FORRESTER®

FOR: Security & Risk Professionals

Determine The Business Value Of An Effective Security Program — Information Security Economics 101

by Ed Ferrara, October 2, 2012

KEY TAKEAWAYS

Cybercriminals Monetize Information; So Should You

Cybercriminals know the value of the information they steal and can quickly convert their loot to cash. CISOs need to combat this reality with financial models of their own to focus security efforts on information assets that produce the most current and future revenue, thereby justifying their budgets and prioritizing their resources.

Quantifying Security Costs Requires Complex Financial Modeling

To fully understand security's financial impact on the organization, CISOs should understand all the various costs of protecting information. This includes the fixed costs as well as variable costs, especially those related to breaches. You may find that you're spending too much protecting the wrong things instead of what is most important.

CISOs Need To Build Their Business Case On Solid Business Principles

True business cases are built on the concepts of profit, loss, and acceptable margins. CISOs should use this same approach by associating costs of protecting information with the revenue that information helps generate. Forrester's Information Security Value Model guides you through this strategy to support smart investment and resource allocation.

Determine The Business Value Of An Effective Security Program — Information Security Economics 101

Business Impact: The S&R Practice Playbook

by Ed Ferrara
with Stephanie Balaouras, Chris McClean, Andras Cser, Andrew Rose, Heidi Shey, and Kelley Mak

WHY READ THIS REPORT

This report outlines Forrester's approach to helping you financially model information security. In today's seemingly never-ending cycle of new technologies, cyberthreats, and regulations, it's almost impossible for CISOs to meet all of the modern organization's security demands. In this difficult environment, senior leadership will evaluate the CISO not only on technical performance but also on how he or she manages information security as a business -- prioritizing expenditures and making tough financial calls. Forrester presents the Information Security Value Model, which you can use to calculate the financial value that information security provides to the business in terms your executive colleagues will understand. With this approach, you'll be able to make tough and effective financial decisions and demonstrate appropriate use of resources.

Table Of Contents

Notes & Resources

In developing this report, Forrester drew from a wealth of analyst experience, insight, and research through advisory and inquiry discussions with end users, vendors, and regulators across industry sectors.

Related Research Documents

Protect Your Competitive Advantage By Protecting Your Intellectual Property From Cybercriminals
July 13, 2012

Source Your Security Services
April 25, 2012

Don't Bore Your Executives — Speak To Them In A Language That They Understand
July 18, 2011

CISOS STILL STRUGGLE WITH SECURITY JUSTIFICATION

Despite growing risk profiles and threat landscapes, security organizations still come under financial pressure. CISOs continually express the need for a method to prioritize their security spending and answer such questions as "Am I spending too little or too much?" and "How can I do more with less?"

Although there are a variety of methods to estimate budgetary requirements, most of those used today fail to provide financial flexibility, objectivity, or the ability to communicate the value of information security. Furthermore, most CISOs admit that they don't think strategically about their spending. As Steve Jobs said, "Deciding what not to do is as important as deciding what to do."[1]

Cybercriminals Have A Business Model . . .

Cyberthieves have well-developed business plans as part of their attack strategy. They target specific information assets because they know the street value of what they steal. This drives their planning and allows them to think in the long term. The result is an environment in which:

- **Cybercriminals don't need to spend a lot to steal a lot.** Attackers looking for private information demonstrate surprising efficiency. In one example of this precision, hackers targeted the payroll accounts of Eastern European home workers representing some 400 American companies. Using relatively inexpensive, off-the-shelf malware toolkits such as Zeus, they netted $70 million before the FBI and other authorities arrested them in March 2012.[2]

- **Well-defined markets exist for stolen information.** There is an underground economy, where supply and demand set prices just as they do for other goods and services. Consider the markets for stolen personally identifiable information (PII) and healthcare records. A cyberthief will earn $1 for a simple Social Security number, but the same thief can earn $50 for a medical identification number. Typically, simple identity theft pays about $2,000, on average (e.g., Social Security number, credit card), but a thief using a medical ID number can earn an average payout of $20,000 per medical record.[3]

- **State-sponsored agents operate under their own rules.** A wave of China-based cyberspies mounted successful attacks on networks of at least 760 companies, research universities, Internet service providers, and government agencies over the past decade. The targets ranged in size from some of the largest corporations to niche innovators in sectors such as aerospace, semiconductors, pharmaceuticals, and biotechnology.[4] China has made industrial espionage an integral part of its economic policy, stealing corporate secrets to help it "leapfrog" US and other foreign competitors to further its goal of becoming a leading economic and military power.[5]

. . . And CISOs Desperately Need Their Own Business Model To Compete

CISOs are at a competitive disadvantage because while the cybercriminals have well-developed business plans, they do not. Most CISOs interviewed for this research think they do "a pretty good job at budgeting" but struggle to define a clear business case for security. When pressed further, however, most ultimately admit they are not sure if they are really good at what they do or just lucky.

CISOs use various means to estimate their budgetary needs. One approach is to benchmark against what other firms spend on security, another is to peg spending as a percentage of IT costs. These approaches don't satisfy either the CISO or senior management and don't represent a sound business case. Some of the biggest challenges include:

- **CISOs don't align security objectives with corporate strategic or functional objectives.** When asked to name their company's strategic objectives, many CISOs were unable to. They also had little understanding of what other departments used as success metrics and were therefore unable to link information security success factors with those of other business functions and units.[6]

- **CISOs use very few quantitative measures to support the budgeting process.** When asked how they set priorities for the year, many CISOs claim they use "professional judgment" to determine where to allocate resources. The resulting budget numbers then represent more a rough order of magnitude than a focused financial assessment of real need driven by loss experience and risk assessment.

- **CISOs use last year's budget to determine this year's budget.** Many firms reported that they wanted to be in the "50th percentile" of peer firms for spending on information security. However, in most cases, benchmarking data like this is difficult to come by or inaccurate. In response, these CISOs tweak their budgets from the prior year. The CISO of a well-respected financial services company explained, "This is the money we had last year, this is what we will have next year, and we make it work." Using this approach doesn't articulate in any meaningful way real budget needs.

- **CISOs don't consider information asset value.** The budgeting process in most cases does not consider the most important questions: "What are your assets worth?" and "How much is the company willing to spend to protect them?" Very few CISOs have accurate and comprehensive information on the type and location of the critical data that resides in their company's infrastructure, let alone how much protection that data needs.

INFORMATION IS NOW THE PRODUCT — IT PRODUCES THE REVENUE

All executives understand at some level that the information created and consumed by the business has value. For example, while the Coca-Cola company locks its secret recipe in a bank vault simply for marketing purposes — because as we all know, the recipe would also have to reside in its manufacturing management systems — the company clearly places significant value on this information.[7] Apple relies completely on information; it does not self-manufacture any of the devices it designs and sells. Because of this, the company takes security of its intellectual property very seriously. Only a few key employees have access to the design area for new products, and development plans are kept top-secret.[8]

Accountants currently view information as an intangible asset, while machinery and other hard assets are considered tangible. Considering that information now drives modern economies, this accounting practice is outdated. We are now at the point where information should be considered a hard or tangible asset — similar to land or machinery. For example, like any other hard asset, information can depreciate in value and can be shipped, broken, or destroyed. Organizations need better methods to value or monetize these information assets.[9]

We can and should use this simple definition:

> *The value of information is a percentage (up to 100%) of the current and future revenue the information will produce less the direct and indirect costs needed to produce, manage, and protect the information.*

SHOW VALUE WITH FORRESTER'S INFORMATION SECURITY VALUE MODEL

The allocation of revenue to information assets is a new idea. Using this method, CISOs can develop a security budget that is more aligned with business needs, with a focus on the revenue streams that feed the business. This is a better way to account for not only the cost of information security but the benefits as well.

Forrester developed the Information Security Value Model to provide CISOs with a worksheet and process to quantify the value of information security, similar to how you would track profits and losses with an income statement. This financial model will help you estimate the value of information assets using percentage of revenue as a proxy for information security value. It also lets you compare the value of information assets with the costs associated with protecting these assets.

First, Determine The Revenue Contribution Of Your Information

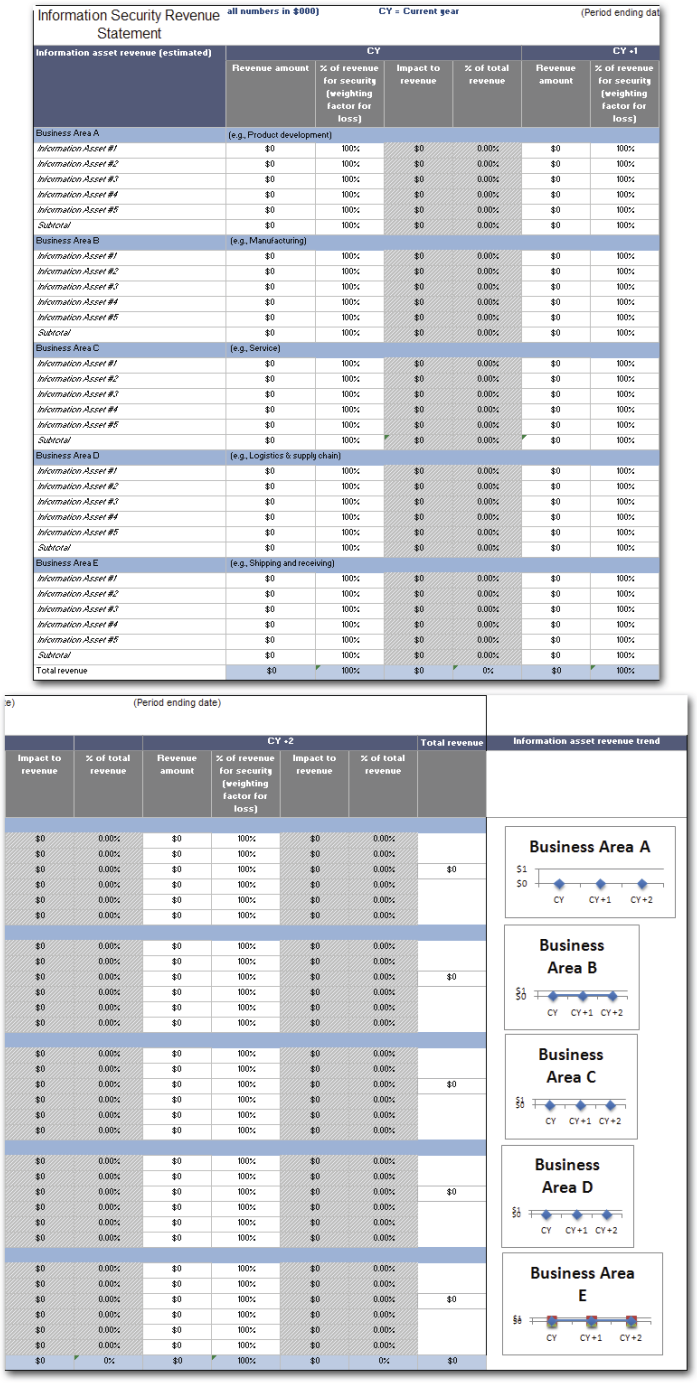
"Cash is king" is the old saying. Tracking how information contributes to revenue quarter by quarter will be important to effectively measure the value of information security efforts. Follow these steps to categorize and quantify the revenue from an information asset (see Figure 1):[10]

- **Categorize information assets by business area.** To understand the role that information plays in supporting revenue generation, you must first associate it with the areas of business that produce, manage, and receive value from the information. Business areas could be complete divisions of the company, or they could be departments, such as product development, manufacturing, or logistics. In some cases, information may be created, accessed, and used by multiple business areas; therefore, revenue produced from these information assets should be allocated to each.

- **Quantify the revenue that the information assets produce.** Study the business plans for the products and services the business unit delivers and for the processes supported by the information assets in question. For example, a large multinational telecommunications company tracks its information security expenditures and controls by product line. This allows the CISO of this company to explain to senior leadership the revenue that the information security team helps deliver by securing these assets. It also lets the CISO focus efforts on the assets that matter most.

- **Quantify risk and compliance implications for non-revenue information assets.** Some information assets need protection to satisfy compliance requirements or to avoid other risks not associated with lost revenue. These need to be quantified as a cost of doing business.[11] For example, employee identity and health records fall into this category because they are not directly product- or service-related. Information requiring protection for SOX, HIPAA, FFIEC, and other regulations would also fall into this category.

Figure 1 Capture Information Asset Revenue



Information Security Revenue Statement — all numbers in $000) — CY = Current year — (Period ending dat

Information asset revenue (estimated)	CY				CY +1	
	Revenue amount	% of revenue for security (weighting factor for loss)	Impact to revenue	% of total revenue	Revenue amount	% of revenue for security (weighting factor for loss)
Business Area A	(e.g., Product development)					
Information Asset #1	$0	100%	$0	0.00%	$0	100%
Information Asset #2	$0	100%	$0	0.00%	$0	100%
Information Asset #3	$0	100%	$0	0.00%	$0	100%
Information Asset #4	$0	100%	$0	0.00%	$0	100%
Information Asset #5	$0	100%	$0	0.00%	$0	100%
Subtotal	$0	100%	$0	0.00%	$0	100%
Business Area B	(e.g., Manufacturing)					
Information Asset #1	$0	100%	$0	0.00%	$0	100%
Information Asset #2	$0	100%	$0	0.00%	$0	100%
Information Asset #3	$0	100%	$0	0.00%	$0	100%
Information Asset #4	$0	100%	$0	0.00%	$0	100%
Information Asset #5	$0	100%	$0	0.00%	$0	100%
Subtotal	$0	100%	$0	0.00%	$0	100%
Business Area C	(e.g., Service)					
Information Asset #1	$0	100%	$0	0.00%	$0	100%
Information Asset #2	$0	100%	$0	0.00%	$0	100%
Information Asset #3	$0	100%	$0	0.00%	$0	100%
Information Asset #4	$0	100%	$0	0.00%	$0	100%
Information Asset #5	$0	100%	$0	0.00%	$0	100%
Subtotal	$0	100%	$0	0.00%	$0	100%
Business Area D	(e.g., Logistics & supply chain)					
Information Asset #1	$0	100%	$0	0.00%	$0	100%
Information Asset #2	$0	100%	$0	0.00%	$0	100%
Information Asset #3	$0	100%	$0	0.00%	$0	100%
Information Asset #4	$0	100%	$0	0.00%	$0	100%
Information Asset #5	$0	100%	$0	0.00%	$0	100%
Subtotal	$0	100%	$0	0.00%	$0	100%
Business Area E	(e.g., Shipping and receiving)					
Information Asset #1	$0	100%	$0	0.00%	$0	100%
Information Asset #2	$0	100%	$0	0.00%	$0	100%
Information Asset #3	$0	100%	$0	0.00%	$0	100%
Information Asset #4	$0	100%	$0	0.00%	$0	100%
Information Asset #5	$0	100%	$0	0.00%	$0	100%
Subtotal	$0	100%	$0	0.00%	$0	100%
Total revenue	$0	100%	$0	0%	$0	100%

e) (Period ending date)

CY +2						Total revenue	Information asset revenue trend
Impact to revenue	% of total revenue	Revenue amount	% of revenue for security (weighting factor for loss)	Impact to revenue	% of total revenue		
$0	0.00%	$0	100%	$0	0.00%		Business Area A
$0	0.00%	$0	100%	$0	0.00%		
$0	0.00%	$0	100%	$0	0.00%	$0	
$0	0.00%	$0	100%	$0	0.00%		
$0	0.00%	$0	100%	$0	0.00%		
$0	0.00%	$0	100%	$0	0.00%		
$0	0.00%	$0	100%	$0	0.00%		Business Area B
$0	0.00%	$0	100%	$0	0.00%		
$0	0.00%	$0	100%	$0	0.00%	$0	
$0	0.00%	$0	100%	$0	0.00%		
$0	0.00%	$0	100%	$0	0.00%		
$0	0.00%	$0	100%	$0	0.00%		
$0	0.00%	$0	100%	$0	0.00%		Business Area C
$0	0.00%	$0	100%	$0	0.00%		
$0	0.00%	$0	100%	$0	0.00%	$0	
$0	0.00%	$0	100%	$0	0.00%		
$0	0.00%	$0	100%	$0	0.00%		
$0	0.00%	$0	100%	$0	0.00%		
$0	0.00%	$0	100%	$0	0.00%		Business Area D
$0	0.00%	$0	100%	$0	0.00%		
$0	0.00%	$0	100%	$0	0.00%	$0	
$0	0.00%	$0	100%	$0	0.00%		
$0	0.00%	$0	100%	$0	0.00%		
$0	0.00%	$0	100%	$0	0.00%		
$0	0.00%	$0	100%	$0	0.00%		Business Area E
$0	0.00%	$0	100%	$0	0.00%		
$0	0.00%	$0	100%	$0	0.00%	$0	
$0	0.00%	$0	100%	$0	0.00%		
$0	0.00%	$0	100%	$0	0.00%		
$0	0.00%	$0	100%	$0	0.00%		
$0	0%	$0	100%	$0	0%	$0	

Source: The Forrester Information Security Value Model

82082 Source: Forrester Research, Inc.

Next, Determine Fixed Costs And Predict Variable Costs

Characterize information security costs as both fixed and variable.[12] Costs should be relevant, reliable, and consequential.[13] It's especially important to review variable costs, because organizations so rarely track them effectively. When asked about unplanned costs, many CISOs respond by saying, "We just handle situations as they arise." The problem with this approach is that, over time, these variable costs add up, which means initial security budget estimates end up wildly inaccurate.[14] Use the following steps to categorize information security costs (see Figure 2):

- **Quantify fixed operational costs**. Add up your fixed operation costs, which include employee compensation, office space, and other support costs for staff; data center allocations for security hardware such as firewalls and net filtering appliances; and license fees for security software such as SIEM, log management, and vulnerability testing.

- **Quantify fixed legal and regulatory costs.** Calculate all the costs associated with preparing for legal and regulatory reviews such as PCI compliance reviews, external audits, and compliance reporting costs. Also include costs of managing legal and compliance obligations, such as legal resources you may have on retainer or compliance management systems.

- **Estimate direct, variable costs.** Variable security costs are those related to breach identification, forensic analysis, and remediation. These costs can include employee salaries, consulting fees, hardware and software charges, as well as costs for data restoration, communication, public relations, breach notification, and, possibly, direct payments made to customers or employees because of the breach. Other direct, variable costs can include write-downs for stolen intellectual property, severance cost for terminated employees, and the costs for selecting new third-party contractors. Estimates for the costs of a breach range from $50 to $215 per record.[15]

- **Estimate variable legal and regulatory costs.** Legal and regulatory costs are those incurred when addressing regulators and other authorities in response to a privacy breach or other security issue with legal implications. These costs can include payment of fines, penalties, and mandatory audits. Variable costs may also include settlements or legal defense against clients, patients, partners, or employees who have suffered alleged harm from the breach.

- **Predict variable operational costs.** Variable operational costs result from the response that follows a data breach or other incident. These costs could include consulting, communications, outside legal counsel, new security processes, and new investments in technology. Your organization may also incur costs of replacing employees, selecting new business partners, and implementing new controls.[16]

- **Calculate the variable reputational costs.** This is one of the hardest costs to quantify, but it's important to try to put a price on the reputation of your organization. Organizations work hard to build a positive reputation in their respective markets. Although difficult to quantify, many organizations view reputation as a priceless asset. Trust is something earned over a long period and can be quickly lost.

Figure 2 Capture Information Security Costs

Information security costs (estimated)	CY		CY +1		CY +2		Total
	Expense amount	% of total revenue	Expense amount	% of total revenue	Expense amount	% of total revenue	
Fixed costs							
Consulting expenses							
External risk assessment	$0		$0		$0		
External penetration assessment	$0		$0		$0		
External vulnerability assessment	$0		$0		$0		
Data center costs	$0		$0		$0		
Fixed internal audit/review	$0		$0		$0		
Fixed legal costs	$0		$0		$0		
Intrusion detection protection costs	$0		$0		$0		
Log management and archive costs	$0		$0		$0		
Network charges	$0		$0		$0		
Salaries and benefits	$0		$0		$0		
Security hardware (acquisition/depreciation)	$0		$0		$0		
Security software (licensing)	$0		$0		$0		
Subtotal fixed operating expenses	$0	0.00%	$0	0.00%	$0		$0
Variable remediation costs							
Breach remediation costs							
Consulting fees and expenses	$0		$0		$0		
Communication costs (media, individual notification)	$0		$0		$0		
Employee training	$0		$0		$0		
Investigation and forensic costs	$0		$0		$0		
Miscellaneous costs	$0		$0		$0		
Security awarness	$0		$0		$0		
Vendor management (change)	$0		$0		$0		
Workforce changes	$0		$0		$0		
Subtotal variable remediation costs	$0	0.00%	$0	0.00%	$0	0.00%	$0
Variable legal costs							
Fines and penalties	$0		$0		$0		
Lawsuits	$0		$0		$0		
Regulatory action	$0		$0		$0		
Subtotal variable operating costs	$0	0.00%	$0	0.00%	$0	0.00%	$0
Variable reputation costs							
Reputation	$0		$0		$0		
Other	$0		$0		$0		
Subtotal variable reputation costs	$0	0.00%	$0	0.00%	$0	0.00%	$0
Total security expenses (fixed, variable)	$0		$0		$0		$0
Net security value	$0		$0		$0		$0
Net security value as a percentage of revenue	0.00%		0.00%		0.00%		0.00%

Source: The Forrester Information Security Value Model

82082 Source: Forrester Research, Inc.

Finally, Calculate Security Value As A Ratio Of Protection Costs To Revenue

Forrester proposes a new measurement of security value that can be expressed by the following formula:

Security costs/revenue = information security value.

Here, security costs are the total costs needed to protect revenue-producing information and information with compliance and risk implications. Revenue is the income produced by the information assets associated with those security costs. Using this approach will help you think more like a financial officer and manage this ratio down over time, so you can demonstrate focused and efficient use of resources.

Recognizing the role information plays in generating revenue is the first step in building a true business case for security. Looking at security value in this way allows senior executives to make better decisions with respect to security because they know what is at stake. This enables you to address the question, "If a product or solution is worth a certain amount to the company in future revenue, what percentage of that revenue are we willing to spend to protect that revenue stream?"[17]

RECOMMENDATIONS

USE A SOUND FINANCIAL MODEL TO DRIVE SECURITY DECISIONS

CISOs have long struggled with techniques to accurately estimate budget requirements. If you're in this situation, focus on the basics of business. The income statement and balance sheet are the primary means to determine the health of a business. Adapt these tools to support the planning process in information security by following these steps:

- **Determine which information assets make the most money for your company and start there.** Different information sets have different value. Some information is critical to the business — for example, the design for the next generation iPad. Other information is not — the design of the original 1984 IBM-PC. CISOs should work with their business partners to focus on protecting the information that is important to current and future revenue first.

- **Use the Information Security Value Model to reallocate resources.** Even though information security budgets remain largely flat, you can still reallocate resources and focus on what really matters to the business. Even security programs with only 5% to 6% of the IT budget still have real money to work with. Don't keep spending on security efforts if they're not associated with revenue.

- **Think like a financial officer.** Use the Forrester Information Security Value Model to develop an information security value statement. Evaluate information assets based on the revenue they generate. Look for ways to remove information assets from the enterprise that don't generate revenue. Not only will this streamline your security budget, but your organization's infrastructure and application costs will go down as well.

SUPPLEMENTAL MATERIAL

Online Resource

The underlying spreadsheet detailing Figures 1 and 2 is available online.

The online version of Figures 1 and 2 is an interactive model that can be used to create an information security income or value statement. This model expresses security expenses as a percentage of revenue. Expressing information security as a percentage of revenue more accurately represents the true value of information security and the role information plays in the organization's value chain.

ENDNOTES

[1] Source: Walter Isaacson, *Steve Jobs*, Simon & Schuster, 2011 (http://www.amazon.com/Steve-Jobs-Walter-Isaacson/dp/1451648537).

[2] Source: "University professor helps FBI crack $70 million cybercrime ring," Rock Center with Brian Williams, March 21, 2012 (http://rockcenter.nbcnews.com/_news/2012/03/21/10792287-university-professor-helps-fbi-crack-70-million-cybercrime-ring?lite).

[3] The American National Standards Institute and the Internet Security Alliance recently published a business case document on the costs of a healthcare breach. This document provides a strong business model and justification for healthcare records. Source: "The Financial Impact of Breached Protected Health Information," American National Standards Institute, 2012 (http://webstore.ansi.org/phi/#.UFd2441lSVI).

Also, for more information on the cost of breaches, see the July 13, 2012, "Protect Your Competitive Advantage By Protecting Your Intellectual Property From Cybercriminals" report.

[4] Source: Michael Riley and John Walcott, "China-Based Hacking of 760 Companies Shows Cyber Cold War," Bloomberg, December 14, 2011 (http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html).

[5] Source: Rodney Joffe, "Frogger — And Other Tales Of APT Leaping Forward," Forrester's Security Forum, May 25, 2012.

[6] For more information, see the July 18, 2011, "Don't Bore Your Executives — Speak To Them In A Language That They Understand" report.

[7] Coca-Cola does list the recipe for Coke on its balance sheet. After Dr. John S. Pemberton invented Coca-Cola in 1886, the Coca-Cola Company kept the formula a close secret, only sharing it with a small group of employees and never in writing. In 1891, Asa Candler became the sole proprietor of Coca-Cola after purchasing the rights to the business. Then, in 1919, Ernest Woodruff and a group of investors purchased the company from Candler and his family. To finance the purchase Woodruff arranged a loan and as collateral, he provided documentation of the formula by asking Candler's son to commit the formula to paper. Coca-Cola placed the recipe in a vault in the Guaranty Bank in New York until Candler repaid the loan in 1925. At that point, Woodruff reclaimed the secret formula, returned it to Atlanta, and placed it in the vault of SunTrust Bank. Source: "Coca-Cola Moves its Secret Formula to The World of Coca-Cola," The Coca-Cola Company press release, December 8, 2011 (http://www.thecoca-colacompany.com/dynamic/press_center/2011/12/coca-cola-secret-formula-moves-to-the-world-of-coca-cola.html).

[8] "The design studio where Jonathon "Jony" Ive reigns (Apple's chief designer), on the ground floor of Two Infinite Loop on the Apple campus, is shielded by tinted windows and a heavy clad, locked door. Just inside is a glass-booth reception desk where two assistants guard access. Even high-level Apple employees are not allowed in without special permission. Source: Walter Isaacson, *Steve Jobs*, Simon & Schuster, 2011 (http://www.amazon.com/Steve-Jobs-Walter-Isaacson/dp/1451648537).

[9] Rear Admiral Grace Hopper said in 1987, "Someday, on the corporate balance sheet, there will be an entry which reads, 'Information', for in the most cases the information is more valuable than the hardware that processes it." Source: Daniel Geer Jr., *Economics & Strategies of Data Security*, Verdasys, 2008 (http://www.amazon.com/Economics-Strategies-Data-Security-DANIEL/dp/B001LZM1BY/ref=sr_1_1?s=books&ie=UTF8&qid=1347909244&sr=1-1&keywords=economics+%26+strategies+of+data+security).

[10] Figure 1 is an example. The information in this worksheet is for demonstration purposes. The actual work to determine an information asset's contribution to revenue takes the following steps: 1) Organize by revenue stream the IT systems that support the revenue stream. In the case of IT systems that support multiple revenue streams, allocate the revenue to the IT system proportionally to the percentage of revenue represented by the revenue stream; 2) categorize the information assets managed by the IT systems, and then associate the revenue streams to these assets. Your company program and product managers should be able to help in this activity.

[11] This paper is not meant to be a tutorial on cost accounting. However, obtaining cost accounting expertise will be beneficial to developing a good profile of all the costs associated with compliance. Quantification of compliance costs depends on the industry and the regulations for which firms are held accountable. These costs include but are not limited to documentation, audit, process change, research, and legal costs.

[12] Variable costs will increase proportionally to the level of security activity in the organization. Depending on type of business, examples could include additional salaries, overtime pay, consulting, communication costs, system restoration or repair, etc. Fixed costs remain the same regardless of the number of breaches you experience. Depending on your type of business, some typical examples would be rent, interest on debt, insurance, plant and equipment expenses, business licenses, and salary of permanent full-time workers. Generally the CFO, controller, or internal auditor can help determine which of your costs are fixed and which are variable, but here the key word is "help." In order to be accurate, the ultimate classification has

to be done by someone who's intimately familiar with security operations — which means the CISO. It's important to realize that fixed costs are "fixed" only within a certain range of activity or over a certain period of time. For example, data center charges are a constant amount per month. Source: "Fixed and Variable Costs," US Chamber of Commerce (http://www.uschambersmallbusinessnation.com/toolkits/guide/P06_7510).

[13] Organizations rarely understand the real costs when cyberthieves steal or destroy information. Part of the problem is that there are no standard cost accounting methods to accurately capture and report these costs. In many cases, organizations create accounting methods and processes as the result of a crisis. Especially concerning is the impact of an event on future cash flows. If a third party stole the design for the iPhone, for example, and produced a similar product, how would this affect the sales of iPhone? The current practice in dealing with this issue often involves simply leaving "unreliable" information unreported. Such a method of accounting has drawn heavy criticism in areas other than information security. However, information security is no different from other areas of business operations, and the loss or destruction of information represents significant business risk. CISOs should recognize the financial impact of information security risk across three dimensions. These are: 1) relevance — relevance measures the value of information in business decisions; 2) reliability — reliability is the "faithfulness with which a measure represents what it purports to represent"; and 3) consequence — consequence measures the potential impact of the loss of the information to the organization. Source: Xiao-Jun Zhang, Information Relevance, Reliability and Disclosure, University of California, Berkeley, 2010 (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1408310).

[14] Source: "The Financial Impact of Breached Protected Health Information," American National Standards Institute, 2012 (http://webstore.ansi.org/phi/#.UFd2441lSVI).

[15] Forrester's research partner CyberFactors estimates the average cost per record to be approximately $200 per record. The Ponemon Institute estimates the cost per record to be higher, at $2,265 per record.

[16] No one can actually predict when or how big a breach will be, and therefore predicting the cost of a breach is difficult. That being said, we can remove some of the uncertainty around breach cost by modeling the breach and the impact it has on the company from a revenue and direct cost perspective. Measuring security is a process of understanding what we want to observe and then measuring the desirable or undesirable result. If it matters at all, it is detectable or observable. If it is detectable, it can be detected as an amount (or range of possible amounts). If it can be detected as a range of possible amounts, it can be measured. Source: Douglas W. Hubbard, *How to Measure Anything: Finding the Value of Intangibles in Business*, Wiley, 2010 (http://www.amazon.com/How-Measure-Anything-Intangibles-Business/dp/0470539399).

[17] The percentage of revenue allocated to information security will vary from company to company and industry to industry. However, CISOs need to think in terms of continuous improvement. The lower the percentage of revenue you spend on security, the more profitable your company will be.

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Focuses On
Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

« **SEAN RHODES,** client persona representing Security & Risk Professionals