A Custom Technology Adoption Profile Commissioned By Verdasys

IT Leaders Should Look At Economic Value To Drive Security Spending Decisions That Protect Valuable Information Assets

February 2013

Information Is The Product — Its Security Is Paramount

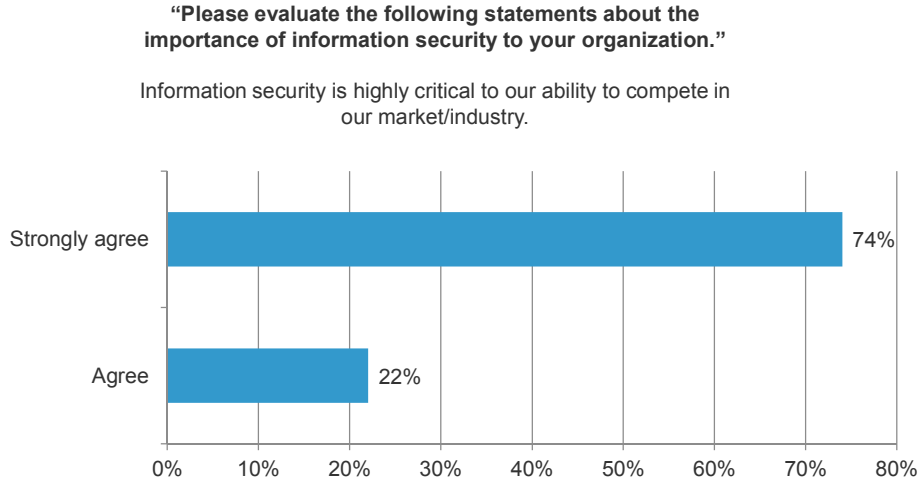
Information represents significant value to all organizations. In many cases today, information is the product, while actual manufacturing is an outsourced commodity. Consider smartphone design as an example. Today's leading smartphone designers create ideas for device functionality, patent these ideas, and then outsource the manufacture of the device to the far reaches of the globe. Most would agree that it's the design of a smartphone that creates the device's value. Players in this industry go to great lengths to protect their designs. In some firms, tinted windows and heavy-clad, locked doors shield the design labs. The doors are guarded, all cell phones must remain with security, and even high-level employees need special permission to enter.[1]

In previous research, Forrester found that CISOs use a variety of ways to create budgets. Approaches include benchmarking against what other firms spend on security; another is to base security spending on a percentage of IT costs. These approaches, lack precision and don't completely satisfy either the CISO or senior management. Some of the biggest financial challenges include:

- **CISOs don't align security objectives with corporate strategic or tactical objectives**. Many CISOs interviewed were unable to articulate their company's strategic objectives. They also had little understanding of other departments' success metrics and were unable to link information security success factors with those of other business units.
- **CISOs use very few real financial models to support the budgeting process**. Many CISOs claim they use "professional judgment" to determine where to allocate resources. The resulting budget represents more of a rough order of magnitude than a focused financial assessment driven by business impact, risk assessment and loss.
- **CISOs use last year's budget to determine this year's budget**. Forrester's research shows that many CISOs want to be in the "50th percentile" of peer firms for spending on information security. However, benchmarking is difficult to come by or is inaccurate. In response, CISOs tweak their budgets from the prior year. For example, one 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."[2]
- **CISOs don't consider information asset value**. The information security budget 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?" Because of the issues already identified 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. It's no wonder they have trouble building the business case for security.

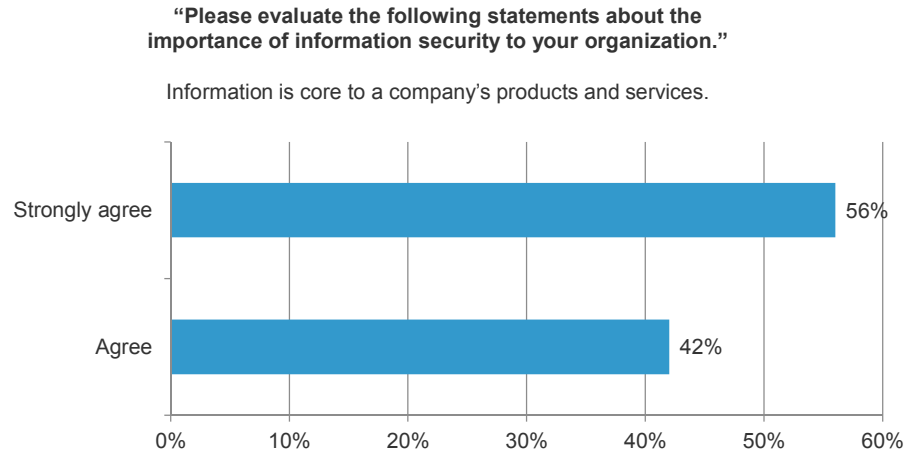
Executives globally have come to the realization that information and its security are critical factors in maintaining competitiveness. It's the design and the intellectual property (IP) the design represents that create a product's value. This is the information that cyberthieves target, and methods exist to monetize this information through either nation-state sponsorship or black-market sales. Because of this, executives now realize that information security is core to a company's product and service offerings. Companies run the risk of competitive loss, damaging their brand, alienating customers, or in the worst case, entering bankruptcy because of a nation-state or competitor stealing the IP (see Figure 1 and Figure 2).

Figure 1
Respondents Agree Information Security Is Highly Critical



Base: 50 North American security decision-makers in organizations with 500 or more employees
Source: A commissioned study conducted by Forrester Consulting on behalf of Verdasys, December 2012

Figure 2
Information Is Recognized As Core To A Company's Offerings



Base: 50 North American security decision-makers in organizations with 500 or more employees
Source: A commissioned study conducted by Forrester Consulting on behalf of Verdasys, December 2012

In the minds of corporate leadership, industrial espionage and its latest method, cybercrime, represents a huge threat to the business. Industrial espionage has been around for a very long time, but computer systems that store tremendous amounts of valuable information present significant new opportunities for insiders and cyberthieves. Nation-states and organized crime are now the major perpetrators of industrial espionage. These organizations are investing millions of dollars to steal billions of dollars in intellectual property.[3] In 2011, the FBI's reported caseload exceeded $14 billion in lost intellectual property.[4]

The growth of both insider attacks and cyberattacks is exponential, with the cost of cybercrime exceeding $114 billion in 2011 and receiving daily attention in the media.[5] At the same time, the audacity and severity of both insider attacks and cyberattacks are growing, and many companies have felt the sting, losing millions of dollars in the process. The recent high-profile breaches at technology, aerospace, oil, and manufacturing companies represent hundreds of millions of dollars in lost revenue, tarnished brands, and, in one noted case, the replacement of senior management.[6] The result has been increased risk awareness at the executive level and increased attention to the protection of intellectual property (see Figure 3).

Figure 3
The Impact Of High-Profile Cyberattacks On IT Security

Base: 1,053 decision-makers in North American organizations with 500 or more employees
Source: Forrsights Security Survey, Q2 2012

Budgeting Is Not A Business Case

As our survey found, executives already agree that security is essential to competitiveness and strongly believe that intellectual property needs increased protection. Therefore, factoring these costs into a comprehensive business case is not only important it's essential. Even though awareness is at an all-time high, senior leaders still demand a sound business case when making investments of any kind. The questions they ask are, "If we spend this money, is our intellectual property going to be any more secure? Are these expenditures enough? Are they worth it?"

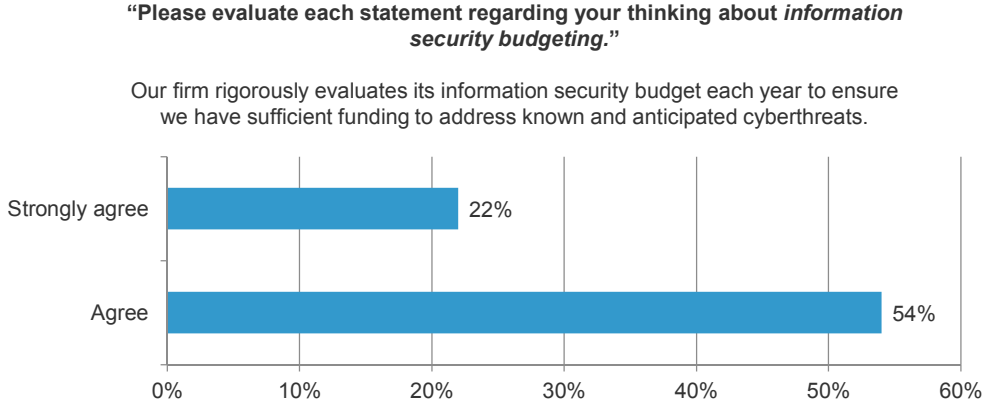
A majority of respondents felt that their firms had rigorously evaluated their information security budget to ensure that the firm had the resources to address anticipated threats (see Figure 4). At the same time, however, these firms failed to consistently calculate information security costs against the revenue potential for new products and services, with more than half (52%) doing so only sometimes, rarely, or never (see Figure 5).

While these firms may believe that they have good budgets in place, it's very likely that they don't. It's even more likely that they haven't made a strong business case for security because they lack information related to

understanding the value of the IP that they're protecting and how it's going to change over time as new products and services come to market.

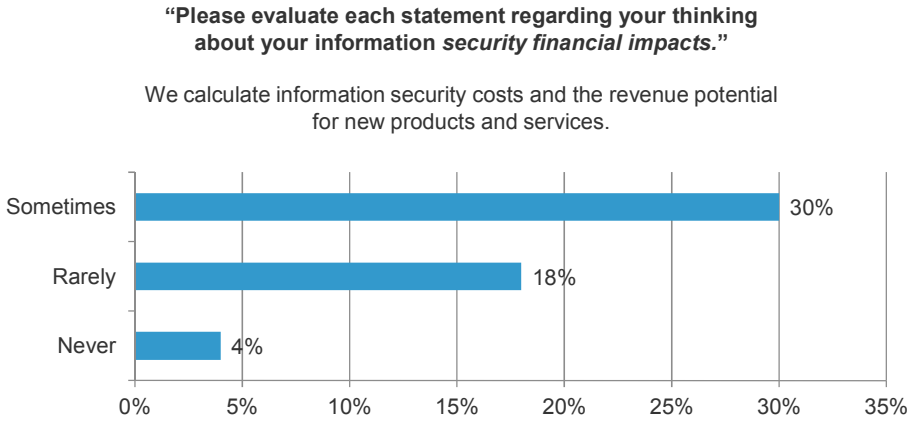
A good business case requires a measurement of the return an investment will make over time when compared with the costs of making the investment. It's often difficult to measure a return on an information security investment, but the information it's protecting almost always has a related revenue stream. The cost of protecting an information asset should therefore be included in the measurement of the return of that asset. The relationship between information security cost and IP value can be measured as security spending over time.[7] Using this approach aligns security investments with the IP that produces the company's revenue stream, which helps create the business case for information security and ensure that spending is proportional to the value of the protected assets.

Figure 4
Respondents Indicate They Review Security Budgets Rigorously



Base: 50 North American security decision-makers in organizations with 500 or more employees
Source: A commissioned study conducted by Forrester Consulting on behalf of Verdasys, December 2012

Figure 5
However Over Half Inconsistently Calculate Information Security Costs



Base: 50 North American security decision-makers in organizations with 500 or more employees
Source: A commissioned study conducted by Forrester Consulting on behalf of Verdasys, December 2012

Data Loss Threatens Your Business — Build The Business Case, Not A Budget

Be assured that cyberthieves have well-developed and profitable business cases. A business case for information security would consistently map current and future revenue to security costs to provide an accurate picture of how much is spent to protect the competitiveness of the business. Security leaders haven't fully made the connection between the value of information and the costs involved to protect it. Although many firms may have budgets, they lack a true business case and can't answer the questions "Are we spending the right amount of money?" and "Are we secure enough?" These need to be financially driven answers, and in many cases for many firms, they're not.

Building the business case for information security requires engaging an additional set of stakeholders involved in the company's product life cycle. The IT department simply budgeting for security based on historic data is no longer sufficient. Organizations need to prioritize their security spending decisions based on real expectations of the impact on revenue if cyberthieves steal important IP. We know the risks are real. If we can monetize information assets, we can monetize the risks to those assets. If we can monetize the risks to the assets, we can make better decisions on how much to spend to protect those assets. This can be expressed by the following equation (see Figure 6).

Figure 6
Information Security Value As A Ratio Of Revenue To Security Cost

Security costs / revenue = information security value

Source: "Determine The Business Value Of An Effective Security Program — Information Security Economics 101," Forrester Research Inc.

Using this approach, information security value is expressed as a ratio comparing the current and future revenue streams information assets produce and the costs of protecting these assets. This model is an effective way of conveying the value of protection relative to the value of the assets revenue stream to non-technical leaders. Recognizing the role information plays in generating revenue is the first step in building a true business case for security. Looking at security value over time and across different revenue streams, allows senior executives to make more informed spending decisions with a greater understand of what is at stake from a financial perspective.

The senior leadership of many firms are now focusing on information security. Attackers looking for private information demonstrate surprising efficiency. There's an underground economy, where supply and demand set prices just as they do for other goods and services. A wave of nation-state cyberspies mounted successful attacks on networks of at least 760 companies, research universities, Internet service providers, and government agencies over the past decade. Data lost includes oil and gas reserve information, networking product designs, stealth technology designs, advanced manufacturing plant layouts and designs, and military electronics information and designs.[8] Although firms are responding, they still need better financial tools and processes to value information, measure and track protection costs, and build the business case for information security.

Methodology

This Technology Adoption Profile was commissioned by Verdasys. To create this profile, Forrester leveraged its Forrsights Security Survey, Q2 2012. Forrester Consulting supplemented this data with custom survey questions asked of 50 security decision-makers in organizations with 500 or more employees in North America. The auxiliary custom survey was conducted in December 2012. For more information on Forrester's data panel and Tech Industry Consulting services, visit www.forrester.com.

Endnotes

[1] Source: Walter Isaacson, *Steve Jobs*, Simon & Schuster, 2011.

[2] Source: "Determine The Business Value Of An Effective Security Program — Information Security Economics 101," Forrester Research Inc., October 2, 2012.

[3] There is a large and lucrative underground economy for all types of intellectual property. According to Verizon's 2012 Data Breach Investigations Report, large organizations are more likely overall to have sensitive organizational data, trade secrets, or classified information compromised in a breach. Stealing or purchasing such information can replace millions if not billions of dollars in research and development. Source: Verizon 2012 Data Breach Investigations Report.

[4] Each year the FBI publishes statistics on cybercrime and the costs of this criminal activity. Source: "Cybercrime Podcast — Crime Statistics and the Nature of Cybercrime," Federal Bureau Of Investigation, 2011.

[5] The cost of global cybercrime, at $114 billion annually, is significantly more than the annual global market for marijuana, cocaine, and heroin combined. A separate Ponemon Institute analysis of cybercrime underscores the steadily rising cost of cybercrime for companies operating in the United States. Businesses based in the US spent $61.5 billion on security and data breaches in 2006. By 2010, those costs had spiked to $101.4 billion, according to the institute, and are forecasted to pass $130 billion in 2011. Source: Alfonso F. Serrano, "Cyber Crime Pays: A $114 Billion Industry," *The Fiscal Times*, September 14, 2011 (http://www.thefiscaltimes.com/Articles/2011/09/14/Cyber-Crime-Pays-A-114-Billion-Industry.aspx#page1).

[6] Source: "Sony Replaces Chief Executive Sir Howard Stringer," *BBC News* (http://www.bbc.co.uk/news/business-16835454).

[7] Forrester's Information Security Value Model helps security leaders calculate the financial value of information security. This approach compares information security costs by business area and product line using a ratio of security cost and product revenue as a planning tool to aid financial investment in information security. Source: "Determine The Business Value Of An Effective Security Program — Information Security Economics 101," Forrester Research Inc., October 2, 2012.

[8] In 2011, China-based hacking affected 760 companies globally. Demonstrating both business and technical shrewdness, the hacking groups targeted a provider of hotel connectivity for an increasingly mobile workforce. The breach may have let hackers see millions of confidential emails, even encrypted ones, as executives from Dubai to New York reported back on everything from new product development to merger negotiations. 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).