Threats and your Assets – What is really at Risk?

Date Launched: Aug 10, 2004
Last Updated: Aug 10, 2004
Section: Articles :: Misc Network Security
Author: Robert J. Shimonski

In this article we will cover some of the most important items you will need to consider when discussing, analyzing, designing or implementing a security posture within your place of business, or perhaps in a company you may be servicing. Considering that threats and their origins are constantly changing... shifting, we need to (as Security Analysts/Engineers) focus on what those threats are, where they originate from and what we can do about them as well as deal with their drift from the norm which was basically from being heavily focused on external threats to being in balance with internal threats. This article covers those details as well as why 'Defense in Depth' is so critical. We will also focus on Microsoft products (as well as other technologies) while doing so.

Introduction

Before we get into detail about what the article is going to cover and help demystify steps need for assessing your current security posture, we would need to know a few basic terms and what they mean so when used in the context of this article, you have complete understanding of what it is they mean and are referring to.

- **Threat**: An expression of an intention to inflict pain, injury, evil, or punishment as well as an indication of impending danger or harm. It's also considered a possible danger or menace. In the Information Technology (IT) arena, a threat is anything that is what was mentioned but in the realm of IT. In simpler terms, a threat is anything that you feel would hurt your company's assets, especially those such as your data, or anything else contained on the computer network and its systems as well as the systems themselves.
- **Assets**: Anything of value, a useful or valuable quality or thing; an advantage or resource. Again, in the IT realm, this would be considered data, the systems that the data is contained on or the infrastructure that connects such systems. Think of the costs associated with your infrastructure, the human resources needed to run them, and the data (your company data) that those systems contain. Most top level executives today are starting to see that all three pieces of this IT paradigm make up the whole... the systems, the people who run them and the data that they contain – in the real word production environments of businesses today, to not consider all three important assets is quite foolish, and together, that sum of the parts should be considered the 'complete asset'.

Why is it important for you to know such terms? Well, when we start to talk about the origins of threat which can be internally and externally, we would need to understand what a threat is, what the differences are between the different sub categories of threats, and what the threat is against, which is generally your assets. Again, the point of this introduction is to really prime you to think (using specific terminology) like an IT Security Analyst, more importantly, define the terms you will hear me talk about throughout. If you do not know what a threat is in basic terms, or what an asset is to you, then the article may not make much sense. That being said lets move on to the meat of the article... which is what the different kinds of threats are, where they come from, what you need to consider about them, and what damage such threats can have on you, your company, and the network and systems you work with.

The 3 part Information Technology Paradigm of Assets and Threats

You should see by now that threats and assets go hand in hand. All three subcategories of IT assets also have very specific and unique threats associated with them. Before we begin this section, I would like to make a disclaimer that what I am mentioning as the '3 part IT paradigm of assets and threats' is something that I created myself to help 'explain' the basic connection between what assets should be considered when considering what threats could be associated with them. Also, it should help you formulate a connection between assets and threats more logically. The three parts can be seen in figure 1.

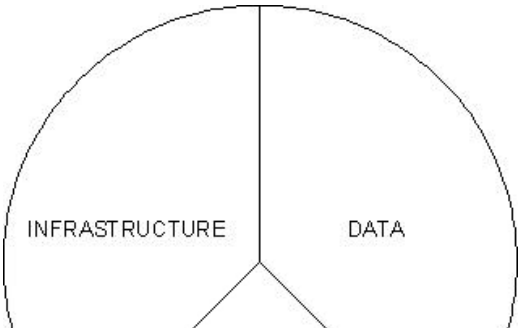


Figure 1: 3 main assets within the IT realm

As an example, let's look at a simple network in theory. If you had a simple network with a one subnet LAN with about 50 hosts (with PCs), 1 database server, 1 file server, 1 print server, one Active Directory (Domain Controller - DC) server a layer three switch, a router and a firewall (for an Internet connection and VPN), as well as 2 administrators running the show, you need to consider what your assets are here. Let's break that down in bullet format:

- 50 PCs with end users connected to them and the applications they run
- Systems - 3 servers (file/print/database and directory)
- Network and security Infrastructure – switch, router and firewall
- 2 administrators
- The data contained on the systems deemed valuable

Yes, there are threats associated with all parts. Think of it like this:

- Your end users can cause you security problems like trying to hack the internal systems, deleting data, downloading malware... the list can go on for about 20 pages when considering what 'end users' can or will attempt to do to the internal network
- Your systems can crash if not maintained properly, they can be hacked from internal and external resources, again, the list can go on and its not this articles intention to tell you what every threat to your assets are, just to make you aware that you have to think about them in general
- Your network infrastructure can suffer much of the same issues that your systems would. Also, both your systems, client AND network infrastructure can be turned into weapons if exploited... DoS attacks stemming from Trojans installed on clients, Smurf attacks launched off your routers, penetration attacks on your firewall and an intruder allowing private address blocks (RFC 1918) to ingress into your LAN – these are just but a handful of what you could expect
- Your administrators could forgo change control and topple your network if not supervised properly and monitored, also they could cut corners and take big chances based on a lack of knowledge of what their managers may know if they are not IT savvy (which is all too common) are just a few of the threats associated with the IT human resources. Also, a big threat that I also consider which many companies do not is the lack of dedicated IT resources in house, which could be a huge threat to a company. For one, if you have only one administrator that knows everything and does not have a 'primary' / 'secondary' relationship with their management team, or another administrator, then you could face a big threat of that one person knowing all your IT systems and if that one person leaves, you are (pardon my French) - completely screwed. All too many times the budget looks great to hack IT resources, but hey, you get what you pay for. You have one guy leave and your network suffers. Another possible threat is not having a dedicated IT security resource onsite and making 'security' some poor dopes collateral duty. If I had a penny for every time I saw this in practical application, I would have been retired comfortably 4 years ago.

In sum, this is just meant to make you aware of only a handful of threats to your three main assets... the systems, the data on the systems and the people who run the systems and take care of the data. Although I took a more casual route to explain this and even used a joking tone here, this is not a joke and as a Security Analyst it's critical that you consider all the direct (and sometimes indirect) threats you can encounter when analyzing your companies assets.

Threat Types and Categories

So, now that we have looked at the difference between threats and assets, defined them and looked at how they relate, we should get more in depth with some very specific categories of threats what could constitute a threat. There are many different types and they fall into very specific and unique categories.

- **Recon (Reconnaissance)**: When an attacker 'probes' your network or systems (knocking on your door) to see if you are there, and if possible, to map your network and systems for a future malicious attack. Looking for vulnerabilities is common, this can be done from scanning systems for open ports, using commands such as ping and traceroute (tracert in Windows) to map a path through the network or what hosts make up a subnet on your edge and DMZ, doing ping sweeps for mapping purposes or just simple eavesdropping if you can start a Man in the Middle attack or somehow get a Sniffer on the network to analyze with. A solid way to do a recon attack would be to find a Linux system on a DMZ, try to gain Root access... get in and launch Tethereal or Tcpdump to gather information crossing the wire after your make the Linux systems NIC promiscuous. This is a simple example, but hopefully this drives home how bad a Recon attack is and what kind of 'Threat' it creates. Figure 2 shows you the use of a commonly used tool that can show vulnerability assessments. It's freely available on the web and can be used by attackers rattling your door, checking to see what you have left opened.

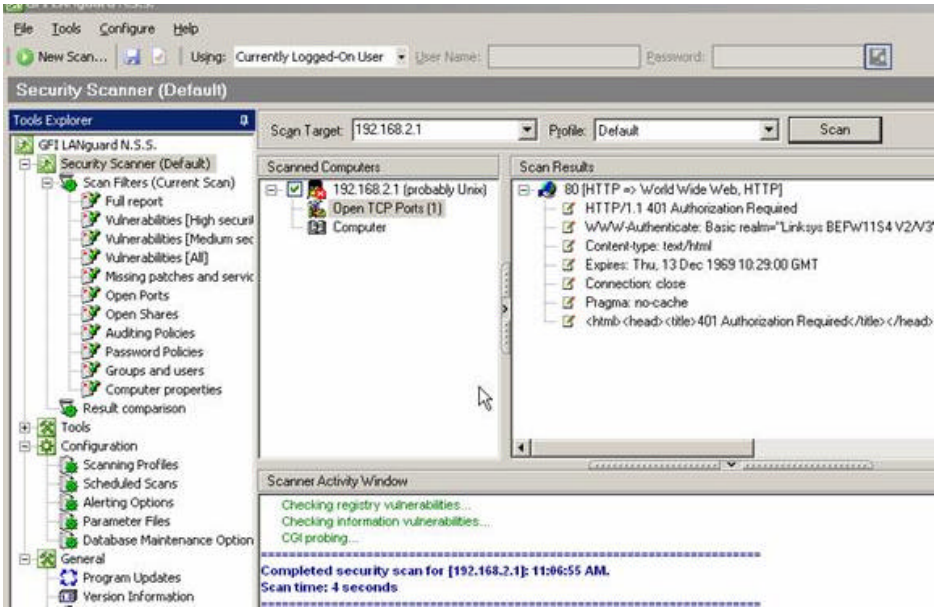
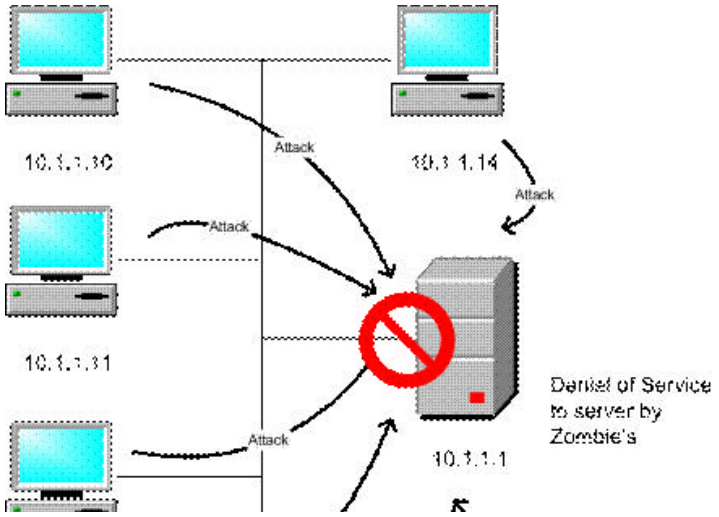


Figure 2: Using GFI LANguard N.S.S.

You can find this software here: http://www.gfi.com/downloads/downloads.asp?pid=8&lid=1

- **DoS (Denial of Service):** I mentioned this before when we discussed the 3 assets and what threats could be associated with them. A *DoS attack* is very serious in nature and it's simple to perform. Many efforts have been made to patch systems that could either launch a DoS attack or be affected by one, but to think that top level hackers (the Elite) aren't constantly working on new ways to exploit systems is foolish. This recent rash of Virus and Malware activity this month should show you that there is no shortage of people working to exploit and topple your systems. Also, to not consider the trillions of Script Kiddies (the bottom of the Hacker barrel – the folks who use the simplified, documented and freely available tools that the Elite create) is also very un-wise. DoS attacks are nothing more than an attack against your system(s) that will result in that system not being able to do its intended job (or purpose). A very common one for Microsoft systems in the buffer overflow. This is only one exploit, there are many others… for instance; consider an Internet access router that sits on the perimeter of your network serving packets to and from. If someone on the Internet can successfully install Trojans (which is simple to do by just emailing/spamming them from somebody's open email relay) on unknowing recipients' PCs, those hacked systems could be grouped en masse and used as a single weapon against your Internet access router. If your Internet access router is not protected or hardened, its more than likely you will feel a pinch when the DoS starts… Once the PC's have been exploited with the Trojan, they can be controlled to send a flood of traffic to your router. Since the group (called a Zombie Hoard) does not know what is being done, they are effectively launching a DDoS (distributed DoS) attack against your router, hogging its CPU and input buffers so legitimate traffic cannot pass it. Simple to do, simple to stop but you have to first consider that your assets (your router and the Internet connection that feeds life into your LAN) and the people who run them (hopefully patching the devices to stop this kind of attack, or using some rate limiting downstream from your upstream ISP… this is all important to consider. Think of an old Windows 95 PC, did you know that this operating system (because of a lack of control on the ping packet size) can be 'used' to perform a ping of death that can crash unsuspecting systems? Did you know that there are freeware utilities (for Script Kiddies) that can send malformed packets to systems and crash them? Knowledge is power – knowledge is another one of your precious assets.



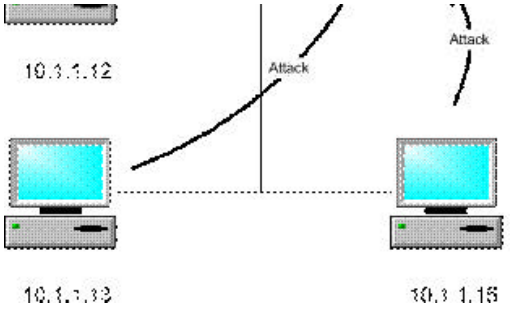


Figure 3: DDoS Attack

- **Manipulation (Data Manipulation):** Data manipulation is considered a very large threat today because data is what our paperless society has come to not only depend on, but dang... can't survive without. Data manipulation is a huge threat. Consider your administrators (or worse, some help desk technician with too many rights to the system) getting upset about managements decision to not give them another raise this year because IT is considered a 'hemorrhaging ulcer' instead of a 'real business asset' – didn't think if it that way, did you? As a Security Analyst, you have to really consider this as a threat. Other threats can include, but are not limited to *Man in the Middle attacks* where an attacker can insert themselves 'between' two communicating parties and intercept the traffic, read it, and perhaps alter is as seen in figure 4. Other ways data can be manipulated if is you have a DNS server on your DMZ, its exploited and records are changed (manipulated) to another IP address of a mock site that your customers now go to (DNS Poisoning), or worse, a bit bucket black hole that leads nowhere sending your customers and business partners into deep thought about how 'on top of things' your company really is. What are the assets? Your systems, the data on them and the people who take care of them. Can you see the threats and how they can vary from asset to asset? Assets like your data may be held liable as legal and simple lack of control over it could cost you a lawsuit as well. Threats should not be taken lightly; taking security lightly could cost you in the long run.

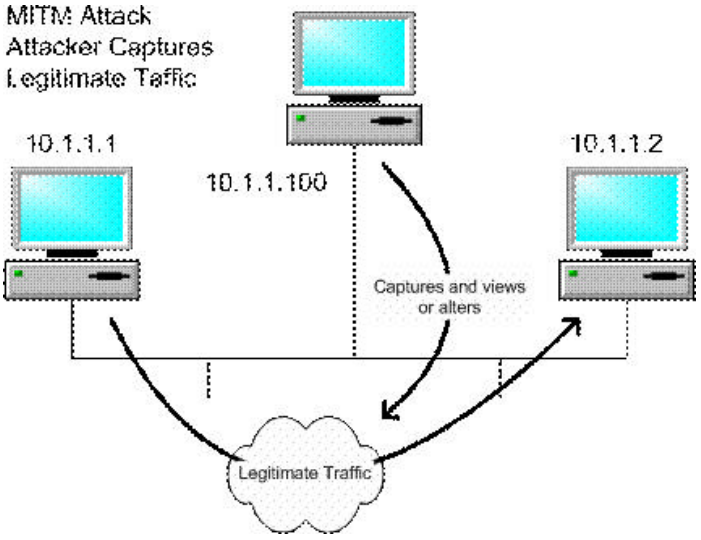


Figure 4: MITM Attack

There are but a few of the categories (the most common) and some of the threats you can associate with them. These should be considered at all times when trying to make a connection between what your assets are and how many threats can be associated with each one. Again, remember this but a few... this is only scratching the surface, tip of the iceberg.

Threats (internal versus external)

Years ago it was common to hear from networking and security professionals that a firewall was a great thing because it 'protected the resources inside your network'. That mentality has been shifting for years and as of the writing of this article, there is proof from the analysis of trends that the security threat model (internal and external) has shifted to be a balanced problem - internal threats (threats originating from within the network) between external threats (threats originating from outside the network). Remember, threats can originate from inside and outside your network. Two common examples can be:

- **Inside**: A disgruntled employee logs on to his network server and goes to their personal user share and deletes all the data in the folder that has not yet been backed up on the server that was important to the company.
- **Outside**: An unknown attacker has maliciously scanned your edge router, has connected to it and it trying passwords in a dictionary attack fashion.

This is important to distinguish between because they originate in completely different ways and you have to defend against them in very different ways, although they both fall under the

same categories... they are both threats against your assets.

What is the difference?

- **Internal threats**: threats originating from within the network. Examples include malicious employees, employees that are not malicious but make mistakes, such as mistakes made from deployments and implementations, etc.
- **External threats**: threats origination from outside your network, the direct opposite of internal threats. External threats can come from Hackers on the Internet, your business competition (yes they do!), your enemies (whether you think you have any or not) and so on.

So what can we do about this?

We have concluded the portion of this article that discussed the terminology and it should be very clear to you… driven home completely. If you still have questions about the terminology, please visit the resource links at the end of this article so you can gather more information if you need it to clear up anything that you may still be confused about.

Now, let's look at tying all this information together so that you can really assess what needs to be done about protecting your assets from the myriad of threats that exist today. There is much we can do as management within the company and security analysts and engineers:

1. **Risk assessments**: You have to know what your tolerance to risk is, once you do know, it's critical that you see how at risk you really are to certain threats. This is done with a risk assessment, which is a big name for 'checking the security of your systems and then seeing how at risk you are to known threats.
2. **Infrastructure analysis**: Now that you know what a risk assessment is, you need to test your systems. This article is not meant to show you 'how' to do this, its more of a guide to let you know that you should be doing this. More articles on this site can be used to show you how to protect your systems, just make sure you do this... make sure you analyze systems for weaknesses against known exploits, and hopefully you are using IDS (intrusion detection systems) to find attacks happening in real time, or possible 'new' attacks – or better known as 'Zero Day' attacks, which are not even known to the general populace yet, the IDS just flagged the activity on your network as 'strange' or 'uncommon'. This is just one way to do analysis, other ways are to do a network walkthrough, configuring and monitoring the auditing of Servers and other critical infrastructure, checking firewall (and other application) logs for uncommon activity, Sniffer analysis of traffic traversing the network (Packet capturing and analysis) are all ways to get a clue as to what your weak spots are. Using simple tools such as NMAP, or GFI LANguard N.S.S. (both freeware) and doing a scan of your edge and your internal critical systems can show you a lot. A vulnerability assessment is one of your first steps as to seeing how at risk your assets are.
3. **Get executive buy-in**: Once you have your analysis done, you need to hand it in. (Hopefully in an official report). You really need upper managements support on taking this seriously. If something needs to be done (whether it be to get new systems, upgrade... whatever), you will most likely need some type of budget to do so. Even though many companies 'talk the talk', they are not 'walking the walk' when it comes to building a secure infrastructure. If you do not have support for this, you will need to achieve it. Having upper management (and Human Resources) blessing will help enforcement of all new policies put in place, help get monies needed to deploy a security network/system's infrastructure and so on. This is critical to protecting your assets… make management aware that the assets are at risk by threats. (Starting to get a clear view between the balancing of Assets/Threat?)
4. **Security budget**: Think of a real security budget that fits the companies business model. To not have anything planned from year to year is very common in many organizations, and it not very wise. Again, security 'is' important. To ignore it, or deal with it as it occurs (reactive instead of proactive) raises your risk tolerance, threats are more common and realistic and you take more chances of losing or damaging your assets. Much like investing in the Stock Market or the Black Jack tables in Las Vegas, you risk when you gamble – no matter what, your risk goes up when you take chances, yes the payback can be larger with the high risk, but the loss can be just as great. You feel like rolling the dice against your Storage Area Network getting toppled? To save a ton of money up front can all be lost in one hour with a brutal attack on your systems... its time to think of a strong security posture as a solid insurance policy against your assets. Look, if Yahoo, Microsoft and the big players in the game can get knocked off the Internet by an attack that should tell you something.
5. **Build a response plan and an emergency response team**: If you do not have this, then you probably do not have a security policy either, which is not good. Other articles on this site cover this in more detail, just remember, you need a security policy and one of the sections in that policy should state what you are going to do when a threat against your assets does emerge. Hopefully you have a guided step by step plan, and also some help in pulling it off. When a threat against your assets emerges, firefighting will become your only option if you are not properly prepared.
6. **Have a DRP**: A disaster recovery plan will help you protect your assets. Disaster prevention can come in the form of high availability, redundancy and backup. With redundancy, whether it is active redundancy or redundancy in the form of spares ready for placement, you should have some kind of disaster recovery plan in case a threat emerges and your systems and data are at risk. To secure your assets, you will need to perhaps be able to replace them or restore them quickly. The most common form would be a 'reliable' data backup that is tested for efficiency and reliability.

For management only:

This extension is for management teams that 'depend' on an IT staff, and vice versa – an IT staff that 'rely' on their management to give them the tools to do their job. It is all too uncommon to expect that if you give someone a hammer as their only tool – everything becomes a 'nail'.

This is what you can do to help....

7. **Understand what your assets are and help protect them**: Look at IT as a real business asset, a strategic part of the plan, not some money vacuum that bleeds the company dry of profit. Yes, in some companies IT is a cost center, but again, unless you are reverting back to a paper society from a paperless one, you need to start to think of IT as a business ally… budget accordingly based on forecasting. If the management team is only motivated by their own bonus by cutting IT staff, monies and projects, then this is probably where you would most likely NOT want to consider cutting… not budgeting for a proper security posture is insane. I think bonus programs are a good way to reward, but when you're rewarded for saving money by increasing risk when some of that bonus money rightfully should have been re-circulated into the growth of the company is wrong. Do you think its fair that your Systems Administrator who may already be saturated with support work and studying at night to keep up with new skills, is it fair to dump something as important as securing your assets which is a separate important job all in itself on an already busy person? Would you do the same to your personal Financial Advisor? Would you call him up and say... Fred, while your working today to make me more money, could you stop what you are doing and please go food shopping for me, then stop by my house and wash my car – oh, and pick up my kids, baby-sit them tonight and then maybe clean my toilet? No, no... I think you would not. This being said, your company's data is that important too. If you do not treat is as such, then you are raising your risk level, you are more exposed to threats, and your take more chances with your assets. Isn't scary how simplified things can get with humor? Yes, I like to joke, but this is serious. Companies and their management need to start to take this more seriously so that they can reduce threat, reduce the risk of damage to the company's assets and good name and consider security as a viable solution in the company and not some suck pump of dollars out of the cost of making widgets. Widgets are more important when it's your core component for business, but when nobody can buy widgets online for a week… nuff said.
8. **Hire a Security Professional**: It should be considered. That should be part of your risk assessment and your action plan based on what you find. Think of it like this, if you find too much at risk, calculate a days lost profits against the hiring of a dedicated resource and generally you will always find that the resource was cheaper in the long run. Remember our last example? The down website for a week? Of course, its human nature to love the risk of gambling, but when working for a public company, what is it you are gambling with? Stockowner's money... for a private company, you are gambling with the profits of the company for the owners and potentially yourself. If you are a very large organization, you should consider a dedicated resource or staff augmentation. I personally don't like staff augmentation because security is very sensitive, the person knows 'too' much about your network and how it runs, all the ways in and out. I like knowing that that person works for me; I get to toss back a beer with that person, know that person a little bit better, and learn their motivations. Not 'someone' who works for a company or me - part time. Not to say that this is not a trustworthy individual, I have met many that are, but this is just personal preference. Many times management teams want to save a nickel and go this route. It's a decent solution, but not the best. That person does not have to be on staff permanently (it can be a consultant who comes in and does analysis work on your network once a month if even that minimal), but again – it's still a little risky. The worse thing you can do is to ignore it completely this will get you in a lot of trouble once a true threat emerges, especially if it's serious enough. Do not ignore security ... you lock your front door when you leave your house?
9. **Create a policy that is enforced by your company:** Yes, it's true – management needs to really get involved with this and back what the policy states. If there is a business use policy in effect (in your security policy), and it states that there will be penalties involved with not following guidelines, if those penalties are not backed and enforced (by management and Human Resources), then the policy's meaning falls apart and anarchy ensues. A lot of work goes into this stuff; to not back it is criminal to the ones who created it and foolish in many cases because it can really help you and the organization keep itself more stable. It also means that the management team should not be hypocritical and install an Instant Messaging utility when others could be fired for it and use the power of their office to justify its use... when a worm based program enters '**your**' system and infects the whole network that was otherwise secure, you will be the one to blame, you only. Backing a policy is important to the organization as a whole and it starts with the upper management team and Human Resources – working 'with' the IT department and the Security Analyst. Create a policy, advertise it, back it and enforce it when needed. Do not be the breaker of the policy as well… its there for safety not control and that's what needs to get across to everyone else as well.
10. **Allow time for training and education**: not only for the IT group, but also the larger grouping of end users of your systems under your management... the end-user community. The more people know how to handle a threat, the less risk to threats you will see, the more protection for your assets you will create. Simple example would be to allow the IT department time to train on security and then pass that training on to the rest of the organization where applicable. This strengthens your whole team, your business, your security... in most importantly, your **assets**. Knowledge is power.

In sum, knowledge is power, assets power the company. Reduce risk; reduce threat against your assets. Budget accordingly, staff accordingly, assess your risk – eliminate threat. Enforce infractions to the policy that ensures that your organization is trying to reduce, eliminate the

threat to the assets. It's all cyclical and all have an interrelationship.

The Risk

Although we have lightly touched on this topic already, it warrants its own section by right. It's important to highlight the 'major' risks for failing to consider security as a key business advantage. This is by no means a definitive list, just a sampling of some of the most important items to consider...

- **Credibility:** Well, depending on what kind of company you own, manage, or run, its important to factor in that other companies you do business with and your own clientele will lose 'faith' in your ability to do business if you cannot maintain your network uptime and access to critical resources, you face the public's intolerance to wait for services and complete embarrassment (can hurt publicly traded companies) if your not running at 100%. Think of this example, your website where you do 'e-commerce' is not up and running from a DoS attack that could have been thwarted with a small investment of 20 thousand dollars, one time cost with a reoccurring cost of about 5-10 thousand a year for training, updates or whatever else is needed for this example. How much would you lose for a half a days lost business? Can you calculate the cost of a lost customer for good? This is what you need to do for your risk assessment, but not to lose the point – its just plan embarrassing. If I was in the position of executive level management, my first question to my next echelon of supervision and management would be – why were we not protected against this? How did we lose credibility? Well – see my *top ten list* above for the answer to that one.
- **Legal issues**: Legal damages depending on what kind of business you operate could potentially cripple you. A simple example would be to not put URL filtering inside your network. Let's pretend that the cost is the same as the solution above. Is that 30 grand worth a lawsuit when someone views pornography on another PC and 'gets offended'? Think it doesn't happen? (Can you hear my virtual laughter now?). It does, more times than you think. Again, this could have been eliminated with a simple investment, to not make the investment saves you 30 grand now, up front, but will raise your risk level against the threat I just mentioned and from that gamble, could potentially cost you way more in the long run with a $300,000 US lawsuit, for example.
- **Customer satisfaction**: I don't know how you feel personally, but I get really annoyed when I pay top dollar for a service that is not reliable. For instance, when I pay for a telecom bill (T1, top dollar) and the thing won't stay up most of the time. Well, I may just take my business elsewhere because I as a customer am not happy with the level of service. Think of the same thing with your own services you provide... something as simple as not taking your Network Administrators request for a clustered database server seriously because the upfront costs are 'in your mind' astronomical, but when the thing goes down, puts all your workers on immediate coffee break because they cant access data, and your customers on hold because they can process their credit cards online when they were trying to buy 'your' goods. Still think that that clustered solution costs too much? Remember... you raise risk, encourages more threats, loss of assets. It's a gamble, really.
- **Competitor advantage**: If you think your competitors don't scheme on ways to take your out you are only kidding yourself. Companies have been known to hire Hackers for just that reason. That is one of the best hypothetical examples you can draw from... your competitor would love to see nothing less than your failure and their gain.
- **Loss of IT staff**: People get fed up eventually and move on to more serious companies, it's just a fact of life. To not look at your staff as an asset is dangerous, very dangerous.
- **Loss of Money, profit and so on**: It can't really be put more easily than that. If you ignore the initial investment, you gamble. When you gamble, sometimes you win, sometimes you lose. It's in my opinion that companies are structured to not be a gamble, especially when people are investing in it because they have faith in the viability of the company. If they knew that internal resources where playing games with the security of the data that they invest in, would they continue to do so?

Can we eliminate threat altogether?

No, and it's as simple as that. Because of the nature of the Internet and all that it offers us (the flexibility to share resources globally), we cannot eliminate risk 100% - this is just not optional. For instance, you have an Internet connection that lets port 80 through. Well, many exploits come through port 80 (like ActiveX controls, Java Applets and so on), so you can't just block the Internet – yes, you can filter it, but cant eliminate the threat completely. Some risk is implied into the cost of doing business. You have to consider that some risk toleration is implied. Also, the field of Information Technology changes so rapidly, it's nearly impossible to really foresee what new risks and threats will emerge. Think of the two hottest technologies being deployed today and you can see why it's so important to consider your assets and the threats that can hurt them in an ever-changing world of Information Technology. Wireless and VPN solutions are emerging faster than you can believe, and they are both very dangerous to your network by nature if not analyzed and secured properly. If the deployment cycle is too fast and you are rolling out these two technologies to stay ahead of competition, it's safe to assume that you are taking risks. If you are not budgeting for this, then you are hurting the staff, which in turn increases your risk.

In sum

In this somewhat lengthy article we looked at some very important topics, but the main gist of the article is to really bridge the 'threat to asset' connection in simple terms for beginning security analysts and management teams that may not know much about information technology security advantages. This article looks to make you aware of what exactly could be viewed as an asset and what threats are associated with them, or if not considering them, what

could potentially occur as a result. The rest of this article sums up Risk, and what you and your management teams can do to attempt to eliminate or lessen risk, what you risk when you don't consider threats against your assets. I hope you found this article informative and helpful in all those areas. Please tell me about it in 'General Discussion' section of the **security forum** on this site…

Links and Additional Resources:

CERT (Computer Emergency Response Team at CMU)
http://www.cert.org/

Cisco Systems: Characterizing and Tracing Packet Floods Using Cisco Routers
http://www.cisco.com/warp/public/707/22.html

Cisco Systems Product Security Incident Response (PSIRT)
http://www.cisco.com/warp/public/707/sec_incident_response.shtml

Federal Computer Incident Response Capability (FedCIRC)
http://www.fedcirc.gov/

ICSA.net (International Computer Security Association)
http://www.icsa.net/

Know your enemy: Script Kiddies
http://www.enteract.com/~lspitz/enemy.html

netscan.org
http://www.netscan.org/

Network World Fusion Research: Denial of Service attack resources
http://www.nwfusion.com/research/dos.html

RFC1918: "Address Allocation for Private Internets"
http://www.ietf.org/rfc/rfc1918.txt

You can visit my personal site link for more information on Security Policies, Incident response, a full list of potential threats, how to calculate losses and risk assessments. There are many articles you can use to help understand this article in great depth. I am also available in the security forums in the General Discussion forum.

http://www.windowsecurity.com/Robert_J_Shimonski/

Learn more about building Highly Available solutions with Windows technologies
http://www.amazon.com/exec/obidos/ASIN/0072226226/wwwwindowsecu-20

Learn basic security fundamentals
http://www.amazon.com/exec/obidos/tg/detail/-/1931836728/wwwwindowsecu-20

Learn to analyze the security and performance of your network
http://www.amazon.com/exec/obidos/ASIN/1931836574/wwwwindowsecu-20

Learn to lock down your Perimeter
http://www.amazon.com/exec/obidos/ASIN/1931836884/wwwwindowsecu-20

Learn to Safeguard your Network, Server and Desktops with an AntiVirus Solution
http://www.amazon.com/exec/obidos/tg/detail/-/1931836817/wwwwindowsecu-20

About Robert J. Shimonski

Robert J. Shimonski (Truesecure TICSA, Cisco CCDP, CCNP, Cisco Firewall Specialist, Nortel NNCSS, Microsoft MCSE, MCP+I, Novell Master CNE, CIP, CIBS, IWA CWP, Prosoft MCIW, SANS GSEC, GCIH, CompTIA HTI+, Security+, Server+, Network+, Inet+, A+, e-Biz+, Symantec SPS and NAI Sniffer SCP) is a Lead Network and Security Engineer for a leading manufacturing company as well as a part time technical trainer. Robert's specialties include network infrastructure design with the Cisco and Nortel product line, network security design and management with CiscoSecure software and PIX firewalls, Systems Engineering with all major operating system platforms and troubleshooting with Sniffer-based technologies. Robert is Author of many security related articles and published books to include the "Sniffer Network Optimization and Troubleshooting Handbook" from Syngress Media Inc (ISBN: 1931836574). You can contact Robert at rshimonski@rsnetworks.net