CERT PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

The ROI of Security

Key Message: ROI is a useful tool because it enables comparison among investments in a consistent way.

Executive Summary

Return on investment is the heart of business -- it's why we form companies, grow them, merge them, and even sell or close them. But, as applied to information security, ROI has always been a bit of a murky issue. After all, how do you prove a negative? How do you quantify the value of something that **is less likely** to happen if you spend lots of money to prevent it? It's not an exact science, and that can be frustrating.

In this podcast, we'll discuss the relationship between ROI and risk assessment, focus on how to apply ROI metrics consistently to an organization's security efforts, and explore why it's important to formalize these metrics using security policy and procedures.

PART 1: ROI AND RISK ASSESSMENT

Definition of ROI

- The comparison between any **expected improvement** and the **cost required** to achieve that improvement
- In security, not measured as a concrete gain, but rather as a reduction in risk
- Must be applied consistently across the organization to have value

What to Measure

- Depends on the individual company/industry
- This is where risk assessment comes in
- The quality of the company's risk assessment will determine the quality of its ROI analysis

Defining a High-Quality Risk Assessment

A high-quality risk assessment:

- is sponsored at the enterprise or business-unit level
- identifies the most critical information "assets" (customer data, trade secrets, custom applications) and where the assets are most at risk
- prioritizes protection action that needs to be taken
- does this on a recurring basis

What to Measure, More Specifically

Possible factors to measure include:

- lost productivity from downtime
- lost revenue from downtime
- loss of data (temporary or permanent) through downtime, corruption, or outright destruction (a loss of availability)
- compromise of data through disclosure or modification (a loss of confidentiality and/or integrity)
- repair costs after a breach

- loss of reputation if the breach becomes publicly known

How far should you go in measuring various factors? It's up to you!

Suggestion: Measure ROI the same way across the board. What are you already using to measure ROI in other divisions of your company? Be consistent! **Security is part of the big picture, not an island.**

PART 2: ROI METHODS

Two Example Measurement Methods: Payback and NPV

Payback:

- compares annualized loss expectancy (ALE) with expected savings as a result of an investment
- if savings are greater, ROI is positive
- annualized loss expectancy = (probability of negative event) * (cost of negative event)
- expected savings expressed as:
    - a reduction in the probability of the event. (For example, implementing a training program to teach users to use stronger passwords likely would reduce the chance of password compromises.)
    - OR a reduction in the impact (cost) of the event. (For example, storing backup tapes in a geographically distant area would reduce the impact but not the likelihood of earthquake damage.)

Payback Example #1

A company faces a 90% chance that an outsider will compromise one of its users' passwords in the coming year, causing a security breach. This is the **probability** of the negative event.

If the company does suffer a password compromise, the **cost** of the incident is estimated to be $150,000 based on historical data.

Therefore:

Annualized loss expectancy = (.9)($150,000) = $135,000

The company is considering a security awareness training program to help mitigate this risk by teaching employees to use stronger passwords and protect their passwords more diligently. The company estimates this training program will reduce the chance of a password compromise to 30% per year.

Therefore:

Annualized loss expectancy = (.3)($150,000) = $45,000

The cost of the negative event, if it occurs, did not change. The probability did!

To find expected savings, just take the difference: $135,000 - $45,000 = $90,000

On average, the company will save $90,000 per year if it implements the training program.

This **expected savings** must be compared against the cost of the training program to determine ROI.

Note that the company is not guaranteed to save $90,000 in **each** year (a password compromise still will occur in 3 out of 10 years). The $90,000 is an average.

So, if we measure savings for 3 years, the security awareness program will produce savings of $90,000 * 3 = $270,000. If the awareness program costs less than that up-front, the ROI is positive (but, as we'll discuss later, that may not be enough!)

Payback Example #2

Let's consider an example dealing with identity theft. If a credit card issuing company expects it would cost $20 million to recover from a website breach leading to widespread identity theft (capture of user-entered ids and passwords), and the chance of such a breach in any given year is 5%, then:

Annualized loss expectancy = (.05)($20,000,000) = $1,000,000

If the company could lower its annual risk to 1% by purchasing a new, well tested web interface with more rigorous authentication controls, then:

Annualized loss expectancy = (.01)($20,000,000) = $200,000
Expected savings per year: $1,000,000 - $200,000 = $800,000

Cost of new software: $50,000
One-time installation cost: $20,000
Maintenance cost (ongoing): $10,000 per year
Time horizon: 3 years
Total costs: $50,000 + $20,000 + $10,000 + $10,000 + $10,000 = $100,000

ROI = (3)($800,000) - $100,000 = $2,300,000

Net Present Value (NPV)

- **Similar to payback** but builds on it
- Takes into account the **time value of money** (money tomorrow is worth less than money today)
- NPV applies to both savings and costs. Because a dollar amount in the future is (usually) worth less than the same dollar amount today, NPV helps you get a more accurate read on the value of all present and future savings and costs **in today's dollars**.
- Depends on discount rate - a larger economic indicator set by the Federal Reserve. Discount rate fluctuates over time, but you can use the current rate since we are interested in finding the overall value in today's dollars.

NPV Example #1

Let's look at our password compromise example from earlier, using the proposed security awareness training program. NPV just builds on payback.

Discount rate = 10%
Expected savings = $90,000 per year
NPV = Expected Savings / (1 + discount rate) ^ t

In one year: $90,000 / (1.1)^1 = $81,818
In two years: $90,000 / (1.1)^2 = $74,380
In three years: $90,000 / (1.1)^3 = $67,618

Add together the savings in all years for **total savings**: $223,816

Subtract the total cost of the training program from the total savings to find the ROI.

NPV Example #2

Discount rate = 10%
Expected savings = $800,000 per year
NPV = Expected Savings / (1+discount rate)^t

In one year: $800,000 / (1.1)^1 = $727,273
In two years: $800,000 / (1.1)^2 = $661,157
In three years: $800,000 / (1.1)^3 = $601,052

Total savings = $727,273 + $661,157 + $601,052 = $1,989,482

Costs right away: $50,000 (purchase) + $20,000 (installation) = $70,000
Costs in one year: $10,000 / (1.1)^1 = $9,091
Costs in two years: $10,000 / (1.1)^2 = $8,264
Costs in three years: $10,000 / (1.1)^3 = $7,513

Total costs = $70,000 + $9,091 + $8,264 + $7,513 = $94,868

ROI = $1,989,482 - $94,868 = $1,894,614

Optimal Time Horizon

- Longer than a year - allows you to unlock the value of NPV
- Shorter than five years - beyond this point, calculations are less accurate due to uncertainty about external factors

When to Invest

Economists Lawrence Gordon and Martin Loeb of the University of Maryland have done studies that showed security investments are only worthwhile if the cost is 37 percent or less of the expected gain.

So, for example, if you calculated you would save $10,000 if you implemented a training program, you should only invest if the program costs $3,700 or less.

However, it's important to note that Gordon and Loeb's standard is only a rule of thumb and may vary according to the business environment.

For example, the business environment for many companies shifted after the Veterans Administration's reported loss of millions of veterans' personal information in May 2006. The root cause was theft of an employee's laptop computer, which contained unencrypted sensitive data. More organizations now may be likely to implement requirements for encryption of sensitive data stored on portable devices - no matter the cost. Refer to the article "U.S. government mandates laptop security" at http://www.securityfocus.com/brief/239.

PART 3: USING ROI IN THE REAL WORLD

The Value of ROI

- The value is not necessarily in the hard numbers themselves
- The value is in two things:
    1. the quality of your risk assessment -- a good, thorough risk assessment will lead to meaningful results; a poor risk assessment will lead to misleading results
    2. consistent use of the same ROI measurement method across multiple projects, which provides a meaningful comparison among alternatives. This means the same factors must be assessed for each

project!

If you consider lost productivity for one investment but not for another one, your comparison will be misleading no matter what ROI method you use.

Likewise, if you use payback to evaluate one investment and NPV to evaluate another, your comparison will be misleading even if you assess the same factors for both projects.

ROI and Timing

- It's best to calculate ROI up-front
- Follow-up assessments can be useful to make sure you're getting the return you expected
- If you didn't calculate ROI up-front, you can start from wherever you are to get a baseline, but in the future always make sure to do an assessment up-front, too!

Consistency Amid Organizational Change

- One of the best tools to ensure consistency is your security policy
- Once something is in policy, it's harder to change it. So:
- Decide what you're going to measure, choose an ROI method, and then write these things into your policy!
- Allows continuity beyond one person's tenure, be it the CEO, CISO, or CIO

Next Steps

- For information on risk assessment: http://www.cert.org/octave/
- Sample security policy dealing with security ROI considerations, adapted from a SANS template and available on this site
- Keep in mind this sample ROI policy is only a starting point, not a binding document

References

Allen, Julia. "Making the Business Case for Information Security: Selling to Senior Management." Presentation at InfoSec World 2003, Software Engineering Institute, Carnegie Mellon University, March 10, 2003.

Gordon, Lawrence A., and Martin P. Loeb. "The Economics of Information Security Investment." ACM Transactions on Information and System Security, Vol. 5, No. 4, November 2002, p. 440.

Losi, Stephanie. "The ROI of Security." Security Matters, Software Engineering Institute, Carnegie Mellon University, May 2006. http://www.sei.cmu.edu/library/abstracts/news-at-sei/securitymatters200605.cfm

Rasch, Mark. "Cleaning Up Disclosure." SecurityFocus, April 11, 2005. http://www.securityfocus.com/columnists/316

SANS Institute Security Policy Project, http://www.sans.org/resources/policies/

Additional background sources and acknowledgments

Jaffe, Jeffrey, Stephen A. Ross, and Randolph W. Westerfield. Corporate Finance, 7th Edition, 2005.

Thanks to Julia Allen and Dave Zubrow for editorial input and advice.
