

booz&co.

First and Last
Line of Defense
*How Business Assurance
Makes Organizations
Resilient to Risk*



Contact Information

Beirut

Ramez Shehadi

Partner

+961-1-985-655

ramez.shehadi@booz.com

Frankfurt

Rainer Bernnat

Partner

+49-69-97167-414

rainer.bernnat@booz.com

London

Louise Fletcher

Partner

+44-20-7393-3530

louise.fletcher@booz.com

Rome

Fernando Napolitano

Partner

+39-06-69-20-73-1

fernando.napolitano@booz.com

Alessandro Gazzini

Principal

+39-06-69-20-73-1

alessandro.gazzini@booz.com

Stockholm

Per-Ola Karlsson

Partner

+46-8-50619049

per-ola.karlsson@booz.com

Sedar LaBarre, Stefano Buschi, and Alexandra Rutherford also contributed to this Perspective.

EXECUTIVE SUMMARY

Rapid advances in technology and the need to deliver goods and services more efficiently have made organizations more vulnerable than ever to systemic shocks and other potentially damaging incidents. In addition, the increasing interconnect- edness of people and businesses means that these events are no longer isolated; rather, they cascade through society, causing many indirect and at times unforeseen consequences.

The traditional security programs put in force by many com- panies and governments to meet these challenges are inefficient and inadequate. Organizations tend to take a fragmented and isolated approach to protecting physical and information resources. Because of this, they are hampered by a number of critical shortcomings: lack of an enterprise-wide view of risks, lack of accountability in dealing with those risks, and duplica- tive responses and investments.

Recognizing these shortcomings, organizations around the world are embracing integrated risk-management strate- gies. These combine the right blend of physical, information, and IT security controls to effectively manage access to vital information resources and ensure business continuity and increased resilience. A model that we call “business assurance” gives organizations the right tools and procedures to identify, manage, and absorb a range of unforeseen events, from minor incidents to full-blown disasters.

KEY HIGHLIGHTS

- The number and severity of systemic incidents are increasing around the globe, and their impact on business operations and society as a whole is more far-reaching than ever before.
- Improved processes and technologies that are helping businesses operate more effectively and efficiently are also making them more vulnerable to these incidents and amplifying their impact.
- The older, traditional security models are inefficient and ineffective because they are based on isolated measures that create organizational redundancy and fail to provide a coordinated front against today's cascading risks.
- Today's changing risk environment demands a "business assurance" approach that focuses on building functional capabilities to mitigate these risks, and incorporates a comprehensive governance framework that orchestrates the optimal use of these capabilities and engages multiple stakeholders.

CASCADING RISKS

In recent years, the number and severity of systemic shocks have been increasing worldwide—earthquakes and tsunamis, blackouts and technology failures, worldwide food shortages, pandemic diseases, and terrorist attacks are just a handful of examples plucked from the headlines (*see Exhibit 1*). For every one of these major events, there are scores of other potential incidents bubbling beneath the surface, threatening the operations or livelihoods of companies, governments, and individuals. Some experts attribute this rise to global connectivity, while others point to an increase in threats due to growing populations, poverty, wealth imbalances, technological complexity, and mass migrations to coasts and other exposed regions.

Regardless of the cause, it is evident that the world today is more vulnerable to the effects of these incidents due to growing digitization, societal interconnectedness, and lean operations. Because of these trends, events have a cascading impact throughout business operations and society. For instance, in 2005, Hurricane Katrina caused direct catastrophic damages to buildings, roads, and telecommunications networks, but indirectly the storm resulted in surging oil prices—due to extensive refinery damage—and paralysis among critical response teams, whose rescue efforts were

compromised by traffic light and telecommunication outages. The situation is further complicated by today's emerging "complexity risks," which cut across all traditional domains, such as the protection of critical infrastructures, cyber security, food and water security, and energy security.

Public- and private-sector mandates for greater efficiency, although critical to growth in productivity, add layers of risk. Operations optimization, process automation, and digitization have measurable benefits, but they also expose companies and governments to significant incremental vulnerabilities (*see Exhibit 2*). The recent surge in electronic identify theft, for example, has been possible only because we became more virtual—and productive—as a society.

Technologies that increase the effectiveness of organizations and drive societal interconnectedness are exposing us to new risks as well. Incidents are felt by more and more people, and cause an increasing amount of widespread damage. Experts estimate that a total of US\$1 billion has been stolen from financial institutions and corporations in the Middle East by organized cyber criminals employing online transactions.¹ In one such case in 2007, a Dubai-based gang stole roughly \$60 million by accessing consumers' online credit card information, even from Web sites that offer government services.² These details were then used by gang members to make cash withdrawals and to buy gold and diamonds online.

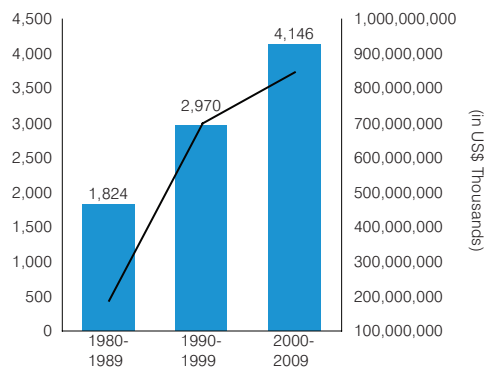
In addition, a rash of online security attacks on Rolls-Royce and Shell in the same year prompted the director general of the U.K. MI5, the National Intelligence Service, to warn all British companies of the threat of state-sponsored cyber espionage. Just as these challenges are highly interconnected, so too are the potential solutions. The answer is not to discourage interconnectedness or to undermine organizational

advancement in technology, but to develop a system that complements this approach, allowing for the adaptability and flexibility necessary to match today's high-risk environment. By the same token, no single organization, government agency, or country can resolve the problems effectively in isolation. The right solutions all call for the interaction of multiple stakeholders, including public-private partnerships

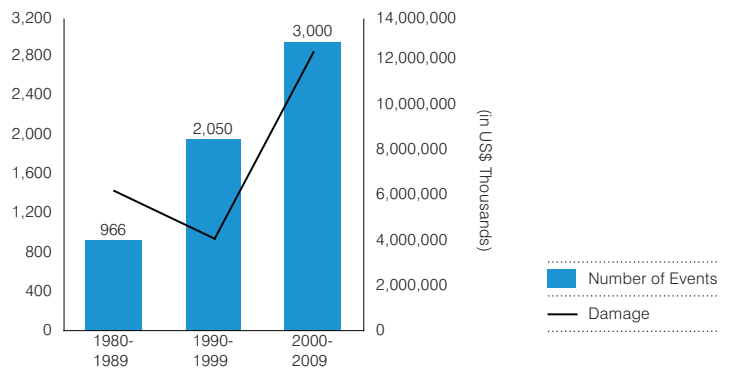
and international collaboration.³ For instance, the U.S. National Security Council recently conducted a review of its cyber-security policy and concluded that the United States “needs a comprehensive framework to ensure coordinated response and recovery by the government, the private sector, and our allies to a significant incident or threat.”⁴

Exhibit 1
Disasters Are Packing a Bigger Punch

NUMBER AND FINANCIAL IMPACT OF NATURAL DISASTERS

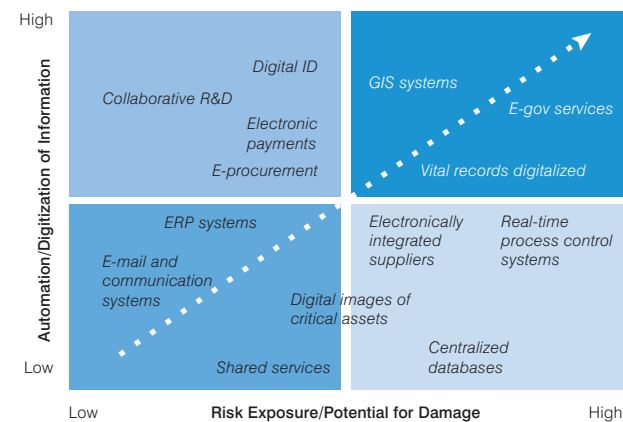


NUMBER AND FINANCIAL IMPACT OF TECHNOLOGICAL DISASTERS



Source: EM-DAT, the OFDA/CRED International Disaster Database

Exhibit 2
Digitization Brings Greater Risk



Source: Booz & Company

Estonia's E-Heist

Estonia's government functions depend largely on the Internet thanks to the country's push for a "paperless government" and its migration toward Web-based banking. For the past few years, it has been hailed as an exemplary "e-government," where citizens and businesses can log on to the Internet to pay taxes and vote in elections.

However, in 2007, Estonia was the target of a cyber attack that compromised international Internet access and many national services (media, e-government services, banks). The attack, the first of its kind on a national government, lasted for more than 20 days and resulted in millions of dollars of losses. It was perpetrated using a network of millions of compromised computers dispersed all over the globe, and presumably coordinated by a few individuals.

The attack was of a sophistication not seen before and demonstrated that the international legislation and laws regarding cyber security and cyber attacks are still immature. It became clear a new cooperative approach is necessary to effectively respond to and prevent these types of events. To help deal with these threats, NATO has created a Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, officially announced in May 2008, which started operations in the summer of 2008.

THE STATUS QUO IS INADEQUATE

Many governments and organizations have continued to build traditional security programs that are inadequate to cope with the new and emerging vulnerabilities of today. Although these programs may have been generally successful in advancing security, continuity, and crisis management capabilities, gains have been limited because they have fostered the development of "stovepipes." Stovepipes occur when functional capabilities are developed to address specific types of risks or vulnerabilities in isolation from each other—for example, the creation of an IT security policy that does not link with the organization's crisis management policy. Stovepipes are problematic because they prevent senior decision makers from obtaining an integrated and consistent view of risks across all domains, and they lead to unnecessary duplication of activities and potential investments

(see "*Shortcomings of the Stovepipe Approach*").

When organizations employ this traditional security approach, they often experience a decrease in efficiency and potency, critical gaps are created, and ultimately, an unacceptable level of risk is reached. One common tendency of companies is to spend so much time and attention on the establishment of extensive physical security controls to prevent the "bad guys" from entering company premises that they ignore critical proprietary information or assets made vulnerable by digitization. Compounding the problem is the fact that in many companies, security and IT directors are often perceived as "techies" and are not represented in board discussions. Their exclusion from strategy discussions hamstring an organization's ability to increase risk awareness and make informed decisions.

Companies and government agencies need an integrated risk management strategy that takes into account the right physical, information, and IT security controls required to effectively manage access to and use of key company information.

Shortcomings of the Stovepipe Approach

Companies that build their business assurance capabilities based on older models in which stovepipes existed tend to experience critical shortcomings across the enterprise. For starters, it is difficult to compare and prioritize exposures from many lists, and risk assessments are often neglected when risks are not consolidated. Boards and management have a limited view, which restricts their ability to act when conditions warrant. Accountability rests in the hands of many, resulting in no clear “go-to” person or function to ensure business continuity. This lack of coordination often leads to wasted efforts and confusion over how one function’s response fits with the company’s overall strategy.

Exhibit A
Typical Organizational “Stovepipes”



Source: Booz & Company

THE CASE FOR A NEW APPROACH

General risk management theory states that organizations cannot feasibly predict or sidestep every risk, or prevent every risk from maturing into a serious threat. At the same time, an organization needs to be able to mitigate and absorb the impact of any risk by establishing and continuously strengthening its ability to maintain operations in the event of an incident, even if operations cannot immediately function at full capacity. That is, an organization needs to develop a security and continuity system that enables it to become organizationally *resilient*.

Over the last several decades, globalization and other competitive pressures have forced organizations to focus on the efficiency of their business as much as their effectiveness

in delivering a better product or service for the same investment. The recent spate of major terrorist attacks and environmental disasters is now pressing them to examine how resilient their operations are to unforeseen shocks. After all, an organization can be ahead in the marketplace—and have mastered the managerial art of balancing the efficiency and effectiveness trade-off—but if something disrupts the organization's delivery of core products or services, it is no longer competitive. In the worst case, it may even no longer have a reason to exist if the trust of key stakeholders is irretrievably lost. In short, resilience has become imperative to survival.

Leading nations and organizations are beginning to understand the need to build resilient organizations in the face of this emerging and cascading risk environment. For instance, the British government has developed a nationwide network of resilience councils, coordinated by the Cabinet Office, to conduct a government-wide integrated risk

assessment called the National Risk Register, and to generally improve the country's resilience to all manner of risks.⁵ Singapore has taken a similar approach in devising its “Whole of Government—Integrated Risk Management” framework.⁶

The U.S. Postal Service (USPS) invested in a resilient system that was credited with blunting the impact of the 2001 anthrax attacks, which forced the agency to close its primary collection facility in the nation's capital. In order to make up for this lost capacity, the USPS rerouted its mail to two other local facilities, and maintained same-day service. Thanks to its extensive planning, the USPS was able to effectively continue its core mission of delivering mail to its customers.

These examples highlight the growing trend of governments and companies in adopting resilient solutions as a way to deal with today's emerging and interconnected risks. This is what we at Booz & Company refer to as *business assurance*.

Leading nations and organizations are beginning to understand the need to build resilient organizations in the face of this emerging and cascading risk environment.

THE BUSINESS ASSURANCE MODEL

The goal of the business assurance model is to ensure the appropriate protection and continuity of an organization's core services or mission. The concept is based primarily on the development and integration of *functional capabilities, enabling factors, and governance capabilities*. The assurance model's first focal point is establishing an organization's *functional capabilities*, which fall under four main categories:

- **Risk Analysis:** Identifies potential “pain points” by establishing an early-warning system for threats, vulnerabilities, and impacts to critical assets and processes. Extends traditional analysis of assets and functions to business processes across the organization.
- **Integrated Security:** Reduces the possibility of occurrence through the design and implementation of protective measures for people, assets, and information against threats. Takes segregated safety and security capabilities and integrates them across physical, IT-based, and personnel domains.
- **Continuity Planning:** Reduces the impact of events through the planning, design, and implementation of recovery targets and a continuity

strategy. Focuses on the portfolio of critical business processes and assets—facilities, infrastructure, IT systems, and personnel.

- **Incident Response:** Prepares an organization to manage all types of events by adopting an “all hazards” approach. Establishes key elements of an incident response framework, including an operations center and crisis communications protocols.

Developing these functional capabilities is essential to reaching the right balance across the security life cycle that is needed to achieve resilience.

The four functional capabilities of the business assurance model are supported by *enabling factors*—the people, infrastructure, and technology that can help an organization recover in the event of an incident. Examples of such factors include communications systems and crisis response centers to keep people in contact or operations groups that have received training to respond to specific circumstances.

Finally, companies must put in place the *governance capabilities* necessary to build and maintain an efficient system, such as the development of

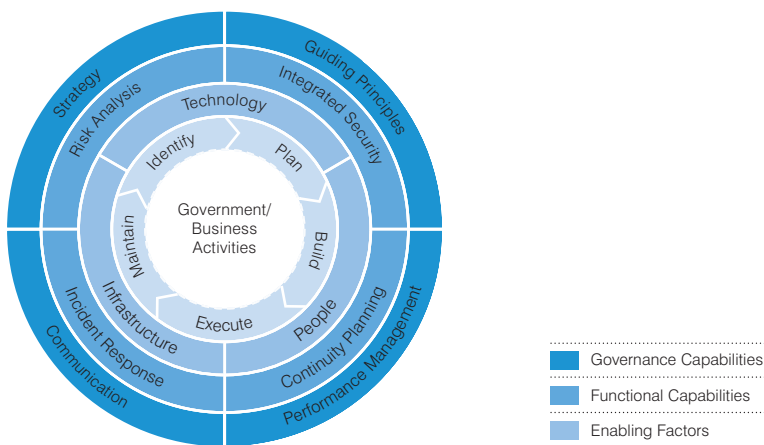
policies and standards that regulate the characteristics of a resilient system and the roles and responsibilities of all stakeholders. These strategies, policies, and performance management efforts mandate that the organization is consistently controlling and checking that the system is functioning.

The integration of functional capabilities, enabling factors, and governance capabilities is of paramount importance. They must work

together through an operational life cycle—identify, plan, build, execute, and maintain—to help form an ongoing resilience framework in which everything is working together to help deliver the organization’s core products or services (*see Exhibit 3*). It is through this life cycle that the business assurance model becomes an operational economy and one can see that all capabilities and factors—governance, functional, and enabling—have a role to play in every phase of the life cycle.

The integration of these capabilities and factors is typically driven by certain stimuli, both internal to the organization and external. These may include the need to identify security coordination shortfalls across similar security domains—physical, information, and personnel security—or the pressure to cut costs and group all security functions under one umbrella with one primary management resource. Whatever the impetus, the integration of these capabilities and factors results in a broad and shared

Exhibit 3
Booz & Company’s Business Assurance Model



Source: Booz & Company

awareness of risks, a reduced chance of overlap or duplication of activities, the optimization of investment and resource allocations, and a single risk and security snapshot for senior leaders across an organization, among other benefits.

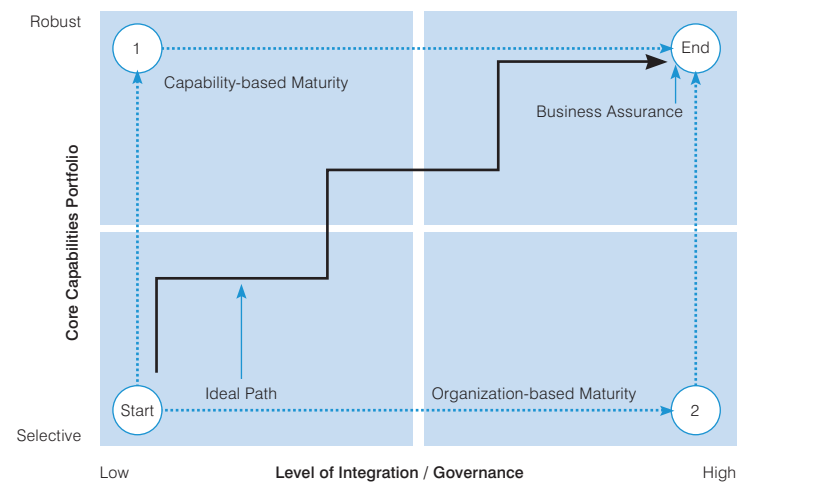
The challenge in creating a business assurance program resides in striking the right balance between facilitating integration and building capabilities. For instance, developing an integrated assurance organization without paying enough attention to

building the right assurance capabilities will yield an organization that is incapable of effectively responding to specific types of risks. Similarly, an organization that develops the functional capabilities but does not effectively address the management of these capabilities risks developing functional “stovepipes,” along with weak coordination and no clear accountability.

Some companies may choose to focus first on developing their capabilities—for instance, those

that have recently gone through a major organizational change and are reluctant to undertake another one right away. Others may choose to emphasize organizational structure first, such as those that have relatively mature capabilities that exist in stovepipes and need to be integrated. But to become truly resilient, companies will eventually have to address both domains, often addressing one, changing tack and focusing on the other, and then changing back (see Exhibit 4).

Exhibit 4
Achieving the Right Path Is a Balancing Act



Source: Booz & Company

CASE STUDY: A EUROPEAN UTILITY COMPANY

In 2003, an unexpected array of cascading effects stemming from a single “ordinary” failure ultimately caused a widespread electricity blackout in Europe. The blackout affected about 60 million people and resulted in an estimated 10 million euros in direct damages. One of Europe’s largest utility companies was significantly affected, with power transmission interrupted in some areas for more than 20 hours.

The blackout highlighted that good incident response and emergency technical procedures, if not completely integrated into a broader risk management culture, are not sufficient for effectively managing large systemic shocks.

The utility company in question called on Booz & Company to conduct an overall review of its resilience framework. We found the company

to be well equipped with a structured set of procedures and capabilities that were focused on single-point solutions, particularly at a technical level. But it was missing the broad and effective integrated perspective that would allow top management to evaluate, prioritize, communicate, and manage multiple and large-scale events. Company executives also lacked a unified, shared vision of the key operational risks across the value chain, along with a clear idea of the critical assets that most needed to be protected.

Booz & Company identified and implemented several immediate fixes:

- Introduction of a revised process and organization for *crisis management with a standardized taxonomy* to ensure communication across business units and geographies

The company was missing the integrated perspective that would allow top management to evaluate, prioritize, communicate, and manage multiple and large-scale events.

- Definition of a *criticality matrix* to correctly define the severity of an event and the associated potential impacts, supported by the development of several key threshold indicators
- Development of a dedicated *decision support tool* to assist executives and decision makers in gathering and managing the necessary information during a crisis with 24/7 situational awareness, and to record and store event data useful for successive analysis and risk evaluations
- Launch of a *testing and training program* to correctly deploy the

new crisis management model and decision support tool

These actions allowed the company to establish a unique and integrated point of view on a wide variety of possible risks and assure a standardized management protocol based on an event life cycle (*see Exhibit 5*).

Booz & Company’s model has now been deployed in more than 15 countries and is accessible by all of the company’s employees. It has generated significant near-term results, including:

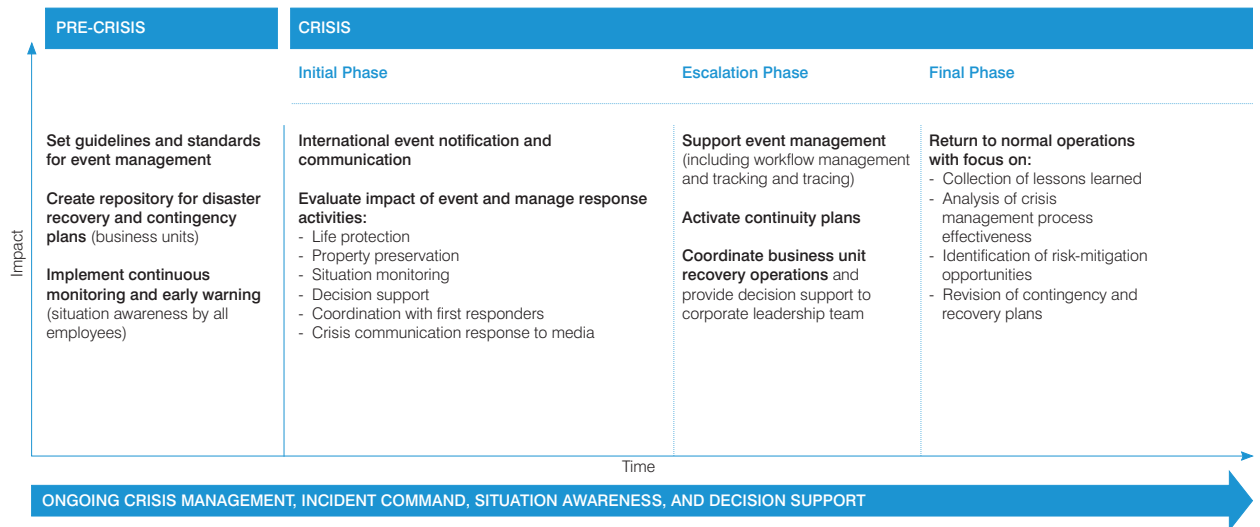
- Management’s anticipation of and attention to “minor” events before

they escalated to “major” status

- A centralized view on risks across the organization with updated information on and control of incidents across the different business units/countries
- Collaboration and communication in case of critical events
- An improved overall response capability with emphasis on establishing an active early-warning system
- Data-intensive post-event analysis that aided risk evaluations and the company’s investment decisions

Exhibit 5

The Business Assurance Model Encompasses Activities for All Stages Before and During a Crisis



Source: Booz & Company

CONCLUSION

At the end of the day, the objective of companies and governments is to deliver a service, but that objective is compromised when an organization is not capable of managing unforeseen incidents or threats to its business. In today's world, those threats are multiplying, and the interconnectedness of businesses and governments around the world means that each threat can do far greater damage than before.

These new and emerging risks are prompting executives and government leaders to take a fresh look at their ability to identify and mitigate them.

They realize that traditional security approaches, although beneficial on the whole, are not suited to dealing with these threats in an increasingly digitized world.

As a result, they are embracing organizational resilience by building the functional capabilities, enabling factors, and governance capabilities required to dramatically improve their ability to weather even the greatest systemic shocks. The business assurance model lets executives know that whatever may come, their organization will have an answer.

Endnotes

¹ Mohamed N. El-Guindy, "Cybercrime in the Middle East," *ISSA Journal*, June 2008.

² Antony Savvas, "Dubai police arrest four in £40m online credit card scam," *Computer Weekly*, December 16, 2008.

³ Ian Kearns and Ken Gude, "The New Front Line: Security in a Changing World," IPPR Working Paper No. 1, February 2008; World Economic Forum, "Global Risks 2009."

⁴ "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

⁵ Cabinet Office, "HMG Security Policy Framework V. 1.0," December 2008 (<http://www.cabinetoffice.gov.uk/media/111428/spf.pdf>) and "National Risk Register," 2008 (http://www.cabinetoffice.gov.uk/reports/national_risk_register.aspx).

⁶ "OECD Studies in Risk Management: Innovation in Country Risk Management," 2009: <http://www.oecd.org/dataoecd/33/18/42226946.pdf>.

About the Authors

Ramez Shehadi is a partner with Booz & Company in Beirut. He leads the information technology practice in the Middle East. He specializes in e-government, e-business, and IT-enabled transformation, helping corporations and government organizations maximize leverage of IT, achieve operational efficiencies, and improve governance of IT services.

Alessandro Gazzini is a principal with Booz & Company in Rome. He specializes in organizational strategy and design, operations design, and efficiency improvement as well as critical infrastructure protection, crisis management, civil protection, business continuity, information assurance, and risk management.

The most recent list of our office addresses and telephone numbers can be found on our website, www.booz.com

**Worldwide
Offices**

Asia

Beijing
Delhi
Hong Kong
Mumbai
Seoul
Shanghai
Taipei
Tokyo

**Australia,
New Zealand &
Southeast Asia**

Adelaide
Auckland
Bangkok
Brisbane
Canberra
Jakarta
Kuala Lumpur
Melbourne
Sydney

Europe

Amsterdam
Berlin
Copenhagen

Dublin
Düsseldorf
Frankfurt
Helsinki
London
Madrid
Milan
Moscow
Munich
Oslo
Paris
Rome
Stockholm
Stuttgart
Vienna
Warsaw
Zurich

Middle East

Abu Dhabi
Beirut
Cairo
Dubai
Riyadh

North America

Atlanta
Chicago
Cleveland
Dallas
Detroit
Florham Park
Houston
Los Angeles
McLean

Mexico City
New York City
Parsippany
San Francisco

South America

Buenos Aires
Rio de Janeiro
Santiago
São Paulo

Booz & Company is a leading global management consulting firm, helping the world's top businesses, governments, and organizations.

Our founder, Edwin Booz, defined the profession when he established the first management consulting firm in 1914.

Today, with more than 3,300 people in 59 offices around the world, we bring foresight and knowledge, deep functional expertise, and a practical approach to building capabilities and delivering real impact. We work closely with our clients to create and deliver essential advantage.

For our management magazine *strategy+business*, visit www.strategy-business.com.

Visit www.booz.com to learn more about Booz & Company.
