Justifying IT Security

Managing Risk & Keeping Your Network Secure

The goal of a security program is to choose and implement cost effective countermeasures that mitigate the vulnerabilities that will most likely lead to loss. This paper discusses the management of Risk and how Vulnerability Management is one of the few counter-measures easily justified by its ability to optimize risk.

By
IRA WINKLER

Justifying IT Security

Managing Risk & Keeping Your Network Secure

by Ira Winkler Author, *Spies Among Us*

Executive Summary

One of the most difficult issues security managers have is justifying how they spend their limited budgets. For the most part, information security budgets are determined by percentages of the overall IT budget. This implies that security is basically a “tax” on IT, as opposed to providing value back to the organization. The fact is that security can provide value to the organization, if there is a discussion of risk with regard to IT, as much as there is a discussion of risk with regard to all other business processes.

Calculating a return on investment for a security countermeasure is extremely difficult as you rarely have the ability to calculate the savings from the losses you prevented. It is akin to being able to pinpoint automobile accidents you avoided by driving safely versus recklessly. There is no way to accurately determine that information.

However, if you start to consider that Security is actually Risk Management, you can start determining the best countermeasures to proactively and cost effectively mitigate your losses. By determining the vulnerabilities that are most likely to create loss, you can then compare the potential losses against the cost of the countermeasure. This allows you to make an appropriate business decision as to justifying and allocating a security budget.

More importantly, if you can make such a business decision, you can justify increasing security budgets for additional countermeasures. The key is to be able to specifically identify an area of potential loss, and identify a security countermeasure that cost effectively mitigates that loss.

What is Security?

By definition, security is the freedom from risk or danger. Security is unattainable. You can never be completely secure. Your information and computer systems will never be totally free of risk or danger. Anyone who tells you that they can provide you with perfect security is a fool or a liar.

Corporate security programs are bound to fail, unless they clearly define their mission to their organization. Security is not about achieving freedom from risk, but about the management of risk.

It is therefore important to define what Risk is.

RISK

Risk is the potential for loss. In other words, *what do you have to lose?*

While there is the dictionary definition, we need a practical definition of risk. I prefer to use the following formula to express risk.

$$\text{RISK} = \frac{(\text{Threat } x \text{ Vulnerability})}{\text{Countermeasures}} \; X \text{ Value}$$

Risk itself is basically the potential loss resulting from the balance of Threat, Vulnerabilities, Countermeasures, and Value.

Usually Risk is a monetary loss. Sometimes risk can be measured in lives. Sadly, many businesses put a value to human life to turn it into a monetary loss. From a computer perspective, Risk is possibly the likelihood of being hacked. More importantly though, Risk is the losses experienced as a result of a hack.

To quickly break down the components of Risk:

- **Threats** are the people or entities who can do you harm.
- **Vulnerabilities** are the weaknesses that allow the Threat to exploit you.
- **Countermeasures** are the precautions you take.
- **Value** is what you have to lose.

RISK COMPONENTS

Fundamentally, **Value** represents the most you can lose. It is important to understand Value so that you can determine the potential return on investment of any proposed security countermeasure. There are several different types of value to consider, including: Monetary, Nuisance, Competitor, and Reputational Value.

The **Threat** is essentially the “Who” or “What” that can do you harm if given the opportunity. They cannot do you harm on their own. They require that you leave yourself vulnerable. Also, while people generally assume that Threats are malicious in nature, most threats that you face do not intend to cause you any harm.

Vulnerabilities are basically the weaknesses that allow the Threat to exploit you. Again, threats are entities. By themselves, they can cause you no harm. There are four categories of Vulnerabilities: Technical, Physical, Operational, and Personnel. Technical vulnerabilities are problems specifically built into technology. All software has bugs of one form or another. A bug that creates information leakage or elevated privileges is a security vulnerability. Any technology implemented improperly can create a vulnerability that can be exploited.

Countermeasures are the precautions that an organization takes to reduce risk. Countermeasures can mitigate a Threat or Vulnerability; but almost always a Vulnerability.

*It is assumed that the reader of this white paper is reasonably familiar with the components of Risk. For a more detailed discussion of this subject, please refer to my book, **Spies Among Us**.*

You Really Can't Counter *Threat*

When you look at the Risk formula, it would appear that Countermeasures can address both Threats and Vulnerabilities. In theory, that is correct. In the real world, it is really difficult to counter Threat. The good news is that it doesn't really matter.

First, let's examine why you cannot counter Threat. Fundamentally, you cannot stop a hurricane, earthquake, flood, or other *What* threats. They will occur no matter what you do.

At the same time, you cannot really counter a *Who* threat. Maybe a background check can weed out known criminals, however this doesn't stop unknown criminals. While there is a "War on Terror", there are still more than enough (known and unknown) terrorists to create a terror threat. Maybe in theory, a government can attempt to hunt down a specific group of people to extinction, but a non-government organization clearly cannot. It is also unlikely that the government will succeed.

However, the good news is that you don't have to address the Threat. If you counter a Vulnerability, you are essentially countering any Threat that may exploit it. For example, by using Vulnerability Management tools, you are mitigating the opportunity for any Threat to attempt to compromise widely known vulnerabilities.

While you cannot stop a script kiddie from existing, you can counter the underlying computer vulnerabilities that allow the hacker to exploit you. Not only do you stop the script kiddie from exploiting you, you stop competitors, cybercriminals, malicious employees, and all other threats from exploiting known computer vulnerabilities.

The 2 Ways to Hack a Computer

From a server/computer perspective, there are two fundamental ways to hack a computer. You either (1) take advantage of the way users or administrators configure and use a system or (2) compromise the underlying software.

With regard to configuration and use, the systems can be set up with poor passwords, be configured to improperly share systems, or be otherwise set up in a way that takes an otherwise secure system and renders it insecure. The underlying hardware and software can be completely without flaw, but users can find an unlimited number of ways to render all other security efforts moot.

Then we have the software vulnerabilities. All software has bugs. Some of them are functional, while some create elevated privileges, cause information leakage, and/or cause a denial of service. The latter bugs are what we refer to as security vulnerabilities. These vulnerabilities are written into the software as a coding error. While the vendors hopefully don't intend to release software with security vulnerabilities, after the software is release for widespread use, they are eventually found.

When vendors learn of vulnerabilities, they can release patches. Unfortunately, users and administrators frequently do not implement the patches, leaving the systems vulnerable to anyone who can access the system with the appropriate attack. For example, the Conficker worm has infected close to 7,000,000 computers around the world, yet the patch to prevent infection has been widely available for close to a year.

Bottom Line: **Vulnerability management tools can ensure that systems are properly patched against widely known attacks.**

What is a Security Program?

Now that Risk is fundamentally defined, we can address what security programs are supposed to do in theory. First, it is important to remember that you cannot stop all loss, if you function in the real world. No matter what you do, you must acknowledge that you will experience some type of loss. Actually, you will experience many losses.

The goal of a security program is to choose and implement cost effective Countermeasures that mitigate the Vulnerabilities that will most likely lead to loss.

In business terms, I would contend that the goal of a security program is to identify the Vulnerabilities that can be exploited by any of the Threats that you face. Once you identify those Vulnerabilities, you then associate the Value of the loss that is likely to result from the given Vulnerabilities.

The intermediate step of a security program is to choose and implement cost effective Countermeasures that mitigate the Vulnerabilities that will most likely lead to loss.

The previous paragraph is possibly the most important paragraph in this paper. Sadly, I find that many professionals do not grasp this concept and fail to understand their role in quantifiable business terms.

Optimizing Risk

It is extremely important to point out that you are not trying to remove all risk. Again you can never be completely secure, and it is foolish to try. This is why your goal is to *optimize*, not minimize, risk.

Let's first discuss the concept of optimization versus minimization of risk. Minimization of risk implies that you want to remove as much risk, aka loss, as possible. Using a typical home as an example, first examine what there is to lose. Assuming you have the typical household goods, various insurance companies might say that a house has from $20,000-$50,000 worth of value, and the house has a value of $200,000. There is also the intangible value of the safety of your family and general wellbeing.

Then consider the potential things that could happen to compromise the home. Obviously, you have physical thefts. There is also the potential for a fire. There have actually been cases of a car crashing into a home. You can also not ignore that objects, including airplanes, have fallen onto homes, destroying them and all of their occupants. You have tornados, earthquakes, floods, etc. If you want to minimize risk, you must account for all possible losses, including some of the most bizarre ones.

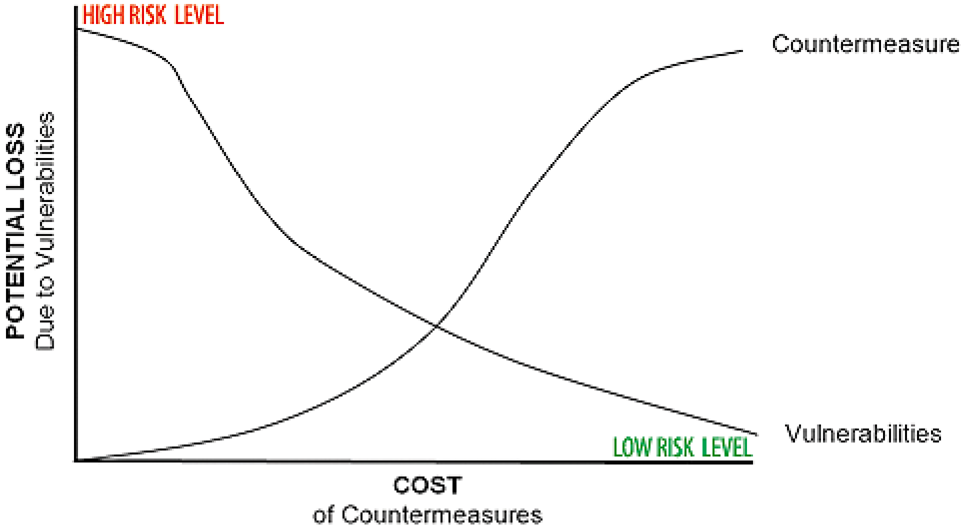
Maybe if you are not in an earthquake prone area, you might think about ignoring that. However even if you want to just limit your countermeasures to account for theft, while you might think of improving locks on all doors, you then have to think of the windows. Are you going to make all glass shatterproof? Then consider that most homes are made of wood. There is technically nothing to stop a motivated thief from taking a chainsaw to the side of your house. Do you then armor plate the entire house?

Minimizing your risk would lead to spending money on a lot of countermeasures that are not reasonable. Maybe if you're an unpopular, high-profile dictator, you would consider all of these issues, but not the typical homeowner.

In the security field, you can solve 95% of the problems with 5% of the effort.

You cannot just broadly discount a great deal of risk. *Optimization* implies that there is some thought to the process. You don't completely ignore any threat or vulnerability, but make a conscious decision that the likelihood of a loss combined with the value of the loss cannot be cost effectively mitigated. So while it would generally be feasible to install a home alarm system for $300, and pay $25 per month for monitoring as a security countermeasure to protect $50,000 from theft, along with your personal wellbeing, it would generally not be cost effective to install armor around the home to protect against the extremely unlikely case of a criminal using a chainsaw to get in your house.

I like to use the following chart to represent risk, and to also clearly demonstrate why only a fool would try to minimize risk. The curve that begins in the upper left corner represents Vulnerabilities and the cost associated with them. The line that begins on the bottom left represents the cost of Countermeasures.

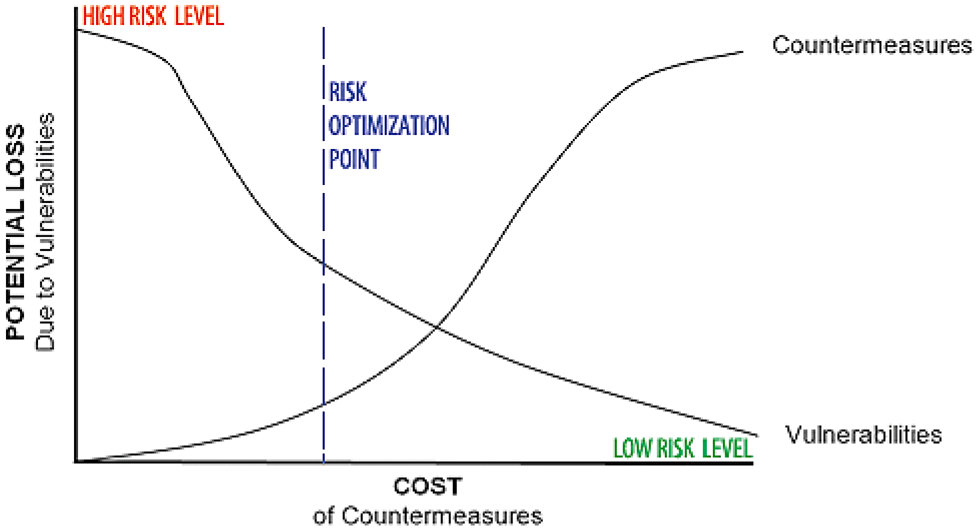


As you begin to implement Countermeasures, their cost goes up, however Vulnerabilities and potential loss decrease. Assuming you implement Countermeasures that actually address Vulnerabilities, there can actually be a drastic decrease of potential loss. It is similar to the 80/20 Rule, where you solve 80% of the problems with 20% of the effort. I contend that in the security field, you can solve 95% of the problems with 5% of the effort.

Since there will always be potential loss, the Vulnerability line never reaches 0 and is asymptotic. The potential cost of Countermeasures however can keep increasing forever. So at some point, the cost of Countermeasures is more than the potential loss of the Vulnerabilities. It is illogical to ever spend more to prevent loss than the actual loss itself, so you never want to reach that point.

You also don't want to come close to that point either. The reason is that the potential loss is only *potential* loss. While it is theoretically possible to experience a complete loss, it is extremely unlikely. You need to base the cost of countermeasures on the likelihood of the loss combined with the cost of the loss.

This is the concept of **Risk Optimization** and the chart below overlays a sample Risk Optimization line on the initial graph. This is the point that you have determined is the amount of loss you are willing to accept and the cost of the Countermeasures that will get you to that point.



While I wish it was feasible to say that an entire security program should be based on this methodology, the reality is that most organizations are extremely far from implementing this on a macro level. Instead, I recommend that people approach Risk Optimization on a micro level.

Vulnerability Management as a Critical Component of Risk Optimization

When considering Risk Optimization, you must consider the losses that come from technical vulnerabilities, or the known vulnerabilities that exist in software. Again, these software bugs can be triggered maliciously by criminals, or be malignant and just happen at random times.

While it is true that there are some Zero-Day Vulnerabilities, where the underlying bugs are not currently known and therefore the attacks are theoretically unstoppable, that accounts for less than 1% of all computer attacks.

The bulk of computer attacks can be easily prevented with the proper implementation of vulnerability management tools such as QualysGuard. Most importantly, these vulnerability management solutions can be extremely cost effective and a critical component of Risk Optimization.

For example, a vulnerability management deployment may cost $10K per year. At the same time, you've determined that a single loss from known vulnerabilities can easily result in a loss of millions of dollars. The likelihood of a known vulnerability of being exploited is almost 100% given the persistent threat on the Internet. The potential loss would otherwise only be limited by the value of the organization as a whole.

Vulnerability Management is one of the most cost effective tools out there and should be part of any Risk Management solution as it can help identify and prevent 95% of the issues… with 5% (or less) of the effort.

Consciously Accept Risk

All Risk Management decisions should be based not on an arbitrary budget assignment, but on the realization that the money invested on a Countermeasure is justified by a reasonable reduction in Risk.

The bottom line: Vulnerability Management is one of the few Countermeasures that is easily justified by its ability to optimize Risk.

About the Author

Ira Winkler, CISSP is President of the Internet Security Advisors Group and on the Board of Directors of the ISSA. He is also a columnist for ComputerWorld.com and considered one of the world's most influential security professionals. Named as a "Modern Day James Bond" by the media for his espionage simulations, where he physically and technically "broke into" some of the world's largest companies and investigating crimes against them, and telling them how to cost effectively protects their information and computer infrastructure. Ira Winkler continues to perform these espionage simulations, as well as assisting organizations in developing cost effective security programs. Ira Winkler also won the Hall of Fame award from the Information Systems Security Association, as well as several other prestigious industry awards.

Ira Winkler is also author of the riveting, entertaining, and educational books, *Spies Among Us* and *Zen and the Art of Information Security*. He was also a columnist for ComputerWorld.com. Ira Winkler has recently been elected Vice President of the Information Systems Security Association.

Ira Winkler began his career at the National Security Agency, where he served as an Intelligence and Computer Systems Analyst. He moved onto support other US and overseas government military and intelligence agencies. After leaving government service, Ira Winkler went on to serve as President of the Internet Security Advisors Group, Chief Security Strategist at HP Consulting, and Director of Technology of the National Computer Security Association. He was also on the Graduate and Undergraduate faculties of the Johns Hopkins University and the University of Maryland.

Ira Winkler has also written the book *Corporate Espionage*, which has been described as the bible of the Information Security field, and the best-selling *Through the Eyes of the Enemy*. Both books address the threats that companies face protecting their information. Ira Winkler has also written hundreds of professional and trade articles. He has been featured and frequently appears on TV on every continent. Ira Winkler has also been featured in magazines and newspapers including Forbes, USA Today, Wall Street Journal, San Francisco Chronicle, Washington Post, Planet Internet, and Business 2.0.

To learn more about Qualys' On Demand Vulnerability Management and IT Policy Compliance solutions, visit: www.qualys.com