Strategy Implementation Insights

Chapter 21

Cybersecurity: A Guide for CEOs and Government Agency Leaders

*This chapter of **Insights** is dedicated to two exasperated CEOs, members of the Connecticut Technology Council (CTC). They challenged us to make cybersecurity management real and actionable for CEOs. We are hopeful this **Insights** chapter will be a starting point. We all have much to learn and share about cybersecurity management, as it continues to evolve.*

Cybersecurity threats are real. They are adversely impacting our clients and the risks are likely to be increasingly dangerous for the foreseeable future.

Most disturbing is the rise in frequency and sophistication of attacks on government agencies, their contractors, and profit and non-profit enterprises. Recent examples in the news include hospitals, health insurers, Sony, and the Office of Personnel Management.

Today and Tomorrow….

Cybersecurity is now a CEO challenge and responsibility. CEOs need to understand the potential for damage and loss. This can involve confidential customer and patient information, intellectual property, reputations, careers and even lives.

CEOs need a strategy in place to manage the risks. They need to be accountable to all stakeholders for ensuring their enterprise has tested plans in place that anticipate and manage cybersecurity risks and events. Understanding the dynamic nature of this threat and keeping all stakeholders aware and involved is key.

Billions of dollars from corporate and venture capital programs are funding talented cybersecurity professionals within corporations and standalone firms. They are diligently designing new solutions to today's cybersecurity threats and anticipating future threats. Because of the ever-changing nature of cybersecurity threats, C-suite leaders will need to stay engaged for several years until practical solutions are in place.

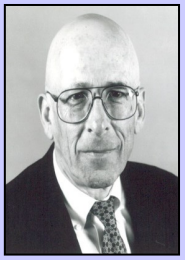
We urge every CEO and senior government leader take the following four steps:

Assign One Individual, An Existing C-Suite Leader, To Have Single Point Accountability and Authority for Understanding and Managing All Cybersecurity Threats and Events. This existing leader should be respected by the board, and be a time-tested, effective communicator with the authority to address shareholders, employees, customers, outside service providers, supply chain partners and the media. This leader will need to reprioritize their responsibilities and dedicate ample time to begin to understand the fast changing facts about cybersecurity and be capable of leading sustainable change.

Cybersecurity threats are beginning to impact every function from talent acquisition and product management to service delivery and legal, including understanding liability related to events. Cybersecurity management can no longer be a separate function. It needs to be fully integrated with other all C-Suite functions.

McCreight & Company
STRATEGY IMPLEMENTATION CONSULTANTS

Cathy Handford



Robert Bush

John McCreight

Special thanks to our Alliance Partners Robert Bush and Cathy Handford. They were critical contributors to this ***Strategy Implementation Insights*** chapter.

We publish ***Strategy Implementation Insights*** periodically to share our strategy implementation lessons learned and to encourage a dialog among senior leaders - including C-suite executives and their senior leadership teams, board members, and in government, agency leaders.

Our Focus... We are determined to be leaders and visionaries, anticipating and pragmatically addressing the needs of our clients.

Our Engagements...We partner with our clients' leaders, worldwide…to ensure their competitive superiority - identifying and addressing management issues and resources that energize or constrain strategic, large-scale change.

Our Alliance Partners...Our firm nurtures relationships with more than 150 partner-level professionals worldwide. Our Alliance Partners bring to engagements in-depth experiences dealing with difficult operational, governance, information and technology challenges.

Our Research & Operations Center Professionals... They focus daily on understanding our lessons learned and emerging best practices to ensure our firm's professionals are informed, competent, proactive and responsive.



Understand Specific Corporate and Government Agency Risk Profiles. CEOs need to understand the value of the data, information, and intellectual property their enterprise owns, where it resides, and the extent to which it is currently being protected. Cybersecurity is fundamentally about risk management. As the primary decision maker, CEOs and their C-suite colleagues must decide the level of risk their organization can tolerate losing data or compromising operations or the reliability of their products.

Product manufacturers need to be aware of the risks posed by other companies in their supply chain. Be certain suppliers have been fully vetted from a cybersecurity standpoint. Be prepared to replace under-protected suppliers.

Lead, Communicate and Educate. Commit to persistently educating every employee, customer, and stakeholder on the best ways to attempt to prevent and respond to cybersecurity events. Cybersecurity awareness training, starting with senior executives, is a must. To be effective, the commitment to managing cybersecurity must come from the top and be integrated into corporate culture.

Each CEO must understand the recommended cybersecurity controls for their industry, and be aware and contribute to, cybersecurity legislation that could impact their industry. Participation in industry groups aiming to educate their membership and engage in the national conversation about cybersecurity is a must for the accountable C-suite leader.

Have a Proactive Communications Plan for Major Incidents. Major incidents can impact an organization in minutes and persist for months. Plan to immediately communicate the right information, at the right level, to major stakeholders. Don't let the media frame the problem and potential solutions. Be prepared to lead the discussion. Be candid and honest as the facts about the incident develop.

CEOs must ensure every function, and all employees, know their role if a breach occurs. Devote some portion of every board meeting to sharing cybersecurity risk mitigation and communications plans - including the anticipated role of board members. Accountable members should share insights into the threats to the enterprise, and their plans to detect and recover from a cybersecurity event.

Partner with law enforcement professionals—before, during and following events.

A footnote: There is reliable data now that has convinced us:

- If you have not yet detected a cybersecurity threat - you likely will within 12 months.
- When cybersecurity adversaries are detected, they have most likely been embedded in your system for over 150 days before they are discovered.

About the Authors:
Robert Bush - Founder and President, Robert L. Bush & Associates, Inc. - rlbmcb@gmail.com
Cathy Handford - Managing Director, C Day Consulting, LLC - cathy.handford@cdayconsulting.com
John McCreight - Founder & Chairman, McCreight & Company, Inc. - jmc@implementstrategy.com

McCreight & Company
STRATEGY IMPLEMENTATION CONSULTANTS

Follow us on LinkedIn

For over 40 years, we have partnered with exemplary clients - implementing strategy involving the United States, Canada, Western Europe, Japan, India, the Middle East, and Southeast Asia. We are proud to have served the following clients. They typify over 100 active or inactive clients listed on our website (www.implementstrategy.com).

EDUCATION
Detroit Public Schools
New York City Public Schools
Stamford, Connecticut Public Schools
University of Pennsylvania, Wharton School of Business

ENERGY
KeySpan (acquired by National Grid)
UIL Holdings
United Illuminating

HEALTHCARE
Dianon Systems
Greenwich Emergency Medical Service
Henry Ford Hospital
Johnson & Johnson
US, National Institutes of Health (NIH)
Yale-New Haven Health System

INFORMATION
American Express
Applied Minds
Bank of America
Citigroup
Covisint
Credit Suisse
Deutsche Bank
eData.com
JP Morgan Chase
LexisNexis
Reed Elsevier
The New York Times
TheStreet.com
The Washington Times

LAW ENFORCEMENT & CRIMINAL JUSTICE
Boston Mayor's Office
Detroit Mayor's Office
Hawaii State Police
Indiana Governor's Office
Michigan Governor's Office
Montreal Police
New Haven Police
New York City Police
San Francisco Police

NATIONAL SECURITY
US Federal Agencies:
Central Intelligence Agency
Deputy Secretary of Defense
Federal Bureau of Investigation
National Geospatial - Intelligence Agency
National Security Agency
Office of the Director of National Intelligence
US Presidential Commission

PROFESSIONAL SERVICES
Capgemini
Elliott Management
ICF
Saatchi & Saatchi
Yankelovich
As Partner or Managing Director:
Hay Group (being acquired by Korn Ferry)
Hayes Hill (Aquired by Towers Perrin)
Touche Ross (Merged to create Deloitte Touche Tohmatsu)

TECHNOLOGY
Alcatel-Lucent
AT&T
Avaya
Bell Laboratories
Boeing
Chrysler
Ciena
Cisco
Corning
IBM
Kodak
Lenovo
United Technologies
Varian Semiconductor
Verizon
Xerox

10.15.15 1:30pm