make intelligent decisions as to when something must be quarantined, and when another measure such as network filtering can give you some time to respond. Another common issue in a large organization is getting every body on your team in the same room for a drill or an actual response. In your streamlined team you have a smaller contact list and the ability to move fast, just remember to use some form of out of band communications if there is any chance that someone could be listening in on your email or other electronic communications. Cell phones and faxes (not e-fax) can keep your team updated with out tipping off the bad guys to your plans. This also brings up another problem. This smaller, faster, cheaper team is not necessarily the most resilient group. Those positions where one person wears several hats will

make your response much less effective if they are unavailable. So you should return to your networking roots and apply defense in depth. Make sure there is a backup for as many of the personnel on your team as possible.

So who needs to be on this incident response team? At an absolute minimum you need to have two roles. First, the technician, someone has to be able to examine the systems and figure out if an incident occurred and then sound the alarm. Second, the decision maker, someone who will make the business decision as to when systems can come down for repairs and when they have to stay up and be treated like a hemorrhagic fever patient that just wandered into an already busy emergency room. Anything else could be brought in on an as needed basis, but then you run the risk of not having those skills available on a timely basis. If a position does not exist at your organization, then you are going to have to rely on outside help when needed. If you read a Fortune 500 size companies' version of an incident response plan you would see a seat at the table for legal counsel, human resources, public relations, physical security, telecom, information security and IT operations as well (Nist, 2004, p. 2-11). Any of these positions that you can recruit will allow your team to handle a wider array of emergencies, and would have the added benefit of helping to keep you from violating internal policy and external laws. On the other hand in a company with 50 people just having two people on the team would be absolutely normal. After you assemble your team it is a good idea to run a practice incident on paper and see if you have the people and organizational authority on your team to respond to the "incident." If not that is your first sign you need to go out and recruit some more people for the team or possibly provide for external help by placing a consulting firm or lawyer on retainer for a future event. This is also a crucial checklist item for your post

incident lessons learned meeting. Make a note of where a lack of the proper personnel hampered your response.

Since what makes the right team varies from organization to organization instead of covering what departments need a seat at the table it may be more appropriate to discuss useful skills that you can fill in with as few or as many people it takes to get the job done in your company.

Recommended skills:

- Business Management – Someone needs to have the political authority to determine when systems can be taken down for remediation and to call in additional help when needed. If this person is missing from your team you may be looking for a job after your next incident.
- Network access – skills in this category include the ability to monitor intrusion detection systems, modify firewall access lists, isolate network segments, and tracing IP addresses and MAC addresses to specific switch ports
- Desktop and Server Administrators – These are the people with admin level access on the systems in your organization. They also have the day to day experience with those systems necessary to notice when an unknown process is running or a configuration change has been made.
- Legal/HR advice – You will eventually find it useful to have someone with experience in navigating the minefield of policies, regulation and potential lawsuits that come with an investigation. While it may feel like all they are doing is hampering an efficient investigation, in the long run they can save you from a lot of problems you might not know

about.

- Other nice to have skills – Forensics, Local law enforcement contacts, public relations, and physical security for access to cameras, card swipe data, etc.

3 Training

Since it is unlikely that you have training budget to send all of your incident response personnel and their backups to training in Incident handling, exploit techniques, forensics, intrusion detection, and legal issues it is likely you will have to learn to make due with some alternate plans.

If you do have some training budget make sure you use it. You can send part of your staff to training and make them responsible for coming back and providing internal training to other staff members. Buy lunch for your team and let your subject experts share what they know. For those people who learn best by reading, offer to pay for relevant learning materials. Having just completed SANS 504 *Hacker Techniques, Exploits and Incident Handling*, and having recently read through Ed Skoudis' latest book Counter Hack Reloaded; I can tell you the similarities in content are not surprising given Ed's hand in working on both. I'm not going to tell you that an intensive six day lab course where students get to take a shot at breaking into a staged network can be replaced by a book, but considering the cost difference you can definitely stretch your budget by having a decent security library on hand. Some of the books I have sitting on my shelf for use by our department are listed in Appendix A for your convenience.

The Internet is also the source of some of the best free training materials

available anywhere. Sites like the Internet Storm Center (http://isc.sans.org) along with providing up to date intelligence on new threats also attempt to provide training opportunities with malware analysis challenges, links to hacker challenges posted by Ed Skoudis and others. Other sources like the Honeynet Project (honeynet.org) also provides monthly packet captures for people to analyze attacks and a forensics challenge. Links to these and many more can be found in the Internet Storm Center diary http://isc.sans.org/diary.php?storyid=1725. The Open Web Application Security Project (www.owasp.org) offers several training aids to teach people about designing applications securely. These aids can help show development staff how to avoid issues like SQL injection attacks and cross site scripting issues. The NIST Computer Security Division (csrc.nist.gov) offers several useful resources including the excellent 800 series of publications covering many security topics including guides on incident management, forensics, the common vulnerability and exposures scheme, and many others.

You may also want to listen to some of the many web and podcasts out there to learn about new threats. SANS has a periodic internet threat update and stories about tools that work well on their site (www.sans.org/webcasts). A popular and entertaining webcast is available at www.pauldotcom.com and there are many others out there of varying quality just search on your favorite site for security webcast or security podcast and try some out.

4 Tools

Assembling a set of useful tools on a budget can be a major challenge. On one hand there are a plethora of open source tools out there, some are even more effective than their commercial competition. Tools like Snort, Wireshark,

The Sleuth Kit, and Metasploit are high quality and low cost tools that in experienced hands could take an incident all the way to court and win a prosecution. On the other hand, they can be extremely time intensive to tune and learn. Then there is the support issue; while in some cases free support can be extremely responsive it can be non existent in others. In the hectic times of an incident, waiting for a newsgroup to respond to your question can drive you crazy, and the day to day maintenance of any software product, not just open source, can be very manpower intensive. It is very important to make sure your toolset compliments your staff's experience and also helps prevent the hiring of new staff just to man the tools. The following list of tools is in no way comprehensive nor will they all be right for your company. They are simply tools that I personally have found to be useful. Some are commercial, some are free, but most are useful for both preventing and responding to incidents.

Websense – How about a tool where a small army of people are constantly on the search for new threats from malware to phishing on top of the standard legal blocking categories to help prevent a "hostile workplace?" Then add in a great deal of protocol level intelligence like the ability to block bot control channels through IRC and instant messaging and logging nearly anywhere your users go on the Internet. Tools like this can definitely help reduce the client side attacks that are becoming so popular now and are definitely worth the money if you can get the budget. Another tool in this category is the Squid caching proxy server using Dansguardian for URL blocking. While the Squid/Dansguardian combination is an excellent tool for the free price tag our department found the ability of Websense to block protocols and the speed with which they block new threats such as phishing and malware distribution site was

worth the subscription price.

Snort – Snort + Sancp + barnyard + squil + packet logging provide for some amazing network forensics. Set this up at important network chokepoints and you can see whether attacks succeeded without even having to check the systems under attack. While this can be a horrible pain to setup, tune and manage it is getting a little better with the availability of pre built VMWare images (http://sguil.sourceforge.net/index.php?page=vm). Somewhat faster to setup is BASE which is an alert console for snort. This will get you a functional alert system, but will require more follow up time to verify the validity of an incident.

Wireshark (Ethereal) – Amazing free network sniffer and protocol decoder. It can automatically reconstruct a tcp stream or dump a VOIP conversation to a wav file. There is no excuse to not have a copy of this around. It runs on wide array of operating systems including Windows and Linux.

Unix scripts – The creative application of the many tools available on a Unix like operating system can slice and dice data an infinite amount of ways. One of my favorite examples was provided by Mike Poor during the SANS Intrusion Detection course. The combination of five commands shown below demonstrates how to mine a Squid caching proxy server user-agent log for useful information. When you think about it there really are not that many different web browsers out there, but a lot of the spyware programs out there that communicate using http use a customized user-agent field in their server requests. Using that confluence of events you can use the following commands in a script and monitor the changes that show up in the output over time. New

entries in the list can identify previously unknown infected computers and other weird happenings on your network even if no anti-virus company has ever released a signature for your particular problem. The command *cat access.log | cut -d \" -f 6 | sort | uniq -c | sort –rn* (Poor, slide 56) can give you a list sorted by most frequently used user-agent. Doing this type of script-fu with your firewall logs, IDS logs and any other relevant data can allow you to build your own poor man's security event management system.

Nmap – Some sort of port scanning tools should be in your toolset. Using Nmap you may be able to catch a system lying when a locally run tool shows a discrepancy between the open ports on the system and what Nmap reports. You can also use it to identify other potentially vulnerable systems on your network, once you have identified how people are attacking you, by identifying the operating system and services running on them.

Incident Response Guides – Sans provides some nice first responder cheat sheets that might be worth giving to first level help desk personnel to aid in determining if something really might be an incident by providing commands to help in identifying running processes and ports on a suspect system. They are available at http://www.sans.org/score/discovery.php, or by choosing SCORE from the sans.org website and looking for the intrusion discovery section.

VMWare – Modern virtualization tools come at the right price, free, and allow you to setup entire labs on a single piece of hardware, test an unknown program in an isolated environment and then rollback to a known good configuration. This is fast becoming a critical tool for malware analysts so much so that some programs now refuse to run if they detect they are running in a virtual

environment. Other tools in this space include Virtual PC from Microsoft and the Xen open source hypervisor.

5 Time

I won't claim to be an efficiency expert. I personally tend to believe that the desire to not have to repeat boring monotonous tasks and occasionally laziness are the true mother of invention or at least most programs. I am on the other hand a proponent of preplanning. Even a few minutes spent at the beginning of the day thinking about what is coming can help you organize, prioritize and figure out that nagging thing that you have been missing the whole time. Incident management on the other hand is constant firefighting so any thought you can put into it ahead of time will make the next fire a little easier to deal with.

Of course we are dealing with smaller organizations here and if incident management was all you had to do then you probably would not be reading this. You may be the network/server/desktop/telecom and everything else that plugs into the wall manager and looking for tips. I am afraid there are no magic bullets here and what advice I will offer is also discussed in other sections but here is where you put it all together. You need to be able to put together a toolset that allows you to prevent as many incidents as you can while also helping you to deal with them when they do occur. This requires some combination of training to allow you to use the free stuff out there, money to buy the tools that are better than the free stuff and the political and business savvy to get that budget. The best tool to use to convince people of the need for new budget requests is your post incident review meeting. Security stinks in that much like engineering nobody notices all the work you did until something goes wrong. Most risk analysis and return on

investment methodologies use subjective data to come up with the justification for a project, but in your incident review/lessons learned process is actual data with real impacts that can be used to show people what happens when things go wrong. You can use this to show management why they need to spend some money to secure their systems other than some law says they have to. If I can recommend any time to stop and think about the outcome you want to achieve in advance it is before you go into the post incident review. The meeting has the potential to be a blame game, a learning opportunity, a budget builder, and a complete waste of time. Spend some time playing mental chess ahead of time thinking about who will be there, what their agendas are and how you might keep the meeting on track and you can both save time and accomplish a longer term goal like taking a vacation sometime.

6 Phases of Incident Management

So let us take a look at the six steps of incident management according to the SANS institute. There are certainly other models out there but we are looking for quick and easy and the SANS model covers all the important steps, and comes with the not so catchy acronym PICERL short for Preparation, Identification, Containment, Eradication, Recovery and Lessons learned (SANS, 2006). Others may rename or breakdown these steps into smaller pieces but they cover the same essential issues.

I will use the six steps of the SANS model to discuss the checklist items from Appendix B in detail. You may find it useful to review the checklist at the end of the paper before continuing and then reference it again as you complete your planning to make sure you have considered the relevant issues for your company.

Just remember every company is different and the smaller your company, the more likely you will not be building an entire team of people to handle incidents. If you are the only person in the IT department it would be highly unlikely to have more than one or two people handling incidents. In that case, you would want to begin with the checklist items marked mandatory and as time went by begin to address other items as you thought they might be useful. Your documentation and overall process would also likely be much less formal unless otherwise required by some form of legislation. If you are just starting out, you should create a simplified process based on the sections below and after a few incidents come back and go through the list again for ideas on what else to consider and add. By starting simple, then adding to your process over time, you can avoid the complexity of trying to do too much at once and over time you will naturally adapt the process to what fits in your environment.

As this section is kind of a cheat sheet section that distills the content from CERT, SANS and other sources it is not appropriate for use in a large organization. Things like response team charter documents and full blown incident manuals that cover all the myriad possible threats have been omitted intentionally to focus on content that is more relevant to the SMB environment.

6.1 Preparation

So much about modern network security reflects and draws from real life warfare. Modern military campaigns are as much about setting up a logistics train, and moving people and weapons to the right place at the right time as they are about shooting at the enemy since tanks and planes without gas and bullets are not very effective. In much the same way if we can get the right people, processes

and tools in place ahead of an incident we stand a much better chance of managing an incident instead of letting it escalate out of control. We have already touched on the people and tools so now it is time to look at the process.

Mandatory Considerations

The preparation phase is crucial to being able to even begin to investigate an incident effectively. Question one: What authority do you have to investigate an incident on the *companies'* network? You may have assumed that as the network administrator it was your job to do such things, but if you do not have an existing policy in place allowing you sniff network traffic, monitor employee's activities, or even check their hard drives then a whole host of federal and state laws are probably going to get you fired and possibly get you put in jail. Since we would like to avoid that, please make sure you familiarize yourself with the relevant laws such as ECPA, pen register statute, and the wiretap act (Schwarz, 2004). At a minimum you must have permission to monitor from the system owner which is the first corporate policy you must have in place usually in the form of an incident handling policy, but this can possibly be a part of an acceptable use policy as well. Then you must make sure that the expectation of privacy is no longer in place. This can be done for your own users by policy alone, but the best way is to have a policy and banner all services that will allow it so that you can monitor trespassers as well. Other policies to consider include search and seizure of any system on the network and a software auditing policy. Sample policies for these and many more can be found at the SANS policy project http://www.sans.org/resources/policies/. My company actually only has three policies related to information technology issues. The first is an acceptable use policy that defines issues such as password

requirements, informs the users that they are subject to monitoring, and details the acceptable use of business owned equipment. The second is a policy on email retention, and the last covers software auditing. We tend to try to keep our policies as limited as possible assuming there is no legal reason to do otherwise and not burden our users with a policy manual they will never read.

Now that you are less worried about going to jail we can start to talk about planning ahead of an incident. Some forethought about certain issues now can make your life much easier when you are actually dealing with an incident and all the pressures that come with it. The next few paragraphs will deal with some topics you will want to think about before the phone rings.

Another concern is sizing your team properly. As I have already mentioned a few times, it is quite normal for incident response to just be another part time duty of a network administrator or other IT staff member. No SMB I know of has any sort of security operations center where someone is just waiting for an alarm to sound, so really it comes down to a question of formality. The most effective team is going to be a flexible one. Our team only has one primary incident handler, with a well known backup not just within IT but to the whole company. Most incidents are handled by those two people; however, when any incident calls for it we can pull in all IT staff members or even activate a corporate emergency response team to handle the whole realm of additional needs such HR, public relations or bringing in outside help. All of that is a combination of one paragraph of policy and strong support from management. So, as you can see, even an informally defined group can get the job done. If you are not blessed with such as situation you will probably want as much policy in place to back you up as you find

necessary to get the job done over the objections of people who think the rules should not apply to them.

Next question, will your company interface with law enforcement? If so when will they be called in and who makes that decision? Do you have the expertise to capture evidence and preserve the chain of custody? Is your company willing to invest the time and resources necessary for a civil or criminal case including forensics and testifying? Some other common questions you may find yourself asking and some good answers are available in the SANS law enforcement FAQ http://www.sans.org/score/faq/law_enf_faq/. These are really questions for the management of the company, so the sooner you bring it up to them to consider, the quicker a response may come when a decision will be necessary. Two notable exceptions are child pornography or imminent threats to life which must be reported to law enforcement even though you can inform your employer first so they know what is going on.

Optional Considerations

When you start talking about law enforcement the next topic is usually will you collect forensic information as a part of your incident handling process? While many other guides will tell you it is a critical addition there are several factors to think about before saying yes as a SMB. Most projects that fail tend to do so because either the end goals of the project keep changing or they are too large a change to implement. If you are just beginning your incident handling process and you include forensics investigation from the beginning you are making things more difficult to get up and running. I would normally recommend starting

without it and then at a later date, when you are ready to take it on, adding it into an already working incident handling process. When the time comes to decide if you want add forensics you still need to decide what data you will collect under what circumstances as well as when to share it with the appropriate authorities. Some useful reading in this area is the NIST special publication 800-86 *Guide to Integrating Forensic Techniques into Incident Response* available at http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf. There is also a use for computer forensics as an information gathering tool. If your company is not interested in attempting to prosecute intruders you can still use forensic techniques to help understand what happened during an incident, but I will cover that in more detail in an example later.

Federal evidence rules allow what is known as the business records exemption (Kerr, 2001) allowing records collected in the normal course of doing business to be admitted as evidence so consider making sure your information collection process can include other sources such as log files, surveillance camera footage, even swipe records from a card access system. You should practice accessing all of these systems ahead of an actual incident to insure that you can do so when needed for real.

Having a set of incident handling forms can also come in handy. They can allow incident responders to make sure they have collected all of the necessary information for a response to continue without having to contact the person who reported the incident for additional basic information. A collection of sample forms that you can start with and modify to suit your environment are available at http://www.sans.org/score/incidentforms/. We usually document any incident that

is not deemed sensitive for any reason as part of our normal helpdesk ticketing system. If it is something that requires more tact, it is documented on paper and using phone communications. Either way, it is a good habit to document your incidents on a regular basis as you will never be able to recall the precise details of an incident clearly after a few weeks or months have gone by.

In order to be able to have a better grasp on the severity of a new incident it is also a good idea to keep an eye on some of the Internet's early warning systems. Spending a few minutes a day reading a few key sources can tell you if what you are seeing is just your problem or part of a larger outbreak. Chances are if you have to deal with a worm in your network someone else has already seen it and spent some time analyzing it for you. I recommend checking sites like the Internet Storm Center (isc.sans.org) every day to stay abreast of the latest issues affecting the Internet. Then on occasion spend some time reading other intelligence sources such as the bugtraq mailing list, and packetstorm.org website where many exploits are published. You may also want to join Infragard an FBI sponsored organization or other similar organizations in your area where people meet to discuss problems that tend to affect multiple companies. These can also be a good place to cultivate law enforcement contacts that could come in handy some day.

Some incident handling guides will also recommend that you setup an incident tracking system. I'm going to go back to my project management argument here and say in a smaller organization getting your team up and running is the more important concern. In an ideal world you will not have so many incidents that you can not keep track of them without another system that will have to be hardened, audited and patched. Plus to foil people sniffing on your

network that traffic will need to be encrypted as well. To start with you are better off using a notebook with numbered pages and only worrying about a tracking system later if your lessons learned process shows you need it.

One final consideration is figuring out how you can turn your users into an alert system. While your users are susceptible to social engineering and phishing attacks they also use your systems on a daily basis and will likely be the first people to notice when something just does not feel right or normal. Perhaps their computer is running slow or new popup windows keep appearing. Training your users to report out of the ordinary behavior could on one hand generate useless help desk calls or it could lead you to an incident before it has a chance to become something larger. If you already have or are developing a security awareness program this maybe something you want to consider adding. I tend to err on the side of caution here and tell my users I would rather hear about something from multiple people then never at all so send something in even if it does not seem important. Internally, when I am doing awareness training I have noticed that I get a much more attentive audience when I provide anecdotes like the absurdly high percentage of people that would give up their password for a candy bar and also give tips for protecting themselves at home (http://news.bbc.co.uk/2/hi/technology/3639679.stm). Anything creative you can do to keep your training from becoming an hour long repetition of "because IT said so" will aid your users in both retaining the message and help them realize they are part of the solution.

6.2 Identification

Mandatory Considerations

You have now reached a critical point in the process from where you will either move forward with an incident or go back to watching. Two very important decisions should have been made at this point in time. First, how are you going to define an incident? Second, how are you going to identify an incident has taken place? These questions are more subtle then they appear on the surface. You will need to have your entire help desk staff trained to recognize and quickly escalate issues to an incident team member so that a severity level can be determined. That will determine the resources necessary to respond to the incident. A simple spyware incident may only require one person to clean up and document while at the other end of the spectrum another incident may require every resource available to prevent the company from going out of business.

My company's simplified incident definition is simply any security or policy event that affects the normal operation of our computing systems. We also further define a high impact incident as one which affects several people's normal computing operations at the same time. The only difference between the two is the amount of resources brought to bear, and a requirement that appropriate management (in our case the CIO or other senior manager) be notified and updated on a regular basis.

Our contact list is pretty easy as well. All primary contacts have a corporate cell phone with a listing of all member numbers. Assuming your budget will not allow for that you will have to do a little more work to arrange for after hours

contact with home numbers. Just be careful to protect and only use those numbers in a real emergency.

Optional Considerations

So how do you get your help desk staff to identify and escalate issues in a timely fashion? Remember those first responder checklists discussed in the tools section? Well now is a good time to use them. They can let less experienced staff identify potentially out of place processes without having to be an expert on the command line or destroying too much evidence. You can also use the system survey forms from SANS to begin documenting what has been found at this point. Remember you are not going to modify anything on the system at this point in time. Any modifications to the system should not start until the containment phase. A word of warning, one peculiarity you may find when collecting information from multiple systems is clock skew. While collecting information you need to know if the time is synchronized or not to build a proper timeline. The United States has decided to further complicate the issue by changing the dates for Daylight Savings Time as of 2007 (US Naval Observatory, n.d.) so you may find yourself in a gap where some computers think the time is an hour away from other systems that have not been updated.

You will also probably want to adopt the philosophy that declaring an incident, even if you are not sure one is taking place, is preferable to not alerting and risking the possibility that something bad really is happening and you gave it/them the opportunity to continue and spread making the situation worse.

Outside of the incidents that come in through the help desk, you should also

be regularly monitoring all the tools available to you such as event logs, IDS/IPS, firewall logs, antivirus reports, file integrity tools, etc. The tools that generate the most alerts in my environment are Websense and Snort. Websense has a category to identify sites that distribute malware and the ability to block certain protocols like IRC that can be used as botnet control channels. We occasionally get an email from the system saying one of our systems is trying to connect to a forbidden place or protocol and it triggers a response to identify if that system has been compromised or not. I also monitor a Snort alert console on a regular basis and use those alerts to trigger a response if necessary. For example, we recently had an IDS alert warning that remote command shell access may have been achieved on a Windows XP workstation. That obviously got my attention, so I followed up by identifying both the workstation in question and checking for unknown processes and open ports. When that failed to turn up anything I ran an Nmap scan on the host to check for a backdoor or rootkit. When that did not turn up anything I decided to check the remote destination of the packets. Using dshield.org I looked up the IP address and it was not listed as a recent source of network attacks. Digging further I looked up the company the IP range was assigned to and found it belonged to a company we contract with for printer service. After asking the computer's user more specific questions they did admit that a printer repair tech had used the computer for about an hour while trying to perform a firmware upgrade. I finally found out that the technician had used a remote support program to get help from his help desk and Snort had caught the command prompt text in the data stream. So after an hour of frantic research I was able to close the issue as a false positive.

Using the information you collect during the identification phase you will

need to determine a severity for the incident and then start activating the proper team members to respond. That step should at least go quickly because you had the foresight to put together a contact list for your team members. Once the proper responders are in place you are ready to move to the next step.

6.3 Containment

Mandatory Considerations

You will probably need to start involving management at this point in time. What you think is critical may be different from the people who use that system to generate money for the company. It's important to both limit the risk to the organization and keep it running at the same time. That being said in a high severity event a quick response can definitely help reduce the window of time an attacker or worm has to spread on your network.

A few questions to ask yourself before you get too far along. Do you or some member of your team have the experience necessary to work on this machine? It is possible you could do more harm than good if you start making configuration changes on an operating system or router when you have no idea what repercussions your change might have on it.

Containment is not just about turning a machine off. This is an especially bad habit to get into, especially if you plan to get into forensic examination in the future. What you are really trying to do is get the system usable by preserving access for legitimate users while locking out the bad guy/worm. That might mean a patch and boot or pulling the power cord, but slow down enough to think about

and write down what you are doing and you will make better decisions.

As an alternative you may want or need to isolate a machine using, firewalls, vlans, or possibly even turning off a switch port. These solutions have the benefit of reducing the times I need to drive back to the office. You could in some situations even get your ISP involved especially in a denial of service attack. If the problem is relatively simple or the system is especially critical you may have to do what you can on the running system such as stopping processes or services and disabling accounts. Once again this all has to take place in the context of the business value of the system.

Optional Considerations

Another tool to consider for use at this point in time is creating a checklist for different predictable situations. This can aid in both preventing you from overreacting and not forgetting something in the heat of the moment. Unfortunately, these can only be built from experience, but there are a few tools that can be used in a multitude of situations and which you should consider as a starting point including, you guessed it, some from SANS in those incident forms discussed earlier.

Just when you thought it was safe to let the vendors back in the door, here is another story from the real world. In the short time period between when the patches for the August 2003 Blaster worm came out and our window for installing them we had patched nearly all of our workstations, but the servers were waiting for a monthly maintenance window. We were feeling pretty confident that the risk for infection was pretty low as we would never allow an RPC port to be available

to attack from the Internet so I saw no reason to rush the patches into production. Suddenly one by one servers start rebooting and the antivirus software alerts start coming in reporting that those same servers are reporting an infection when starting up. That is enough information to bring the entire IT staff to bear on the problem including the programming staff. About an hour later the servers have stopped rebooting but many of them show signs of infection. Within this time our lead developer has put together a script to comb through the admin shares on the servers and find out which ones need attention by identifying files left by the worm giving us the scope of the problem. The good news is after the reboot the exploit caused, our antivirus software prevented the worm from starting and propagating further. We did continue on and cleanup the files and install the patch but those are part of the eradication and recovery phases respectively coming up next. A couple of hours later we were able to track the infection to a phone vendor who had brought an infected laptop in to program a PBX and plugged into our network.

6.4 Eradication

Mandatory Considerations

Now that you hopefully have control of your system again it is time to pause and consider if you missed anything. Make sure you have at least looked at all machines with the same potential vulnerability to make sure that you are fully cleaning up the problem. Then when you have the full scope of the problem understood it is time to clean up. You need to understand the attack vector and remove it permanently as well as cleanup any remnants left over from the attack.

The cleanup can take many forms. In a simple situation it could just be running a virus or spyware scanner to remove the offending files and services and updating signatures. In a more complex world you may be faced with restoring systems from backup and then applying any patches if they exist. If not you will have to implement another compensating control such as firewalls, IPS or proxy server capable of blocking attack traffic while waiting for one. In a worst case scenario such as when a rootkit has been installed or the operating system integrity has been violated in any way it is best practice to reinstall from original media, apply patches and then restore your data. While this can be painful it may be the only way to insure a final system that you can trust again.

This is where we have started to implement an idea normally seen in larger companies. Over the last five years we have steadily been moving to a standardized environment where all hardware, laptops and desktops, are bought to match a standard configuration for a minimum of a year. Before being accepted as the new year's standard the system must be supported by a single Ghost image that we use on all end user systems. Now that our staff is experienced in building systems this way, it is usually easier to format a machine and start over again then it is to try and do any cleanup of an infection. This goes for normal troubleshooting as well. If they spend more than 4 hours working on any problems without a resolution we just reimage the computer and transfer the user's profile back on. That process only takes about 2 hours and returns the system to a known good configuration. We are even beginning to use VMWare and known good server images to provide a similar but more complicated server rebuild.

Optional Considerations

One additional note, while I cannot discuss specifics for privacy reasons I can relate that on several occasions I have found it necessary for one reason or another to collect a forensic image of a system so that one, we can have a copy of it in case that becomes necessary and two, so that we can examine the system in detail without having to tamper with the machine in question. These images are not really intended to be used for prosecution even though they could be if needed. What using forensic techniques does, is allow me to get a better picture of what happened on a computer especially compared to just examining a live system. I normally perform the collection using a distribution of Linux called Helix (www.e-fense.com/helix) that is designed to boot off a cd-rom and includes all sorts of useful tools. Once I have used a program on the disk called DD to copy an image of the hard drive to a network location I can then examine that image with several tools such as The Sleuth Kit[1] (http://www.sleuthkit.org) which allows me to look at times files were modified as well as deleted files. I can also use a tool called Liveview (liveview.sourceforge.net) to load that raw disk image into a VMware virtual machine so that I can even log into Windows and look at logs, the registry and history files easier. Liveview is nice in that it sets up the virtual machine to never modify the original image so that you can always go back to an exact copy of the original machine with no changes easily. These tools are often

[1] The Sleuth Kit is a rather advanced open source forensics tool and while it is very useful requires a basic knowledge of forensics to begin to use effectively. Start with an easier tool to learn like Liveview and if it does not meet your needs consider some training in forensics or be prepared for a lot of reading.

helpful during the eradication phase as they can give you a better picture of what is actually happening especially if the system in question has been infected by some sort of rootkit that may be actively altering the results from the operating system in order to cloak its presence.

6.5 Recovery

Mandatory Considerations

Finally, it is time to put things back into production. You will likely need to involve the end users at this point. It is time to take the system through any validation process you have before putting it into production. These tests should be the same ones used to evaluate that the system is providing good data after a new application is installed or a major upgrade has taken place.

Then once you think you have everything under control and back the way it should be it is time to monitor the system for suspicious activity. You could very well be wrong and have missed a backdoor or extra account and if the bad guys come back you want to know as soon as possible. So you need to watch log files, accounts, services, and perhaps even hash critical binaries and monitor traffic to and from the machine. After a reasonable amount of time you can reduce your vigilance to periodic checks.

6.6 Lessons Learned

Mandatory Considerations

Now is the time to put together all the information you have acquired and sit

down and figure out if your security posture needs to be modified to help prevent future attacks. This is something you will want to think about in advance and then present for comment to the entire incident management group in a post incident review meeting. There are several questions you will want to address but the one you will want to avoid is the assigning of blame if possible. If your meeting descends into finding someone to blame you will expend a lot of time and energy without improving the security of your company. Some of the questions you will want to ask:

- How can the security of the systems be improved? Are new tools available? Do you have the personnel and training necessary?
- Can your incident response capability be improved? Do you need to get training for team members? Do you have the right or enough people on the team? Is the team working well together?

Running an information system is inherently a risky activity which requires deciding what security controls needs to be in place and what risks the business will accept. These meetings should be a time to analyze if controls are doing their jobs as expected and for the technical staff to recommend new tools, training, or staff that will allow the company to proceed in a safer fashion and back that recommendation up with evidence as to why it is necessary. Your lessons learned meetings and final reports are a great source of documentation when it comes to justifying a business case or just recommending items for a new budget. Unfortunately, as with any meeting, if you go in without a clear agenda or goal most likely you will just waste a lot of time and probably not come out with your

intended results.

So you now have your meeting with the right people and the agenda setup to discuss what is working and what needs improvement. This is the time to discuss your ideas for how to improve the process. Maybe your forms need to be customized or you think you have handled enough cases and think a forensics capability would allow you to better determine what happened on a system. This meeting is the time to get your management sponsor on your side and give them the information that will allow them to build a case for you and decide what is best for the business.

Optional Considerations

In a smaller team these meetings can be much more informal. You do not need to spend a half day meeting discussing an incident everyone in your meeting was involved in. It could just be a short discussion of what is working and what is not. You just need to make sure that the discussion actually takes place whatever level of formality that requires at your organization.

One more thing you may wish to consider at this point in time is whether a drill would help the team perform better in the future. Just like testing a disaster recovery plan drilling your team with hypothetical situations can aid the team's response in a real emergency. These tests can vary from a table top exercise where people are walked through a hypothetical situation and asked what their responses would be to actually authorizing someone to be a red team and attempt to break in to the network to test the response under more realistic conditions. Just make sure you have the proper management approval and a plan to deal with

accidental collateral damage if you do go ahead with a full scale test.

As a follow up to the two examples provided earlier during our post incident reviews, which were a relatively informal meeting of the IT staff and the CIO, the decision was made in the first case (Printer tech causes remote shell alert) that while we would talk to the vendor about using company machines without talking to the IT staff, no policy or technical changes were needed. In the case of the Blaster worm it was decided that a new procedure was needed directing that no computers would be allowed to be connected to the network without being examined first for malicious processes and current antivirus software by a member of the IT staff. The procedure was created and distributed to the company. A network access control solution was also evaluated and decided to be too immature at the time, but continues to be re-evaluated periodically.

7 Conclusions

The goal by this point in time in the paper is for you to have a basic incident management process that you can take and modify for you own purposes. As discussed earlier this is may not be a comprehensive process for every company, but is intended to be a starting point and discussion of some issues relevant to the SMB environment. After completing the basic process with a few incidents, you will want to add items from the optional considerations to it as necessary to fit your environment.

Throughout the process there were a few things I recommended against trying to implement right from the beginning as they can unnecessarily complicate the process and lead to a greater chance of failure in getting an incident handling

capability up and running. Once your team has handled a few incidents it would be a good time to evaluate some tools that larger teams use. You will still want to implement them in a careful fashion to reduce the number of changes to a manageable level. A possible list includes:

- Should you begin using forensic image collection to allow for deeper analysis of the intrusion and allow for possible usage as evidence?
- Do you need a dedicated incident tracking system?
- Do you need additional resources dedicated for team usage such as cell phones, fax lines, a private meeting room or budget for purchasing items outside the normal acquisition process?
- Do you want to start cross training with systems administrators and help desk staff to improve initial identification?

It is my hope by this point in time you have enough information to begin to organize your team but you will definitely want to look over the multitude of information available out on the Internet on the subject. I have tried to point out several sources throughout the paper but you can just search for incident handling and find many more. For a quick review of the points discussed in this paper you can use the Checklists section in Appendix B.

8 References

Kerr O. (2001).

Computer Records and the Federal Rules of Evidence. Retrieved Dec. 2, 2006, from

http://www.usdoj.gov/criminal/cybercrime/usamarch2001_4.htm

National Institute for Standards and Technology [NIST] (2004). *Computer Security Incident*

Handling Guide (NIST Special Publication 800-61). 2-11.

Poor, M. (2006).

Network Early Warning Systems. Retrieved Oct. 15, 2006, from http://intelguardians.com/mikepoorkeynote.pdf.

SANS. (2006). Security 504.1 *Hacker Techniques, Exploits and Incident Handling.* Book 1

Schwarz J. (2004).

Cyber Security: The Laws That Govern Incident Response. Retrieved Oct. 20, 2006, from

http://www.educause.edu/LibraryDetailPage/666?ID=SPC0411

US Naval Observatory. (n.d.).

When Does Daylight Time Begin and End? Retrieved Jan. 10, 2007, from

http://aa.usno.navy.mil/faq/docs/daylight_time.html

9 Appendix A – Useful books in my security lending library

Counter Hack Reloaded – Ed Skoudis and Tom Liston

Malware – Ed Skoudis with Lenny Zeltzer

Google Hacking – Johnny Long

Beyond Fear – Bruce Schneier

Practical Cryptography - Niels Ferguson and Bruce Schneier

Applied Cryptography - Bruce Schneier

Information Warfare Second Edition– Winn Schwartau

The Cuckoo's Egg - Cliff Stoll

The Art of Deception – Kevin Mitnick and William Simon

Hacker's Challenge 3 - David Pollino, Bill Pennington, Tony Bradley, and Himanshu Dwivedi

Hacking Exposed - Joel Scambray, Stuart McClure, George Kurtz

Pearl Harbor Dot Com - Winn Schwartau (Fiction)

Building Internet Firewalls - Elizabeth D. Zwicky, Simon Cooper, and D. Brent Chapman

10 Appendix B - Checklist for incident response capability

Preparation phase

Mandatory considerations

- Do you have the necessary policies in place to allow you to respond to an incident?
    - Explicit authority to monitor traffic and search systems
    - Limitation of expectation of privacy for users
    - Will you banner systems?
- Do you need a formal incident response team based on your company size?
- Are you going to interface with law enforcement? If so under what circumstances?

Optional considerations

- Are you going to use forensic techniques?
- Will you practice collecting information from non computer sources such as video systems and card access logs?
- Will you use formal Incident forms and documentation?
- Should you assign someone to intelligence gathering and threat assessment?
- Do you need an incident management system?

- How will you get employees to report suspicious activities? Maybe develop a security awareness program

Identification phase

Mandatory considerations

- How will you define an incident and its severity?
- Who will respond and do you have contact information for those people?

Optional considerations

- Should you create a formal incident response plan defining incident categories and the required response capability activated?
- Can you provide tools to help desk staff to aid them in identifying problems faster such as cheat sheets?
- Do you need to consider synchronizing the clocks on your systems and network equipment to aid in creating a timeline for an event?

Containment phase

Mandatory considerations

- Do you have someone available to make the business decision about taking down a system?
- Do you have someone with the proper training to examine the system in question?
- Do you have someone with the ability to isolate the system at your network level? The ISP level?

Optional considerations

- Will you develop checklists or forms to aid responders with information they should collect or notifications that need to be made?

Eradication phase

Mandatory considerations

- How will you identify all systems that could have potentially been affected and check those systems?

Optional considerations

- Should you use forensic techniques to study the attack and understand it better?

Recovery phase

Mandatory considerations

- Do you have a procedure to make systems put back into production contain all needed patches or other controls if a patch does not exist?
- Do you have procedures to maintain a close watch on all affected systems once put back into production?
- Do you have procedures in place to make sure end user validation testing has taken place before returning systems to production?

Lessons learned phase

Mandatory considerations

- Do you have a procedure in place to make sure that all incidents are discussed at least informally?

- Do you have the right people on your team? Is the group able to communicate effectively, and does it possess the right skills to respond?
- Does your incident response capability need additional resources?
    - Dedicated resources – war room, out of band communications
    - Additional training – could be for new skills or using current tools more effectively
    - Additional staff to aid in response
    - New software or hardware to help prevent future incidents
    - Are your current tools working? This would include forms and incident management systems
    - Should you consider adding a forensics capability either for evidence collection or to just better understand what is happening on systems?

Optional considerations

- Do you need a formal lessons learned meeting?
- Do you need to produce a formal report or summary of incidents for management?
- Would a drill help fine tune your response capability? Either a table top exercise or authorizing someone to attack your systems under controlled circumstances?

Last Updated: July 27th, 2017

Upcoming SANS Penetration Testing

Security Awareness Summit & Training 2017	Nashville, TN	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, India	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Mentor Session - SEC542	Des Moines, IA	Aug 14, 2017 - Sep 13, 2017	Mentor
Virginia Beach 2017 - SEC560: Network Penetration Testing and Ethical Hacking	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Memphis SEC504	Memphis, TN	Aug 21, 2017 - Aug 26, 2017	Community SANS
Mentor Session AW - SEC504	Milwaukee, WI	Aug 23, 2017 - Sep 29, 2017	Mentor
Mentor Session AW - SEC504	New York, NY	Aug 24, 2017 - Sep 08, 2017	Mentor
Mentor Session - SEC504	Denver, CO	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS vLive - SEC504: Hacker Tools, Techniques, Exploits and Incident Handling	SEC504 - 201709,	Sep 05, 2017 - Oct 12, 2017	vLive
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor AW - SEC504	Santa Clara, CA	Sep 11, 2017 - Sep 22, 2017	Mentor
Community SANS Columbia SEC560	Columbia, MD	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Toronto SEC542	Toronto, ON	Sep 11, 2017 - Sep 16, 2017	Community SANS
SANS Dublin 2017	Dublin, Ireland	Sep 11, 2017 - Sep 16, 2017	Live Event
Mentor Session - SEC560	Dallas, TX	Sep 13, 2017 - Nov 15, 2017	Mentor
Community SANS Madrid SEC560 (in Spanish)	Madrid, Spain	Sep 18, 2017 - Sep 23, 2017	Community SANS
Mentor Session - SEC504	Arlington, VA	Sep 20, 2017 - Nov 01, 2017	Mentor
Mentor Session - SEC560	Manchester, NH	Sep 21, 2017 - Nov 02, 2017	Mentor
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, Netherlands	Sep 25, 2017 - Sep 30, 2017	Live Event