Leveraging Corporate Security for Business Growth and Improved Performance: The Transformative Effect of 9/11

CEOs are expecting more from their security functions and chief security officers (CSOs). The security function’s role in the post-9/11 era is now, more than ever, a business one. It is integral to business growth and to meeting critical business challenges. Moreover, enlightened business leaders recognize the value of the security function as fundamental to the business process. No longer an afterthought, security has become a core function, embedded in disciplines like finance, law, human resources, quality, supply chain, marketing, and operations.

The Security Function Transitions to Tomorrow’s Environment

Having evolved rapidly into a value-added function, security is, and will continue to be, a critical strategic player. Today, it’s not just about security, but, rather, business and security, with CSOs acting as partners across functions and business units at the early planning and budgeting stages to identify risk and optimize costs.

As new generations make their mark in the workplace, the traditional notion of a security professional continues to be challenged. Even with the many positive changes that have already taken place, senior management must ensure that security executives do not revert to “what was,” but continue to focus on “what is” (Table 1).

<table>
<thead>
<tr>
<th>What was</th>
<th>What is</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reactive</td>
<td>Pro-active</td>
</tr>
<tr>
<td>After-the-fact executor</td>
<td>A voice in strategy</td>
</tr>
<tr>
<td>Business preventer</td>
<td>Business enabler</td>
</tr>
<tr>
<td>Cost center</td>
<td>Value add</td>
</tr>
<tr>
<td>Skill set focused on security issues</td>
<td>Business acumen</td>
</tr>
<tr>
<td>Security jargon</td>
<td>Communicator/business language</td>
</tr>
<tr>
<td>Silos</td>
<td>Network builder</td>
</tr>
<tr>
<td>Security for security’s sake</td>
<td>Integrated with the business</td>
</tr>
<tr>
<td>Focused on operations, not people</td>
<td>Personnel developer/manager</td>
</tr>
<tr>
<td>People just like me</td>
<td>Diversity of thought and skills</td>
</tr>
</tbody>
</table>
Corporate Security: Meeting Business Challenges in 2012 and Beyond

For U.S. CEOs responding to The Conference Board CEO Challenge® 2012 survey, their biggest challenges reside outside the corporate walls. They cite Government Regulation and Global Political/Economic Risk as their top two challenges, followed by Innovation, Human Capital, and Cost Optimization—all of which are connected to the growth chain and link directly back to the security function.

With globalization comes increased scrutiny of the corporate operating environment, vast information flows, and the demand for transparency across new markets and geographies. As a result, to be effective and relevant, security leaders must continue to develop their business acumen and risk management skills.


From September to December 2011, CEOs were asked to rank order the top three challenges they anticipate their companies will face in the coming year. The 776 responses were weighted according to their portion of global GDP. Only two challenges ranked in the top five in all three regions: Global Political/Economic Risk and Innovation.

Innovation and Human Capital Top the Global Challenge List

Regional ranking differences reflect unique local business environments.

<table>
<thead>
<tr>
<th>Rank</th>
<th>Global n=776</th>
<th>United States n=248</th>
<th>Europe n=158</th>
<th>Asia n=259</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Innovation</td>
<td>1</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>Human capital</td>
<td>2</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>Global political/economic risk</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>Government regulation</td>
<td>4</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>Global expansion</td>
<td>5</td>
<td>10</td>
<td>T4</td>
</tr>
<tr>
<td>6</td>
<td>Cost optimization</td>
<td>6</td>
<td>5</td>
<td>T4</td>
</tr>
<tr>
<td>7</td>
<td>Customer relationships</td>
<td>7</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>8</td>
<td>Sustainability</td>
<td>8</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>Corporate brand and reputation</td>
<td>9</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>10</td>
<td>Investor relations</td>
<td>10</td>
<td>10</td>
<td>9</td>
</tr>
</tbody>
</table>

N=Number of overall responses. The response rate varies for each challenge. T=Tie.

Government Regulation

Government oversight and regulation is growing in all regions of the globe, placing new demands on leaders. The ability to influence policy anywhere in the world is becoming even more important.

The security function plays a key role in educating staff about the practical implications of complying with such legislation as the Foreign Corrupt Practices Act, the UK Bribery Act, and the UK Corporate Manslaughter and Corporate Homicide Act.¹

In this role, security is an effective partner with the legal, compliance, and risk management functions to identify risk and sensitize employees to the legal and cultural pitfalls of doing business in different cultures, especially in emerging markets.

On a macro level, the security function, if properly aligned with business goals and strategies, provides a critical perspective on influencing public and government policy and regulations that affect company employees and assets. This is especially true in developing markets, where large multinational corporations can have significant influence on the formulation of security-related issues, such as the enforcement of intellectual property rights.

Also, with the proliferation of global security standards from associations and industry groups (which your security function should be influencing), effective, proactive self-regulation can improve corporate reputation, mitigate risk, and level the competitive playing field in a given geography.

A multinational corporate consortium in hi-tech manufacturing contributed to the updating of an espionage statute in an Asia-Pacific country.

One financial services firm recognized the added value that security could play in influencing potential legislation and government regulation and includes its CSO as a standing member of its public affairs committee.

Global Political/Economic Risk

Every business, regardless of location or industry, deals with risk, ranging from big-picture strategic challenges to day-to-day financial, transactional, and operational risks. The security function plays a critical role in identifying and mitigating risks that are sometimes overlooked or undervalued.

With the expansion of risks in a post-9/11 world, a partnership between the security function and enterprise risk management (ERM) is essential. ERM’s responsibility for developing a holistic view of all significant risks facing an organization requires the security function’s full participation.

Enterprise Security Risk Management

While traditional ERM embraces a wide range of strategic and financial issues, these programs often neglect to look closely enough at asset protection, IT security, cyberterrorism, and crime. An emerging concept, enterprise security risk management (ESRM) addresses precisely those sorts of risks and integrates with ERM. ESRM uses traditional ERM methodologies and practices to coordinate risk assessment and mitigation across the enterprise and includes the full range of security risks from asset protection to brand protection.

A Role in M&A

In visionary organizations with fully integrated security functions, security professionals (working with the legal and finance functions) are members of the business team, performing due diligence in advance of a global merger, acquisition, or divestiture. Security’s value is not just in conducting physical assessments, but now includes integrity checks, compliance, ethics, and reputation—all areas where security brings much to the table.

In one financial services company, security is actively advancing the ERM function, assessing over-the-horizon security risks relative to the Arab Spring and their implications for business performance.

A security function that embraces an organization’s business goals and strategies can play an important role in shaping policy and public regulations, thus maintaining a competitive edge and a fair playing field.

¹ Among other things, the Foreign Corrupt Practices Act (FCPA), a U.S. federal law, and the UK Bribery Act prohibit the bribing of foreign officials for business gain. The UK Manslaughter Act states that gross failures in the management of health and safety, causing death, will be liable to prosecution as corporate manslaughter.
**Innovation**

Security’s role in many organizations is being challenged by significant changes in technology, business innovation, and transformational workplace dynamics. While protecting and supporting a company’s innovation efforts is an important part of the security function, integrating security early into these processes will speed time to market and yield a competitive advantage.

A major business consulting firm, with challenges in attracting the best and brightest new talent has formed a cross-functional team, including security, to create safe and secure collaborative workspaces essential to innovative thought and synergy.

Security needs to be aligned with the innovation principles within a company and be involved early in R&D to create a competitive advantage.

**Human Capital**

If people truly are an organization’s greatest asset, the Human Capital challenge so highly rated by CEOs is an essential part of the CSO’s overall responsibility. If careless or malicious employee behaviors—from ignorance about foreign laws and cultures to outright criminal activity and ethics violations—are many corporations’ greatest potential weakness, then perhaps no other security contribution is as consequential. Today’s security is involved from “cradle to grave” in promoting quality employment practices and enhancing the employment experience. These contributions can be as varied as a pre-hire investigation to the evacuation of employees in a remote location affected by human or natural disaster.

Some examples of effective security operations that bring value to the business:

- Complementing HR hiring priorities with key ethical attributes.
- Inculcating security behaviors aimed at protecting the employee and company assets for which the employee is responsible.

**Cost Optimization**

As an integrated member of the executive team, the CSO understands and conveys the hidden risk transference accompanying otherwise seemingly cost-conscious decisions. On an individual basis, business-savvy security professionals understand budget dynamics, accept the reality of finite dollars, and develop sound strategies to bolster the business.

A decision by a business unit to cut transportation costs by going with a lower-tier company (that may not have the same established security procedures of a higher cost competitor) is problematic. The hidden costs may create a false economy and actually increase the risk profile of the company and its people—which has a potential negative impact on insurance and associated premiums.

By being innovative, identifying unnecessary risk, improving processes, and working across functions with an enterprise-wide perspective, the security function provides savings and optimizes costs.
Moving Forward: Understanding the Evolving Role of the CSO

Since 9/11, the security function in many organizations has become an integral part of the business process. To further develop the enhanced value of security, senior leaders must set expectations and provide critical support. Ultimately, it is up to the CSO to develop credibility within the organization to spur this progression. Today’s CSOs need to think of themselves as business leaders first, with specialization in security and risk mitigation.

For example, CSOs need to:

- Become enablers of business strategy, not just a function that seems to always say “no.”
- Continue to link security to other functions across the organization.
- Build relationships and networks across business units, geographies, and functions.
- Invest in succession planning that embraces these concepts.

Conclusion: Building a Security-Aware Culture

To help meet the major challenges identified by the The Conference Board CEO Challenge 2012 survey, security needs to be thought of as a core function, working seamlessly across the organization (Figure 2).

- It is up to an organization’s top leadership, including the CSO, to change any lingering perceptions that security is an imposition rather than an essential component of how you do business.
- Business units ultimately own the risk, with security as a critical partner, identifying those risks and developing ways to manage them. In organizations that are on the road to developing a security-conscious culture, security metrics and meeting security standards the security function developed are often a component of performance evaluations and compensation plans.
- In some organizations, executives still overlook the role that security can play in promoting business growth and improving performance. As a result, they are unsure about how to maximize the function’s contribution, and they may not know what type of qualifications and experience work best for a CSO in a world of expanding markets and more complex global risk. Clearly understanding security’s role in an organization and assembling a team with the right diversified skill set are important factors in building a truly high-performing organization.

Figure 2
The security function needs to be well integrated across the enterprise
About This Report

This report is based on discussion and presentations during a series of meetings in 2012 involving The Conference Board Council of Corporate Security Executives, The International Security Management Association, and the CSO Roundtable of ASIS International. The meetings were held under the Chatham House Rule by which participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s) may be revealed. Portions of the meetings were considered off the record and are not reflected in this report.

The following individuals from The International Security Management Association (ISMA), the CSO Roundtable of ASIS International, and the Council of Corporate Security Executives of The Conference Board participated in the preparation of this report:

- Brian Allen
- Chris Berg
- Michael Bouchard
- Brad Brekke
- Tom Catalano
- Kevin Donovan
- Mark Geraci
- Michael Gips
- Richard Gunthner
- Van Harp
- John Imhoff
- Mike Mason
- Jeff Meaney
- Charles Mitchell
- Robert Morrissey
- James Murphy
- Ray O’Hara
- Joe Petro
- Bill Phillips
- Peter Piazza
- Bob Pocica
- Bob Reilley
- Bill Schieder
- Pete Sullivan
- Tony Vermillion
- Tim Weir

The Council of Corporate Security Executives

The council provides an exclusive forum for chief security executives. Members engage in thoughtful peer exchange and best practices development on security management issues. Because of the confidential setting, the trust that develops is significant. Members include:

- Accenture LLP
- Bank of America
- Corning Incorporated
- Eli Lilly and Company
- Emerson
- Fidelity Investments
- Johnson & Johnson
- Kimberly-Clark Corporation
- McKesson Corporation
- Microsoft Corporation
- Monsanto
- New York Life Insurance Company
- Peabody Energy Corporation
- PepsiCo, Inc.
- Pfizer Inc
- QUALCOMM, Inc.
- Symantec Corporation
- Target Corporation
- The McGraw-Hill Companies
- The Walt Disney Company
- Waste Management Inc
- Western Union Company

Related Resources from The Conference Board

Publications

- Strategic Risk Management: A Primer for Directors
  Director Notes, Vol. 4, No. 15, July 2012
- No Company Is an Island: Building Resilient Communities
  Executive Action No. 384, June 2012
- Strengthening the Weakest Link: Building Resilient Supply Chains
  Executive Action No. 382, June 2012
  Conference Keynotes 58, December 2011
- Preparedness in the Private Sector--2011
  Research Report 1484, October 2011
- Achieving Resilience: A Systems Approach
  Executive Action No. 358, September 2011
- Achieving Resilience: Planning for Flexibility during Crisis
  Executive Action No. 361, September 2011
- Achieving Resilience: Establishing Networks--Before the Crisis Comes
  Executive Action No. 362, September 2011

Webcasts (On Demand)

- Emerging Markets: The Quest for Global Expansion
  June 14, 2012
- Economic, Political, and Regulatory Risk: External Challenges for CEOs
  May 23, 2012
- Build Stress Resilience--Grow the Business
  March 16, 2012
- Re-Thinking Risk: How to Proactively Approach Large External Risks
  March 6, 2012
- Market Presence Risk: Macro Issues and Your Risk Profile
  February 22, 2012
- Re-Thinking Risk: Turning Water into Opportunity
  January 10, 2012
- Growing Beyond Borders, Minimising Risks
  November 28, 2011
- How the UK Bribery Act Is Getting Companies to Re-Think Anti-Corruption
  June 30, 2011
- Human Capital Metrics to Manage Risk and Quantify ROI
  February 10, 2011
- Catastrophes and Human Failure: Assessing Risk, Building Plans and Preparing to Face Extreme Events
  September 16, 2010
Council Perspectives®

Members of The Conference Board Councils are among the most experienced and savvy executives in the world. Their private deliberations produce rich insights on the most challenging business and societal issues of our time. With their permission, we have channeled their energy and expertise into Council Perspectives, a new platform to voice their views.

Council Perspectives is based on sessions from selected council meetings, post-meeting interviews, and other pertinent data, and may sometimes include original content written by council members. It is not intended to be a research report; rather, Council Perspectives provide a unique look into the minds of executives from leading global organizations as they assess, analyze, and develop ways to address critical issues.

About The Conference Board Council Program

Membership in one of our councils affords entrée into a select and trusted community of 2,500 executives from a broad array of industries, functions, and regions — executives who know the value of this rich source of insights and new approaches. Enduring relationships are the cornerstone of the Councils experience. Enhanced by our global, enterprise-wide reach, these relationships span the world and extend value across your organization. Confidential peer dialogue combines broader perspective, specific knowledge, and shared experience to save you precious time and public missteps.

To learn more, contact:
Katie Plotkin, Councils Membership Manager,
+1 212 339 0449 or katie.plotkin@conferenceboard.org.

Council participation is by invitation only and is an exclusive benefit for The Conference Board member organizations.

To download this publication free of charge, visit www.conferenceboard.org

Public relations contact: Carol Courter, Manager, Corporate Communications, +1 212 339 0232, courter@conferenceboard.org

THE CONFERENCE BOARD, INC. www.conferenceboard.org

The Conference Board is a global, independent business membership and research association working in the public interest. Our mission is unique: to provide the world’s leading organizations with the practical knowledge they need to improve their performance and better serve society. The Conference Board is a non-advocacy, not-for-profit entity holding 501(c)(3) tax-exempt status in the United States of America.

For more information or to become a member of The Conference Board contact:

AMERICAS +1 212 759 0900 / customer.service@conferenceboard.org

ASIA-PACIFIC +65 6325 3121 / service.ap@conferenceboard.org

EUROPE/AFRICA/MIDDLE EAST +32 2 675 54 05 / brussels@conferenceboard.org

SOUTH ASIA +91 22 23051402 / admin.southasia@conferenceboard.org

THE CONFERENCE BOARD OF CANADA +1 613 526 3280 / www.conferenceboard.ca

Council Perspective CP-041 © 2012 by The Conference Board, Inc. All rights reserved. Printed in the U.S.A. The Conference Board® and the torch logo are registered trademarks of The Conference Board, Inc.