February 14, 2012

Navigate The Future Of The Security Organization

by Stephanie Balaouras and Andrew Rose
for Security & Risk Professionals
February 14, 2012

Navigate The Future Of The Security Organization

by Stephanie Balaouras and Andrew Rose
with Laura Koetzle, Ed Ferrara, Eve Maler, and Nicholas Hayes

**EXECUTIVE SUMMARY**

This report outlines the future look of Forrester’s solution for security and risk (S&R) executives working on building a high-performance security program and organization. This report is designed to help you understand and navigate the major business and IT trends affecting the security organization during the next five years. Today’s chief information security officers (CISOs) continue to concentrate too much on tactical activities and day-to-day security operations, unable to escape the reactionary hamster wheel. Additionally, businesses and other parts of IT routinely circumvent today’s security organization in order to innovate and avoid hearing the predicted “no” response. So despite all the sensational headlines about major security breaches, many CISOs find themselves marginalized by their business colleagues. In this report, Forrester details what CISOs can do to realign with their businesses and transform themselves into chief business security officers, reasserting their position with management, the board, and the company as a whole.

**TABLE OF CONTENTS**

2 Despite The Hype, Security Has Declined In Priority For Business And IT Leaders
   - CISOs Have Not Focused Enough On Business Results And Innovation
   - CISOs Struggle To Create An Appealing Vision Of The Future
   - CISOs Are Not Breaking Through The IT Ceiling

5 Turn Yourself Into A Chief Business Security Officer
   - Build A Business-Centric Security Program And Organization
   - Strengthen Your Position By Expanding The Scope To Deliver Additional Value
   - Seek To Embed Security Into Architecture And Processes Across The Extended Enterprise

WHAT IT MEANS

9 Resist The Urge To Sell Fear, Uncertainty, And Doubt — Sell Value Instead

10 Supplemental Material

**NOTES & RESOURCES**

Forrester interviewed more than 16 vendor and user companies, including Cisco, CSC, Dell SecureWorks, Ernst & Young, HP, Juniper, KPMG, McAfee, Microsoft, Orange Business Services, RSA Security, SAP, and Verizon.

**Related Research Documents**

“The Extended Enterprise: A Security Journey”
November 9, 2011

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

“Build A Strategic Security Program And Organization”
May 10, 2010

“Define A Road Map To Accelerate The Organizational Maturity Of Your Security Program”
May 7, 2010
DESPITE THE HYPE, SECURITY HAS DECLINED IN PRIORITY FOR BUSINESS AND IT LEADERS

Despite all the sensational headlines about major security breaches, from RSA to Lockheed Martin to Sony and the continued avalanche of federal, state, and industry-specific regulations, upgrading security has actually declined as a critical priority from 2008 to 2011 among enterprise IT budget decision-makers and influencers (see Figure 1).1 It probably seems incomprehensible to most CISOs that security could decline in importance, especially when the board is dragging them in to present as many as four times per year. However, between 2008 and today, although the number of security threats and regulations increased, the grim global economic outlook forced many executives to focus their attention on IT initiatives that either cut costs (e.g., virtualization, consolidation) or drove growth and differentiation (e.g., analytics for better decision-making, mobile for employee productivity).

Figure 1 Upgrading Security Has Declined As A Critical Priority

“Which of the following initiatives are likely to be your IT organization’s top technology priorities over the next 12 months?”

(Respondents selecting “significantly upgrade our security environment” as a critical priority)

<table>
<thead>
<tr>
<th>Year</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008</td>
<td>20%</td>
</tr>
<tr>
<td>2011</td>
<td>16%</td>
</tr>
</tbody>
</table>

Base: Global enterprise IT budget decision-makers at companies with 100 or more employees

Source: Forrsights Budgets And Priorities Tracker Survey, Q2 2011; Enterprise And SMB IT Budgets And Spending Survey, North America, Europe, And Asia Pacific, Q4 2007

CISOs Have Not Focused Enough On Business Results And Innovation

It’s pathetically clichéd but still true: The business continues to view the security organization as a policy cop and paranoid custodian that is a barrier to progress and innovation. We spoke to one expert from a consultancy who routinely hears board members from some of his largest clients express frustration with the information security (IS) function. He noted, “Many top executives have had poor relationships with CISOs in the past, and that continues to shape their perceptions today. They see people in the IS profession as technologists, not equals. The No. 1 complaint from the board is that they are stuck dealing with very complex and technical people.”

In fact, business leaders at many firms — particularly in the financial services industry — have become so frustrated with their CISOs that they have created a new, separate position, often called a “VP of IT risk” or “business information security officer,” specifically to align with the business and to understand business requirements. This individual then brings these requirements to the CISO, who is now solely responsible for operational execution. Why is this CISO evisceration happening? Well, for the past several years, CISOs have not been able to:
• **Show how ongoing operational costs and investments support business activities.** Demonstrating return on security investment (ROSI) is a challenge that even top security teams struggle with. Thus, most CISOs are not even outlining how their day-to-day activities are adding value to the business or helping protect key corporate assets, such as reputation.

• **Manage or keep pace with business demand.** Organizations have recognized the importance of technology and have processes in place to speed its adoption. The business, and in some cases, other parts of IT, bypass the security organization; they only bring their security colleagues in at the end of the project and then ask them to “make it secure.”

• **Focus on business innovation.** Modern business relies on technology. Much of the productivity enjoyed by business throughout the past decade has been due to extensive automation. This rise in automation introduced new opportunities for data breaches. In 1990, a T1 line providing 1.544 MB per second was very fast. Now connections of 1 to 10 GB per second are routine. Hackers can compromise a lot of information very quickly. At the same time, business has been very innovative in the use of technology. Security organizations have not kept pace with these changes.

**CISOs Struggle To Create An Appealing Vision Of The Future**

The current threat landscape is bleak. Not a week goes by without news of another large enterprise or government agency leaking data or of hackers compromising valuable intellectual property. The CISO finds it almost impossible to create an appealing view of the future. The risks to the organization develop at breathtaking rates, making it difficult to keep up. In addition, the traditional controls that form the mainstay of the security function are becoming obsolete. These circumstances force the CISO to:

• **Explain why historical solutions are no longer effective.** The rapid development of new threats means that existing controls have become marginalized and ineffective. In a recent discussion with a global antivirus vendor, we learned that signature-based antivirus (AV) software accounts for less than half of malware detection on workstations, yet many organizations rely solely on AV software. Employees who fall for phishing attacks foil the firewalled perimeters we once relied on to stop known threats. Executives do not enjoy hearing how this arms race is leaving them increasingly vulnerable.

• **Constantly ask for more money to treat new risks.** Addressing these developing threats can require both significant investment and business disruption — and in the current uncertain economic climate, anyone approaching the board asking for additional resources is unlikely to be popular. The board often sees the processes and tools commonly required to protect information as awkward, uninviting, and prohibitively expensive, because the speed of threat development quickly undermines point solutions. At the same time, CISOs do not have the necessary metrics programs in place to measure the effectiveness of their controls and demonstrate the value of these investments.
• Regularly act as the bearer of bad news. When incidents occur and the security organization identifies new risks, the CISO has to deliver those messages. “When the IT security manager comes to my desk, I can often feel the chill in the air before I realize he is there, undoubtedly to bring bad news again,” said an IT operations manager at a global law firm. To exacerbate the problem, most CISOs don't publicize positive security-and-risk-related developments. Thus, senior executives end up with an unbalanced, unduly negative view of the CISO and of the organization's security posture.

CISOs Are Not Breaking Through The IT Ceiling

For many years, Forrester has talked about the importance of business engagement and the ultimate ambition of security leadership to break through the IT ceiling, to take a business-focused position, and to provide advice, guidance, and governance to business executives and initiatives. Unfortunately, many CISOs today remain far too technology-focused — they fail to balance the requirements of stopping information loss and security breaches with other business priorities. This is because many CISOs:

• Lack experience at the boardroom level. To get the attention of C-level executives and boards, CISOs must communicate in business terms. However, many CISOs are C-level executives in title only; a majority still report up through IT, typically to the CIO. Most CISOs don't have a strong track record of successfully presenting to C-level executives and the board of directors.

• Cannot command respect and influence across multiple business units. CISOs and other senior security managers most often rise through the security ranks. Since they have not worked in other parts of IT or in the business, they haven't developed the relationship- and influence-building skills and connections that come with moving around the organization. Their siloed expertise also makes it difficult to work with other IT departments, such as application development, enterprise architecture, and sourcing and vendor management. Executives in those departments feel that CISOs don't speak their language and don't understand their department's unique pressures and challenges.

• Need to develop stronger business and financial acumen. For a long time, the ability to understand deep technical threats was a key part of the CISO skill set. No longer. Communication, budget management, and business acumen are now more important than deep technical skills. Successful CISOs balance their business focus with the ability to work well with and learn from specialist technical staff as necessary.

• Are not able to acquire the talent they need. Many CISOs want to build more business-focused security organizations, but they find that their staff lacks the necessary skills to interact with the business. As one expert from a security vendor stated, “Some CISOs will make the leap, but they’re only as good as their teams.” Another security consultant noted that “the No.
1 thing is the availability of capable people. With our large global clients, their ability to move and transform quickly is inhibited by the expertise and skills of the team, especially the soft and personal skills.” Talking in business terms is not limited to the CISO; the entire security organization must understand the business priorities as well.

**TURN YOURSELF INTO A CHIEF BUSINESS SECURITY OFFICER**

If CISOs want to remain the most senior security and risk executives at their firms, they will need to rethink the roles and responsibilities of the security organization, its top priorities and initiatives, and the services and value it delivers to the business. They must also reexamine the individual skills that they build within the security organization and embrace a fundamental redesign of security architecture and processes. In fact, chief information security officers should view themselves as the chief business security officers (CBSOs) (see Figure 2).

<table>
<thead>
<tr>
<th>CISO</th>
<th>CBSO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mentality</strong></td>
<td>Operational execution, absolute security</td>
</tr>
<tr>
<td><strong>Reputation</strong></td>
<td>Technologist, purveyor of fear, uncertainty and doubt</td>
</tr>
<tr>
<td><strong>Approach</strong></td>
<td>Reactive, bolted-on security</td>
</tr>
<tr>
<td><strong>Focus</strong></td>
<td>Security technology and point products</td>
</tr>
<tr>
<td><strong>Value delivered</strong></td>
<td>Operations, technology selection, efficiency</td>
</tr>
<tr>
<td><strong>Next job</strong></td>
<td>CISO, VP of operations</td>
</tr>
</tbody>
</table>

*Figure 2 CISOs Must Transform Themselves Into CBSOs*

*Source: Forrester Research, Inc.*

**Build A Business-Centric Security Program And Organization**

CISOs must continue to develop business skills and consultative skills in addition to their technical foundations. This is critical to ensure that the business brings the CISO into any business or IT initiative early, rather than after the fact. It continues the evolution that security began years ago (but never quite finished), whose goal was to transform itself from policy cop to business enabler. The earlier that the business brings security into discussions about business and IT transformation, the more confidently the business can accelerate these initiatives without fear that it is ignoring security, regulatory, or privacy risks. To deliver on this promise, CISOs must:

- **Ensure traceable alignment between business and security objectives.** The ability to show the relationship between the activities of the security organization and the business’ goals and objectives is critical. Thus, a CISO should start with the chairman’s letter to shareholders in the firm’s annual report and show a direct, traceable alignment between those top business
initiatives, the CIO’s initiatives, and her own initiatives (see Figure 3). If one of your company’s top initiatives is international expansion, then enabling remote employee productivity and protecting intellectual property should feature among your top security initiatives. Furthermore, Forrester recommends that executive-level security metrics include metrics that measure strategic and functional alignment.6

• **Adopt more financial and risk management discipline.** With increased awareness comes increased scrutiny, and CISOs need to develop the ability to prove economic value or ROSI to the business. As one security consultant we interviewed put it, “CISOs need to place security in the context of risk: ‘How do I make sure this boat doesn't crash?’ is different from ‘How do I make sure this boat doesn’t even reach the ocean?’” This means both finally developing those metrics that do in fact matter to the business and taking a stab at demonstrating ROSI — no matter how imperfect. CISOs will still need to make tough decisions about budget allocation and prioritization. Beyond the essential security controls dictated by security standards such as PCI, CISOs will need to use risk management skills to identify the most probable, high-impact risks to priority initiatives over other initiatives.

• **Manage the security organization like a business within a business.** With maturity comes increased accountability. Project and program management is an important discipline to infuse into all security projects. Assert what benefits the project will provide and then track the project from inception through deployment to prove those claims. Even though security budgets are not growing rapidly, they still represent significant amounts of spend in most organizations.7 CISOs who demonstrate that they can manage budgets and deliver results will earn respect from fellow executives.

• **Use process improvement to do more with less.** Security is a people, process, and technology business. Forrester interviewed several successful CISOs who used process improvement to define better processes for core security activities like identity and access management, patch management, and employee screening. None of these required implementing any technology. In one case, the CISO and his team built policy-to-process models to show the relationship between the company’s security policies and its enabling processes.8

• **Devolve responsibilities for tactical security operations.** To finally escape the reactionary hamster wheel, CISOs must devolve tactical responsibilities to IT operations professionals who are closer to the line of business owners who own the data. This will free up time to focus on strategic initiatives (risk management, architecture redesign, etc.). In addition, IT vendors will embed more and more security functionality into their products — this is partly driven by requirements, and partly by the consolidation of security vendors (e.g., Intel’s acquisition of McAfee). And like their counterparts in IT operations, CISOs will look for opportunities to strategically rightsource security functions and processes to the cloud and other managed security service providers. There’s little sense in continuing to dedicate resources to commoditized but necessary security functions like email security.
• **Rebalance the skills within the security organization.** The size of and makeup of the security organization will change from a large organization to a leaner organization made up of internal consultants and architects that define strategy, architecture, and policy and outsource security operations to other IT operations or to cloud or managed security service providers. In addition, as the business extends itself, the security organization needs more business-savvy security architects who can understand how to secure and protect complex business processes that are a composite of both internal and externally hosted IT services and applications.

**Figure 3 Example Of Aligning Security With Business Initiatives**

<table>
<thead>
<tr>
<th>Business initiatives</th>
<th>CIO</th>
<th>CISO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Derive 30% of revenue from emerging markets.</td>
<td>Equip new employees with remote access and communication and collaboration technology.</td>
<td>Protect sensitive IP while supporting the growth in emerging markets.</td>
</tr>
<tr>
<td>Drive down costs by 5% year over year.</td>
<td>• Consolidate data centers and IT infrastructure with virtualization.</td>
<td>• Ensure that security is embedded in the industrialized data center.</td>
</tr>
<tr>
<td></td>
<td>• Outsource noncompetitive IT operations to the cloud.</td>
<td>• Work with vendor management to assess the security posture of cloud providers.</td>
</tr>
<tr>
<td>Improve customer retention by 5%.</td>
<td>• Improve the availability of customer-facing applications from 95% to 99%.</td>
<td>• Formalize collaboration with developers to code secure applications — including mobile applications.</td>
</tr>
<tr>
<td></td>
<td>• Rapidly deploy new consumer-facing mobile applications.</td>
<td></td>
</tr>
</tbody>
</table>

Strengthen Your Position By Expanding The Scope To Deliver Additional Value

The S&R role is pivotal to the organization, standing at the center of many crucial business processes. CISOs must recognize this and widen their spheres of control, taking opportunities to maximize the business value that the S&R function can offer. Traditional role expansions include business continuity, physical security, and, more recently, fraud management, all of which have seen clear transition to the security organization over the past three years. To expand their responsibilities and influence, CISOs can:

• **Give archiving and records management a new home.** The management and retention of corporate information is something that Forrester has included under the S&R role for some time. However, in many enterprises today, it is often a function that doesn’t have clear ownership; often, a cross-functional team of legal, the CIO, and VP of IT operations attempts to address it — usually poorly. Sadly, in some enterprises, archiving and records management is a subfunction of a backup and recovery. This is the worst possible situation because using backup as an archive creates enormous inefficiencies and risks. Given the increased legal and regulatory risk associated with eDiscovery and the overlap with data leak prevention (DLP) and information classification, this becomes a clear opportunity for a CISO to step up and add value.
Take an active role in enterprise content management. All organizations create and use information, and much of that information is unstructured. It includes documents and spreadsheets stored in a variety of places and presents significant risks in case of loss. The CISO can provide management oversight for this valuable resource and undertake to organize both structured and unstructured data for the organization. One CISO we interviewed who has done this spoke of the natural extension of his role to include the management of data across its entire life cycle. The initial CISO focus is clearly to secure corporate information. However, it is only a small step to consider access control not only as a barrier but as a collaborative space and, from there, to selectively identify, sanitize, and publish data that may have wider corporate value.

Seek To Embed Security Into Architecture And Processes Across The Extended Enterprise

CISOs must stop allowing their direct reports to present point products as silver bullet solutions to challenges like data leak protection. In a world where rapid technology innovation and disruption is the norm, IT must embed security in the design and architecture of systems and devices, rather than bolting security point products on later. “Embedded security” is imperative in a world where billions of IP-enabled devices and sensors connect to the Internet. CISOs must:

- Apply the Zero Trust Model to the extended enterprise. We’ve built strong perimeters, but well-organized cybercriminals have recruited and co-opted insiders and developed new attack methods that pierce our current security protections. To confront these new threats, security professionals must eliminate the soft chewy center by making security ubiquitous throughout the network, not just at the perimeter. To help security professionals do this effectively, Forrester developed a new model for information security, called Zero Trust. In the Zero Trust Model, security professionals eliminate the idea of a trusted internal network and an untrusted external network. In Zero Trust, all network traffic is untrusted. You must verify and secure all resources, limit and strictly enforce access control, and inspect and log all network traffic.

- Adopt a data-centric approach to security. In an extended enterprise where security doesn’t control the users or the devices, security must take a data-centric approach. By adopting a posture of Zero Trust and coupling that with good data protection strategies, security pros can go a long way toward mitigating the ever-changing threats to our data. More specifically, Forrester recommends that you: 1) Conduct a data discovery and classification project; 2) embrace encryption; 3) deploy network analysis and visibility tools to watch data flows and user behaviors; and 4) begin designing a Zero Trust network.

- Embrace security analytics. Security professionals need to have a better understanding of the threats at the edge of the network and awareness of the vulnerabilities in their environment and the breaches that have already occurred. Improved correlation technologies will emerge that will allow CISOs to benefit from the experience of hundreds of other companies that deal with the same issues. Used in conjunction with an intelligent outsourcing of commodity security functions, analytics and improved threat intelligence will give CISOs the necessary lead time to address new threats.
• **Invest in vulnerability management, incident management, and forensics.** According to our survey data, 25% of enterprises have experienced at least one serious security breach in the past 12 months. You will suffer a serious security breach — the only question is when. Security must do a better job of detecting, prioritizing, and addressing vulnerabilities in the environment, but when all else fails (and it will), the security organization must be prepared to respond appropriately to the breach. As one CISO for an enterprise technology manufacturing company put it, “Differentiation comes from your ability to respond.”

• **Treat identity and access management as services.** Employees are increasingly reaching out to use business software-as-a-service (SaaS), joint-venture partners are reaching in to your extranet, and all sorts of users are bringing their own devices to the mix. The days are long past when IT organizations could rely primarily on tightly coupling their authentication and access controls into Integrated Windows Authentication and Windows Active Directory. As one large civil engineering firm told us, “We can’t just ’Kerberize’ our apps anymore.”

To apply a data-centric approach to access control, you need to treat identity and entitlement information as items to be produced and consumed by security services in a loosely coupled fashion. This involves, for example: 1) accepting external identities through single sign-on (SSO) connections “in” where appropriate, instead of relying on brittle manual account synchronization; and 2) centralizing your authentication policy and applying risk-based authentication methods so that you can support strong authentication even “out” to cloud service access and “in” from unmanaged mobile devices.

---

**WHAT IT MEANS**

**RESIST THE URGE TO SELL FEAR, UNCERTAINTY, AND DOUBT — SELL VALUE INSTEAD**

Fear, uncertainty, and doubt (FUD) may work on executives once, but it won’t work a second time. In fact, it can often backfire. High-profile security breaches increase executive awareness; this translates into more scrutiny for you but not necessarily into actual investment. Executives make investment decisions when regulatory compliance compels them to do so or when it directly contributes to the bottom line. For a private enterprise, the bottom line is shareholder value, while for a government agency it’s citizen services, and for a hospital it’s patient care. CISOs must clearly demonstrate how they contribute to the bottom line, not how they stop every possible security threat to the organization. As one head of security for a hospital discussed his own team’s journey, he told us, “The No. 1 issue is patient care above all else, above security and privacy; it required a change in philosophy.”
SUPPLEMENTAL MATERIAL

Methodology

Forrester’s Forrsights Budgets And Priorities Tracker Survey, Q2 2011 was fielded to 2,741 IT executives and technology decision-makers located in Australia/New Zealand, Brazil, Canada, China/Hong Kong, France, Germany, India, Japan, Mexico, Russia, the UK, and the US from small and medium-size business (SMB) and enterprise companies with 100 or more employees. This survey is part of Forrester’s Forrsights for Business Technology and was fielded during April 2011 and May 2011. LinkedIn Research Network fielded this survey online on behalf of Forrester.

Each calendar year, Forrester’s Forrsights for Business Technology fields business-to-business technology studies in more than 17 countries spanning North America, Latin America, Europe, and developed and emerging Asia. For quality control, we carefully screen respondents according to job title and function. Forrester’s Forrsights for Business Technology ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of IT products. Additionally, we set quotas for company size (number of employees) and industry as a means of controlling the data distribution and establishing alignment with IT spend calculated by Forrester analysts. Forrsights uses only superior data sources and advanced data-cleaning techniques to ensure the highest data quality.

The purpose of Forrester’s Enterprise And SMB IT Budgets And Spending Survey, North America, Europe, And Asia Pacific, Q4 2007 was to analyze 2008 budget plans for enterprises in North America, Europe, and the Asia Pacific region, as well as SMBs in North America and Europe. The survey examines IT budgets as a whole, paying close attention to their makeup, structure, and growth rates. We have paid further attention to each subcategory of the typical IT budget, looking in depth at hardware, software, and services trends and spending. In addition, the survey examines IT business trends, the 2008 market outlook, R&D, consulting, financial analysis methodology, and choice of vendors.

Forrester surveyed 3,272 technology decision-makers at North American, European, and Asia Pacific companies. Of these, 812 were from North American enterprises, 306 were from European enterprises, and 705 were from Asia Pacific enterprises; 1,019 respondents were from North American SMBs (companies with six to 999 employees), and 430 were from European SMBs. Of all respondents, 16% were from companies with six to 99 employees, 18% were from companies with 100 to 499 employees, 10% were from companies with 500 to 999 employees, 27% were from companies with 1,000 to 4,999 employees, 16% were from companies with 5,000 to 19,999 employees, and the remaining 13% came from companies with 20,000 or more employees. All respondents were screened for significant involvement in IT decision-making, as well as IT purchasing processes and authorization.

Evalueserve fielded the telephone-based survey from September 2007 through December 2007 and motivated the respondents by offering them a summary of the results.
We have illustrated only a portion of survey results in this document. For access to the full data results, please contact Forrsights@forrester.com.

Companies Interviewed For This Document

Cisco  
CSC  
Dell SecureWorks  
Ernst & Young  
HP  
Juniper  
KPMG  

McAfee  
Microsoft  
Orange Business Services  
RSA Security  
SAP  
Verizon  

ENDNOTES

1 Source: Forrsights Budgets And Priorities Tracker Survey, Q2 2011 and Forrester’s Enterprise And SMB IT Budgets And Spending Survey, North America, Europe, And Asia Pacific, Q4 2007.


3 Even in the past year, we have seen a number of high-profile corporations get exposed due to hacks. This list of companies includes RSA, Lockheed Martin, L-3 Communications, Nintendo, Acer Europe, and Sony, just to name a few. For a more detailed list, see the November 1, 2011, "Updated Q4 2011: The New Threat Landscape — Proceed With Caution" report.

4 Forrester has identified three dominant organizational structures and four fundamental professional archetypes. Chief information security officers (CISOs) and senior security leaders seeking to deliver a highly effective service need to have the right skills, staff, and structure in place and understand the models that commonly deliver success. By crafting a tailored road map that builds on the unique strengths and weaknesses of the organization and staff, the CISO can drive organizational maturity. This can't be simply mandated to happen; to bring about lasting change, CISOs cannot act alone and need to delegate, influence, and collaborate with others to achieve their objectives. See the May 7, 2010, "Define A Road Map To Accelerate The Organizational Maturity Of Your Security Program" report.

Additionally, against the backdrop of today's increasingly complex and intimidating threat landscape and significant increases in the expectations of the business, the security organization has begun to realize its ambition to have a much more visible role in the organization. Years of austerity also mean that the business expects security will effectively combat the new threats while taking on additional responsibilities and keeping headcount virtually flat. As a result, there is often a disconnect between the business’ expectations and what a security organization can realistically deliver. Security organizations today must be agile and high-performing — capable of addressing a multitude of responsibilities and needs simultaneously. See the May 10, 2010, "Build A Strategic Security Program And Organization" report.
5 Security groups continue to struggle with achieving appropriate visibility at senior levels and with securing appropriate funding. To increase their visibility, they must run security as a business, with marketing being job one. This report lays out a four-step process that CISOs should follow to create and manage a marketing and communications plan that addresses all key constituents and includes multiple visibility-increasing activities. See the January 12, 2011, “How To Market Security To Gain Influence And Secure Budget” report.

6 The ability to communicate effectively has always been a core competency for any business executive, and today’s chief information security officer (CISO) is fast becoming a business executive. The CISO’s role is evolving and moving out of IT; its responsibilities and focus are shifting from IT risk to business risk. As with other business executives, the enterprise expects value creation from the CISO. We need a common language for the business and the security organization, and it needs to reflect a communication style that serves the business and the CISO. Program reporting is one important communication method, and formally reporting the value a program contributes to the organization is an important skill. This is especially true when reporting to executives. Adopting the metrics proposed in this report, as part of information security reporting, moves the CISO toward a common language for business. See the July 18, 2011, “Don’t Bore Your Executives — Speak To Them In A Language That They Understand” report.

7 The global downturn has negatively affected security budgets for several years now, and chief information security officers (CISOs) have become accustomed to accommodating increasing responsibilities with minimal change to resource levels. The year 2011, however, was a dramatic one for information security, and a catalog of high-profile breaches at major organizations cannot fail to have had some impact on the C-suite. This paper draws on Forrester’s analysis of large organizations to understand how 2012 looks from a CISO’s budget perspective and how the security team can keep it all together as the chill of austerity continues to grip industry. For more information, see the December 15, 2011, “2012 Budget And Planning Guide For CISOs” report.

8 Mapping policy-to-process models shows the relationship between the governing security policies and how the organization implements those policies. Most business processes will have some security elements, and these should be traceable back to company security policies. If they can’t then there is a gap in the security policy and process hierarchy.

9 “What’s the difference between a backup and an archive?” and “Do I need to have separate backups and archives?” are two common questions that Forrester receives from enterprise clients. Despite the fact that neither backup nor archiving are new concepts, there’s still a significant amount of confusion between the two. Although it’s been several years since we first produced this report, the best practices for establishing backup and archiving have not changed. What has evolved are the technologies that enable backup and archiving: Disk deduplication has become more prevalent, tapes have become much denser, adoption of cloud-based archiving approaches has accelerated, and new data classification and eDiscovery platforms make it easier to find the information needed in a timely manner. For more information, see the July 6, 2011, “Updated Q3 2011: Backup Versus Archiving: Firms Need Separate Strategies For Each” report.

10 Enterprises face major challenges in effectively managing information risk on a global basis. Navigating application shortcomings, addressing widely varying jurisdictional privacy and regulatory requirements, and confronting rapid adoption of social media, smartphones, and cloud computing complicate this journey. Compounding this effort, decision-makers in different geographies approach information risk
management from markedly different perspectives. This document outlines these challenges and provides best practices for successful global information risk management programs. See the December 1, 2011, “Grappling With Global Information Risk Management” report.

Successful businesses don't work in isolation. Today's businesses must constantly create new products and services, expand their geographic presence, streamline operations, and deliver top-notch customer services. To do this, your business will increasingly use third-party and cloud services to reduce cost and increase speed-to-market. Your business will unleash the creativity of your employees and customers with mobile, social, and rich media technologies. More and more devices come equipped with microprocessors, which mean cameras, cars, home electronics, and even musical instruments will all become conduits for businesses to deliver services and engage customers. To stay relevant, your enterprise must continuously extend itself to include new peripherals and meet new business scenarios. See the November 9, 2011, “The Extended Enterprise: A Security Journey” report.

There's an old saying in information security: "We want our network to be like an M&M, with a hard crunchy outside and a soft chewy center." For a generation of information security professionals, this was the motto we grew up with. It was a motto based on trust and the assumption that malicious individuals wouldn't get past the "hard crunchy outside." In today's new threat landscape, this is no longer an effective way of enforcing security. Once an attacker gets past the shell, he has access to all the resources in our network. We've built strong perimeters, but well-organized cybercriminals have recruited insiders and developed new attack methods that easily pierce our current security protections. To confront these new threats, information security professionals must eliminate the soft chewy center by making security ubiquitous throughout the network, not just at the perimeter. To help security professionals do this effectively, Forrester has developed a new model for information security, called Zero Trust. See the September 14, 2010, “No More Chewy Centers: Introducing The Zero Trust Model Of Information Security” report.

You are part of an extended enterprise — a new extended ecosystem of customers, clouds, service providers, partners, supply chains, and empowered users. The business expects you, the security professional, to somehow magically secure this ever-expanding universe despite budget restrictions and compliance pressures. This new reality will force security professionals to realign strategies in new and more efficient ways and discard many legacy world views. This is particularly true of network security. We can no longer control the perimeter, control the number of users that must access the network, or lock down the devices that connect to the network. We must take a fundamentally new approach to network and device security — we must take a data-centric approach, so that no matter where the data is, security travels with it. See the August 5, 2011, “Applying Zero Trust To The Extended Enterprise” report.

In today's threat environment, the network perimeter has disappeared. Insiders are as insidious a threat as outsiders. In the past, the "trust but verify" model did not facilitate insight into internal and nontraditional threats. Forrester's new Zero Trust Model of information security demands that organizations know what types of activities take place on their internal network as well as their external network. To provide this type of deep insight into internal and external networks, Forrester has defined a new functional space called network analysis and visibility (NAV). NAV is comprised of a diverse tool set designed to provide situational awareness for networking and information security professionals. See the January 24, 2011, “Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility” report.
It's not a question of if — but when — your organization will experience a serious security breach. Cybercriminals are using more sophisticated and targeted attacks to steal everything from valuable intellectual property to the sensitive personal and financial information of your customers, partners, and employees. Their motivations run the gamut from financial to political to retaliatory. With enough time and money, they can breach the security defenses of even the largest enterprises. You can't stop every cyberattack. However, your key stakeholders, clients, and other observers do expect you to take reasonable measures to prevent breaches in the first place, and when that fails, to respond quickly and appropriately. A poorly contained breach and botched response have the potential to cost you millions in lost business and opportunity, ruin your reputation, and perhaps even drive you out of business. See the November 9, 2011, “Planning For Failure” report.

Fast-moving cloud and consumer identity trends are driving shifts in how IT professionals control user access and provide personalized service to networked applications. As IT professionals move to take advantage of new, lightweight ways to improve security, efficiency, and business agility through federated identity techniques, these changes will ripple out to more traditional B2B scenarios. Several standards enable federated identity. See the June 3, 2011, “The ‘Venn’ Of Federated Identity” report.
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, customer insight, consulting, events, and peer-to-peer executive programs. For more than 28 years, Forrester has been making IT, marketing, and technology industry leaders successful every day. For more information, visit www.forrester.com.