Six Steps To A Better Security Strategy

Strategic Plan: The S&R Practice Playbook

by Martin Whitworth

January 22, 2016

Why Read This Report

Creating and maintaining a security strategy is fundamental for CISO success. Unfortunately, many of today's strategies fail to connect with the business or create a compelling case for action, which undermines the CISO's support and credibility. In this report, we provide you with the six steps to create an effective security strategy linked with key business interests and success factors.

Key Takeaways

Without Clear Business Alignment, Your Company Will Not Prioritize Security

Security leaders have often struggled to gain the attention of top corporate decision-makers -- unless something goes wrong. If you can't explain how your security efforts help them achieve their objectives, there is no compelling reason for them to support you with budget, communication, or inclusion in projects.

A Truly Business-Savvy CISO Will Have A Truly Business-Savvy Strategy

Security leaders need to demonstrate how their strategy supports a business technology agenda that allows the organization to successfully compete and grow.

If You Can't Communicate Your Strategy Simply, You May As Well Not Bother

Your business colleagues need to be able to understand your strategy. If you cannot communicate it in a clear and concise manner, then all of your work will have been in vain.

Six Steps To A Better Security Strategy

Strategic Plan: The S&R Practice Playbook

by Martin Whitworth
with Christopher McClean, Claire O'Malley, and Peggy Dostie

January 22, 2016

Table Of Contents

Notes & Resources

Forrester interviewed numerous security and risk (S&R) leaders from global companies and supplemented this with reviews of multiple strategy documents and insight and experience from key S&R analysts.

Related Research Documents

CISOs Need To Add Customer Obsession To Their Job Description

Develop Your Information Security Management System

Security Leaders, Earn Your Seat At The Table

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

CISOs Without A Strategy Should Step Down

Rather than addressing business needs, most current security strategies — when they in fact exist — tend to be catalogs of individual work items that address already identified risks, threats, and vulnerabilities. While it's important to address these weaknesses, this approach explains why most security strategies are not compelling.

Without Business Alignment, There Is No Strategy

The current approach will only result in a security program that constantly reacts to external threats and internal demands. Most CISOs struggle because the very nature of such a reactive approach is self-defeating. Other business executives feel the same way, too, looking at their organization's security function with two common perceptions:

- **The security team just reacts to incidents.** If your business executives only ever see a plan of action that addresses security issues and only speak about security when there has been an issue, it can come as no surprise that they think of security as reactive and not strategic.
- **The security team is not relevant to the business.** If there is no documented link between the security strategy and the priorities of the organization, business leaders will never perceive security as contributing to their success. As a result, they will be unlikely to consider security in either their strategic planning or day-to-day decisions.

Follow These Six Steps To Build Your Security Strategy

Experts have lauded business-aligned security for many years, but they have offered little guidance on how to achieve this. Just as other technology leaders are shifting their attention to the business technology (BT) agenda to better support top-line objectives, security leaders should position themselves by anticipating and addressing business needs.[1]

This alignment isn't easy, but there are straightforward steps you can take immediately to start building a truly business-savvy security strategy.

Step No. 1: Become A Credible Stakeholder

As a security leader, your job is far more than just ensuing compliance; you have to be an expert, a collaborator, a consultant, and a decision-maker. For business executives to take your security strategy seriously, they must first see you as a capable executive. This requires some work:

- **Understand your organization.** To be credible, you have to demonstrate that you understand what your organization does, makes, or sells, along with how it's doing financially. More importantly, you should get to know its customers and what they care about.

› **Know the personalities.** It's vitally important that you understand who the key stakeholders are in your company and what their responsibilities are; their specific goals and pet projects will drive security requirements.

Step No. 2: Connect With The Business

Now make use of your newfound status as a credible stakeholder and begin the process of business alignment. Taking any shortcuts here may prove disastrous down the road, as it's here that you determine and document the potential impact security will have on your environment (see Figure 1):

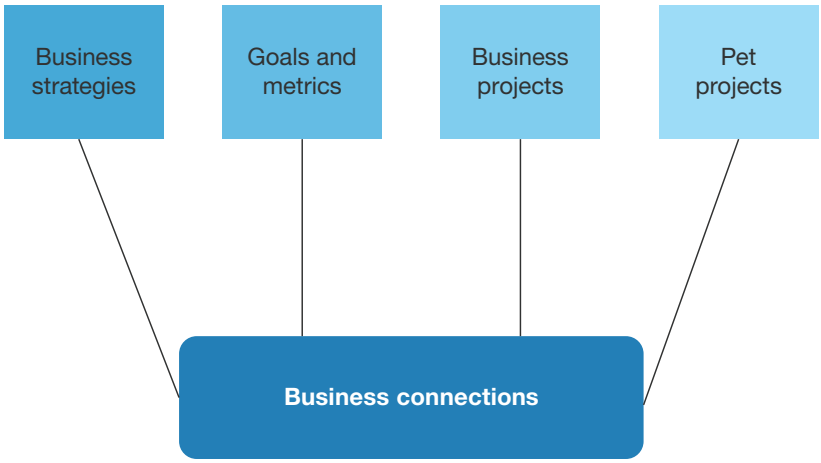
› **Understand current business strategies.** Become familiar with any existing business strategies, whether they be product strategies, information strategies, or IT strategies. You may use similar language or reference these documents in your strategy.

› **Get to know business projects.** All projects have some security implications. Get to know what business projects are planned or currently in progress so that you can identify the security requirements and any possible common themes between projects.

› **Pick up on pet projects.** Every organization will include some pet projects in its portfolio. These projects are particularly important to members of your executive management, and security efforts that support them are more likely to get visibility and support.

› **Align with goals and metrics.** It's essential that you understand the goals and metrics that the business uses to measure progress and evaluate success (or failure). Your security strategy must align its metrics with these. For example, if the business uses a KPI about customer satisfaction, how does the security strategy help to achieve this? Are there customer satisfaction questions related to the authentication process or logs of password resets you can use to demonstrate improvements?

FIGURE 1 Connecting With The Business

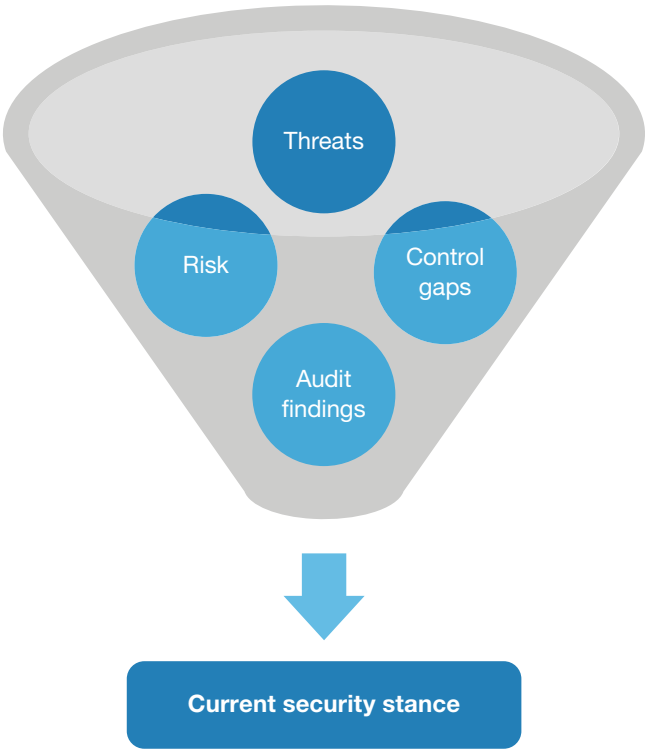


Step No. 3: Find The Gaps

This step is about getting a clear view on the security risks that threaten your organization (see Figure 2). Most security strategies don't go much further than this and just produce the aforementioned catalog of individual work items that address the risks, threats, and vulnerabilities. However, with steps 1 and 2 complete, the information you gather here will have business context and will be more valuable:

- **Record control gaps and vulnerabilities.** Use current audit findings, penetration and vulnerability test results, and control gap analysis to identify shortfalls in your current security environment. Prioritize systems and processes you know to be critical to your business.
- **Identify and quantify risks.** Document and prioritize security risks that threaten the business' strategic initiatives.[2] Quantify the different ways those risks might impact the business; even if you can't measure the potential financial costs, use a qualitative scale to prioritize the risks that could cause the most regulatory, operational, strategic, and reputational harm.[3]
- **Identify potential controls.** For each of the identified areas from above, identify potential security controls that could mitigate the underlying risks, and establish what the residual risk would be if your team implemented those controls.

FIGURE 2 Establishing Current Security Stance



Step No. 4: Identify Security Challenges

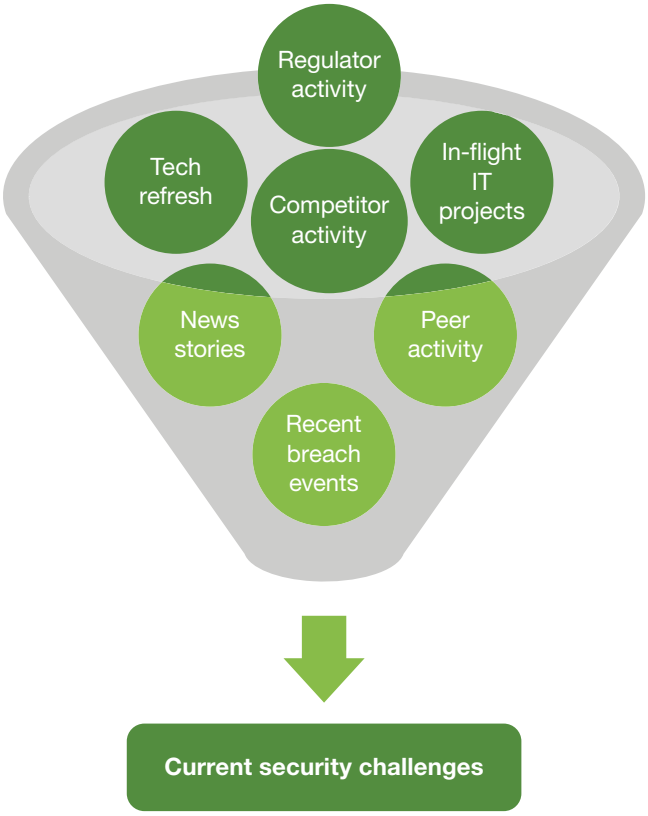
In addition to the threats, it's also useful to uncover security challenges that may need to be addressed within your environment. These will be potential risks and hurdles for your business that the security team can help mitigate (see Figure 3). Identifying them will require several different sources of input. You will need to:

- **Monitor regulatory activity.** Are there any regulatory or legal changes on the horizon? Do you know what the impact of these will be in your environment? Working with your legal counterparts or external legal services will help you avoid compliance surprises.
- **Track relevant news stories.** Stay abreast of news about your business, customers, partners, suppliers, and competitors — not just the security headlines. Make a point of reading the business pages, trade publications, and popular media, especially the publications that are read by your executives!

› **Watch the activity of your peers and competitors.** Are you aware of any development announcements or product launches that will inevitably have an impact on your business? If your company has to shift its strategy in response to the market, there could very well be security implications.

› **Anticipate new technology projects.** Connect with your technology management department to make sure you're aware of any current or planned projects and refreshes that may affect your organization.

FIGURE 3 Current Security Challenges



Step No. 5: Brainstorm New Opportunities

Work with your immediate team and other colleagues to identify additional opportunities to enable, accelerate, or add business value. This step gives you the prospect of creating a new security initiative, or implementing a new technology, that will both support and protect business interests. For example:

- **New technology offers new possibilities.** Do any of your proposed new technology controls open up the possibility to provide greater business value? For example, additional logging or behavioral monitoring may open up the possibility of more detailed customer analytics.
- **Hidden process improvements can appear.** Are you planning to introduce additional compliance checks that may allow process improvements across the business? For example, you can streamline your company's joiners/movers/leavers processes with the addition of Active Directory compliance checking.

Step No. 6: Bring It All Together

Having completed the previous actions, you now need to craft a comprehensive, logical, and clear document explaining your priorities. Knowing that some people will look at this document without the benefit of you being there to describe the details, make sure your decisions and thought processes are evident:

- **Generate the *big* list.** Collate the identified security tasks, removing duplicates, into one comprehensive list of security activities associated with known business plans — a potentially big list (see Figure 4)!
- **Create security initiatives.** Now, working with the big list of tasks and the identified business and IT projects, group your security tasks — by business initiative, customer offering, threat, technology, etc. — to create a number of security initiatives. Examples might include a new online customer experience program with authentication, verification, and logging controls or a vulnerability management initiative with vulnerability scanning, penetration testing, OWASP testing, and remediation.
- **Connect security initiatives to business interests.** Business interests, consisting of goals, projects, and proposals, represent the surface area to which you can link your security initiatives. The stronger and more direct those links are, the more compelling your business case for each initiative will be. It may require some creativity and brainstorming with your team to create these connections at first, but ultimately you should be able to connect most if not all security projects to a business interest and show this graphically (see Figure 5). To avoid any forcing of square pegs into round holes, start with a top-down approach connecting security initiatives to business programs, then roll up any leftover security initiatives into larger security programs with a bottom-up approach.

› **Agree on priorities.** It's essential that there be a shared view of the relative priorities of each of the security initiatives in your strategy. The only way to make this happen is to work with your business colleagues to achieve a common list. You must all understand and agree on business drivers, compliance requirements, interdependencies, and technology plans.

FIGURE 4 Creating A Big List Of Security Tasks

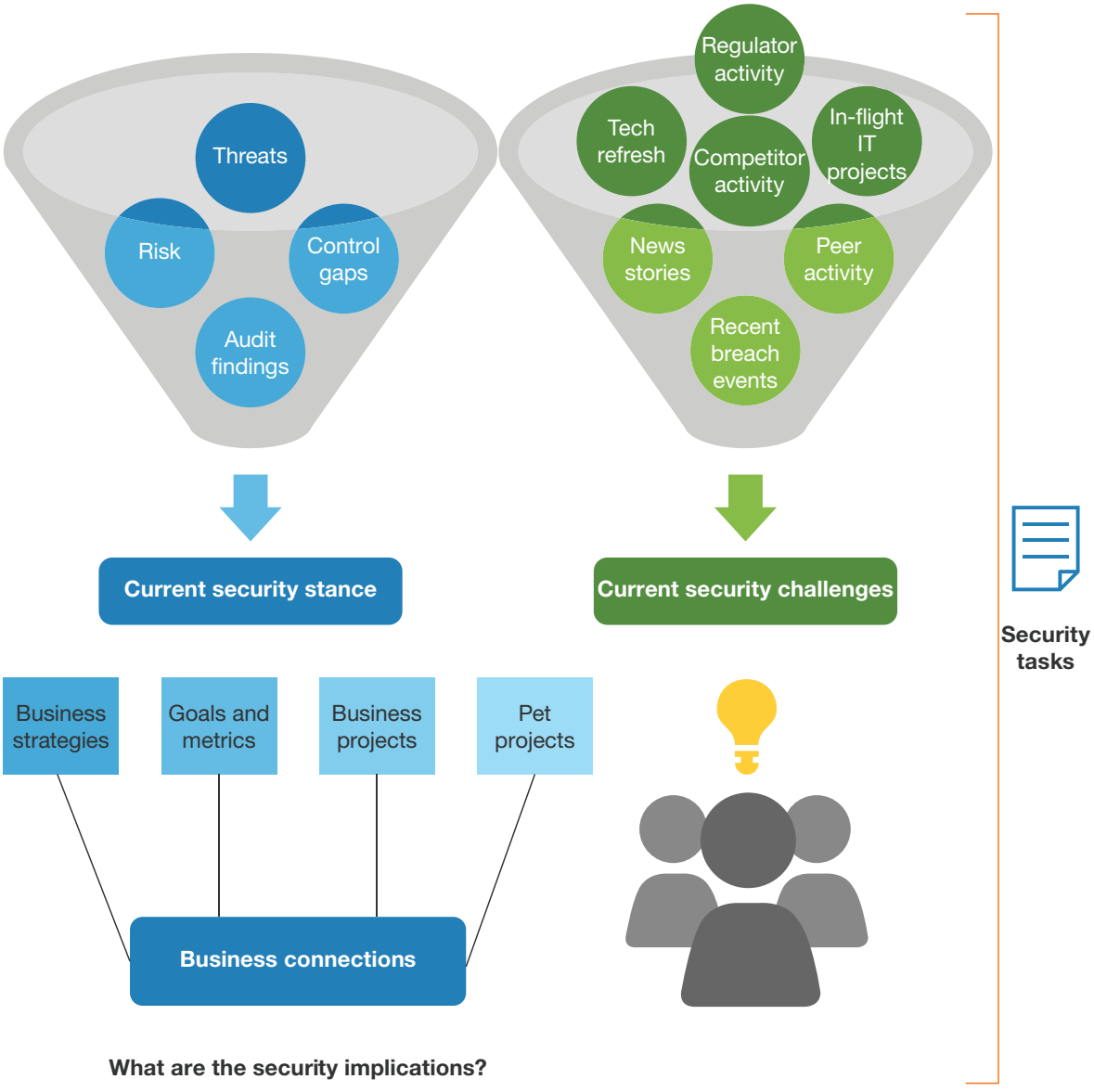
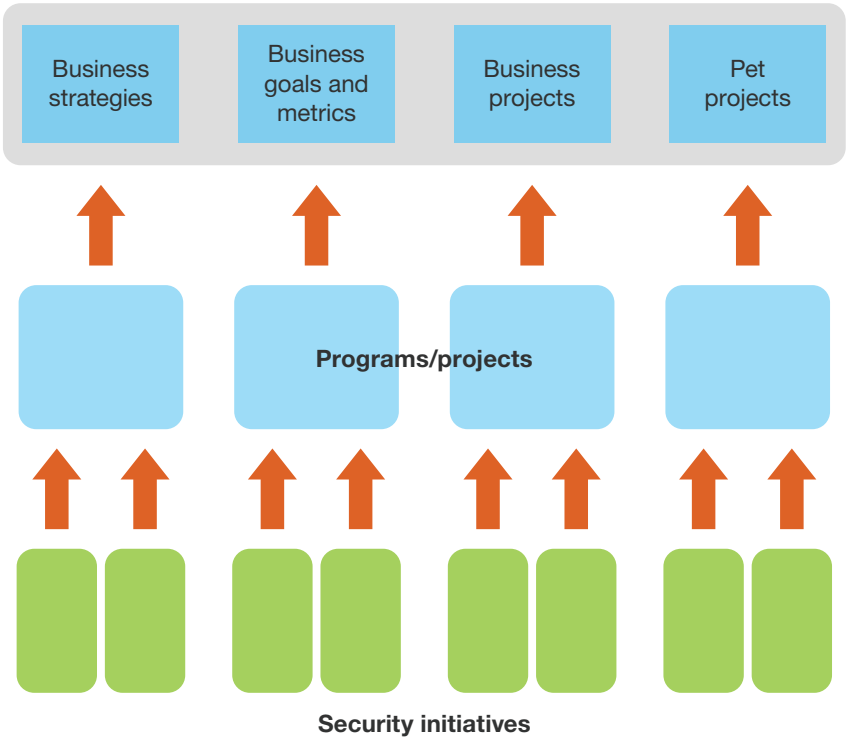


FIGURE 5 Showing Business Alignment



Communicate Your Strategy And Demonstrate Effectiveness

The next step is to describe your strategy in a way that will engage the business rather than scare them away. Remember that the aim is to prove that security contributes to the business and is not merely an insurance policy against bad things. There are two tactics that work well for this:

› **Accentuate business benefits rather than mitigated negatives.** Too frequently, security practitioners are known just for reducing risk, removing threats, and preventing breaches. While each of these is laudable, they can all have a negative tone and perpetuate the perception of security as an inhibitor. Simply reversing the language can have a remarkably positive effect on the outcome. For example, instead of reducing risk of DDoS disruption, improve retail platform resilience; instead of removing an eavesdropping threat, create a new secure communication channel; instead of preventing website incidents, enable efforts to improve customer loyalty.

› **Describe security initiatives in business terms.** When writing your strategic plan or project business case, use language that describes how it supports or enables the associated business interests. For example, the strategic description of a typical identity and access management project should not talk about segregation of duties and least privilege but should include statements like maximizing staff utilization and building customer trust.

Create Visibility With One-Page Summary Documents

It's vital that you can quickly and effectively communicate your security strategy to a variety of audiences. One of the most effective ways to achieve this is with a one-page statement of each security initiative and, if possible, a one-page summary of the entire security strategy. The format for such one-page security strategy documents will vary from organization to organization, but the fundamentals will be the same (see Figure 6).

FIGURE 6 Sample One-Page Strategy Content

Security vision: To ensure that _____ is viewed as a trusted partner in the _____ marketplace, by:
- Protecting the data we hold on behalf of our customers, our employees, and the business.
- Enabling the business to evolve into the digital world, per business vision statement.
- Providing a safe and secure working environment.

Regulatory/compliance objectives
- Clear L1 audit points.
- Become PCI DSS 3-compliant.
- Refresh privacy statement.
- Perform privacy impact assessment.

Business objectives
- Launch a new online customer account management facility.
- Allow purchases to be made online via credit/debit card.
- Provide an online employee access portal.

Technology objectives
- Refresh core OS.
- Implement patch management.
- Create new SAN infrastructure.
- Investigate cloud (IaaS, SaaS).
- Integrate IT/DR in overall resilience plans.

Assumptions
- Digital transformation received board approval.
- Requested budget was approved.

Initial security posture
- Level 2 — Forrester Information Security Manual Model
- No external systems access
- Security ops a component of IT ops
- No threat intel

Security initiatives
- PCI DSS CDE, tokenization, update policy framework
- External access customer access, employee portal access via 2FA
- Establish first and second lines.

Planned security posture
- Level 3 — Forrester Information Security Maturity Model
- 2FA (soft token) for external systems access (customer and employee)
- Establish SOC within IT ops (inc SIEM).
- Basic threat intel established (open source feeds and tools)

What It Means

Poor Security Strategy Is Career Limiting

Security leaders seeking to take on bigger leadership roles have to be business-savvy, refining their ability to create logical associations between security initiatives and actual business value or corporate aspirations.[4] In the age of the customer, this is achieved by delivering a truly business-savvy security strategy, not a lightweight attempt to fool business colleagues that they should read policies and invite security team members to occasional meetings. Creating a business-savvy security strategy is not optional. An effective security regime is essential for business success, and the CISO is responsible for making this happen. Rest assured, if you can't deliver this for your business, they'll find someone who can!

Endnotes

[1] The age of the customer is redefining how technology is used, which will transform how it's managed — how the CIO's organization is structured and operates, especially relative to customer experience. Digitally empowered customers demand more personalized and focused products and services, forcing firms they do business with to understand and respond to individual needs and expectations. To make this happen, CIOs have to adopt a dual agenda: business technology (BT) — the technology, systems, and processes to win, serve, and retain customers — and information technology (IT) — the technology, systems, and processes to support and transform an organization's internal operations. See the "Develop Broad Tech Management Capabilities To Accelerate Your BT Agenda" Forrester report.

[2] Enterprise risk management (ERM) programs are helping to break down organizational silos so that executives can gain insight on the risks that may affect all aspects of their business. Unfortunately, this trend is taking a toll on risk managers. It's becoming impossible for them to wield subject matter expertise across a growing number of risk domains, so instead they must be masters of procedural guidance. In the second core step of the risk management process, which the ISO 31000 standard labels "identify the risks," this means developing a comprehensive risk taxonomy, establishing a recurring set of risk assessment techniques, and guiding the documentation of risks in a way that will direct future decisions during the risk analysis and risk evaluation steps. For more information, see the "The Risk Manager's Handbook: How To Identify And Describe Risks" Forrester report.

[3] Successful risk managers need to overcome complaints by developing methodologies that support the needs and expectations of both those that will be contributing to and those that will be relying on the risk measurement information. In the third core step of the risk management process, which the ISO 31000 standard labels "risk analysis," you will consider relevant data points and inputs to determine the magnitude of risks. The output of this stage will help determine whether and how to act in response. For more information, see the "The Risk Manager's Handbook: How To Measure And Understand Risks" Forrester report.

[4] The role of the CISO is shifting to one of a business manager who specializes in change management and process oversight. This trend is giving CISOs their long-desired opportunity to interact with the high-level business decision-makers; however, it's also driving a metamorphosis. CISOs will need to realign their priorities and build new skills if they want to remain in their jobs. There are dramatic changes occurring in the business world generally, and the information security function specifically, and it's critical that S&R pros understand what all this means for their career paths moving forward. For more information, see the "Evolve To Become The CISO Of 2018 Or Face Extinction" Forrester report.

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.