

Strengthening Ties Between IT Security And The Business

February 2012

Introduction

Getting executive support, justifying investments, and showing results in a business context: These familiar challenges pervade IT security and risk teams in all organizations, regardless of type, size, or location. While there are no universal solutions, common trends are emerging that promise to help these teams improve the way they work with their business counterparts. This Technology Adoption Profile™ examines the degree to which executives and business decision-makers pay attention to IT governance, risk, and compliance (GRC) concerns and how security decision-makers view their current relationship with the business regarding GRC issues. Most importantly, it looks at what these decision-makers believe can be done to strengthen the relationship between IT and the business so they are better able to show the value of their efforts.

IT Risk Management's Organizational Profile Continues To Grow

While IT security professionals have historically felt that their function lacked visibility in the organization, this situation has been slowly changing over time. One of the biggest drivers of this change is the recurring presence of high-profile cyberattacks in the news. In fact, 70% of security decision-makers report increased executive awareness of IT security as a direct result of recent high-profile attacks and breaches — the most commonly cited result of such public events (see Figure 1).

Figure 1

Attacks And Breaches Mean That Greater Attention Is Paid To IT Security



Base: 1,608 North American security decision-makers
(multiple responses accepted)

Source: Forrsights Security Survey, Q2 2011, Forrester Research, Inc.

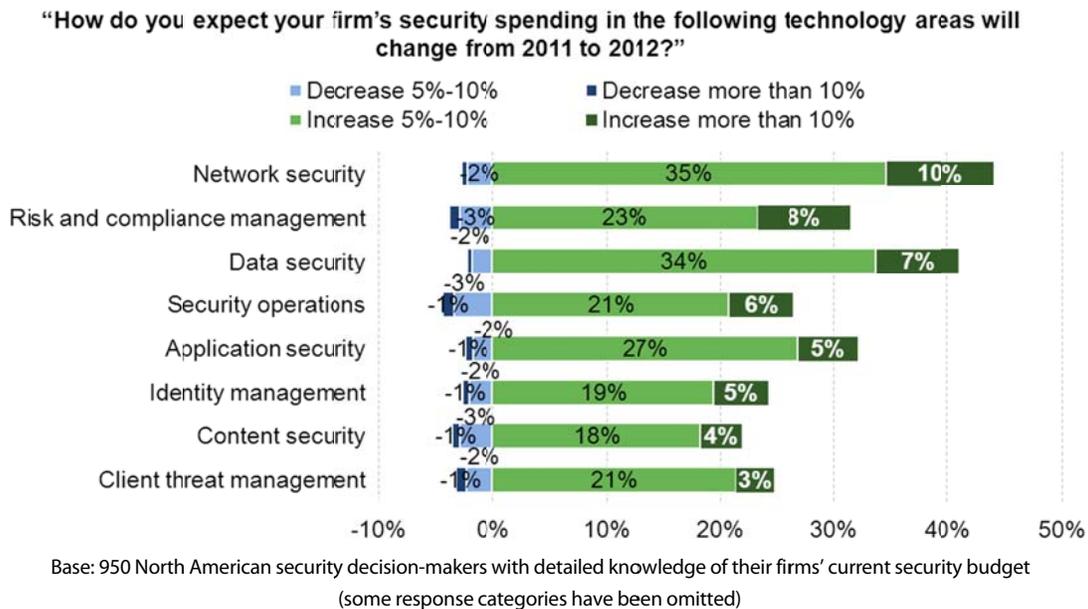


Headquarters

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617.613.6000 • www.forrester.com

As the business turns its attention to information security issues, information security professionals see risk management as a growing priority. A full 20% of security decision-makers surveyed in Forrester's Forrsights Security Survey, Q2 2011 have already adopted or have immediate plans to implement GRC technologies to help measure and manage their risk and compliance efforts; a further 36% are interested in adopting these technologies in the long term. Meanwhile, although risk and compliance management currently represents only 10% of total security spending on average, it is an area in which security professionals expect to see growing investment. Among the budget priorities expected to grow by more than 10%, risk and compliance ranks second only to network security; nearly one-third of respondents predict an investment increase of 5% or greater (see Figure 2).

Figure 2
Risk And Compliance Spending Will Grow Strongly

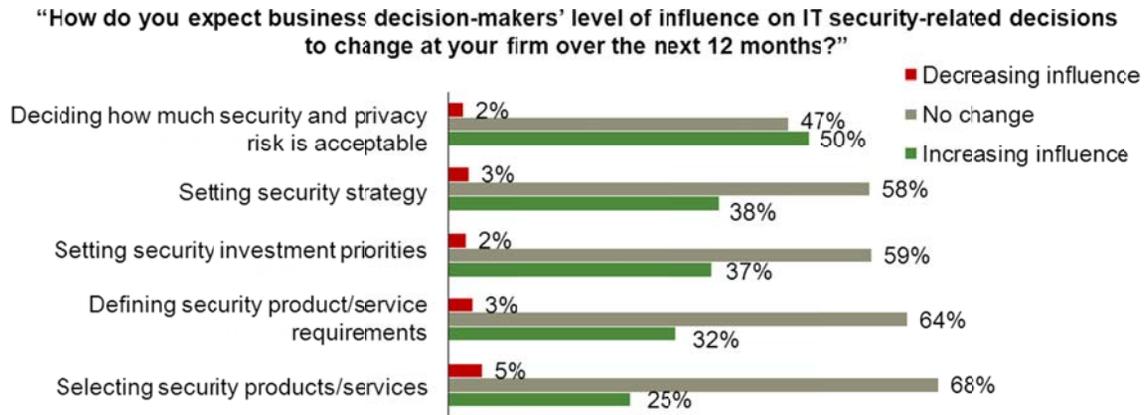


Source: Forrsights Security Survey, Q2 2011, Forrester Research, Inc.

But security professionals are not just going to change to meet business expectations without expecting more from the business in turn. Security decision-makers see several aspects of their job where input from their business counterparts should increase, but none more than decisions about how much risk the organization should be willing to accept. In fact, half of these security professionals said that they expect business decision-makers to increase their influence in the risk management discussion (see Figure 3).

Figure 3

Business Influence On Security Will Increase, Most Notably In Risk Management Decisions



Base: 1,453 North American security decision-makers
 (“Don’t know” responses have been omitted)

Source: Forrsights Security Survey, Q2 2011, Forrester Research, Inc.

IT Risk Management Connects With The Business, But There Is Room For Improvement

In a commissioned research study, Forrester Consulting surveyed 53 decision-makers responsible for IT governance, risk, and compliance at North American enterprises to evaluate how they function within their organization.

Starting with the methods by which they prioritize their security and risk mitigation efforts, the results show that these organizations consider a wide range of factors. But the most common approach for 58% of respondents is to prioritize based on regulatory requirements (see Figure 4). Prioritization based on the reduction of risks to the business is currently the least common approach. However, when asked how their organization should be prioritizing security efforts, nearly half of the respondents said it should consider a holistic view of the financial, operational, regulatory, and reputational risks to the business. It’s interesting to note that while this holistic, risk-based approach was the most common desired approach, meeting compliance requirements was seen as a close second, suggesting that even with more mature, risk-based decisions, regulations and standards will still be significant drivers of security budgets.

Figure 4

Holistic Risk Measurement Is Seen As An Uncommon, But Desired Method To Prioritize Security



Base: 53 IT GRC decision-makers at North American enterprises
(multiple responses accepted)

Source: A commissioned study conducted by Forrester Consulting on behalf of Symantec, January 2012

Naturally, using business risk as a way to make mitigation decisions requires input from colleagues within various business functions, so Forrester also asked respondents to rate the current frequency and effectiveness of their interactions with the business concerning risk. While most report at least a somewhat positive and effective relationship, a full 32% of GRC decision-makers admit that these interactions are ineffective or even counterproductive, leaving substantial room for improvement (see Figure 5). This is particularly interesting to note, given that the vast majority of these decision-makers report that they have regular, if not frequent, meetings with their business counterparts across a full range of risk management topics. Considering the trend toward more participation and input from the business in risk discussions, the challenge does not appear to be a lack of communication, but the quality of that communication.

Knowing that a positive rapport with the business is essential for a successful IT risk management program, we asked respondents to tell us what changes they think would have the greatest positive impact on this relationship. Nearly half say they would like to see improvement in their ability to communicate the value of security and risk management in business terms — more than any other change (see Figure 6). The next two most common answers reflect a desire for more timely and accurate data and more frequent reporting of risk and compliance information.

The responses to this question also confirmed that having more meetings is simply not the answer; just 12% see merit in a fuller calendar. Respondents are actually more likely to want to give business counterparts direct access to risk measurement and reporting tools than they are willing to meet with them more often. This suggests that the IT security and risk professionals are truly looking to partner with the business and help them participate in risk processes rather than simply telling them what to do.

Figure 5

Interaction Between Security And The Business On Risk Issues Is Common, But Not Always Useful

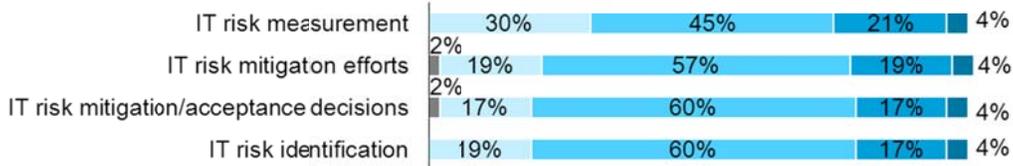
“How would you rate the effectiveness of interactions between IT risk/compliance and colleagues that represent business units or functions (such as finance, HR, sales, or operations)?”

- We do not interact with business functions
- Negative, generally not productive
- Positive, generally helpful
- Very negative, almost always counterproductive
- Neutral, neither particularly helpful nor counterproductive
- Very positive, almost always helpful



“How frequently do you participate in organized discussions, conference calls, or meetings with colleagues outside of IT about the following topics?”

- Not sure
- Never/Rarely (once per quarter or less)
- Regularly (two to three times per quarter/once a month)
- Frequently (two to three times a month)
- Continuously (once a week or more)



Base: 53 IT GRC decision-makers at North American enterprises
(percentages may not total 100 due to rounding)

Source: A commissioned study conducted by Forrester Consulting on behalf of Symantec, January 2012

Figure 6

Improved Interaction With The Business Is About Better Data And Context, Not More Communication

“What changes to your IT risk management program do you think would have the biggest positive impact on your relationship with business counterparts?” (Select up to 3, in order of most positive impact)

- Ranked 1
- Ranked 2
- Ranked 3



Base: 53 IT GRC decision-makers at North American enterprises

Source: A commissioned study conducted by Forrester Consulting on behalf of Symantec, January 2012

Successful IT Risk Management Is About Better Data And Business Context

For today's IT governance, risk, and compliance decision-makers, increased visibility in the organization is both a notable achievement and a difficult challenge. Working more closely with business colleagues is essential to make sure mitigation efforts and investments are on point, but that interaction can often be difficult without the right approach. The natural tendency might be to set up more frequent interactions to exchange information and ideas; however, the overwhelming sentiment among IT GRC professionals is that improvement will come primarily from better — not more — communication. This means being prepared to talk about IT risks within the context of financial, operational, regulatory, and reputational impact. It also means having timely and accurate data to support assessments and decisions.

Methodology

This Technology Adoption Profile was commissioned by Symantec. To create this profile, Forrester leveraged its Forrsights Security Survey, Q2 2011. Forrester Consulting supplemented this data with custom survey questions asked of 53 North American GRC decision-makers at enterprises with 5,000 or more employees. Survey questions related to current and desired prioritization of security efforts, the quality and frequency of GRC interactions with the business, and aspirations on how to improve IT and business interactions related to GRC. The auxiliary survey was conducted in January 2012. For more information on Forrester's data panel and Tech Industry Consulting services, visit www.forrester.com.

About Forrester Consulting

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit www.forrester.com/consulting.