

July 24, 2009

Articulating The Business Value Of Information Security

by Khalid Kark
for Security & Risk Professionals



July 24, 2009

Articulating The Business Value Of Information Security

by **Khalid Kark**

with Robert Whiteley and Allison Herald

EXECUTIVE SUMMARY

Many CISOs struggle to articulate the value of their security programs and justify the security budget to business and executive management. This problem was acutely evident in the current economic downturn: Many security managers saw their budgets slashed, their projects postponed, and their employees laid off. CISOs have always struggled to effectively communicate the value of information security to business, but now there is a lot more at stake if they don't. Working closely with top CISOs at large, global organizations, Forrester has identified five areas of value for the business: reputation, regulation, revenue, resilience, and recession. Depending on your audience, we recommend that you use all or a combination of these business value propositions to make the case for continued investment and maybe even an increase in your security spending.

TABLE OF CONTENTS

2 **CISOs Struggle To Answer Some Basic Questions**

2 **Business Value Is Subjective; Therefore, You Need A Value Tool Kit**

Focus Your Security Value On Helping The Business Better Manage Its Information Risk

4 **Remember The Five R's When Making The Case For Information Security**

Reputation: Security Protects Your Brand Equity

Regulation: Security Reduces The Cost Of Meeting IT Regulatory Mandates

Revenue: Security Protects Existing Revenue Streams And Helps Generate New Ones

Resilience: Security Ensures Your Business Functions Even During Adverse Conditions

Recession: Security Affects The Top Line And The Bottom Line Of The Business

RECOMMENDATIONS

8 **Use 10 Steps To Overcome Security's Image Problem**

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

["Case Study: DTCC Implements A Process-Based Approach To Security Metrics"](#)

April 29, 2009

["Case Study: Harland Clarke Turns To Corporate Objectives For Defining Security Metrics"](#)

April 29, 2009

["Security Budgets, Reporting, And Responsibilities Are All Rising In 2009"](#)

January 20, 2009

["Twelve Recommendations For Your 2009 Information Security Strategy"](#)

January 20, 2009

["Best Practices: Security Metrics"](#)

July 22, 2008

CISOS STRUGGLE TO ANSWER SOME BASIC QUESTIONS

Many CISOs have been so focused on responding to threats and managing day-to-day operational issues that they haven't focused on answering some very basic questions their business peers are posing. This approach was sufficient when information security was embedded deep inside IT and was only responsible for technical and tactical activities associated with protecting the organization. Today, however, security teams must work very closely with the business to understand and meet its expectations. Moving forward, it's important that CISOs position information security to proactively answer such questions as:

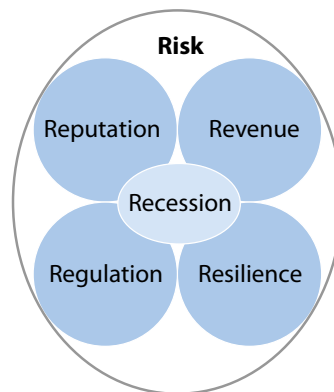
- **What have you done for me lately?** No news is definitely good news as far as information security is concerned. But this also brings the risk of "out of sight, out of mind." Information security teams endeavor to ensure that there are no security issues or incidents in the organization, but therein lies the problem: When they do a good job and prevent the incidents and attacks, then there is nothing to report, and the business may think that security isn't doing much.
- **Why should I add cost, effort, and time to my project?** Project are almost always restricted by time, resources, or money, and information security usually adds to a project's requirements for all three. As a result, security either gets ignored — or worse, the security team is called in at the last minute to "approve" a project so that it can go live. However, when security teams want to be proactive and add security controls, they are labeled show stoppers.
- **What language are you speaking?** A CIO once commented, "Every time I get a security report, I cringe a little, because I am sure I won't understand at least half of it." Similarly, a CEO recently echoed similar sentiments when he said, "I would love to take my CISO to my board, because the board really is interested in security and risk, but he speaks a different language and would not be able to communicate well with the board." These comments are clear examples of security failing to communicate effectively with management and the board.
- **Security is not my job; why should I pay attention to it?** When the security team asks a business area to take responsibility for security initiatives within its organization, the business area commonly responds: Security is not my job, so I shouldn't be held accountable for it. People in the business wonder: If other positions such as a network manager can be held accountable for issues in the network, then why can't a security manager be held accountable for security issues?

BUSINESS VALUE IS SUBJECTIVE; THEREFORE, YOU NEED A VALUE TOOL KIT

The root cause of all these questions is that the business does not understand the value of information security. If CISOs and security managers could articulate the value of information security to the business, they could prevent many value-related questions from ever arising.

While talking to the business, keep in mind that “business value” is a very subjective thing and may mean different things to different executives. Therefore, you must adjust your message and communication based on the audience. Forrester recommends using the fives “R’s” to articulate the value of information security to the business. These five values — reputation, regulation, revenue, resilience, and recession — should be part of a larger umbrella program focused on information risk (see Figure 1).

Figure 1 Information Security Is Best Articulated Using The “Five R’s” Of A Risk-Oriented Program



54908

Source: Forrester Research, Inc.

Focus Your Security Value On Helping The Business Better Manage Its Information Risk

A few years back, Forrester asked a group of CISOs, “What is the primary driver for implementing security controls in your organization?” The majority of respondents answered, “Because we need to comply with a regulation or a mandate.” When we asked the same question to a group of CISOs this year, the answer was different: “Because we want to manage our information risk.” This anecdote is a testament to how far CISOs have come in their thinking and maturity around security issues. Many organizations today realize the benefits of managing information risk, especially in an increasingly digital world. But in addition to the offering the obvious advantage of helping the business align its limited resources to its priorities, a successful information risk program should be:

- **Consistent.** Historically, IT risk management initiatives have often been fragmented, particularly in large, distributed, global businesses. Today, executives are trying to establish a more consistent, enterprisewide approach to IT risk management that will help better aggregate and analyze data for decision-making. In addition, risk-related functions such as reporting and auditing are more economical when practices and technologies are consistent.
- **Efficient.** Lines of business object to multiple risk assessments that ask the same questions for different purposes. One week an assessment for operational risk might pose a question, and the

next week a business continuity or Sarbanes-Oxley (SOX) compliance assessment may ask the same question. Each assessment requires information about the relevancy of business processes and the state of controls, and the business ends up providing the same information for different assessments and audits over and over again. Many mature security programs have developed standard assessment processes that leverage the information and reduce redundant efforts and costs.

- **Sustainable.** Companies often implement a risk management program as a one-time assessment or project. But more-mature firms are increasingly replacing these point-in-time assessments with ongoing and continuous IT risk management processes to reduce information gaps. If done well, risk management implements a sustainable process to manage and monitor risk in a dynamic business environment, which is an asset when inevitable changes in businesses or economic environments cause unexpected opportunities or threats.

By developing consistent, efficient, and sustainable IT risk management processes, organizations make timely, accurate, and consistent decisions around IT risk management, saving hundreds and even millions of dollars in the long run.

REMEMBER THE FIVE R'S WHEN MAKING THE CASE FOR INFORMATION SECURITY

There was a time when security and risk teams could get buy-in for security initiatives by creating fear, uncertainty, and doubt (FUD) — but not anymore. Executive management is demanding that security teams justify security spending with solid business justifications and demonstrable business value. It's no longer enough to rely on a particular regulation that mandates a security control; security managers now have to prove business value. Forrester recommends articulating security's value by using one or more of the five R's of an effective risk program.

Reputation: Security Protects Your Brand Equity

It's no surprise that executive boards and CEOs are very concerned about security breaches; in recent years, security breaches have caused well-established brands to suffer huge financial losses. Not only are the external threats increasing and are hackers becoming more sophisticated and targeted, but the amount of damage internal threats — intentional or unintentional actions by your own users — incur has also been steadily increasing.¹ Additionally, security breaches originating with third parties and business partners have also been responsible for significant damage to corporate reputation and brand. Thus, CISOs must underscore security's importance in maintaining their company's reputation. Security accomplishes this by:

- **Protecting against an increasingly complicated internal and external threat paradigm.** A CISO once bragged to his CEO that the security organization was responsible for blocking 17,000 spam messages a day. The CEO responded, "Isn't that your job? What is unusual about it?" The CISO went back and recrafted the message to say, "the security organization saves the

company approximately 40 hours of employee time every week by stopping unwanted emails.”² The latter message translates the security initiative in terms of business value; therefore, the CIO had a much more positive reaction to it.

- **Preventing abuse from third parties and business partners.** A pharmaceutical company started getting complaints of adverse patient reactions from South America, a geography where it had miniscule sales. The security team, working in conjunction with the fraud department, was able to uncover that a business partner account had accessed manufacturing details and packing specifications for the product a few months back. Moreover, this partner was suspiciously monitoring the company’s business and marketing plans from a centralized server. Further investigation uncovered that counterfeit drugs were being manufactured and sold in South America under the company’s brand name. By stopping the activity, the security team protected the corporate brand from further damage in South America.

Regulation: Security Reduces The Cost Of Meeting IT Regulatory Mandates

Complying with regulations has been a struggle for many organizations, and as regulations stack up, requirements seem to increase exponentially. The security organization is tasked not only with managing the IT compliance requirements but also with doing so efficiently so that a single audit or assessment can be used multiple times. When articulating the value of regulation, CISOs should focus on:

- **Complying with multiple regulations efficiently.** By developing a common framework that maps to multiple regulations, a utilities company in the US was able to reduce its compliance costs by one-fourth. On top of that, the business was very happy that it did not have to go through multiple audits and that the security team was able to reduce its audit hours by about 35%.
- **Meeting compliance requirements while ensuring business value.** A hotel chain spent \$300,000 on implementing monitoring and reporting tools on its critical servers. This investment not only made the company compliant with Payment Card Industry Data Security Standard (PCI DSS) requirements but also improved revenue and customer satisfaction by reducing aggregate downtime for those critical servers.
- **Avoiding fines and penalties.** Although FUD does not generally work, the fines and penalties associated with noncompliance can be useful in demonstrating business value. Regulations such as SOX have huge implications for business executives — potentially even leading to jail time. PCI DSS, on the other hand, has stiff financial penalties, and recently Health Insurance Portability and Accountability Act (HIPAA) regulations have been getting serious about creating incentives for enforcement. As a good example, a retail outlet was able to avoid potential fines of \$50,000 a day by putting in place an application firewall that carried a price tag of a little more than \$100,000.

Revenue: Security Protects Existing Revenue Streams And Helps Generate New Ones

Although information security may not always contribute directly to a company's revenue, it's often instrumental in protecting corporate intellectual property. But savvy CISOs go one step further, bolstering their value articulation by pointing out that security also helps with:

- **Protecting intellectual property (IP) from being stolen or disclosed.** An engineering company developed a product after three years of research and development (R&D) but lost almost half of its business to an upstart that miraculously was able to produce exactly the same product in five weeks for 20% less cost. After further investigation, the company discovered that an engineer at its business partner had left the partner with the company's designs and started his own company to manufacture the product himself. The company also discovered painfully late that it had not included security and privacy provisions in its third-party contracts and had made no attempt to test the security controls and practices of its partners.
- **Finding new business via marketing that highlights better security.** In some industries such as financial services, information security is part of the corporate marketing. Bank of America, for example, has successfully marketed itself as a bank that values its clients' privacy and security, coming up with innovative ways to increase revenue through consumer security, such as offering two-factor authentication tokens for a small fee. For companies in such industries, security is an absolute necessity for both their internal users and their customers.

Resilience: Security Ensures Your Business Functions Even During Adverse Conditions

Resilience is a top concern for many organizations due to pandemic scares including disasters such as Hurricane Katrina or the tsunamis in the Far East. Many companies realized during these unfortunate disasters that they had no plans and processes in place to deal with them effectively. But security can help by:

- **Ensuring continuity of critical business processes during pandemics or disasters.** A service provider in the Gulf region lost all its business when both its data centers — 30 miles away from each other — were destroyed in Hurricane Katrina. The company did not recover from this loss; it had to file for bankruptcy. On the other hand, another financial service company was not only able to switch over to its backup facility in the Northeast without any major hitch, but it was also able to account for 99% of its staff within three hours of the hurricane hitting the coast. This company's security team spearheaded its business continuity efforts and coordinated with the disaster recovery team from IT. Although the company did suffer a loss, it was able to recover completely in less than 48 hours.
- **Coordinating and responding efficiently to threats and incidents.** Security breaches have huge financial and operational ramifications. But, as many have found, a company's response to a breach is what ultimately determines its fate and acts as a good indicator of the full potential

financial impact. A well-coordinated, well-prepared response catches the breach early and limits its impact and also demonstrates to customers and clients that the company is in control and on top of things, which further limits downstream damage and prevents a similar breach in the future. A clumsy, uncoordinated, and confusing response leads clients and customers to lose their trust in the company from that point on. Thus, it's essential to ensure not only that you focus your energies on protecting against and preventing a breach but also that you have a smooth communication process that does not disrupt business activities.

Recession: Security Affects The Top Line And The Bottom Line Of The Business

Some would argue that talking about the current recession doesn't help articulate the business value of information security. But many CISOs have found that in the current environment, this approach may be the only way to get management's attention. CISOs can help their company achieve its goals in tough times by:

- **Creating efficiencies in business processes.** A manufacturing company spent approximately \$3 million every year on manual compliance processes. The CISO of the company proposed purchasing a governance, risk, and compliance (GRC) tool that would streamline efforts by creating efficiencies around the audit and compliance processes. The company was able to save close to \$2 million during three years by combining its various IT GRC activities such as auditing, assessing, testing, and reporting.
- **Lowering costs by investing in strategic vendor relationships.** A European company had worked closely with a few strategic security vendors and service providers for several years. But when the current downturn in the economy forced the company to reduce its security budget by 30%, it asked these vendors to cut their contract values by 30% with minimal change to its existing contracts. The vendors complied with the understanding that when times get better, they will continue to be the firm's preferred security suppliers. The CISO was able to demonstrate to the business that in tough times the security team and its strategic partners were willing to pitch in and do their part to tighten belts.
- **Using existing products and tools more effectively.** Many customers are demanding a lot more customization and many more enhancements to their existing products to get additional functionalities and capabilities. Unfortunately, this often results in multiple tools that perform the same task or a situation in which an existing security product could deliver the functionality of a tool the organization is considering purchasing. An up-to-date inventory and capabilities assessment can help companies avoid costs by offsetting unnecessary purchases, leading to quicker deployment of security tools.

RECOMMENDATIONS

USE 10 STEPS TO OVERCOME SECURITY'S IMAGE PROBLEM

Implementing the five R's will help you better articulate your security program's value. However, as you seek to build a better business case, you may have to undo the damage of the security team's bad rap. Conduct an image makeover with these 10 steps:

- 1. Hold the business responsible and accountable.** Move away from day-to-day operational and tactical activities and toward more of an advisory role. Your goal should be letting the business decide on risk issues rather than making the decision on its behalf. This may be tough to do in the beginning, and the business may require a lot of awareness and training to make these decisions, but this approach will pay huge dividends later on.
- 2. Push security costs to the business and IT.** Organizations typically view security as a cost center that offers little to show for corporate spending on information security. Get security embedded throughout the organization by tying key security operational costs to IT and pushing other security costs out to business units. This will provide a more accurate distribution of costs for internal accounting and, more importantly, provide a much more accurate foundation for articulating the five R's of security value.
- 3. Redirect the conversation away from threats and toward risks.** Focus on risk management rather than threats and vulnerabilities. Business execs understand and are much more responsive to risks associated with their own services and products. Also, risk management activities preempt and prevent costly threats from materializing.
- 4. Work with the business to protect corporate IP.** Businesses do not often realize the extent to which their IP is exposed, but they do understand the impact of its improper disclosure. Therefore, security team needs to work with the business to identify the "crown jewels" of the company, where they reside, and the appropriate ways to protect them. This may sound simple, but be prepared for a tedious process. It's excruciatingly difficult to find where in the corporate environment the IP — including all of its copies — resides.
- 5. Retool the security team.** Require security personnel to attend business courses, spend time with their business peers, and demonstrate an understanding of business objectives and drivers. The goal is to get the *entire* security team, not just the CISO, speaking to the business on business terms.
- 6. Understand and improve processes.** Security managers must wear a risk management hat and embed security capabilities in business processes. Many CISOs have positively affected established processes such as the software development life cycle, IT operations, and disaster recovery, making them both more resilient and more efficient.
- 7. Focus more on value articulation and less on return on investment (ROI).** Many business managers today understand that, except for a few instances, security initiatives don't produce ROI. Therefore, instead of trying to prove vacuous ROI, focus your energies on articulating value-add and having business-impact discussions.

- 8. Make security processes transparent.** This may sound like motherhood and apple pie, but if you are not completely transparent in your processes, then people in the organization will not take you seriously. Transparency will breed trust and in turn make it easier to drive security into the business processes.
- 9. Create a formal business liaison.** Many successful CISOs, however small their security team, have found that they absolutely need to have a business liaison role within their security organization. By default, this role will fall to the CISO; otherwise, create this role and make the person holding the position responsible for representing the security perspective in all business decisions. Some companies have even experimented with a reverse tactic, embedding security people in business units.
- 10. Move beyond basic compliance to a sustainable risk management model.** Compliance should not be a goal unto itself. Rather, the goal should be to manage risk — and complying with policies, standards, and procedures is just a means to that goal. As you mature in your compliance processes, don't become too tied to individual controls or audit requirements; keep the bigger objective of managing risk in mind.

ENDNOTES

- ¹ For more information see the Verizon Business 2009 Data Breach Investigations Report (http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf).
- ² This calculation was built assuming it takes about eight seconds to view a spam message.

FORRESTER®

Making Leaders Successful Every Day

Headquarters

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617.613.6000
Fax: +1 617.613.5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

Australia	Israel
Brazil	Japan
Canada	Korea
Denmark	The Netherlands
France	Switzerland
Germany	United Kingdom
Hong Kong	United States
India	

For a complete list of worldwide locations, visit www.forrester.com/about.

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 Research, Inc. (Nasdaq: FORR) is an independent research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. Forrester works with professionals in 19 key roles at major companies providing proprietary research, consumer insight, consulting, events, and peer-to-peer executive programs. For more than 25 years, Forrester has been making IT, marketing, and technology industry leaders successful every day. For more information, visit www.forrester.com.