Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Small Business: The New Target What can they Do?

The increased security in larger companies is making life more difficult for attackers. Since thieves still have to make a living -- they adapted. Traditionally, small and medium sized companies have less secure systems due to reduced awareness, staff, and capital. Attackers simply retargeted their efforts. Small business averaged a cost of $1088 per employee due to cyber-attacks last year alone. (Ponemon Institute LLC, 2011) While attackers no longer score as big with each hit there are thousands more potential target...

Copyright SANS Institute
Author Retains Full Rights

AD

Small Business: The New Target
What can they Do?

GIAC (GCIA) Gold Certification

Author: Robert Comella, Gremlinscs@aol.com
Advisor: Rick Wanner

Accepted: May 22nd 2012

Abstract

The increased security in larger companies is making life more difficult for attackers. Since thieves still have to make a living -- they adapted. Traditionally, small and medium sized companies have less secure systems due to reduced awareness, staff, and capital. Attackers simply retargeted their efforts. Small business averaged a cost of $1088 per employee due to cyber-attacks last year alone. (Ponemon Institute LLC, 2011) While attackers no longer score as big with each hit there are thousands more potential targets. But what can these potential new targets do?

The simple answer is: A great deal. While it is possible to spend many thousands of dollars on security, many solutions simply require some time to implement. Others require only small capital investments. No security system, no matter the cost, is fool proof. It is often good enough for a company to simply have better security than its peers. Many attackers are looking for simple targets and will move on if they meet resistance.

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

1. Introduction

When many think of IT security they think about what they see in movies and on TV. All the meaningless technobabble about computer security in the media leads people to believe that they could not possibly understand how to protect their business. Nothing could be further from the truth! A great deal of security is not terribly complex and often does not even deal with a computer. Luckily for small business, the cost of security usually is proportional to its size and complexity. Which means that the main reason big business spends so much in security is because they have more to protect.

While security does not have to be complex or expensive it does touch almost everything a business does, and therefore can seem daunting. The silver lining of that is that it is possible to start almost anywhere in the business and make improvements. All improvements create a more secure environment over all so a business that starts a program of continued security improvement will be doing itself a favor.

It is best to have a plan. Therefore this paper shows one process for evaluating a company's current security and prioritizing projects according to their importance. Finally it gives some practical examples seen in real life.

2. Threats: Spam, Malware and Hackers …Oh My!

Anti-malware companies spend millions proclaiming to the public that there is a serious problem. Of course their next goal is to convince that same public that the product they sell is the solution to the problem. This is not exactly a bad thing because while the ads can lend themselves to hyperbole, the companies are correct. Spam, malware and hackers are a serious problem. (Ponemon Institute LLC, 2011) Their products do, to varying degrees, protect computer users from certain vulnerabilities. Unfortunately, most small businesses are too trusting. They conduct a little research, compare different security products, choose one, and install it. Then, assuming they are completely protected, they check "computer security" off their list and forget about it.

Spam, malware and hackers are a subset of all the possible threats a business may face. In addition, no single product will completely protect a business from all of them.

Robert Comella, Gremlinscs@aol.com

© 2012 SANS Institute, Author retains full rights.

Actually, it is not possible to completely protect any business. Being in business involves accepting some level of risk. Successful businesses find ways to reduce the number and severity of the threats. To do that a business must first identify the resources it needs to protect and the threats to them. Then it must systematically avoid, confront, or transfer each risk.

2.1. What are businesses trying to protect?

Businesses provide goods, services or both. Every business maintains a collection of data that enables the business to bring their particular good or service to market. Each knows where to obtain raw materials, how to add value to them, and finally how and to whom to market the final product.

Businesses must make certain information about their products available to the public to facilitate sales. They must also maintain private records of those sales as well as track the costs they incur brining their product to market. A company must protect and manage this information carefully if it wishes to stay in business and make a profit.

Not all data is created the same. Each piece of information has a different use and therefore must be protected in different ways. Product information is an example of public data. (Conrad, Misenar, & Feldman, 2010) Companies need to share it with potential clients to facilitate sales. If the data becomes unavailable sales will suffer. Another type of data would be transaction data. (Conrad, Misenar, & Feldman, 2010) In this case accuracy is of paramount importance. A customer may or may not care if anyone knows they purchased a product but if an unauthorized person changes the price after the transaction is agreed upon, either the buyer or the seller will be very unhappy. Finally there are company secrets. Things like the recipe for Coke or Hershey's chocolate. This data must be kept private -- away from anyone who does not absolutely need to know it.

There are of course other types of data but the three above represent the three major ways that data must be protected. Businesses must see to it that data is only accessed by those permitted to see it. They must also provide a means by which authorized individuals may view the data. Finally they must control who may change the data and when. In the security world, these three tenants are called confidentiality (Who

© 2012 The SANS Institute Author retains full rights.

may see the data) availability (the means to see it) and integrity (who may change it). (SANS Institute - 401, 2010) In order to survive and make a profit as stated above, a company must define and manage these three aspects of data security for all the different data types.

In order for a company, small or large, to begin the process of securing its data it must first define where that data is stored. The obvious places are in servers, desktops, laptops and even the venerable filling cabinet. Huge repositories of data exist in those places and clearly must be secured but that is only the beginning. Mobile devices are becoming a greater and greater part of the business world. Those devices are incredibly powerful and can contain as much data as a laptop of only a few years ago. Removable media devices now may contain significant amounts of data in small places. Gone are the days of the 1.44mb floppy. Today it is possible to fit several terabytes of data in someone's pocket. (Office Depot, 2012) In addition, with today's big move toward "Cloud Computing", large portions of a company's data may be hosted off site. Along those same lines, some companies outsource parts of their business. That means that some of their data is held by the company they hired to do work for them. Last, but absolutely not least are company employees. Employees carry around far more data in their heads than would fit on any laptop or smartphone. (Frank, 2012)

Each repository of data must be considered and secured differently. While it may be good practice to lock a server away in a dark, cool room, employees generally sue (or at least quit) if someone tries to do the same to them.

2.2. What is threating a company's data?

Once a small business defines what they need to protect, the next question they need to ask is, "Against what are we securing our data?" In short, there are three major factors against which companies must protect their data. The first is a direct deliberate attack. Secondly, they need to consider accidents that cause loss or disclosure. Finally, they must protect their data from the world around us. (SANS Institute - 401, 2010)

Deliberate attack is the type most think of when they begin to consider information security. Attackers, malware, denial of service and phishing all fit into this category. (Ponemon Institute LLC, 2011) These types of attacks can be launched from

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

outside the network in an attempt to gain access. An external attacker can fool an employee into doing something insecure (like installing software or clicking a link) or they could exploit vulnerabilities in a system. Doing so grants the attacker a foothold in a network. From there they can look for more vulnerable systems or people. Since many organizations implement security like a turtle shell, once a hacker penetrates the shell there is little else to stop them from infecting the entire network.

While external attacks are dangerous, internal attacks are even more so. Many companies consider their employees as above reproach. They believe that no one who works at the company would ever openly work against it. Unfortunately this is simply not true. Some of the most devastating attacks come from inside a company. (Ponemon Institute LLC, 2011) Insiders have privileged knowledge of internal systems, company policy, and corporate secrets. They also may have physical access to many pieces of critical hardware. With relative ease internal attackers can exfiltrate sensitive company information for profit, destroy hardware that provides accessibility to critical data, or simply embezzle company funds.

Security is further complicated in today's networks because it is becoming more difficult to decide the difference between internal and external systems. (Brenton, Stearns, Baccam, & Northcutt, 2009) As corporate networks expand into the cloud, outsource, and interconnect with business partners; the line between the inside and the outside of a network is beginning to blur. Any organization must carefully consider the security implications of their decision to expand their network in these ways. They could be essentially allowing the barbarians into the gate without realizing it.

Attacks are not the only thing against which companies must secure their data. People both inside and outside an organization can cause significant issues for a company's data without actually intending to do any harm at all. (SANS Institute - 401, 2010) Users lose computers and smart phones, disclose sensitive information, and delete or overwrite important files all the time. There are countless stories of employees inadvertently causing denial of service issues by plugging network wires into the wrong switch. Others tell of how people unplug power to critical servers or equipment because

Robert Comella, Gremlinscs@aol.com

© 2012 The SANS Institute Author retains full rights.

they are unaware of the effect of their actions. Data entry experts can miss-key information causing what could be deadly consequences in certain instances.

In addition, it is possible for well-intentioned employees to leak data without realizing it. (SANS Institute - 401, 2010) An HR manager who places an advertisement to hire someone familiar with Checkpoint Firewall systems inadvertently tells anyone who might be interested that their company most likely relies on Checkpoint firewalls. Many employees forward e-mails without fully reviewing the entire conversation that occurred before. The new recipient may receive more information than they were supposed to know. Social networking sites contain all kinds of data about the employees, their families, likes, and dislikes. All of which can be used by crafty people to manipulate an otherwise conscientious employee into doing something insecure or worse blackmail them into doing something illegal.

Employees and the data they possess must also be considered. (Frank, 2012) Sickness or other factors may prevent an employee from performing their normal tasks. If that employee is the only one who knows how something is done, it can cause a serious business interruption if they are sick or injured. That is why businesses considering information security must account for employee safety and attrition.

Humans are not the only thing from which companies must protect their data. Sometimes the earth itself seems out to get them. Pretty much no matter where a company is located it will have to deal with the possibility of some sort of natural disaster. (SANS Institute - 401, 2010) Wild fires, floods, hurricanes, tornados, earthquakes, blizzards, lightning, and extreme heat or cold can all have an adverse effect on computers and employees. A natural disaster may only cause a minor inconvenience or it could cause a company to lose an entire site. In the case of small business it may only have one site which makes this all the more important.

In addition to external events that could cause data loss, there are internal ones as well. (SANS Institute - 401, 2010) Fires can destroy entire plants but even a small fire that is quickly contained using the wrong type of extinguisher can destroy all of the electronic components in a server room. All computers use power to operate. Therefore losses, spikes, or times of low voltage may cause harm to servers and other computers.

Robert Comella, Gremlinscs@aol.com

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

Another issue is heat. Computers usually produce a significant amount of heat during their operation. A room that houses many computers will need cooled in order to keep the computers running otherwise permanent damage can occur.

Even if there is constant power and perfect indoor conditions machines wear out and fail, ink fades, and people retire. It does not matter how it happens, but eventually a system or person containing data will become unavailable.

All the attacks, all the mistakes, and all the disasters discussed above are all risks to a business's data. Just as each company has its own set of data; it also has a unique set of risks it must combat. Defining and combating the unique threats a company faces is what data security is all about.

3. Generic Steps to Success

Companies face all sorts of risks; government regulation, supply chain, legal, market, and information risks are common categories. While each company faces a different set of risks all companies share many of them. The techniques discussed here to combat information risks can be expanded to cover other categories as well.

After reading the first section, information security may seem too overwhelming an issue to grasp and tackle. That is not a good reason to give up. It is important for the people working to improve information security, especially those in management positions, to understand that information security is a project that is never really done. The general process of security improvement is simple but repeated forever.

First a company must identify the threats it faces. There are several methods any business can use to break the task down so they can do a thorough job of assessing their own security. Second a company must prioritize which risks they wish to tackle. Attacking them all is not possible and some will be more important than others. Third the company needs to create and implement a plan to mitigate a risk. Finally they need to check back every once in a while to make sure that the plan is being followed and that it still makes sense.

Robert Comella, Gremlinscs@aol.com

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

3.1. Identifying Risks

Before any organization can begin to make itself more secure it must first identify what threatens it. Only then can the work of correcting or avoiding those factors begin.

A company can start by making a list of everywhere it stores its data. They need to think of the categories mentioned in section two (Computers, mobile devices, removable media, paper, people etc.). (Conrad, Misenar, & Feldman, 2010) It is important to be specific about each device or location but it is possible to group like items. For example a web server is different from a file server because each has different needs, even though they are both computers. On the other hand, two user computers from accounting are likely to have very similar needs therefore they can be grouped. A business can then order the list of most important to least important.

Starting with the first item on the list an organization needs to brainstorm about ways data stored there can be accessed, modified, or destroyed without permission. They also need to think of ways the storage or delivery system for the information could fail or be disrupted. (Conrad, Misenar, & Feldman, 2010) It is not necessary to be extremely specific. A power outage is a power outage regardless of its reason. Employees given this task do not, in fact should not rely only on their own experience. They should use the internet, search out subject matter experts, or possibly hire consultants.

Despite their best efforts, the list will be incomplete. There will always be new and exciting ways for hackers to attack a business's data or some new event that no one ever thought of. Companies also tend to forget about some of the places where data is stored. Since it is a known fact that something will happen that a company never thought of, it is wise to prepare as best as possible even for the unknown.

Dealing with issues that no one thought of is part of something called incident handling. Incident handling covers more than unexpected events it also covers specific instances of known events like a virus breakout. While incident handling can fill several papers itself, it is best if companies know the highlights. There will be more on handling incidents later.

Once a company compiles a list of risks to their data they must evaluate the list in some way to determine which order to address the issues. There are two major methods

© 2012 The SANS Institute Author retains full rights.

to set the order. The first is quantitatively and the second is qualitatively. (Project Management Institute, 2004) Quantitatively is usually more complex and asks the group to look at possible losses in terms of dollars. This is a great approach especially if there is a need to convince reluctant management to back a security initiative. Most small companies on the other hand can use a qualitative approach. The qualitative method assigns categories of severity and likelihood to each risk then either charts or orders them according to the product. (Project Management Institute, 2004)

For example here is a slightly modified version of the DOD qualitative categories. (United State General Accounting Office, 1999)

For Severity:

Category I: Death, loss of critical proprietary information, system disruption, or severe environmental damage

Category II: Severe injury, loss of proprietary information, severe occupational illness, or major system or environmental damage

Category III: Minor injury, minor occupational illness, or minor system or environmental damage

Category IV: Less than minor injury, occupational illness, or less than minor system or environmental damage

For Likelihood:

Category A Frequent - Possibility of repeated incidents

Category B Probable - Possibility of isolated incidents

Category C Occasional - Possibility of occurring sometime

Category D Remote - Not likely to occur

Category E Improbable - Practically impossible

The company must assign a severity and likelihood category to each risk then build a Risk Assessment Matrix and see where each falls. Below is an example of a Risk Assessment Matrix. They can vary from company to company.

Robert Comella, Gremlinscs@aol.com

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

Severity Level	Probability of occurrence				
	Frequent	Probable	Occasional	Remote	Improbable
Category I					
Category II					
Category III					
Category IV					

	Extremely: important deal with issue immediately
	Important: Implement corrections soon
	Moderate: Implement fixes as time permits
	Low risk: Ignore with Management approval

Another method follows the same idea but simply assigns a numeric value (usually from 1-5 or 1-10) to Severity and Likelihood. The two numbers are multiplied and the projects ordered by the product of the values. (the table below assumes a scale of 1-10)

Risk	Severity	Likelihood	SEV*LIC
Antivirus out of date: Computer infection	7	8	56
Loss of Company data	9	6	54
Perimeter weak: Attack from outside firewall	6	9	54
System patch level low	4	8	32
User misuse of systems	3	10	30
Administrative Access by users	5	5	25

No matter which method is used the idea is to prioritize the list of risks so a business will know where to begin addressing them.

Understanding the severity and likelihood of a risk are the two most important factors in figuring out which order address them. There is another somewhat less important factor that should also color the decision. It is solution's difficulty. Some risks are far more difficult to solve than others. When implementing security, especially if security is new for a corporation, it may be best to tackle a few easy solutions first before hitting the big ones. Getting a few "quick wins" in builds confidence in a security team, shows management that the team is effective, and builds political capital that can be used when the security rules to be implemented later cause a little friction.

Robert Comella, Gremlinscs@aol.com

© 2012 SANS Institute, Author retains full rights.

3.2. Addressing the threats

Once a company has taken the time to understand and catalog the threats that it faces, the next logical step is to begin to address them. Companies can address threats by implementing countermeasures that reduce the likelihood or the impact of a given threat. It is not necessary that any countermeasure reduces the impact or likelihood of a threat to zero. It simply needs to reduce it to a level that is acceptable. (Project Management Institute, 2004)

Steve Jobs employed a guard for his laptop to prevent people from stealing it (it is likely he had other countermeasures in place as well). There is of course a possibility that someone could have disabled or distracted the guard and still take the laptop, but the possibility is far lower. For other less brilliant people, simply encrypting the hard drive of the laptop may be enough. While posting guards is of course more secure, most companies do not need to incur such a large expense to secure their laptops. Companies must balance security and cost to be successful

It is best to record what countermeasures a company will use to counter the risks it faces in a written format. That record should include data such as what risk(s) the measure counters, who/what it affects, how often it must be completed, who should implement it, how often it must be audited, and what happens if it is not implemented correctly. Security experts call these documents policies. (SANS Institute - 524, 2007)

A company's first step in dealing with a threat is to draft a policy that addresses it. Policy should explain what is to be done but not how precisely how to do it. (SANS Institute - 524, 2007) That way if technology or minor details change then policy is still valid. If, for example, a company writes a policy about creating backups it should state:

> *The administrator must create a full backup of company critical data (see Critical_Data_List.doc) to an encrypted removable media source each Sunday. (S)He must also create an incremental backup to different encrypted removable media on all other days of the week.*

It is clear to the reader that what is required and who is to do it. But if the company hires a new administrator the policy stays the same. The same goes for the method of backup. If a new system uses removable hard disks instead of tapes the policy still stands.

Robert Comella, Gremlinscs@aol.com

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

This policy also refers to another document. It does this to save work and keep consistency between policies. Maybe there is a policy that requires critical data to be encrypted. If both the backup policy and the encryption policy listed the critical data separately, both policies must be updated if there was a change. There is a possibility that they could get out of sync and list different sets of data. By creating one list that both policies use it is only necessary to update the list in one place. This is a two edged sword though since it is possible to update the list without informing the administrators in charge of the backup and encryption policies. Therefore it is important to list the all the policies that use a document within it. That way all appropriate administrators can be informed.

As previously stated a complete policy does more than tell the reader what is to be done. It must also define several other topics. Policies state who or what they affect. This is also known as their scope. (SANS Institute - 524, 2007) Policy authors must make certain that the scope is broad enough to encompass all pertinent parties which may be both internal and external to an organization. It must also define when and how often the policy is executed. A backup policy is likely to require daily action while a disaster recovery policy may not be used for years (never if a business is very lucky). Two other time related topics a policy must cover is how often it is reviewed and audited. Policies must be reviewed from time to time to make sure that the business has not changed so much as to make the policy in its current form irrelevant. When that occurs it needs to be updated or scrapped. Businesses must from time to time check to be certain that employees are adhering to the policies they enact. The frequency of these audits should be defined within the policy itself.

Finally, the consequences for noncompliance should be written into the policy. The consequences should be serious enough that employees are willing to change their behavior to avoid them. In many cases consequences include the phrase: "…up to and including termination of employment…" Policies without out serious "teeth" tend to be ignored and therefore are not successful in mitigating any risks. (SANS Institute - 524, 2007)

Robert Comella, Gremlinscs@aol.com

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

Policies can deal with risk in three different ways. The first and most obvious is direct confrontation. If there is no viable backup for a file server, the risk and likelihood of losing data is very high. Implementing some sort of backup plan directly deals with the problem limiting the likelihood of loss. The second way of dealing with a problem is by transferring the risk to someone else. Insurance is a good example. If a company is located in a flood plain the likelihood of flood is high and could cause major damage. Building dikes around the entire facility to keep out the flood waters or moving the facility are likely not good solutions. Therefore that company pays and insurance company to assume the risk of flood. When a flood occurs, insurance pays for the company to get back into business. This effectively reduces the impact of the risk. Finally the best solution may be to simply avoid the risk altogether. For example, some companies disable the USB ports on their employee's computers because they believe the inconvenience of not being able to plug in certain devices is outweighed by the security risks associated with the ability to use them. These companies reduce the likelihood of certain malware infections and data breaches by avoiding the problem altogether. (SANS Institute - 524, 2007)

Policy is designed to change the behavior of employees in a business and change is not always easily accepted. Employees tasked with authoring and implementing new policies must be careful not to "Bite off more than they can chew." After a company takes the time to identify and catalog possible risks to their company's data they tend to find that there are an enormous number of issues to tackle. If they attempt to define policies and inflict them on the rest of the organization all at once they are extremely likely to meet a great deal of resistance and fail in their attempt to secure the business.

A better approach is to be selective about which risks are confronted. The security team should choose one or two issues, craft policy, then implement the policy only for those issues. This approach accomplishes several goals. First the scope is manageable. A team is not trying to change the fundamental way a company does business. Next, the task can be completed in short order which means that the risk is nullified faster. There is also less push back from the employees affected by the new policy. Finally, it can be used as a learning experience for the future. Teams that

© 2012 The SANS Institute Author retains full rights.

approach security in this manner find that data security continuously improves over time. (SANS Institute - 524, 2007)

When implementing security one problem at a time, it is important for a security team to select the highest priority items (the ones with high likelihood and impact) on the list and work their way down. In the case of brand new security teams, when choosing their first few projects it is good to consider how fast policy can be implemented as well. New teams need to show their effectiveness so that C-level Employees will back them in the future when more difficult decisions are needed. If it is possible to choose a few pieces of low hanging fruit for the first projects, and get those projects completed quickly, it will raise morale and increase the team's political capital for when they need to address a more difficult issue. (Conrad, Misenar, & Feldman, 2010)

Writing policy is an art and sometimes it is best to get some help before wading in too deep. SANS maintains a site with many example policies written by IT professionals (http://www.sans.org/security-resources/policies/). Finding a policy there that is close to the needs of a business and then modifying it is much easier than creating one from scratch. Another more thorough and much more expensive option is the book: Information Security Policies Made Easy. It is an excellent resource but it does cost about $800 dollars.

3.3. Implementing Policy

Simply authoring policy does not of course make it real. It would be nice if all a company had to do was draft a backup policy and all of a sudden all the servers are automatically purchased and set up ready to go. Writing the security policy is only the first step in a project. Implementing the policy can require purchasing new equipment, reconfiguring current equipment, hiring new employees, retraining current employees, or a combination of all.

Policies that are well written will state what is to be done but it will be up to the project team to figure out exactly how they are to be accomplished. The policy can be used as a guide to create the scope of the project. In some cases a policy may require several projects to implement completely. That is okay, each scope needs to set forth specific definable requirements. The better they can be defined, the more likely the

© 2012 The SANS Institute Author retains full rights.

project will be completed successfully. The scope of a project is used to create the next necessary document called the project plan.

The project plan details what is to be done, by whom, and when it is to be completed. (Project Management Institute, 2004) It also estimates what materials are necessary to accomplish the tasks. When creating the project plan companies should consider not only what it will take to implement a policy but also what it will take to maintain the policy after it is set up. Intrusion detection systems are notorious problems in this way. SNORT, an excellent IDS, is free. It can be implemented relatively easily too. Unfortunately, setting it up is only the beginning. If no one is assigned to monitor the system after installation, the protection it can provide is never realized.

While creating the project plan a project team may realize the project will cost too much to be realistic. Since nothing has been purchased or set up this is a great time to come to such a conclusion. It gives the team the opportunity to revisit the policy (and therefore the scope) and make changes. (Project Management Institute, 2004)

Once the scope is settled, it is important to obtain "sign off" from the project team as well as the appropriate management staff. Once approval is given, the scope should hardly ever change if at all. (Project Management Institute, 2004) Other parts of the project plan may need to be adjusted to account for changing conditions but the scope should stay stagnant. If the scope of the project is permitted to change after it is agreed upon, the project usually grows and becomes unwieldy. Such projects usually end in failure.

Security projects are not different than any other project during implementation. Standard project management techniques apply. A great resource for how to manage a project is the Project Management Body of Knowledge.

Projects need a leader (or a champion) and if there is none or the person who is chosen to lead it is too distracted with other responsibilities, the project will fail. It may be a good idea to hire an external project manager for several reasons. First an external project manager has no other responsibilities in a business other than the project. That focus allows the project to move forward despite the day to day distractions that occur at all businesses. Secondly sometimes it can be difficult for existing employees to get

© 2012 The SANS Institute Author retains full rights.

others to take them seriously. For example a young IT professional may have a difficult time getting the grizzled old executive to follow a new procedure. An external expert may not have any greater knowledge than the internal staff, but the old executive perceives differently. Finally an external project leader can afford to be the bad guy in some situations. They do not need to live with the employees after the project is complete so management can use them as a scapegoat. (Kubisek, 2011)

All projects end. There are three possible outcomes. The most desirable is success. A project team created a realistic scope and managed it well. They were able to fulfill all the project's requirements. The second outcome is abandonment. If a company's situation changes it is possible that some of the projects it is working on become irrelevant. When that occurs it is important to stop work immediately as further effort is wasted. Finally a project can simply fail. There are countless reasons this could be even if the project was well managed. No matter the outcome of a project, the last thing that should be done is a review meeting. (SANS Institute - 525, 2008)

A review meeting takes a look at what occurred during the project. The point of the meeting is not to assign blame for what when wrong but to learn from both the good points and bad points of the project so future projects can do their best to implement what went well and avoid things that went poorly. (SANS Institute - 401, 2010) A review meeting can also be useful in identifying any pieces of failed or abandoned projects that could be useful to other projects so the work is not wasted.

Again a stepped approach is key. Companies who create specific well defined goals are more likely to be able to accomplish them. (SANS Institute - 525, 2008) Each time a new security goal is realized the total security of the company is increased. Over time even the most insecure businesses can protect themselves.

3.4. Maintaining Implemented Policy

Policies must be maintained in two ways. First they must be reviewed at set intervals to make certain they are still relevant. Second, it is important to check up on employees to make sure they follow the current policies.

Robert Comella, Gremlinscs@aol.com

© 2012 SANS Institute Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

Policies are not good forever. They need to be updated to reflect the current state of business and technology. (SANS Institute - 524, 2007) A policy controlling use of the internet from the 1990's would be completely obsolete in a company today. That is why many policies include date ranges for which they are valid. Otherwise employees may find themselves attempting to adhere to an outdated policy. Companies should review their policies and make sure that current technology or changes in the organization have not rendered the policy obsolete. Older policies may need to be abandoned and new ones drafted in order to keep up. Sometimes only minor changes are necessary (i.e. changes in contact information, addition or removal of systems, etc.) When changes are necessary it is important to communicate them to the necessary parties.

Checking to be certain an employee is maintaining a policy is called an audit. How often and in what manor a policy is audited should be defined in the policy itself. (SANS Institute - 524, 2007) Care must be taken at the time the policy is written to be certain that it asks employees to accomplish tasks that can be measured. For example with the backup policy above it is possible to check to make sure backups are made according to the policy by checking the logs or looking at the physical media created. If the policy simply stated that employees should "protect important company data" there are too many interpretations to decide if such a policy is fulfilled.

The purpose of an audit is to make sure that policy is enacted. Policy exists to secure the business's data. Therefore an audit's main focus should be on increasing security not trying to get an employee into trouble. To that end it may be better to think of audits as checkups. An auditor may find that a policy goes unfulfilled because of some employee's laziness or apathy, but it could also be due to a of lack of knowledge, unclear policy language, inadequate equipment, lack of manpower, or other factors. Before chastising someone, a company should work with the employee or department to remove any legitimate obstacles that prevent the policy from being fulfilled.

3.5. Incident Management

There is a less vulgar version of a popular bumper sticker that reads "Doo Doo Occurs". All organizations from the very large to the ones with only one computer experience incidents. Some attempt to confront them head on; others try to ignore them

© 2012 The SANS Institute Author retains full rights.

as long as possible. Most organizations are somewhere in the middle. Since it is an absolute certainty that an incident will occur it is always better to prepare then to try to ignore it. (SANS Institute - 401, 2010) Like so many other topics described here, handling incidents is an extremely broad subject. Many papers go into the rich detail of all of its parts. For those who wish to protect their small business from what attacks it every day an overview is enough to get started.

There are six main steps in incident handling according to SANS. They list them in the following order: Preparation, identification, containment, eradication, recovery and lessons learned. Other texts leave out preparation or lessons learned and still others reorder them slightly but the SANS list sums it up well.

3.5.1. Preparation and Identification

Preparation is the largest step but the easiest to describe. It is anything and everything a company does to reduce the likelihood or the impact of adverse events on the business.

Preparation is not the largest by a little bit it is by far the largest phase. It encompasses training of the employees or of the IT staff, building a solid perimeter, backups, building secure systems, installing countermeasures, and even reading this paper. Preparation should be the normal state of an organization. A company is always either experiencing an incident or preparing for its next one.

Apart from education and creating a secure environment, companies serious about incident handling crate a "Jump Bag". A jump bag contains all the tools and instructions necessary to deal with an incident. (SANS Institute - 401, 2010) One would expect to see things like external hard drives, floppy disks, networking tools, cat 5/6 patch cables, hubs, switches and taps in a jump bag. Usually there is an assortment of software on CD's (or some other write once read many devices). In some cases it even contains changes of clothes, MRE's, inflatable matrasses and toiletries (It is amazing how good it feels to wash your face and brush your teeth before seeing your boss the morning after an all-nighter). If a company chooses to create a jump bag the biggest rule is -- no one can ever borrow from the jump bag. It must remain fully stocked at all times. The second rule is after it is used it is immediately restocked for the next incident.

© 2012 The SANS Institute Author retains full rights.

As it sounds, identification is where someone or something detects that something is wrong. (SANS Institute - 401, 2010) Sometimes it is easy to notice. Maybe a script kitty defaced a company web site or locked up a server with a DOS attack. Other times it can be very difficult to detect. Some rootkits are designed to go completely undetected when installed. They can operate for months or years before anyone notices their presence.

Many different systems usually come together to help to detect when something is wrong. Because most data is stored electronically today many of systems are technical in nature. There are many great tools. Two examples are Snort which looks for irregularities in network traffic and tripwire that will detect unauthorized file changes. Other techniques are far less technical. Separation of duties, rotation of duties, closed circuit TV cameras, and guards are other methods used to tell when something is out of place. The most basic of all though are the eyes of a company's employees. They know how their computer is supposed to act, who should be wondering the halls, and what is usually sitting around in the office. If they are encouraged to be observant they can be extremely helpful in identifying possible issues. (SANS Institute - 524, 2007)

When either a system or individual notices something out of the ordinary, a mechanism should be in place to inform the correct people. Who the correct people are depends on the organization. Sometimes there is a dedicated individual or team. Other times organizations call an external resource. In any case once more qualified people arrive on the scene they can make a determination if the observed event is truly troublesome or only a glitch in the system. If the event turns out to be an incident it is time to move on to…

3.5.2. Containment, Eradication, and Recovery

Once an event is designated an incident, responders must make quick but competent decisions about how to prevent the situation from becoming worse. In these first few minutes responders must act very much like EMT's to contain the problem. In simple situations all that may be necessary is to shut down the problem machine or unplug it from the network. However containment can get much more complex if the computer hosts a website that generates revenue for the business or law enforcement

© 2012 The SANS Institute Author retains full rights.

wishes to gather evidence about the attacker. If the incident happens in the middle of the night and no one is around except for some lone tech, (s)he may be unsure how to respond or be concerned that an incorrect decision may endanger their employment.

A containment policy protects both the business and, more importantly its employees. Questions like whether or not to inform law enforcement, which servers can be removed from the network, under which circumstances they can be removed, and who to call should be answered in writing and communicated to everyone involved with protecting the network. That way when the inevitable incident occurs, the tech on duty is not terrified into inaction because they don't know if they will get into trouble. (SANS Institute - 401, 2010)

Once the situation is stabilized the incident moves to the eradication phase. Responders are to now clean up the issue. Depending on what the issue it how that is done can very radically. If the incident is unauthorized physical intrusion, it means the intruder is escorted from the secure area and possibly handed over to authorities. If the incident was a malware infestation then the affected machine will likely be replaced or rebuilt.

Once the problem is taken care of it is important for an organization to do more than simply go back to the exact state it was in before the incident occurred. Returning to the malware example, administrators should not simply rebuild the machine and place it back on the network. They should make sure to patch the system (or take some other action) to prevent a reoccurrence of the same issue again. This process is known as the recovery phase.

3.5.3. Lessons Learned

Once the incident is over and everything is working, everyone breathes a sigh of relief. Sometimes individuals worked with very little sleep for days in order to restore systems as quickly as possible. Once the incident ends they all can go and get deserved rest. Once everyone is rested, they can begin the very important final phase of incident handling; lessons learned.

© 2012 The SANS Institute Author retains full rights.

Shortly after the incident everyone should get back together to review what happened. They need to ask themselves which parts of the incident response went well and which did not. Were there tools that were not handy that could have made the job easier? Did a particular log entry save the day? It is important to take note of these things so the incident response team can adjust the process for the next time. This meeting is to assess the process not assign blame for things that went poorly.

Doo-doo is inevitable. An organization that has a plan to deal with it is less likely to panic and get straight to addressing the problem. When that happens issues are dealt with as quickly as possible and the organization can return to providing its normal services.

4. Policies Small Companies Should Consider

Every company is a little different. Each has its own special set of data that it holds dear, which is why security actually means something different to each. The sections above discuss the basic thought process a company must undergo in order to improve its security level. They are building blocks that any organization can use to create the unique set of security rules to protect itself.

Even though each business is different many of them face similar situations. It is logical then to study what others have done and adapt it to the specific needs of the business. The next sections convey many of the issues common to small businesses. It also suggests some solutions. The solutions presented are not by any means the only correct answer and may not fulfill all the needs of another business but, they will give a starting point for research into the best solution for a specific business.

While it is possible to make a bullet point list of all the different systems that most companies share and then discuss each one, it makes for dry reading. It also leaves out some very critical context. Managers or a security engineers must understand that almost everything they do to secure an environment will change the daily life or job of some or all of a company's employees. A bullet list of issues and possible solutions has difficulty conveying such information.

Robert Comella, Gremlinscs@aol.com

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

Deborah Sole and Daniel Wilson suggest that a story is an excellent tool to use to convey complex topics such as this one. (Sole & Wilson) Therefore, the next sections tell of a fictional company called Widgets-4-You. While Widgets-4-You does not exist, the issues it faces are very real and the solutions provided will work. Widgets-4-You is a small manufacturing company. They employ about 100 people about 80 of them work on the shop floor and the other 20 consist of sales people, engineers, accountants, and managers.

4.1. The Push

Roy set down his cup of coffee and collapsed into the chair behind his desk. He had just wasted another morning fighting with a server that should be working, but suddenly decided to lock up. There was never an explanation, not that he would understand it if he had one, so he simply rebooted the machine then logged everyone back in to keep things going. It was not even his job -- he was the plant manager not an IT guy. He had requested the owners hire an IT person to help but they were convinced that it was an unnecessary expense. So Roy did his best to keep things together and moving.

Susan from accounting appeared in his office doorway looking grim. "We have a problem." She said. She leaned against the door frame and folded her arms across her chest.

Roy took a sip of his coffee and grumbled, "E-mail's blocked again? I'll call our ISP and see if they will remove us from the black list." He sat forward in his chair and wiggled his mouse to stop the screen saver.

"More serious this time," She responded.

Tim stopped and looked at her intently. There was something in her voice that gave him a chill.

"We are missing about fifty thousand dollars from our checking account."

Roy stared at her slack jawed as she continued.

"Gene from the bank called me to ask if we initiated several transactions yesterday." Susan spoke quickly, as if the situation would end as soon as she told

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

someone about it. "Since we normally do payments on Thursday, Gene though it was strange we did so much on Tuesday. The transactions were made through our web account … they transferred not quite 50k to several other accounts at the bank." Susan took a breath. "I told her it wasn't us. The bank is investigating now to see what can be done."

4.2. Never again

A few weeks later, Roy sat at his desk relating the troubling story to Walter his new security consultant.

"Luckily Gene from the bank knows us as well as she does." Roy explained. "The bank was able to reverse the transactions and place the money back into our account before the attackers had a chance to withdraw it. The police were on hand to arrest the person who came to withdraw it but it did not matter... Turns out the woman they arrested had no idea that she was part of a scam. She told the police that she was working from home for a company overseas. She cooperated fully with the cops but their investigation stalled when they could not reach anyone at the phone numbers she provided."

Roy shifted his weight in his chair and looked across his desk at a middle aged man in a suit seated in his office. "The incident scared the pants off the owners though, and I finally got my wish for an IT staff. It took me two weeks to find and hire a smart kid named Tim. Tim suggested I find someone like you Mr. Schmitt."

Walter Schmitt was the owner of Security Pro IT. Walt often consulted with small companies about their security needs. He sat leaning forward in his chair listening as Roy recounted the events of the last few weeks. "Very lucky indeed, have you made any changes since then?" he asked.

"We stopped using web banking and told the bank to disable our account." said Roy. "The accounting folks are not very happy about it though, now Susan has to send someone to the bank almost every day."

Robert Comella, Gremlinscs@aol.com

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

"That's good for now." Walt responded. He leaned back and steepled his fingers, "What is your goal? What do you expect me to do for you?"

"The banking incident made clear to the owners that our level of IT security is severely lacking." explained Roy. "We need to improve if we plan to stay in business." "Before the incident the owners assumed the old antivirus software, the firewall sitting here in my office," Roy gestured to a computer tower in the corner of the office with a bunch of folders on it. "…and the backup server sitting beside it was good enough." Roy chortled darkly. "Clearly they were wrong."

Walt looked wryly at the server on the floor then returned his attention to Roy.

"I need you to work with Tim to make improvements to prevent this from occurring again. We don't know where to begin and need your guidance."

Walt smiled. "I can't promise you that no one will ever manage to steel money from Widgets-R-Us again. But I can tell you that we can make it much more difficult for any potential future thieves." Walt paused before continuing. "It sounds like you have management buy-in for now. That is important. I believe with the help of you and Tim we can do much."

"Great!" Exclaimed Roy, "What should we do first."

"I need information," Walt began, "Do you mind if I get Tim to collect it?"

"Not at all," Said Roy, pulling out a post-it and a pen, "I'll call Tim in now…"

4.3. Where to start

A few minutes later Tim walked into Roy's office and shook hands with Walt. After pleasantries, Tim took out a notepad so he could take notes as Walt spoke. Walt asked him to begin gathering information about the network and the systems. He requested that Tim create a network map including all the computers, printers, and servers. He also noted that Tim should pay careful attention to networking equipment, especially border devices such as routers, firewalls, and Wireless access points. After all the machines were identified Walt requested that he find out what software was installed on each. Finally, Walt asked him to locate any documentation that may exist on how the systems were built and maintained or any policies that currently exist in written form.

Robert Comella, Gremlinscs@aol.com

© 2012 SANS Institute, Author retains full rights.

Walt instructed Tim in the use of Nmap to do ping sweeps and warned him to be careful when using it for OS detection. Walt recounted the story of when he tried to detect the OS of a network node that turned out to be a plotter. The machine did not understand the mishmash of data Nmap sent it and responded by spitting an entire roll of paper out onto the floor.

He also told Tim about a tool called "The Dude" which makes a quick map of what it can find on the network. The interface can be a little flaky but it made the mapping process easier. His final piece of advice to was to check out Spiceworks. There were several powerful free tools there but cautioned him, "Spiceworks is an on-line tool that uses advertisements for their revenue stream." Walt told him. "Read the terms and conditions carefully before agreeing to use the software."

Tim reviewed his notes as he walked back to his office. It was clear that he was going to need both a Windows and a Linux workstation to use all the tools mentioned.

His first task was to download the latest versions of VMware player and Ubuntu 32 bit. He noticed that the Ubuntu 64 bit version was there too, but was concerned that some of the tools may be difficult to compile on a 64 bit operating system. Tim installed VMware player and then built an Ubuntu virtual machine, then got to work.

4.4. The first issues

A few days later Tim called Walt with his findings. After some small talk Tim got to business.

"Walt, there is very little documentation here." he started, "What docs I did find had not been updated in many years."

"I am not surprised," Replied Walt. "I see that at many companies. How did you make out with the network information gathering?"

"Pretty well," Said Tim. "The tools you told me about made it easier. I created a spreadsheet with all the systems and their information. It includes things like owner, MAC addresses, IPs, Hardware, and warranty information. I downloaded a free tool called DIA and used it to draw a map of the major sections of the network. I tried to get

© 2012 The SANS Institute Author retains full rights.

into the firewall and the wireless access points but no one remembers the passwords for them. Finally I made a list of the software I found on people's machines."

"Good job" Said Walt, "Send that information to me. What is the patch, backup and antivirus situation?"

Tim groaned. "All over the place. We have a central backup server but it only backups up the ERP package and a few public files. A lot of data is stored on employee computers and it is up to them to back it up." Tim rolled his eyes. "You can imagine how often that happens."

"All the time I'm sure!" quipped Walt.

"Exactly… Patching is left to the individual users. Some of them are rather religious about it while others have not updated since they got their computer. AV is mostly OK. We use one of the major brands. I went around to all the computers and checked the definition dates. Most of them are relatively up to date from what I saw. There are some computers where it does not seem to load properly though."

There was a slight pause then Walt began, "OK, let's start by formalizing what you have done already. The list of assets you created is very important and should be maintained going forward. We will draft an IT inventory policy were we will document how often it needs to be audited, what information should be collected and stored, and who is permitted to view it." Walt took a breath before continuing.

"The computers with the failing antivirus concern me. You will need to look into that very soon. Fixing it may require you to rebuild the machines –"

Tim interrupted Walt, "I already did. I found that Debbie's computer was one of the ones that failed. It was her job to do the on line banking before the breach. She is using the conference room computer while I reinstall her original computer."

"Good" Walt answered, "Ask Roy to if he could purchase a few new machines. That way you can have some spares around and will not have to steal the conference room machine."

Tim chuckled "I did that too."

Robert Comella, Gremlinscs@aol.com

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

Walt pressed on, "That leads me to the next thing we will need an endpoint security policy that deals with AV as well as other software we want to see on the client machines. It should have some sort of centralized console so you don't have to run to all the computers to check compliance."

"Agreed" Said Tim

"We also need to draft a Policy about system patching." Walt stated. "Look into WSUS it is free -- we also need to look at the backup situation and create a policy that addresses your needs. Finally we need to get your firewall under control. See if there is anyone who maybe noted the passwords. If you can't find anything we may need to start over. I know some great programs that will turn spare computers into decent firewalls"

Tim and Walt worked together over the next few days to write an antivirus, backup, patching, and firewall policy. Walt then helped Tim create project plans to comply with the goals set forth in the policies.

Tim presented the plans to Roy who signed off on them.

4.5. Implementing the first policies

The implementations went well but were not without their difficulties. As Tim implemented WSUS he came across several machines that would not update properly and required special attention. Some he could get to work by installing updates manually before allowing the WSUS server to take over. Others were so corrupted that he had to reinstall them. Luckily Roy agreed to purchase several desktops and laptops. Tim was able to keep employees working while he reinstalled the machines. He also had some difficulty with third party software that stopped functioning when the updates were installed. In most cases the fix was to simply update the third party software as well but there was one homemade package that needed a little extra work.

The AV package they owned did have a central Management console but it was never implemented. So Tim took the time to create a server machine and install the management software. Like the WSUS install there were several machines that would not play nice with the server. Tim ran each of the issues down and corrected them all.

© 2012 The SANS Institute Author retains full rights.

Tim never was able to get into the firewall. He decided to take Walt's advice and create a new firewall from a computer and some NIC cards. He looked at IPCOP, Endian and PFsense. After some experimentation he built his firewall using PFsense because it had all the features Tim wanted. Walt and Tim had created a rather open firewall policy to start and Tim implemented the appropriate rules in the firewall. He turned on the logging too and set a time in his calendar to review them each day.

The Backup policy needed the most work. The backup at the beginning only dealt with a few files on the server as well as the ERP package. After Tim investigated he found that the current backup did not even grab all the files necessary to do a full restore of the ERP package. He corrected that immediately and began a regular restore test.

The major problem was the amount of data on individual computers. People had folders on the file server where they were supposed to backup their data but few remembered to do it regularly. Tim decided to redirect the "My Documents" folders for the employees to the server. That way if people stored data in their "My Documents" folder it got backed up. The desktop users did not really notice the difference but the laptop users had to synchronize before they left and when they came back.

The new settings worked great but it greatly increased the amount of data stored on the file server. The tape backup unit installed there was no longer adequate. After some investigation of different solutions, Tim convinced Roy to move backup to the cloud. It was the most cost effective solution. Roy's biggest concerns were that others may have access to the data and that the company chosen would go out of business tanking their data with them. Tim explained that since he was able to set the encryption key locally the vendor has no way to decrypt the data themselves. He also deliberately chose a large well known vendor to reduce the risk of them "going away". Roy and the owners were satisfied that benefits outweighed the risks.

After a few months of work Tim had managed to complete the projects he had started. The process took longer than he had anticipated because there were many distractions. Not only did Tim need to implement the projects he had to deal with the day to day issues that came up. All in all he was doing well. The changes largely did not

© 2012 The SANS Institute Author retains full rights.

affect the employee's day to day life and average number of issues uses experienced was falling.

Last week Tim was able to restore a directory that Jim, one of the owners, had deleted by mistake. Jim was quick to spread around how happy he was about it.

4.6. Back to Web Banking

"What will it take to start using web banking again?" Susan asked. She was seated across from Tim while Walt sat at the head of the conference table.

"Up until now Tim and I focused on hardware and software issues." Said Walt. "He has made great strides in improving your networks reliability and reducing the number of incidents. There is still much to do on that front but we also need to focus on more procedural security measures."

Susan sat forward in her chair "OK, what do you need from me?"

"How many people have complete access to the accounting package?" Asked Walter.

"Most everyone I imagine," Started Susan, "Everyone in my accounting staff has worked here for years I trust them completely."

Walter nodded, "How about access to the bank accounts?"

Tim shot Walt a look of warning.

"That is restricted – it was before the incident too." Replied Susan defensively. "Only Debbie and I have access to it, though we turned it off so now technically no one has access."

Walt did his best to soften his face. "I am not questioning your team's integrity I am sure they are all good people. The problem is not with your people. The problem is, if everyone has complete access, an attacker only needs to fool one person to gain access.

"It does also allow for insider attacks too." He added quickly.

Sally noted the comment be let it slide.

© 2012 The SANS Institute Author retains full rights.

Walter continued, "If we separate people into mutually exclusive groups where each group can execute part of a transaction but not the whole thing we make it much more difficult for any potential attacker. The malicious user must fool two or more people in order to get something to occur." Walter paused and took a sip of coffee.

"Do we do this for our ERP or the bank?" Sally asked.

"Both preferably" answered Walt "But I would start with the bank. Most banks have the ability to create separate on line accounts one which can set up the transactions the other one can execute them."

"I will call the bank and see what needs to be done to make that happen." Said Sally smiling. "No more daily trips to the bank!"

Walt smiled back, "Exactly – When you set up the accounts please choose strong passwords. Tim and I are putting finishing touches on a password policy as well as an Appropriate Use Policy. He can help you choose a satisfactory password for the on line accounts."

"I will also work with you in creating security groups for our ERP package too." Added Tim.

Sally nodded. The three of them left the conference room.

4.7. Second round of projects

Sally and Tim took the next few days and created function based groups within the local accounting package then matched employees with their respective roles. They made sure that there were backups for each position just in case. When they were finished most employees had the exact same responsibilities. There would need to be some training in certain cases though.

Tim extended the functional group idea to the files stored on the file server creating permission groups for the major departments. He noted what users were to go into each group but did not pull the trigger on either policy yet.

Instead Tim started a series of security awareness meetings. At the meetings he gave employees information about how to protect themselves on line at work as well as at

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

home. He told them about tools they could add to their browsers like add block plus and NoScript. He showed them tools to help maintain their passwords like KeePass. Finally he gave the employees an idea of what types of computer malfunctions or e-mails should be considered suspicious and what to do when they noticed one.

Tim introduced the password, appropriate use, accounting security and file security policies at the awareness meetings as well. He introduced them one at a time. It gave the employees the chance to ask questions about each of the new policies and understand why they were important. Many of the employees had no problems accepting the new rules but there were some loud mouthed opposition.

Tim had the full support of Roy and the owners. They were quick to speak to the loud mouths and opposition died quickly for the most part. Bob from marketing was the biggest problem. No one knows what was said but he shut his mouth after being called into Jim's office one afternoon.

The implementation of the new security policies went fairly well. It was quickly discovered that he and Sally had missed some required access for some of the jobs but he was able to grant the appropriate access. The same held true for the new file level security.

Some of the employees started placing post it notes with their new passwords on their monitors. Tim worked with these employees to create complex passwords that were easy to remember and the incidents he found became fewer and fewer. There were some though that he theorized simply found a better hiding place for their post-it notes.

In a few weeks the employees began to accept the new policies as normal and the number of issues began to fall off. Tim began to think about what he wanted to tackle next.

4.8. Continuous improvement

With Walt's input over the next several months Tim slowly implemented more security projects. Shortly after the appropriate use policy Tim worked on remote access. He was able to implement a rather inexpensive two factor system that utilized employee cell phones. After that he moved the wireless access points outside the internal network

© 2012 The SANS Institute Author retains full rights.

and required employees to log into the wireless network using the new two factor authentication.

The next large project Tim attempted was log consolidation. It began with a time server implementation to make sure all the log sources were time synchronized. He drafted his log retention policy himself and sent it to Walt for approval. Walt was impressed with it.

Tim redirected machines to the central log server one at a time. It took him a little while with each new system. He needed to categorize the log entries. Slowly with Walt's help he was able to tune the filters on his log aggregator so that only truly interesting items got through. He slowly added systems over the next several months, each time repeating the process. It took some time but eventually he had all the machines reporting to the log server and the messages filtered.

Tim also created a separate network zone for visitors. He found that there were a lot of people who came to the company. Salespersons, and clients were often on site and many of them wanted access to the internet. The new zone allowed filtered access to the internet but not access to the internal network. The company owners and salespeople were thrilled they had a method for dealing with the common request.

While Tim was implementing the new central logging server and the guest network he spent much of his other time writing. He documented as many of the various IT procedures he could. Tim also helped others document their jobs as well. Eventually it was clear that there was need for a central place to display all of the procedures that were written.

Tim installed a wiki server and taught a few people how to update it. Once there were enough policies posted he introduced it at one of his now monthly awareness meetings. People were thrilled and it was not long before Tim's policy wiki became a central place for storing all sorts of data.

He also worked with Walt, Roy and the owners to create an incident response policy which included the creation of a jump bag. The policy gave Tim the power he needed to make emergency decisions about the network without first consulting Roy or

© 2012 The SANS Institute Author retains full rights.

the owners. The policy was put to use shortly after it was written when one of the salesmen returned from a business trip. His laptop was infected with a worm which tried to infect as many other systems as possible.

When Microsoft introduced a new version of their operating system Tim seized the opportunity to standardize the workstation and laptop image. He built a standard image with all the software he commonly installed on the computers. It made the conversion much simpler.

It took a while but Tim eventually convinced the owners to build a server room out of an unused old literature storage closet next to the service elevator. The room was actually rather large and easily had space for all the companies servers. The doors were secured with different keys so that only a select few had access. It also had its own air conditioner and power supply. The power supply was wired into a large UPS system into which Tim plugged all the servers.

4.9. Three years after the initial incident.

Tim's phone rang he answered and was happy to hear Walt's voice. "How have you been? I have not spoken to you in a while!" Tim said

"Doing great" replied Walt. "I just thought I would check in and see how things were going."

"Very well" Tim answered. "I just finished encrypting Roy's laptop. I showed him how to encrypt his smart phone and he told me that he could take care of it. Once his devices are finished the encryption project will be complete."

"Sounds good" Walt said proudly. He was proud of Tim too. He had spent a lot of time teaching him about secure computing and Tim was a good student. "What do you want to tackle next?" he asked.

"I am thinking about intrusion detection." Said Tim. "Maybe OSSEC for the hosts and Snort for the network."

"A laudable goal, Tim, be ready though, both of those systems will generate a great deal of logging information. If you have the time to review and act on the

© 2012 The SANS Institute Author retains full rights.

information, they provide excellent protection. If you don't, they only use up resources." Cautioned Walt.

"I understand. It will likely be best to experiment with a few systems and move on from there." Replied Tim.

"Do you see many incidents like the one that started this process?"

"I investigate several events a week. A few turn out to be incidents, but nothing as bad as the bank theft." Said Tim. "One of the salesmen had his laptop stolen while he was a conference a few months back. That prompted the encryption project."

Walt was genuinely pleased and told Tim, "I am very glad it worked out there as well as it has. Please let me know if I can help you in the future."

"I appreciate your help." Replied Tim. "Goodbye for now." With that Tim hung up the phone, turned to his computer, Googled OSSEC and began reading.

5. Conclusion

Back in the '80's a popular cartoon used to run little 30 second shorts aimed at kids. The show warned kids not speak to strangers or gave other useful tips. Every one of them ended with the same quote: "…and knowing is half the battle!"

As cheesy as those little cartoons were, the message is largely the same for small business today. Once they know the threats they face, they can find ways to mitigate them. Small businesses must also be aware that security is not a fix it and forget it process. The bad guys are always finding new ways to steal data so business must always update their security to match. Finally there is not always a need to spend great amounts of capital to combat a threat. Sometimes it is better to simply avoid a situation than to try to mitigate the threat it poses. When that will not work there are many low cost and open source tools available.

The short story about Tim described many of the things a business can do. While it was of course fiction the concepts and tools are real. Some examples of the tools used to accomplish the things Tim did in the story are listed in the Appendix. Also listed are their costs and where to look for them. Bottom line -- it is a risky world out there but

© 2012 The SANS Institute Author retains full rights.

small businesses can keep themselves safe with forethought, preparation and a little capital.

6. Bibliography

Brenton, C., Stearns, W., Baccam, T., & Northcutt, S. (2009). *Security 502 Perimeter Protection In-Depth.* Washington DC: SANS.

Conrad, E., Misenar, S., & Feldman, J. (2010). *CISSP Study Guide.* Burlington: Elsevier.
Frank, B. (2012). Five Tips to Reduce Knowlege Loss.

Kubisek, J. (2011, 08 15). Tricks From a Successful Project Manager. (R. Comella, Interviewer)

Office Depot. (2012, 4 29). *Fantom Diamond 2 TB 3.5" External Hard Drive*. Retrieved 4 29, 2012, from www.officedepot.com: http://www.officedepot.com/a/products/878782/Fantom-Diamond-2-TB-35-External/

Ponemon Institute LLC. (2011, August). Second Annual Cost of Cyber Crime Study. Traverse City, Michigan, USA.

Project Management Institute. (2004). *A guide to the Project Management Body of Knowlege Third Edition.* Newtown Square: Project Management Institute.

SANS Institute - 401. (2010). *Sans Security Essentials.* Washington DC: SANS.
SANS Institute - 524. (2007). *Management 524 Security and Policy Awareness.* Washington DC: SANS.

SANS Institute - 525. (2008). *Project Management and Effective Communications for Security Proffessionals and Managers.* Washington DC: SANS.

United State General Accounting Office. (1999, November). Information Security Risk Assessment Practices of leading Orgaiizations. Washington DC, USA.

Robert Comella, Gremlinscs@aol.com

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

7. Appendix

This is a quick list of the tools that Tim could have used for each of his projects in the story. These are only a few examples of each class. Please do not think of this as an endorsement of any of them. A business should evaluate carefully any tool they are going to add to their network to make sure they are complying with any license agreements required as well as to make sure the tool fits their needs.

Category	Product	Site	Cost	Description
General	Ubuntu	http://www.ubuntu.com/	Free	Ubuntu is an entire operating system based on a Linux kernel. It is easy to install and use. Some Software requires a Linux box to use.
	Dia	http://projects.gnome.org/dia/	Free	Diagramming software Like Visio but not quite as nice.
	Open Office	http://www.openoffice.org/	Free	Microsoft Office clone that is free.
	LibreOffice	http://www.libreoffice.org/	Free	Fork of Open office that has slightly different features.
	Vmware Player	http://www.vmware.com/	Free	Vitalization software that works on Both Windows and Linux. Great for testing.
Info Gathering	NMAP	http://nmap.org/	Free	Versatile tool. Mapping, packet generation, os identification, some security testing
	The Dude	http://www.mikrotik.com/thedude.php	Free	Tool to help map networks automatically installs and graphically maps the network for you.
	Spiceworks	http://www.spiceworks.com/	Free	A complete set of tools for a network. Very comprehensive but on line
Firewalls (PC Based)	Endian	http://www.endian.com/en/community/download/	Free/Paid	Great firewall with lots of features
	PFSense	http://www.pfsense.org/	Free	Fantastic firewall with tons of features available

© 2012 SANS Institute, Author retains full rights.

				through add-in modules. Fast and small – Slightly advanced setup
	IPcop	http://www.ipcop.org/	Free	Great Firewall with fewer features but simpler setup
AV	Avira	http://www.avira.com/en/avira-free-antivirus	Free/Paid	Free for home use. Paid business licenses. Very good detection rate
	E-eye	http://www.eeye.com/	Paid	Great complete endpoint protection. Price not bad
	Symantec	http://www.symantec.com/index.jsp	Paid	Huge market presence. Not a bad product (especially newer versions)
	Avast	http://www.avast.com/en-us/index	Free/Paid	Good product with very small –and frequent-definition updates
	ClamAV	http://www.clamav.net/lang/en/	Free	Completely free but has limited cleaning options and tends towards false positives. (better safe than sorry though)
Backup	Mozy	http://mozy.com/?ref=3f9a896b&kbid=143547&sub=main&m=8	Paid	Online backup tool with large following. Pay per month
	Dropbox	https://www.dropbox.com/	Free/Paid	Can be used for small time backup but mostly for easy file sharing.
	Carbonite	http://www.carbonite.com/en/3	Paid	Online backup tool with large following Pay per year
	Wuala	http://www.wuala.com/en/pricing/	Free/Paid	Online backup tool focused on security.
	Crashplan	http://www.crashplan.com/	Free/Paid	Interesting tool that uses computers in other locations (all owned by client) for completely free backup solution.
	Rsync	http://ss64.com/bash/rsync.html	Free	Completely free backup solution based in Linux command line (front ends are easy to find) very efficient.
Updates	Wsus	http://technet.microsoft.com/en-us/windowsserver/bb332157	Free	Microsoft's free tool for maintaining its own software.
	Secunia	http://secunia.com/	Free/Paid	Free for home use tool that

© 2012 The SANS Institute Author retains full rights.

				will keep all software up to date. More comprehensive paid tool for business available.
Encryption	Truecrypt	http://www.truecrypt.org/	Free	Tool to encrypt files, partitions or entire drives. Extremely secure
Internet	Keepass	http://keepass.info/	Free	Tool to maintain strong passwords across all sites that need them easily.
	Noscript	http://noscript.net/	Free	Prevents websites from running unauthorized scripts inside your browser.
	AddBlock Plus	http://adblockplus.org/en/	Free	Blocks most adds from appearing on sites
Log Aggregation	Splunk	http://www.splunk.com/	Free/Paid	Free for small amounts of logs but has great interface and filtering tools
	Rsyslog	http://linux.die.net/man/5/rsyslog.conf	Free	Drop in replacement for syslog for a Linux log server.
	loganalyzer	http://loganalyzer.adiscon.com/	Free	Front end for rsyslog
	SYSLOGNG	http://www.balabit.com/network-security/syslog-ng	Free/Paid	Replacement for syslog with additional features.

Robert Comella, Gremlinscs@aol.com

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced