Microsoft

Practical Security Metrics

Effective Security Practices Series

Figuring out the "Return" part of a Return on Investment (ROI) calculation requires one to accurately assess the benefit accrued. A lack of good IT security metrics has made this exceedingly difficult for security professionals. In this paper we look at innovative approaches in industry to estimate the return on some of their security investments. This paper is based on discussions with several Chief Security Officers (CSOs), Chief Information Security Officers (CISOs), and other security executives of leading companies across multiple industries. We look at some of the innovative approaches businesses have taken to better measure IT security risk and express the benefits of security investments in monetary terms.

Herbert H. Thompson, Ph.D.
Chief Security Strategist, People Security

Microsoft Corp. • One Microsoft Way • Redmond, WA 98052-6399 • USA

Preface

Information security is a very dynamic field: legislation keeps changing, technology keeps evolving, and the attacker community continues to become more sophisticated. This turmoil has forced security practitioners to think creatively to address some very difficult problems. Much of this innovation has been locked away within corporations as they have made isolated progress on issues like security metrics, security risk management frameworks, and security policy. In order to address this discrepancy, Microsoft commissioned a whitepaper series to share key security innovations. Whitepaper topics came from participants in Microsoft's CSO Council - a semi-annual gathering of security executives from leading global organizations who serve as advisors to Microsoft's Trustworthy Computing Group.

Our goal is to share practices "from-the-trenches" that address some of the toughest problems in security. After numerous interviews, discussions, and debates with these though leaders, a collection of effective practices emerged. While much remains to be done, we hope that these whitepapers fuel the discussion and help facilitate further sharing in the field of IT security.

Overview

Preventing a negative security incident has a clear business case if the cost of prevention is less than the impact of the incident. While in theory this formula is simple, in practice, businesses are often faced with defenses that are of unknown effectiveness against an incident (or attack) with an unknown probability of occurring and an impact cost that is difficult to quantify. Further complicating the issue, there are new attacks and attacker techniques that may be completely unknown and unanticipated. This paper discusses effective practices used by some of the world's largest enterprises to assess the value of security investments. It is based on interviews and discussions with security executives and architects from several Fortune 500 companies. Our intent in this paper is to drive discussion of innovative measurement approaches within the security community.

Many security executives interviewed for this project indicated that they do not have fixed budgets for infrastructure security improvement. Instead, projects are justified on an as-needed basis. Participants indicated that justifying spending on projects has become increasingly difficult. Security projects that are not already on an approved roadmap are most often done after some security event or precipitating incident that serves as their justification.

For budget justification in the past, security executives had to convince business owners to protect against attacks that may or may not happen. Security spending has therefore been reactionary in many areas: investment has followed the direct pain of a security incident or breach. In the wake of Slammer and Blaster for instance, few companies asked for ROI calculations when they deployed new patching processes or made needed network security infrastructure improvements. While some security technologies are now considered a required cost of doing business (such as firewalls) as an industry we still struggle when measuring risk and justifying investments in defense.

Justifying security spending can also be very difficult retrospectively. If you installed steel bars over the windows and doors of a home, and then no one broke into your home over the next year, was it worth the investment? Could you have used a cheaper alternative to secure your home or done nothing and achieved the same result? In the same way, if one truly prevents an uncertain incident from occurring in IT security it can be difficult to measure the real value of that defense. This sometimes gives rise to questions from non-security executives like: How many incidents did we prevent with the security investment we made in a particular process or tool? With a lack of metrics and

nebulous data on prevented incidents, one possible conclusion is that the business is overspending on security. In many cases, this perception of overspending has restricted budget for security improvements that are important to the business.

Legislation such as Sarbanes Oxley has made certain IT security infrastructure pieces non-negotiable. Similarly, industry standards such as the Payment Card Industry Data Security Standard (PCI DSS) mandated additional infrastructure security elements. These regulations and standards changed the economics of IT security. They created an impending event; even if systems were not attacked, they would be audited. Security improvements that fell under the umbrella of compliance were again non-negotiable costs of doing business (as they had been during the onslaught of the major internet worms). Several security executives interviewed during this research indicate a divergence of core compliance and security. This divergence creates a justifiability gap for security: security controls that do not fall under compliance requirements but are needed still must be justified.

C-level sentiment showed a shift from messaging risk reduction to messaging cost reduction. In some cases, participants were able to leverage risk management frameworks to create risk benchmarks for applications, processes, etc. This data would then be used to motivate individual businesses units to move in-line with the rest of the organization. When a business can see that they significantly fall below other areas of the organization from a security/risk perspective, it serves as strong motivation for risk-reduction practices and tools.

Most participants did not have a mandated threshold for risk, instead they viewed their role as providing decision-oriented risk visualization to business owners. They considered this to be one of their primary functions: to enable business decisions by working to reduce risk and then capturing and communicating residual risk as accurately as possible.

Case Studies

For business areas where security risk was difficult to quantify, there was a clear shift in sentiment from guessing about risk as a spending justification to instead looking for security improvements that also reduce hard costs. While very different, each of the cases below represents an innovative use of metrics for pre-investment and post-investment justification.

Case 1: Improving credentials to reduce investigation costs

In this case, a large publishing company wanted to improve the strength of credentials issued to customers for a subscription-based information portal. One of the primary concerns was that simple username/passwords chosen by users that could be guessed, stolen, or passed to others resulting in theft of service and lost revenue. The security improvement was to add password complexity policies and look at other factors such as the IP address of users. This represented both a technical investment and an increased burden on customers (and IT support). This security improvement was justified by looking at the resulting reduction in investigations into misused (or stolen) credentials. Investigations were often very expensive and eliminating even a small number of them were enough to retrospectively justify the security improvements.

Case 2: Reducing exposure (and cost) through consolidating access to documents

In this case, a large transportation company took steps to reduce data exposure by looking for files that were stored but no longer accessed. The company also looked for files with multiple copies stored on file servers that were accessible by different users. For each file, several questions were asked:

Is this file older than (or has it not been accessed since) a specific date?
Are there duplicates of this file on the system?
Who "owns" this particular file?
Who should be the legitimate owner (and thus determine access rights)?

Based on these answers, the company was able to archive old, unreferenced files and also consolidate redundant copies of files through better access management. This left the

company with a measurable improvement in their data surface but also forced true owners/originators of the data to examine who should have access to what. This approach resonated with stakeholders and helped justify the process. The company also factored in the reduced disk space, reduced file management overhead, and more centralized management for data owners in their business case.

Case 3: Benchmarking new security controls against "dwell time."

"Dwell Time" refers to the period of time in which an attacker has had access to (or control of) a system. While this metric can be used in many ways, in this case, dwell time was used by a large company in the defense industry as the benchmark for effectiveness of new security controls. While it may be difficult to quantify the impact of an intruder's sustained presence on a machine or network, this metric can be used to benchmark an array of potential security technologies (as well as security policies and practices) against each other. In this particular instance, dwell time was considered to be of paramount concern. In pilot deployments of new security technologies (such as antivirus, etc.) this metric was used to sift through alternative solutions. These solutions could then also be compared on acquisition cost, maintenance, user impact, etc.

Conclusion

In this paper, we looked at some innovative methods that companies are using to capture and communicate the benefits of IT security improvements. Justifying the money spent on security improvement remains a core challenge of IT security. If one can tie an investment in security improvement to how that investment is going to help the company make money, help the company save money, or help reduce risk (avoid losing money), then that investment can compete on the battlefield of corporate budget. There will always be activities that *must be done* to comply with a regulation or standard such as VISA PCI or Sarbanes Oxley and security spending here is more about compliance than risk reduction. Outside of compliance, it is becoming common for companies to actually *reduce* their security budgets because the nature of security can make it difficult to measure its worth. This preventative property of IT security in particular can make it difficult to show value, even historically, and thus makes justifying future security spending difficult. Spending in many cases has been reactionary; adding security improvements after an incident has occurred or in the face of a looming threat. While many companies have adopted risk management frameworks to help them calibrate risk across different areas of IT a clear gap still remains in justifying security improvements to defend against threats which are difficult to measure. Responses from council members showed that there is significant innovation in value-oriented IT security metrics within many companies. The goal of this paper is to be a first step in better sharing and communication these innovations within the council.

Appendix 1: Survey Questions

In preparing this whitepaper, we spoke with several members of Microsoft's CSO council. Some of these interviews were informal, while others involved asking a specific set of questions around the topic. Respondents were leaders in the field of IT security and hold operational responsibility for security in their organizations. Below are some of the key questions asked:

How does the output of your internal risk management exercises tie back to metrics you can communicate with stakeholders?

How do you show improvement in a security area? Can you give an example of a specific area where you've made improvement and how you've measured it?

Do you gather data on "prevented attacks" by looking at IPS logs, etc. to justify the spend on network security solutions?

How do you calibrate your security spend: peers? Previous budgets? Based on a risk-management framework?

Do you think this calibration reflects true risk?

Are there defenses that you know you should buy/adopt but cannot justify the security spend? Why? Lack of metrics?