The Changing Faces of Cybersecurity Governance

CYBERSECURITY GOVERNANCE

Five Reasons Your Cybersecurity Governance Strategy May be Flawed and How to Fix It

Written By:

Peter Iannone,
Alsbridge Managing Director

Ayman Omar,
Associate Professor, Kogod School of Business,
American University

KOGOD
SCHOOL of BUSINESS
AMERICAN UNIVERSITY • WASHINGTON, DC

KOGOD CYBERSECURITY
GOVERNANCE CENTER

Previous publications in The Changing Faces of Cybersecurity Governance Series

March 2015

CYBERSECURITY ACT OF 2015 REVIEW: WHAT IT MEANS FOR CYBERSECURITY GOVERNANCE AND ENTERPRISE RISK MANAGEMENT

By Joseph J. Panetta & R. Andrew Schroth

September 2015

CYBERSECURITY REGULATION AND PRIVATE LITIGATION INVOLVING CORPORATIONS AND THEIR DIRECTORS AND OFFICERS: A LEGAL PERSPECTIVE

By Perry E. Wallace, Richard J. Schroth and William H. DeLone

EXECUTIVE SUMMARY

As threats to cyber security become increasingly ominous, sophisticated and unpredictable, CIOs must address risks ranging from denial of service attacks to natural disasters to disgruntled employees. Global organizations must also manage complex networks of service providers and scores of third-party suppliers, many of whom have access to customers, sensitive data and critical technology.

In this environment, many organizations struggle to maintain the continuous vigilance and end-to-end visibility across the entire service delivery chain that is essential to a viable cybersecurity strategy. In many cases, internal and external governance mechanisms that directly impact cybersecurity are neglected or ineffectively managed. The result is a significant increase in financial and operational risk for business enterprises.

This paper examines five key challenges of cybersecurity governance and how to more effectively address them. The areas discussed are:

- Defining risk posture
- Balancing global and local requirements
- Managing data
- Responding to change
- Applying relevant metrics

The paper incorporates industry research and input from several tier one service providers, including cybersecurity experts at Cognizant, IBM and Wipro.

DEFINING RISK POSTURE

Developing a cybersecurity governance strategy requires understanding and defining the enterprise's risk posture in the context of the overall environment. The global supply chain of a business organization today is characterized by myriad moving parts and multiple and constantly evolving potential threats. However, many cybersecurity governance strategies adhere to an obsolete "weakest link" strategy of identifying and mitigating specific, discrete risks. The reality is that organizations today confront potentially dozens of constantly changing weakest links, each of which can pose a significant threat.

Another common mistake is to treat all risks equally. Failure to prioritize different types or sources of risk can result in insufficient attention being paid to the most significant risks, or, conversely, can lead to overkill, where massive resources are funneled to manage negligible threats.

A reactive approach to risk is also problematic, as it can actually create additional effort and complexity, as well as additional vulnerability. Several recent major breaches were followed by reactive initiatives by the companies attacked. Such initiatives rarely lead to a better comprehensive strategy in defending against future attacks.

The key to gaining the necessary insight into today's dynamic landscape is to view the enterprise as a series of inter-connected concentric circles comprising data, networks, infrastructure and the user ecosystem. To complement this high-level perspective, many enterprises are applying NIST and COBIT standards to achieve granular insight into specific processes and potential vulnerabilities.

In addition, organizations must segment tolerance for different types of risk and focus on how and where to manage risk effectively as well as efficiently.

The same concept applies to outsourcing and third party management in the context of cyber governance. Specifically, a business must analyze every third party for its potential impact to the company if that third party is somehow compromised, either through an external threat or an internal vulnerability. Global enterprises typically have hundreds of suppliers, so segmentation of those suppliers based on the level of potential exposure or risk is essential. Applying the same level of oversight or risk control mechanisms to all relationships across the entire supply network is untenable and will drain unnecessary resources.

THINKING GLOBAL, ACTING LOCAL

Companies with extensive operations worldwide must apply a global perspective to cyber governance, while at the same time ensuring that risks at the local, regional level are not overlooked. For a global organization, regional considerations can make enforcing consistent standards a challenge, since operations in different geographies often use different carriers and suppliers, or different policies and redundancy systems.

Most businesses today are confused as to how best to achieve a global/regional balance, and are torn between, on the one hand, taking a centralized approach and, on the other, allowing each region to operate independently. While myriad models and approaches are deployed, some type of a centralized global steering committee that provides one view of business operations across the world is imperative. The goal should be to collect data and enable governance at a local level, while at the same time providing continuous input and analysis of security and compliance across the global system.

In recent years, in response to changing regulatory requirements in many industries, we've observed these centralized control structures evolve to be more agile and responsive to changes affecting local entities or individual business units. Top-performing organizations are recognizing that governance structures and policies can't be hard-wired. Concurrently, accountability for governance and cyber security is increasingly shared across business owners, reflecting a cultural shift towards shared responsibility.

MANAGING DATA

A global business manages data across a number of categories such as financials, employee records and intellectual property. These multiple categories of data – which have multiple levels of security and protection – are in turn shared across a wide spectrum of subscribers, ranging from senior management and individuals with the highest level of trust, to employees, partners, suppliers and contractors with access to less sensitive data, all the way down to any individual who can access data in the public domain.

Certain data has to be kept confidential and secured at the highest standards of integrity, so that it's not altered or changed inappropriately. At the same time, security processes should be designed to enable data access to appropriate parties. To achieve this balance, data categorization standards must apply appropriate levels of security and recognize that not all data requires secure protection.

Finding that balance is the challenge – businesses frequently apply too much security into a process, which creates additional operational complexity. For example, many enterprises are aggressively encrypting different types of data without a coherent approach to segmentation, which can have a negative impact on availability. In addition, the multiple security products in today's market can present integration challenges and require a wide range of skill sets to manage and maintain.

An effective governance strategy defines categories for data and provides insight and visibility into the flow of data across this spectrum, as well as the interfaces and touch points between the different players accessing different types of data. The governance model must identify and assess where data is in motion, as well as who accesses, evaluates or changes data.

The assessment of risk at any given point of interface within this data flow model applies rules and processes in a formula-based and repeatable manner to identify risks, authenticate users and enforce policies. The objective should be to create a data loss prevention culture characterized by training and awareness programs for the multiple levels of subscribers to a business' data. Policies that govern data management and security levels vary by industry – a healthcare insurer's customer data requires different policies than does a manufacturer's. Once sensitivity criteria and levels are defined, standards-based measures can be applied to provide appropriate levels of security to data traveling over the network, accessed from home computers or by a third party.

On a positive note, the data collection and analytic capabilities of Robotic Process Automation (RPA) applications are helping executives address challenges in areas like asset management and updating Configuration Management Databases (CMDBs), incident management and threat intelligence.

RESPONDING TO CHANGE

Change presents another inherent challenge to a global cybersecurity governance strategy. As business processes are constantly evolving, security standards, reporting mechanisms and metrics are changing as well. This means the governance model faces a constant threat of obsolescence.

In this environment, many organizations make the critical error of conducting security audits on an annual or regularly scheduled basis, rather than in response to changes in the organization's security posture. This check-box mentality can convince executives that "we're doing all the right things" and create a false sense of security, as well as lead to serious new risks being overlooked.

One way to address the challenge is through a "threshold map" of risk that establishes a mechanism that monitors and evaluates risk on an ongoing basis and enables continuous improvement. Tailored to different business units and operational towers, the threshold map defines specific criteria that, when met, require a reassessment of an organization's security posture.

Under the threshold model, in other words, any change that results in the risk threshold being crossed triggers a reassessment of the organization's security posture. Using this approach, an organization might require a security assessment on a monthly basis, or every two months, or every two years. By basing the assessment on changes in the risk environment rather than on an arbitrary schedule, this approach facilitates responsiveness to new threats and drives continuous improvement.

METRICS

Effective cyber governance is built on a foundation of relevant metrics that provide actionable data. In many cases, enterprises today lack the ability to measure what controls they have in place. As a result, they don't know if those controls are operating effectively.

Organizations often equate a third party's road map to a cybersecurity initiative with a security certification. Similarly, many companies who have engaged third parties for some type of cyber security initiative become complacent about their security posture and forego the steps needed for actual accreditation. Put bluntly, a plan for improvement or some ad hoc measures in no way equate to the rigors of an actual accreditation or security certification.

Another critical error is to rely on internal audits and questionnaires to assess security capabilities. The questionnaires are typically ad hoc and inconsistent, and the responses are rarely validated. In many cases, companies engage third parties to monitor devices and have no way to screen the people actually doing the monitoring. An effective metrics framework shows who is seeing the activity, who's signing into what system and build in alerts around that activity.

Effective governance metrics assess the ability to continue to conduct business when the organization's security posture is impacted – whether by a power outage, natural disaster, loss of equipment or malicious activity. This approach enables the business to make business case-based security investment decisions with an understanding of the potential return on that investment in terms of the continued ability to generate revenue in the event of a cyber threat, or in terms of the risk posed if the cyber threat prevents the ability to generate revenue.

Equally important are metrics that enable an ecosystem-wide view of risks, impacts and processes. The metrics dashboard must provide insight into the upstream and downstream risk implications of actions taken (or not taken) by individuals and business units, as well as changes to processes, technologies or third-party relationships. For example, a failure to adequately review the renewal of a multi-million dollar IT services contract can introduce risk into the service delivery chain, if the provider has brought in new sub-contractors that haven't been properly vetted. More specifically, something as seemingly innocuous as neglecting to upgrade an anti-malware program potentially creates a weakest link scenario.

To enable the necessary visibility into actions and consequences and cause/effect linkages, the metrics dashboard must collect information from disparate sources and locations, so that it feeds into a centralized repository. The challenge – and the key to success – is achieving the critical balance of local insight and global oversight.

TAKEAWAYS

Effective cybersecurity strategies incorporate advanced technology solutions as well as sophisticated governance mechanisms. Firewalls and identity detection technologies alone are insufficient.

Understanding, segmenting and prioritizing cybersecurity risks is essential to allocating resources where needed, and to improving the efficiency of data management and protection.

Dealing with third party providers and a global network of suppliers requires a comprehensive governance strategy to ensure visibility into the entire network.

Audits and certifications are important but not sufficient to protect against cybersecurity attacks. Reviews of risk postures must be undertaken in response to changes in the environment, rather than to an arbitrary schedule.

Ongoing communication with supply chain partners is critical to maintaining a defense system that adapts to rapid changes and threats in the environment.

To manage the cybersecurity governance ecosystem on an ongoing basis, comprehensive internal and external metrics are needed to identify potential new threats and to monitor data access.

ABOUT THE AUTHORS

PETER IANNONE,
MANAGING DIRECTOR, ALSBRIDGE INC.

Peter Iannone has over 20 years of experience assisting major corporations evaluate, implement and optimize IT and Business Process Outsourcing. He has negotiated major contracts for outsourcing transactions, with a combined total contract value exceeding $15 billion. Prior to joining Alsbridge, he held leadership positions in a number of advisory firms including KPMG, EquaTerra and TPI. His corporate experience includes serving as COO of JP Morgan's Global Technology Organization, where he was responsible for "running the business" of a $1 billion unit, including budgeting, capital projects, board presentations, etc.

AYMAN OMAR,
ASSOCIATE PROFESSOR OF INTERNATIONAL BUSINESS, KOGOD SCHOOL OF BUSINESS, AMERICAN UNIVERSITY

Ayman Omar is an Associate Professor of International Business at the Kogod School of Business at American University and a Research Associate at the Kogod Cybersecurity Governance Center. His research interests target different aspects of global supply chain management, with a primary focus on drivers and outcomes of global supply chain integration with an emphasis on supply chain relationships and responsiveness. Ayman's interests also include global supply chain sustainability and cybersecurity. He has worked for several years in the oil industry in Europe and Northern Africa and has consulted for numerous governments, multinational, public, and private corporations.

ADVISORY COMMITTEE

Ben Beeson,
Lockton

John Brady,
FINRA

Dr. Erran Carmel,
Dean

Steve Cooper,
US Department
of Commerce

Jim Dinegar,
Greater Washington
Board of Trade

Donna Dodson (liaison),
NIST

Tracie Grella,
AIG

Bruce Hoffmeister,
Marriott International

John Honeycutt,
Discovery
Communications

Gary LaBranche,
Association of Capital
Growth

Scott Laliberte,
Protiviti

Israel Martinez,
Axon Global Services

Jim Messina,
The Messina Group

Hitesh Sheth,
Vectra Networks

Stuart Tryon,
U.S. Secret Service

Dr. David Swartz,
American University

Ralph Szygenda,
Senior Fellow

Leif Ulstrup,
Executive in
Residence

David S. Wajsgras,
Raytheon

KCGC LEADERSHIP

Dr. William DeLone,
Executive Director

Dr. Richard Schroth,
Executive Director

Dr. Gwanhoo Lee,
Director of Center Operations

Dr. Parthiban David,
Faculty Research Director

THIS PUBLICATION IS SPONSORED BY

Discovery COMMUNICATIONS™

FINRA®

Marriott®

protiviti®

Raytheon

KOGOD SCHOOL *of* BUSINESS
AMERICAN UNIVERSITY • WASHINGTON, DC