Global Knowledge™

Expert Reference Series of White Papers

Risk Management: Bridging Policies and Procedures – Fundamental Security Concepts

1-800-COURSES

www.globalknowledge.com

Risk Management: Bridging Policies and Procedures

Bernie L. Dixon, CISSP, SSCP

Introduction

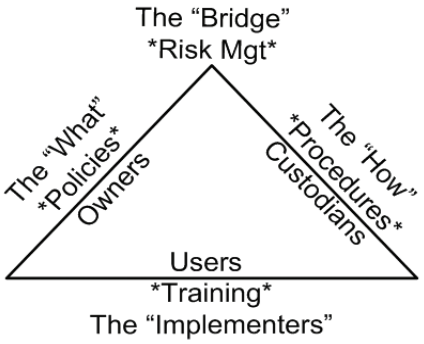
Designing security architectures is not so difficult, providing you have a good road map. Policies and procedures within the organization are that road map to effective and efficient security designs. Risk Management is the bridge between the two. One huge element in the risk management process is determining the security return on investment (ROI). As the Security Manager for your firm, how do you justify security spending for firewalls, intrusion prevention systems, content filters, two-factor authentication systems, and so forth to business managers? Many managers see security spending as red ink on the ledger. In today's business environment, companies want or demand an ROI. This white paper discusses risk management as a key process in designing security architectures, including a better way for security managers to approach the security ROI issue.

One thing that security professionals know for a fact is that security is about processes, not about the technology. It has never been about the technology. I constantly see very good technology incorrectly implemented each day. Organizations blame the vendors, the software, the hardware, and their consultants, yet the real blame belongs to the people within the organizations themselves. They do not understand their processes, yet they are ready to throw technology at any given problem without analyzing what it is that they are trying to solve. The key to security is to match the technology to the process, but you have to know the process first. Policies and procedures are the requirements, and risk management is the bridge between the two. Collectively, they are the road maps that lead to effective and efficient security designs.

The Security Triangle

With any road map, you must first establish your starting location in order to plan out a route. In security, this start point can often be found in a guide to setting computer security policies and procedures, called RFC 2196, which states that a security policy is a formal statement of rules by which people who are given access to the IT resources of an organization must abide. Well, just what the heck does that really mean? Let's break it down into smaller parts and form a triangle of the "people" and processes. First, who in the organization can put out formal rules that everyone within the organization must follow? That would have to be the owners as it is quite conceivable that they may have to prove in a court of law that they have protected shareholder investments in that company, which includes all network resources. So owners are responsible for policy, or what is expected in regards to security within the organization. However, policies typically are very high-level statements that don't always indicate how we are going to get there in regards to security.

This is where procedures come into play. Procedures say how we are going to meet the "what" of policies. The custodians of the owners' information assets and data are typically responsible for the procedures. The custodians are the security managers, network administrators, system administrator, and other administrative types that take the policies and determine how to best implement those requirements. The bridge that makes that happen is risk management. Risk management takes into account several factors to determine actions necessary to reduce risk to an acceptable level. Finally, the last and most important piece of the triangle is the users, for they are the true implementers of security. Policies and procedures are not secrets. They must be disseminated to the users, and the users must have a buy-in. The users need security awareness training that includes how to use the security technology being put in place.



Policies, Procedures, and Risk Management

Risk management is nothing more than the technical and physical implementation of the written policies. Policies are passive – they enforce nothing as they are just words on paper; however, they set the corporate culture towards security for the organization. In other words, what the owners expect in regards to security requirements. They cover many topics such as configuration management, change control, business continuity and disaster recovery, network security, human resources, acceptable use, and so on.

However, they typically do not cover the step-by-step procedures on how to make it all happen. Custodians take the policies and begin to translate them into procedures, or the "how." Risk management will bridge the two processes together by identifying

- What the organization has that is worth protecting (assets),
- What could do harm to those assets (threats),
- What weaknesses (vulnerabilities) currently exist that would allow the harm to materialize, and
- How probable would it be that the threats would exploit the weaknesses to cause risk to the assets.

Once all this is understood, we are ready to make recommendations as to what safeguards or countermeasures need to be put into place to reduce the risk to an acceptable level for the organization. This is where technology will finally make its appearance – it is where we will match the technology to all these processes to design the most effective and efficient security architecture.

Risk Management 101

Reducing risk is not just looking at security in a vacuum and ignoring other factors such as costs, performance, usability, and productivity. The safeguards and countermeasures that we recommend for implementation into existing architectures will have an impact in each of these areas. Implementing firewalls, proxies, virtual private networks (VPN), two-factor authentication mechanisms, sending people to training, and so forth will help reduce risk, but they will never eliminate all risks. It is impossible, regardless of the amount of resources that we may be able to throw at the risks. In fact, we actually could cause problems by putting too much security into place.

I've often said that if security prevents business objectives from being met, then the security is wrong. However, we do have to have a balance between business needs and security needs. There are always trade-offs. We have to balance security with costs, security with performance, and security with usability and productivity. We are looking for a logical point on a graph where acceptable risks meet acceptable costs at acceptable drops in performance, usability, and productivity. Of course, one of the biggest obstacles for any security manager to overcome is in cost factors. How much is security going to cost the organization and what will be the return on such an investment (ROI)?

What Is ROI?

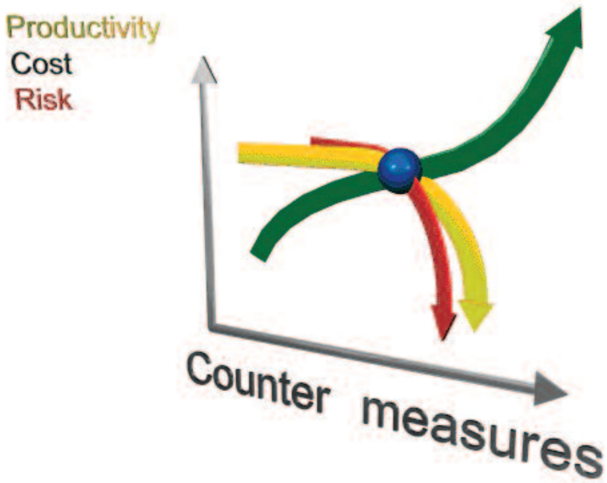
In finance, ROI is the ratio of money gained or lost on an investment relative to the amount of money invested. The amount of money gained or lost may be referred to as interest, profit/loss, gain/loss, or net income/loss. Unfortunately, too many business managers use this definition of ROI as a means of generating revenue. They will use this as a mechanism to choose projects to fund. For example, if they have $1,000 to allocate to one of two projects, the project with the higher rate of return would be the prudent choice.

- Project 1: invest $1,000 generates $1,050 return = 5% ROI
- Project 2: invest $1,000 generates $1,100 return = 10% ROI

But business managers are short-sighted when they see ROI as simply wealth creation. ROI could be any capital expenditure that increases the company's value. Security spending does not generate revenue, or at least in most cases it doesn't. Instead, you could categorize security spending as wealth preservation, which certainly increases the company's value.

Wealth Preservation

I completely agree with Richard Bejtlich, Director of Incident Response at General Electric, when he said on his Web blog that wealth preservation (savings) is not the same as wealth creation (return). For instance, let us say that you were planning on purchasing a computer 6 months from now at a cost of $1,500; however, the seller is willing to knock $500 off the price if you buy it today. It would certainly make sense to buy the computer now instead of in 6 months. It will not make you $500 richer, but it does avoid unnecessary spending. This is wealth preservation, or loss avoidance, which is not a bad thing?.



Calculating Security ROI

So, how do security managers show an ROI to business managers from a wealth preservation perspective instead of wealth creation? Security managers will need to show that their project will save a certain amount of money. This is typically done by performing a risk assessment or analysis. The problem security managers will face is that a risk assessment, including costs/ benefits analyses, does not always deal in certainties, but probabilities. The reasons for this are many:

- Determining asset value is not always clear, or is not easily determined.
- Threats are unpredictable and not always properly evaluated.
- All vulnerabilities are not known, and new weaknesses are discovered every day.
- Certainty cannot be proven; only a level of probability that a threat will exploit a vulnerability to cause potential harm or damage to the asset. (

Therefore, business managers may see a risk assessment as largely guesswork on the security managers' part. It can be more art than science; however, security managers still can demonstrate potential savings by conducting the analysis.

For example, let's say that we have 1,000 members in our company. Our acceptable use policies (AUP) concerning E-mail and Web services state that we monitor these services for improper use and will take legal action against violators. However, we have no technical solution in place to prevent this type of security violation. Improper use of these services by employees could lead to viruses, spam, and spyware, not to mention unproductive use of company resources on company time. We know that words on paper (our acceptable use policy) never stopped anyone. So, we go to management to make a case for purchasing a content inspection capability to enforce company policies. We need $10,000 to purchase the hardware and software to implement our technical solution. How do we show a security ROI (savings not return) for this project?

First, we need to determine the probability that members of our organization will violate our acceptable use policy regarding the use of company E-mail and Web services. We can call this the exposure factor (EF) or exposure value (EV). Surveys of Fortune 1000 companies have shown that 25 to 30 percent of employees violate AUP. Let's use 25% as the EV.

1,000 x 25% = 250 violators

Next, we need to determine a potential dollar loss factor for a single incident. We can call this the single loss expectancy (SLE). If we go to the finance officer, we should be able to get the average payroll broken down into an hourly rate for the whole 1,000-member company, as any one of the 1,000 members could be a violator. For our example, we will use $50 per hour. This would not be unusually high, because you must factor in everyone from the top wage earners down to the bottom in the company. Also, we must determine how many hours out of the work week these 250 people will spend violating our AUP. Using that EV of 25% and a 40-hour work week, we would get 10 hours. Calculating the SLE:

250 x $50 x 10 hours = $125,000 SLE

Finally, we need to determine how many times we could expect this loss to occur over a full year. We can call this the annualized loss expectancy (ALE). Violations could occur each and every work week, except perhaps when the employees are on vacation. Assuming two weeks vacation, this means we can expect the losses to occur 50 times. This is our annual rate of occurrence (ARO). The formula to calculate ALE then is SLE x ARO:

$125,000 x 50 = $6,250,000 ALE

Therefore, the company stands to save, or avoid, over $6 million per year in potential losses by enforcing the AUP through technical security controls. This does not mean that the company will have $6 million as a profit line in the revenue report. However, it clearly makes sense to spend the $10,000 to avoid the potential $6 million annual loss.

Conclusion

Without understanding the security processes, technology to solve security problems is of little value. Policies and procedures combined with risk management are the processes that help identify the correct technology to help secure the organization's infrastructure. Without these processes in place, it is just a guessing game in trying to solve security issues.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge.
Essentials of Information Security - Security+
CISSP Prep Course
CISA Prep Course
Foundstone Essentials of Hacking

For more information or to register, visit www.globalknowledge.com or call 1-800-COURSES to speak with a sales representative.

Through expert instruction, you will understand key concepts and how to apply them to your specific work situation. Choose from more than 700 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and management training needs.

About the Author

Bernie L. Dixon is a Certified Information Systems Security Professional (CISSP) and System Security Certified Practitioner (SSCP). He has over 30 years experience in the field of computer and network security, including cryptography. Bernie served 25 years in the United States Air Force, where his responsibilities included analyzing and resolving communications and computer security-related problems. Upon retirement, Bernie became the Manager of Information Protection for AT&T Technical Services in San Antonio, TX, where he was responsible for communications-computer security. After 3 years, he served as the Director of System Security for Access Research Corporation. Bernie started his own company in November 1997 and has done network security consulting for companies like TRW, Unisys, Ascend (now Lucent), Department of the Treasury, Department of the Air Force, and NSA. He wrote two security courses for Global Knowledge titled Designing Security Architectures and Check Point NGX CCSA/CCSE.

References

1. Richard Bejtlich, "No ROI? No Problem," TaoSecurity Blog, posted 14 July 2007.
http://taosecurity.blogspot.com/2007/07/no-roi-no-problem.html