

An ILLUMANT White Paper



Budgeting for Information Security

WRITTEN BY

MATIJA SILJAK

DATE

MARCH 2009

Budgeting for Information Security

How much is enough?

A necessary evil

Security is a cost center, which by itself is not a bad thing. A cost center can be defined as a business unit or function whose purpose is primarily to enable revenue or profit centers. The problem for security is cost justification. The benefits, while intuitive, are at best difficult to measure and at worst completely intangible. In rare cases effective security can actually become truly marketable and help drive revenues; however, this objective is out of reach for most organizations so we won't delve into it here.

A successful security strategy is one that minimizes the combined costs, both direct and indirect, of maintaining the security program and recovering from successful security breaches. However, even if breaches are completely avoided, it is never clear that the objective couldn't have been achieved more cheaply, or that a breach event isn't just around the corner and won't overwhelm the money invested in security to date.

So security becomes a risk management problem involving equations of breach likelihood and impact, as well as risk mitigation costs and benefits. However, assessing risk is problematic as well. Organizations often find it difficult to obtain reasonable information on security breaches and to apply that sparse data to their particular circumstances. Also, for many organizations the cost of a top-to-bottom, in-depth risk assessment may itself blow the security budget and possibly do little more than confirm what was already intuitively known. However, rather than do nothing, there are simpler, less expensive risk assessment methodologies that can help these organizations.

Make no mistake, breaches mean real (and big) dollars

The correlation between security dollars and breach avoidance may be blurry, but certain elements of cost for a breach are clear and can mean lots of money.

Intuitively, the costs of a security breach include:

- Breach notification and credit monitoring for affected parties (required by law for certain types of information)
- Service and/or business interruption, lost revenues
- Forensics
- System, application, database repair and breach remediation
- Lost productivity
- Reputational damage
- Lost clients and degraded client acquisition potential

There are some surveys that try to quantify these costs. Here are some key statistics surrounding security breaches that should serve to motivate investment in security:

- Since 2005 when the Privacy Rights Clearinghouse began tracking data breach incidents, more than 250 million customer records containing sensitive and confidential information have been lost or stolen.
- According to this year's *Ponemon Institute Annual Cost of a Data Breach* study, the average cost of a data breach has risen to \$202 from last year's \$197 per customer record.

- \$152 pertains to indirect cost including abnormal turnover or churn of existing and future customers and in-house investigations and communication.
- \$50 are attributed to direct costs and include line items such as engaging forensic experts, outsourced hotline support, free credit monitoring subscriptions, notification services and discounts for future products and services.
- In a recent survey by the Ponemon Institute of 43 organizations victimized by security breaches the range of total cost was between \$613k and \$32 million. The magnitude of the breach event ranged from 4,200 to 113,000 lost or stolen records. The average cost was \$6.65 million.
- In another recent survey of 577 respondents 92% of IT security practitioners reported their organization had a cyber criminal attack.
- 42% of security breaches are caused by lost or stolen laptops
 - Business travelers lose more than 12,000 laptops per week in U.S. airports.
 - More than 42% of respondents admit that they do not back up the data in their laptop computers.
 - The types of company information contained on business traveler's laptop computers included customer or consumer data (47%), business confidential information (46%), intellectual property such as software code, drawings or renderings (14%), and employee records (13%).

These statistics serve to reinforce our intuition about the costs associated with security breaches or failure to make an appropriate investment in security to avoid these breaches.

But how to budget?

Given that breaches can be accompanied by significant costs, how should one set a security budget and feel confident that an appropriate allocation has been made? There are a number of approaches that can assist in making informed decisions.

Rule of thumb

Up to 5% of your IT budget. In the 2008 Annual CSI Computer Crime & Security Survey, 53% of the 522 respondents indicated that they spend less than 5% of their overall IT budget on information security. 31% spent more than 5%. 15% did not know.

5% is a number that is tossed around in security circles as a reasonable commitment to the security of sensitive information. It is considered a bit ahead of the curve but hardly exorbitant. However, by itself, the number is meaningless and one should take a closer look at a company's specific circumstances to justify budget.

Keeping tabs on your peers

Understanding what others in your industry are doing about information security is another way to gauge whether your efforts or investments are reasonable. It's probably best to try to stay ahead of the curve, as doing so is certainly more justifiable to board members, executive management, shareholders, and even clients. If a breach should occur, it is a more defensible position to have done more to protect yourself than to have been doing less than might be reasonably expected within your industry.

Spending enough on information security to keep up or stay ahead of one's peers is another way to gauge the appropriateness of your security budget.

Keeping tabs on emerging threats

Statistics like those presented above help characterize the threat landscape, what people are doing to prevent these threats, and what they are doing after these types of breaches occur.

Staying on top of security trends can present opportunities for investment to head off major security breaches and can be useful in setting budget.

Security assessment

Knowing your weaknesses is a good way to prioritize remediation activities and security expenditures. There are security assessments of many flavors used to evaluate security from a variety of perspectives and to evaluate resilience to different types of threats:

- Perimeter security assessment – evaluation of security from a hacker's perspective
- Internal network security assessment – assessment of defense in-depth, protection against malicious insiders, attack propagation
- Wireless security assessment – war-driving, discovery of rogue access points and insecure deployments
- Security policy and procedures review – analysis of security governance and comparison with best practices and regulatory compliance requirements
- Data loss prevention assessments – analysis of communication protocols for disclosure violations (e.g. credit card numbers or SSNs sent in the clear)

Having a recent security assessment in hand can help prioritize information security spending in explicit areas of weakness to avoid possible breaches.

Risk assessment

Unlike the security assessments above which are very tactical scans of security vulnerabilities or exposures, a risk assessment takes a top-down, strategic approach to security. Risk assessment is comprised of inventorying assets, analyzing which are the most sensitive, and determining the potential impact if the assets are destroyed, disclosed or corrupted. The assessment then looks at existing controls to mitigate the threats and highlights areas of weakness, essentially where the security investment is not appropriate to the risk.

This approach provides a way for an organization to align its security efforts with its overall strategic business objectives and can help arrive at longer-term security plans.

Note that attempts to be overly quantitative and precise with risk assessments can become an exercise in futility. It's best to stay at a higher level and use qualitative or loose quantitative metrics to perform the assessment. Doing so will cost far less to perform and yield comparable results, especially with respect to strategic planning.

Conclusion

Unfortunately, it remains that attempts to quantify risk are still inadequate, which makes it difficult to calculate the return on investment or internal rate of return for security, which in turn makes it difficult to set appropriate information security budgets. The tools for budgeting discussed above help to at least approach the problem from a number of angles and can provide enough information to make sensible, justifiable decisions about security expenditures.

In the years to come, efforts to quantify risk will become more successful which will increase the ability to deterministically budget for security. Until then it's best to keep an eye on the security landscape, know your weaknesses, and stay ahead of the curve.

About the author



Mat Siljak is Director, Advisory Services, at Illumant, where he drives compliance and enterprise security services. Leveraging deep technology, regulatory, and risk management expertise, he has managed over 100 consulting engagements for firms ranging from Fortune 500 to pre-public companies along with numerous University clients. Mat has participated in many high profile conferences, including "Sarbanes-Oxley: Lessons from the Trenches" and "Sarbanes-Oxley and the CIO." He is CISA certified and is a member of ISACA, and the San Francisco Bay Area

Chapter of InfraGard which provides channels for the exchange of information about infrastructure threats and vulnerabilities.

Prior to joining Illumant, Mat co-founded OLOSEC Network Security Solutions, an information security consulting firm based in Menlo Park, California. He previously held the position of Chief Technology Officer for Bullhound, Ltd., a global technology hedge fund based in London.

Mat holds a B.S. and an M.S. in Electrical Engineering, both from Stanford University.



ILLUMANT

2672 Bayshore Parkway
Suite 505
Mountain View, CA 94043
Phone: +1 650.961.5911
Fax: +1 650.961.5912

www.illumant.com

ABOUT ILLUMANT

Illumant is a trusted strategic and tactical risk management advisor to Fortune 500 companies, higher education institutions, and other public and pre-public enterprises.

Leveraging best practices and deep knowledge of governance, risk management, compliance, and information technology, we partner with our clients to assess and solve critical business problems. Whether the focus is on initiatives driven by regulatory compliance, corporate mergers and acquisitions, or operational pain points, Illumant plays a major role in helping clients consistently meet their objectives.