The IBIT Report
A Publication of the Institute for Business and Information Technology

Tamara Schwartz
Lt. Colonel, US Air Force (retired)

David Schuff
Department of Management Information Systems
Fox School of Business

The Cyber-Based View of the Firm

A FRAMEWORK FOR SURVIVAL IN THE INFORMATION ECONOMY

Fox School of Business
TEMPLE UNIVERSITY®

The IBIT Report

Bruce Fadem
Editor-in-chief
Retired VP and CIO, Wyeth

Laurel Miller
Managing Editor
Director, Fox School of Business, Temple University

Munir Mandviwalla
Publisher
Executive Director, Fox School of Business, Temple University

Kent Seinfeld
Associate Editor
Retired CIO, Commerce Bank

BOARD OF EDITORS

Andrea Anania
Retired VP and CIO, CIGNA

Michael Bradshaw
EVP & CIO, NBCUniversal

Jonathan A. Brassington
Founding Partner and CEO, LiquidHub Inc.

Larry Dignan
Editor-in-Chief, ZDnet
SmartPlanet Editorial Director, TechRepublic

Niraj Patel
CIO, Lending Platforms, IBM

Wyndetryst Graphic Design Studio
Art Direction, Layout, Editing | wyndetryst.com

© 2018 Institute for Business and Information Technology, Fox School of Business, Temple University, Philadelphia, PA 19122, USA.
All rights reserved. ISSN 1938-1271.

The IBIT Report is a publication for the members of the Fox School's Institute for Business and Information Technology. IBIT reports are written for industry to provide actionable knowledge and are based on rigorous academic research and vendor neutral analysis. Each report focuses on an important cutting edge topic that is of interest to our members.

For additional reports, please visit our website at **http://ibit.temple.edu.**

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. General inquiries and requests to the Publisher for permission should be addressed to Institute for Business and Information Technology, Fox School of Business, Temple University, 210 Speakman Hall (006-00), 1810 N. 13th Street, Philadelphia, PA 19122, USA, 215-204-5642, or ibit@ temple.edu.

Disclaimer: The conclusions and statements of this report are solely the work of the authors. They do not represent the opinion of Temple University or the members of the Fox School's Institute for Business and Informational Technology (IBIT).

Review process: IBIT reports are sourced, reviewed, and produced as follows. The managing editor oversees this process. The editor and editor-in-chief consult on topics and identify new sources of reports. The editor typically works with authors who are interested in writing reports and provides feedback on initial drafts. Completed reports are first screened by the editor-in-chief. After approval the report is sent out for review to two members of the editorial board. The editor-in-chief assesses the completed reviews and provides further guidance to authors. Final reports are then professionally produced and made available to IBIT members.

Foreword

Cybersecurity refers to the set of technologies, processes, and practices designed to protect the integrity of networks, programs, and data from attack, damage, or unauthorized access.

Cybersecurity is on many business executives' minds today. But this IBIT Report postulates that cybersecurity is only a tactical response to the challenges that are confronting companies. What is really needed is an adaptive, strategic approach that recognizes the integration of the company with the interactive and virtual environment known as cyberspace. This "Cyber-Based View" of the company is the first step in developing a dynamic, adaptive cyber capability that will not only protect the company, but also generate revenue and grow competitive advantage.

This *IBIT Report* defines the cyber environment, explains why cybersecurity is insufficient, provides direction for constructing a cyber-based view for your company, and details specific recommendations to proceed. For anyone concerned with the potential impact of a cyber breach, this report is educational and thought provoking.

Bruce Fadem
Editor-in-Chief
March 2018

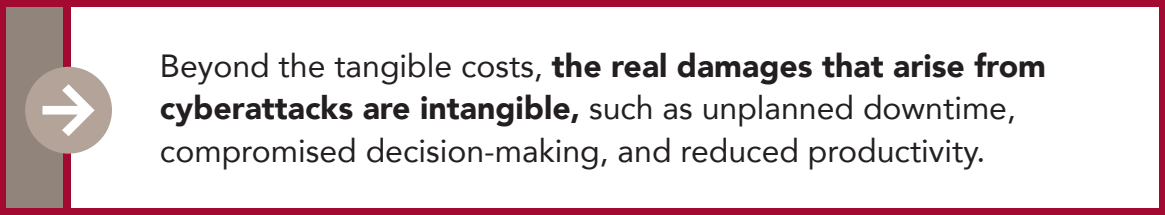
Introduction

There is no such thing as cybersecurity. Cyber is an inherently compromised and hostile environment, and cybersecurity is a tactical approach to a strategic challenge. Organizations cannot hope to compete in the information economy until they acknowledge this one simple fact and adapt accordingly.

According to a 2016 McKinsey report, globalization is entering "a new phase defined by soaring flows of data and information."[1] The GDP increase from global data flows is $2.8 trillion, with the potential for a 50% boost in GDP for some countries.[2] But these benefits can only be realized if a firm is equipped to adapt to a rapidly changing operational environment rife with threat. Beyond the tangible costs, the real damages that arise from cyberattacks are intangible, such as unplanned downtime, compromised decision-making, and reduced productivity.

Just as a company would not enter a new market without a clear understanding of its market position, a company cannot hope to compete in the most highly contested operational environment in the information economy without a clear understanding of its posture within that environment.

Currently, firms lack the necessary tools that provide a strategic view of themselves—a view that integrates the organization and cyberspace. **This report conceptualizes a comprehensive Cyber-Based View of the firm as the first step in developing a dynamic adaptive cyber capability.**



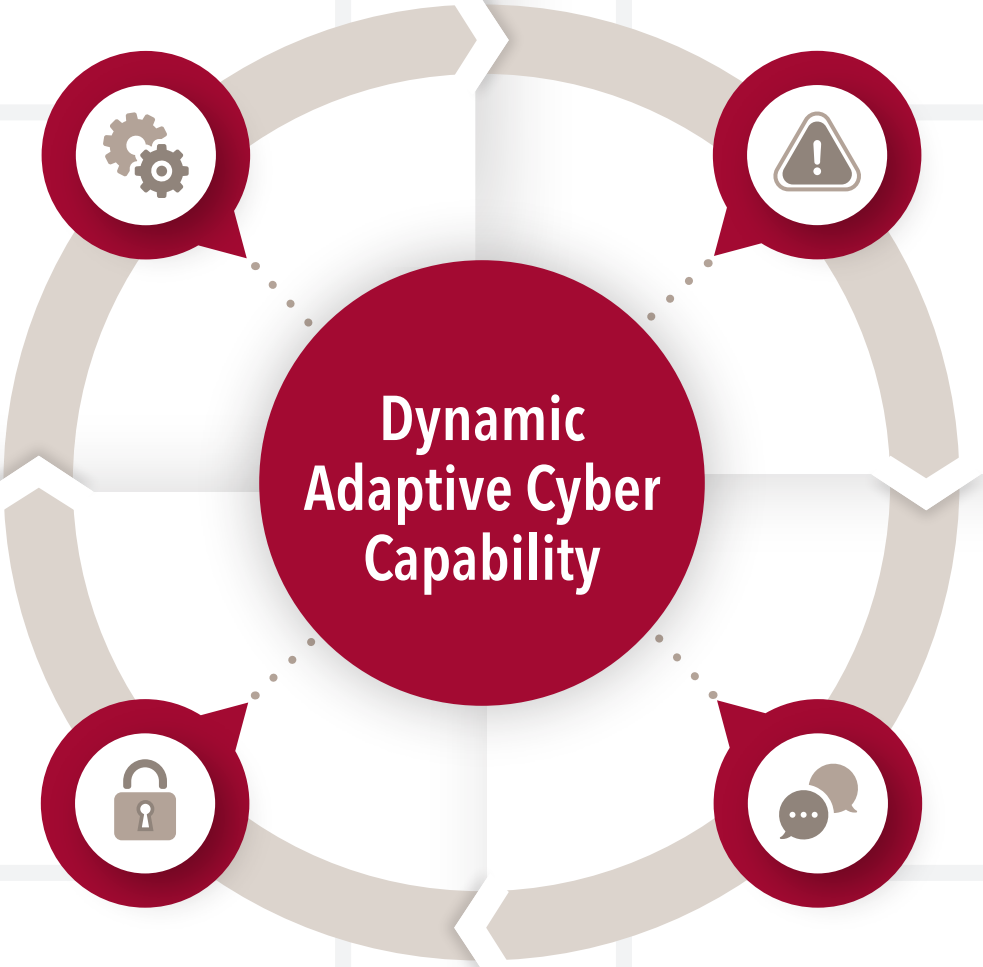
Operate & Compete

- Operations
- Manufacturing
- R&D
- Supply Chain
- Sales
- Product Development

Characterize Environment

Build CBV*

- Business Intelligence
- Threat Assessment
- Risk Assessment



Deter Rivals

- Cybersecurity
- Cyber Defense
- OPSEC
- Physical Security
- Strategic Communications

Shape Environment

- Automation
- Enhanced Decision Making
- Spectrum Occupation
- Strategic Communications
- Corporate Social Responsibility

**A key strategy that is the central topic of this report.*

Executive Summary

Despite the persistent growth of automation and digitization, there does not currently exist a strategic view of the firm that explores the integration of the organization and cyberspace. To be clear, the Cyber-Based View (CBV) is not cybersecurity. Cybersecurity is tactical. It is a computer science approach, using a one-to-many tactic to build hard boundaries. While there is movement toward Cyber Defense—an operational stratagem that takes into account softer boundaries and a many-to-many defensive posture, including the need to identify the "crown jewels" within our data—this, too, is insufficient. In order to engage rivals in the relentlessly fluid environment of rapid growth and metastasizing threat that is cyberspace, firms require an adaptive, strategic cyber capability that understands weaponized information.

Evolved from the integration of Information Security, Knowledge Management, and Social Engineering ideas, the CBV is intended to leverage existing firm resources for the purpose of building an adaptive cyber capability, of which cybersecurity is only a very small piece.

THE THREE DIMENSIONS OF CYBERSPACE

Cyberspace is comprised of three interdependent physical, informational, and cognitive dimensions. These dimensions continuously interact between systems, individuals, and organizations both within and beyond the firm.

1

Physical Dimension

Devices, wired and wireless networks, and sensors of both information technology and operational technology

2

Informational Dimension

Data, information, knowledge, and software

3

Cognitive Dimension

The human mind; employees, customers, rivals, and stakeholders

Technology is a strategic asset not only for the firm, but also for hackers who understand how to leverage a firm's own technology investments to facilitate theft, hijacking, and manipulation of a firm's data, knowledge, and core capabilities for profit. A lack of an adaptive cyber capability puts a firm at risk, but building a dynamic adaptive cyber capability can lead to significant reward outcomes, and can facilitate the growth of new capabilities and resources.

Operating in an Inherently Compromised Environment

Risk outcomes:

- **Decision manipulation,** such as the April 2013 hack of the Associated Press's Twitter feed, which led to a 143.5-point drop in the Dow Jones Industrial Average[3]
- **Financial loss**, such as the computer theft of $81 million from the New York Federal Reserve and the Central Bank of Bangladesh in February 2016[4]
- **Degradation and disruption of operations**, such as the June 2017 global Petya ransomware attack, which denied victims access to their knowledge assets and core capabilities[5]

Reward outcomes:

- Operational resilience
- Monetization of firm data to generate revenue
- Creation of new products and service

What is a Cyber-Based View?

The Cyber-Based View of the firm conceptualizes three interdependent dimensions of cyberspace – physical, informational, and cognitive (see Figure 1). Where these dimensions interact, within and beyond the firm, represent potential points of vulnerability within an organization's cyber infrastructure.

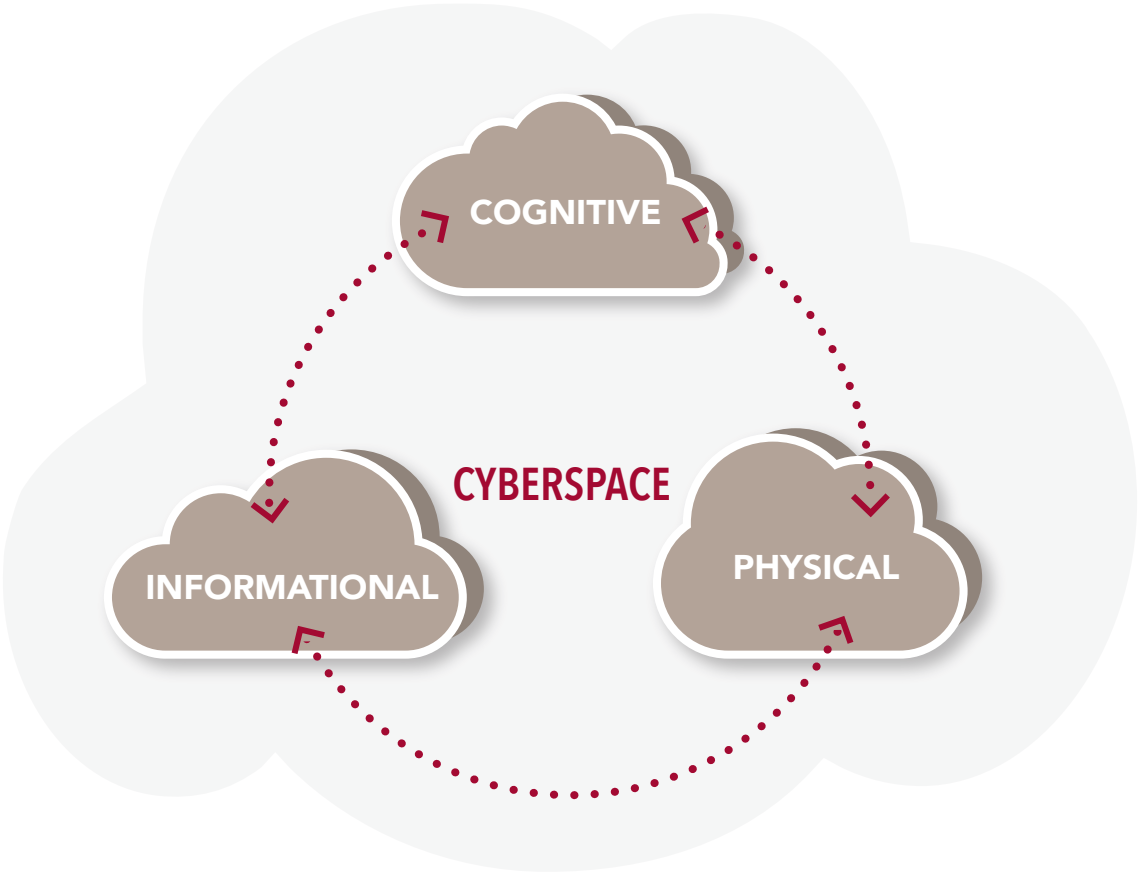


Figure 1: The Cyber-Based View

Impact of Cyber Attacks: Case Study

MAERSK, PETYA RANSOMWARE ATTACK

Damaging effects of the attack:

- **17 of 76 global ports not in operation for 6 days**
- **Loading and unloading of cargo stopped at multiple locations**
- **Booking operations closed down for 5 days**
- **In-transit visibility of cargo lost for over a week**

MAERSK

Impact of Cyber Attacks: Case Study

KIEV, URKRAINE POWER BLACKOUT

Troubling details and damaging effects of the attack:

- **225,000 customers impacted**
- **December 17-18, 2015**
- **330 kilowatt substation "North" influenced by external sources outside normal parameters**
- **Power distribution equipment sabotaged, complicating attempts to restore power**
- **Advanced Persistent Threat appeared to have been in network for 6 months prior to turning off power**

Why a Cyber-Based View?

In military doctrine, "key terrain" refers to territory that, when controlled, affords an advantage to the attacker or defender.[6] Rapid convergence of Information Technology (IT) and Operational Technology (OT) is increasing firm vulnerability by placing the majority of an organization's key terrain in cyberspace as if it were a permissive, unchallenged environment. Gone are the days of the "air gap," as evidenced by the 2010 Stuxnet attack on the Iranian nuclear facility.[7] Historically, IT and OT departments operate separately, with IT spending 7% to 9% of its budget on cybersecurity,[8] while OT has had zero expenditure because of the misperception of an absence of threat.[9]

A firm's interdependence with its technology has evolved to a greater degree than many realize, largely because there is no tool to build a strategic picture of the organization's key cyber terrain. Traditionally, automation is viewed with an operations perspective, while cybersecurity or cyber defense is viewed with a risk-mitigation approach, as if cyberthreat is a natural phenomenon such as weather damage to physical infrastructure. Adaptive cyber behavior integrates automation, defense, strategic communications, and enhanced decision-making with the full spectrum of a firm's operations, with the understanding that cyber threat is both opportunistic and strategic, not an unpredictable act of nature.

Lacking a CBV of the firm limits dynamic adaptation to mutable threats, digital revenue models, influencing campaigns, and evolving opportunities. Illuminating the complex relationships between a firm's humans, data, and devices, the CBV is the first step of a dynamic adaptive cyber capability. From a military perspective, the CBV is the map of the key terrain, but unlike geographic terrain, where this concept is clear, key terrain in cyber exists in all dimensions of cyberspace – physical, informational, and cognitive. Building the CBV may seem like an academic exercise, but it is not. In military-speak, building the CBV is comparable to the intelligence preparation of the operational space. No military commander would enter a highly contested operational environment without it, and no information-driven organization should either.

Why is "Cybersecurity" insufficient?

Locks are for honest people. If hackers want to gain access to an organization, they can. Momentary control of key tactical terrain will not guarantee achievement of operational or strategic objectives. Cybersecurity measures such as firewalls are the cyber attempt to build a physical boundary around key terrain. Antivirus software patrols the local area or wide area network the way security guards patrol office hallways to protect something physical.

But cyber knows no boundaries, and technology allows threats to masquerade as authorized personnel. There is a single, global network. We are all a part of it, and anyone with the knowledge and skills can gain access. Each new device or sensor added to a firm's network provides a new point of entry through the firm's boundaries—even something as seemingly inconsequential as sensors added to a fish tank.10 Cybersecurity technologies are a critical element of adaptive cyber strategy, but they are only a tiny piece of a much larger picture. In order to succeed, firms must first concede that they are operating in an insecure environment, not a fortress.

The Changing Face of Cyberattacks

From Nuisance Incidents to Information Warfare

STRATEGIC COMMUNICATIONS

Timeline of Convergence of Strategic Communications and Cyberattacks:

From Nuisance to Information Warfare

CYBER ATTACKS — 1998

The Morris worm, one of the first recognized worms to affect the global cyber infrastructure. It slowed down computers to the point of being unusable.

Source: http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm

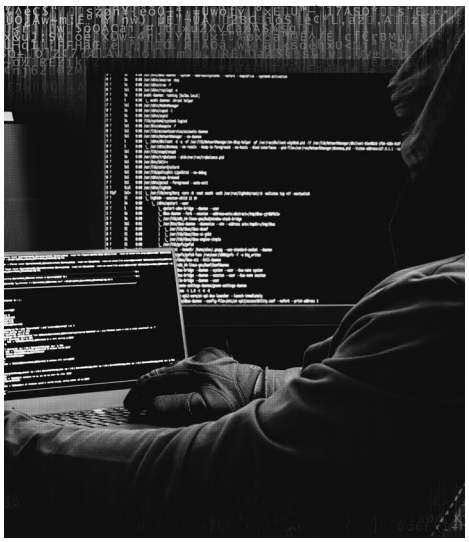
In the early days of the Internet, computer viruses and even denial-of-service attacks were considered a nuisance. However, the speed of technological change has both expanded the cyber domain within and enabled rapid mutation of cyberthreats from without (see Timeline below).

Hackers look for ways to disrupt operations or monetize a firm's data using data theft, manipulation, or hijacking tactics. As the Internet of Things continues to grow, and business becomes more and more digital, the firm's dependence on cyber for critical capabilities and knowledge assets increases. What was once a nuisance has progressed to no-holds-barred Information Operations, such as the 2015 hack of Sony Pictures[11] or the 2016 hack of the Democratic National Committee.[12]

2006

WikiLeaks created. Publishes stolen documents. Will become the location of choice for hackers to release stolen information.

2008



Russia launches a multi-faceted cyber attack against the Georgian infrastructure and key government websites.

Source: https://www.defensetech.org/2008/08/13/cyber-war-2-0-russia-v-georgia/

1999

Melissa virus began in AOL email, and distributed via Outlook email. Shut down desktop computers and LANs by overloading email servers.

2008

Insider threats gain attention. Private Manning releases stolen U.S. national security information on WikiLeaks.

STRATEGIC COMMUNICATIONS • 2010

Timeline of Convergence of Strategic Communications and Cyberattacks:

From Nuisance to Information Warfare

CYBER ATTACKS • 2010 • 2012

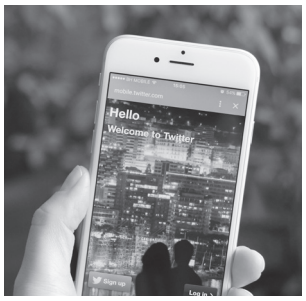
Stuxnet, a complex piece of malware designed to interfere with Siemens industrial control systems, was discovered in Iran, Indonesia, and elsewhere, leading to speculation that it was a government cyber weapon aimed at the Iranian nuclear program.

Source: http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm

The Russian firm Kaspersky discovered a worldwide **cyber-attack dubbed "Red October,"** operating since at least 2007. The virus collected information from embassies, research firms, military installations, and critical infrastructures.

Source: http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm

2013

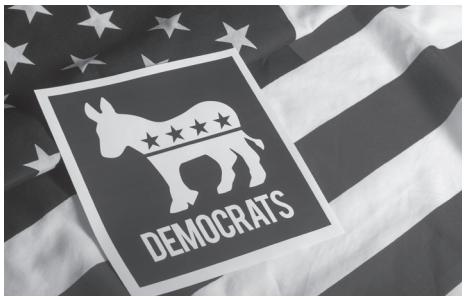


Associated Press **Twitter feed hacked**, markets react.

2015

North Korean hack of Sony Pictures, followed by document release on WikiLeaks to force the company to change behavior.

2016



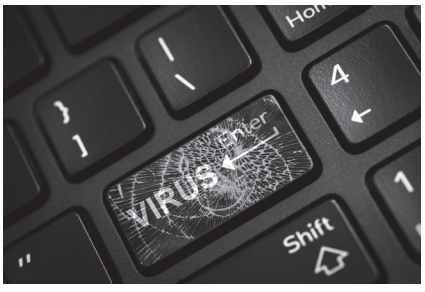
Democratic Committee hacked, documents released on WikiLeaks. Botnets and other Denial of service tools reapplied to distribute fake news.

2013

2015

2016

2017



Ransomware attacks global shutdown.

Constructing a CBV for Your Firm

The first step toward safer, more adaptive cyber capability? Addressing a series of key considerations in each cyber dimension.

The Physical Dimension

With respect to cyberattack, the physical dimension is critical, not simply because of its value as a target for hackers, but because the physical dimension acts as an on-ramp to cyberspace, granting access to the informational and cognitive dimensions.

To begin construction of a CBV, ask questions about the physical dimension in your organization. For example:

- What devices and sensors are connected to your networks?
- What critical operational and business assets are connected to your networks?
- Do you allow employees to connect personal devices to your networks?

The Informational Dimension

In a knowledge-driven organization, the informational dimension is where valuable information assets reside. It includes knowledge assets such as patents, training, and business intelligence. It also contains critical software that runs the devices, networks, and sensors of the physical dimension—the software that supports core business processes—and it feeds the cognitive dimension for decision-making (see below). While it is impossible to defend everything, understanding what is housed in the informational dimension allows the organization to prioritize the defense of potential targets. Issues such as asset colocation can be critical. For example, hackers breached a water utility intending to steal customer-billing information, only to discover that systems responsible for water treatment and flow control were collocated. What began as a hack of the billing system for the purposes of data theft allowed hackers to manipulate the water supply.[13]

In constructing your CBV, ask questions about the informational dimension in your organization. For example:

- How does data or software support our critical physical assets?
- Where in the enterprise architecture does that data or software reside?
- Where do we have critical and non-critical assets collocated?
- What are the most critical data assets for decision-making?
- How do we prioritize the data assets within our organization?

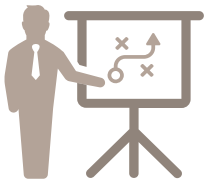
The Cognitive Dimension

Cyber defense strategy begins in the human mind. It requires a thorough knowledge of key personnel, business processes, core capabilities, and critical data assets. The minds of hackers and other rivals are also part of this dimension. The cognitive dimension contains a firm's tacit knowledge resources and decision-making capacity. The relationship between the human mind and the physical and informational dimensions is the most critical element of cyber defense; human behavior is often the entry point through which attacks are launched using the physical and informational dimensions.

As you construct your CBV, ask questions about the cognitive dimension of your firm. For example:

- Who are the key personnel and where are they located within the firm?
- What kinds of decisions are included in our key business processes?
- Who are our core knowledge assets within the firm?
- Where are critical decisions made and who makes them?

Expanding Resources & Capabilities with the CBV



Using the CBV to build an adaptive strategy helps a firm think through how hackers might monetize its data or how rivals can influence stakeholder opinions.

This, in turn, can reveal potential ways to for the firm to harness its data to generate competitive advantage. The CBV moves firm strategy from risk mitigation, which assumes hazards can be identified, toward seizing opportunities and building resilience into firm operations, which prepares the firm for the unexpected. For example:

AT&T

AT&T built excess network capacity to ensure reliability and restoration in instances of outages, **creating additional capability** that can be used to generate revenue.[14]

amazon

Amazon's **proactive cyber defense strategy** to secure their e-commerce model and cloud infrastructure led to the development of Amazon Web Services (AWS) Cloud Security as a new product offering.[15]

How Does the CBV Translate to an Adaptive Cyber Capability?

The CBV can inform many different kinds of adaptive cyber strategies, both to generate revenue, such as a marketing campaign, or to defend against morphing threats, such as identifying a target at a public utility site.

Example 1: Geofence Marketing Strategy

Geofencing is creating a virtual boundary that enables the physical location of a mobile device to trigger an event. In marketing, the event may be a marketing message delivered to a customer's mobile device as she enters the store. The CBV of a geofence marketing strategy could ask:

Cognitive

- **Who is the customer?** *People near brick-and-mortar locations.*
- **How does the customer make decisions?** *Convenience and a trigger.*

Informational

- **What kind of information does the customer seek out to make this decision?** *Price, availability, physical access to item, special deals.*
- **What information can we provide as a trigger?** *Coupon, when customer is nearby.*

Physical

- **How does the customer access the information?** *Smartphone.*
- **How do we access the customer?** *Brick-and-mortar store.*
- **How can we use the smart phone to bring them into the store?** *Geofence to trigger coupon delivery.*

Example 2: Target Identification at a Public Utility Transmission Station

As mentioned previously, public utilities are a high-visibility target for hackers. There are not only opportunities for theft, but also opportunities to disrupt and disable critical infrastructure. A CBV for a public utility could ask:

Cognitive

- **Who might want to interfere or manipulate critical infrastructure?** *Nation states, terrorists, criminals*
- **If a nation state, for what purpose?** *To thwart defensive action.*
- **If a terrorist, for what purpose?** *To instill fear and cause maximum damage.*
- **If a criminal, for what purpose?** *To generate revenue or gain access to controlled area.*

Informational

- **What kinds of applications control service delivery?** *Transformation of transmission voltage, control of power flow, management of multiple voltage levels, power distribution.*
- **What kind of data is transmitted?** *Power-line communications, voltage, power flow, environmental.*
- **What kind of data is collected?** *Voltage, power flow, environmental.*
- **What new threats are emerging?** *Malware that uses infrared signals in surveillance cameras.*[16]

Physical

- **What devices are in place to automate process?** *Circuit breakers, capacitors, voltage regulators, transformers.*
- **How is data collected?** *Sensors.*
- **What transfers data from sensors to automation equipment?** *Air-gapped network for power-line communications.*
- **What controls do we have in place?** *Fences, networked security cameras, air gap.*

Recommendations

1. BUILD YOUR TEAM

The single most important qualification is a willingness to challenge existing norms, but it helps to choose people who are comfortable with complexity, ambiguity, and crossing organizational boundaries. This experience can be very uncomfortable, because the word "cyber" can make non-technical people feel very outside their comfort zone. That discomfort, coupled with the resistance they will likely encounter, can feel extremely risky. Interestingly, through this experience, the individuals who were most resistant often become your most vocal champions. At a minimum, you will need representation from the following areas of the organization:

- Representative(s) who understand(s) where and how **operational technologies** such as sensors, wireless networking, robotics, and industrial controls are implemented
- Representatives from each department (ex: finance, contracting, HR, operations, logistics, product development, R&D, manufacturing, marketing, sales, etc.) who understand **how decisions are made**, what the most critical data is for decision-making, and how the business processes work, including the workarounds for flawed IT applications
- Representative(s) who understand(s) **information strategies** related to influencing and being influenced by stakeholders in the organization and the industry
- Representative(s) from the information technology department who understand how the **IT infrastructure** stores information, where applications and data reside, and existing cybersecurity technologies
- Representative(s) who understand **physical security** and defense of physical assets

2. DEFINE THE COMPETITIVE LANDSCAPE

Ask questions that focus on leveraging information both within the organization and from outside the organization to either advance or thwart your strategic objectives. Consider who your competitors are from an information-operations perspective.

- Are there **grassroots organizations** who might not like the way you do business, such as Anonymous?
- Are there **projects your organization is pursuing** that might have caught the attention of foreign governments, such as the Sony Pictures movie "The Interview"?
- Do your operations support **critical infrastructures** that could be targeted to break down civil order?
- Does your organization have **information that might aid or hinder organized crime**, such as money laundering?
- Who are your **rival organizations**, and how do they apply information strategies to compete with you?

3. BUILD YOUR CBV

There is a reason that Step 1 recommends choosing people who are comfortable with complexity and ambiguity. There is no correct (or incorrect) point to begin building your CBV. It is an iterative process to create a "living document." The starting point for building the CBV is to start asking questions.

The questions in the previous section discussing each of the three dimensions are a good place to start. You may want to have physical security, OT, and IT staff start with the physical dimension, while the department representatives may be well-suited to begin with the cognitive or the informational dimensions.

After the initial brainstorming leads to a rudimentary view, begin to integrate the three dimensions. The greatest vulnerabilities are at the integration points, and this is where the CBV can be particularly effective. As your situational awareness grows and you become more comfortable with the tool, your CBV will expand beyond the sample questions offered in this report and become more organizationally specific.

4. INTEGRATE THE CBV INTO THE STRATEGIC PLANNING PROCESS

The CBV for your organization will inevitably reveal both threats and opportunities. Think about what makes your data valuable to people within the organization and outside the organization, and even the industry.

- **How can your information be weaponized?** By hackers? Against hackers?
- **How can a hacker monetize your data?** Are you so information-driven that you will be willing to pay ransom to get your operations back online? Can your data be sold? Is your data a form of currency in and of itself?
- **Who would pay for your data?** And if someone is willing to pay for your data, could you turn it into a new product? If your data cannot be productized, what is the likelihood that someone will still want to procure it, and why?
- **Just because something can be automated, does it make sense to do so?** Is adding sensors and wireless networking to your fish tank an operational necessity? Does adding new elements to the Internet of Things create benefits for the organization to a degree that it makes sense to add new points of entry to your network (aka vulnerabilities)?
- **What are your most valuable knowledge resources?** How can they be defended? How can they generate revenue?
- Having asked the previous question, how do you prioritize the **data assets** within your organization?

5. TAKE ACTION

Incorporating the CBV into your strategic planning process will identify specific actions required to defend your critical assets while also creating the potential to benefit from them. Perhaps your strategic plan will identify required capital investments to build resilience, or allocation of resources to productize your data. The plan may identify the need to remove non-critical objects (such as the automated fish tanks) from the organization's Internet of Things, or identify the need to create training programs for your employees. Perhaps you will find that you are defending yourself so well that you could market your capacities to others. As the CBV becomes integrated into your strategic planning process, it will be a valuable tool to growing new resources and capabilities, including a dynamic, robust adaptive cyber capability.

Conclusion

Cyberattacks have evolved from nuisances to full-blown information operations.

Digital technologies have become fundamentally entrenched into the fabric of firm activity, making people, process, and technology inseparable, and offering hackers unprecedented entry into internal operations. This changing nature of the firm requires new strategic tools.

Characterizing the environment and mapping the key terrain is the critical first step in developing a dynamic adaptive cyber capability to generate revenue, strengthen defenses, build resilience, expand resources and capabilities, and grow competitive advantage. The Cyber-Based View, with its interdependent physical, informational, and cognitive dimensions, offers corporate leaders the means to take that critical first step.

References

[1] Manyika, J. et al. (2016). Digital Globalization: The New Era of Global Flows, Executive Summary. *McKinsey Global Institute Website.* Retrieved 26 July 2017 from: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.

[2] Ibid.

[3] Prigg, M. (2015). The Tweet That Cost $139 BILLION: Researchers Analyse Impact of Hacked 2013 Message Claiming President Obama Had Been Injured by White House Explosion. *DailyMail.com.* Retrieved 3 July 2017 from: http://www.dailymail.co.uk/sciencetech/article-3090221/The-tweet-cost-139-BILLION-Researchers-analyse-impact-hacked-message-claiming-President-Obama-injured-White-House-explosion.html.

[4] Stone, J. (2016). "Hacker's Typo Stopped $1 Billion Bank Robbery, But Thieves Still Made Off With $81 Million." International Business Times. Retrieved from: http://www.ibtimes.com/hackers-typo-stopped-1-billion-bank-robbery-thieves-still-made-81-million-2334701.

[5] Perlroth, N., Scott, M., & Frenkel, S. (2017). Cyberattack Hits Ukraine Then Spreads Internationally. *New York Times.* Retrieved 16 July 2017 from: https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html

[6] Raymond, D. et al. (2014). Key Terrain in Cyberspace: Seeking the High Ground. *6th International Conference on Cyber Conflict.* Retrieved 25 September 2017 from: http://www.usma.edu/acc/SiteAssets/SitePages/Publications/06916409.pdf

[7] Weinberger, S. (2011). Is This the Start of Cyberwarfare? *Nature, 474 (7350)*, 142-145.

[8] Filkins, B. (2016). SANS Survey: IT Security Spending Trends. *SANS Institute Website.* Retrieved 14 August 2017 from: https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697

[9] Chapple, M. (2015). Security Matters: Malware Jumps the Air Gap. *Go Certify.com.* Retrieved 14 August 2017 from: http://www.gocertify.com/articles/security-matters-malware-jumps-the-air-gap.html.

[10] Schiffer, A. (2017). How a Fish Tank Helped Hack a Casino. *The Washington Post.* Retrieved 26 July 2017 from: https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/?utm_term=.2189d00e6773.

[11] Haggard, S. and Lindsay, J. (2015). North Korea and the Sony hHck: Exporting Instability through Cyberspace. *Analysis from the East-West Center, 117*, 1-8.

[12] Mihailidis, P. & Viotty, S. (2017). Spreadable Spectacle in Digital Culture: Civic Expression, Fake News, and the Role of Media Literacies in "Post-Fact" Society. *American Behavioral Scientist, 61(4)*, 441-454.

[13] Kovacs, E. (2016, March 22). Attackers Alter Water Treatment Systems in Utility Hack: Report. *Security Week.* Retrieved from: http://www.securityweek.com/attackers-alter-water-treatment-systems-utility-hack-report

[14] Ambs, K. et al. (2000). Optimizing Restoration Capacity in the AT&T Network. *Interfaces, 30 (1)*, 26-44.

[15] Novet, J. (2015). Amazon Launches Inspector, a Tool that Automatically Finds Security and Compliance Issues. *Venturebeat.com.* Retrieved 29 June 2017 from: https://venturebeat.com/2015/10/07/amazon-launches-inspector-a-tool-that-automatically-finds-security-compliance-issues/

[16] Goodin, D. (2017). Infrared signals in surveillance cameras let malware jump network air gaps. *ARS Technica.com.* Retrieved 25 September 2017 from: https://arstechnica.com/information-technology/2017/09/attackers-can-use-surveillance-cameras-to-grab-data-from-air-gapped-networks/

About the Authors

Tamara Schwartz

Lieutenant Colonel Tamara Schwartz, United States Air Force (retired) is founder and owner of LLamrai Enterprises, a Pennsylvania based consulting firm. She is currently pursuing her Doctorate of Business Administration at the Fox School of Business at Temple University, and serves as an Adjunct Professor of International Business, Organizational Development and Management practices at Gettysburg College. She is a recognized Cyber Thought Leader and gifted speaker who has presented at business and government conferences throughout the world. During her military career she served as the Chief Technology Officer (CTO) for U.S. Air Force Enterprise Networking, where she assembled and led a team comprised of technologists from the Mass High Tech and Silicon Valley communities and newly designated Air Force "cyberwarriors" to develop cyberwarfare concepts during the standup of the Air Force's Cyber Command. Her leadership informed the technology investment strategy that enables the Air Force to leverage cyber as a non-kinetic weapon, a battlespace, and an element of the supply chain. Her guidance also shaped the design of various command centers throughout the military supporting Joint Space, Cyber, and Global Strategic Operations, as well as the National Military Command Center. She now applies her knowledge of cyberwarfare to practices in business and industry.

Tamara has previously served as program manager for 8 different technical programs with annual operating budgets ranging from $10 Million to over $1.3 Billion; managed international programs and partnerships of 2 – 51 countries. She served as Executive Assistant to the Program Executive Officer of the F-35 Joint Strike Fighter, the first Department of Defense International Cooperative Development, including 8 partner nations and 2 foreign military sales customers with $3 billion annual operating budget. She was later handpicked to design, develop and implement the first comprehensive DoD/DoS export program to ensure adherence to the U.S. International Traffic in Arms Regulation between foreign nations and the DoD, fostering collaboration across the 400+ U.S. and foreign defense contractors in 9 countries for the F-35 Lightning II.

Tamara is known for her game-changing, collaborative strategies to drive technological, cultural and process innovation. With 20+ years of experience in complex government organizations in international policy, security assistance, and cyber policy and strategy, she has advised senior Department of Defense leadership regarding technology adoption strategies to enhance the decision cycle through the use of big data and artificial intelligence strategies. A skilled information operations professional, she is comfortable with ambiguity and the complexity of today's information driven environments, enabling her to work with organizations ranging from highly classified intelligence organizations, to high-tech startups such as Oblong Industries, to multibillion dollar analytics companies like SAS Federal, to advanced research institutions such as Rensselaer's Institute for Data Exploration and Applications (IDEA). Her understanding of organizational development and her personality enable her to work with individuals and groups at all levels of an organization from entry level individuals to Boards of Directors with an approach that fosters down to earth solutions to complex, high tech problems and integrates those solutions into all aspects of the organization.

Tamara has received numerous awards including the Air Force Materiel Command Information Operations Officer of the Year and Honorable Mention for the Massachusetts Veteran of the Year. She holds a B.S. in Industrial & Management Engineering from Rensselaer Polytechnic Institute and an M.S. in Engineering Management from the University of Dayton. She is a graduate of the Air Force's Squadron Officer's School, Air Command and Staff College, and Air War College.

David Schuff

David Schuff is Professor and Chair of the Department of Management Information Systems. David's research interests include the application of information visualization to decision support systems, tools for self-service business intelligence, and the impact of user-generated content on organizations and society. David has published over 40 refereed journal articles, book chapters, and conference proceedings. His work has appeared in numerous journals, including Management Information Systems Quarterly, Decision Sciences, Decision Support Systems, Information & Management, Communications of the ACM, IEEE Computer, AIS Transactions on Human-Computer Interaction, and Information Systems Journal.

David was the founding Academic Director of the Fox School's Executive Doctorate in Business Administration. The program has 70 executives enrolled from 17 states and six countries. The centerpiece of the program is an innovative, personalized mentoring experience beginning in the first year and continuing throughout the program. The program graduated its first class in May 2017.

He is also the creator and organizer of the Temple Analytics Challenge, an annual University-wide data analytics and visualization competition. The national version of this challenge is run through the Association for Information Systems at their annual Student Chapter Leadership Conference; in 2017 David received the Fox School IMPACT award for developing those competitions. David also created Temple University's first General Education course in Data Science; in 2015 he received the Teradata University Network Teaching Innovation Award for the course.

David has taught in the BBA, MBA, the Executive MBA programs in Colombia and Japan, and the Executive DBA program. He teaches courses in data analytics, information systems strategy, process design and improvement, and application development. David has received the MIS Department's teaching award 13 times (most recently in 2016), and in 2013 received the University-wide Lindback Award for Distinguished Teaching. In 2014, he received the Fox School Musser Award for Excellence in Teaching. In 2007 he received the MBA Faculty of the Year award.

David holds a BA in Economics from the University of Pittsburgh, an MBA from Villanova University, an MS in Information Management from Arizona State University, and a Ph.D. in Business Administration from Arizona State University.

Before earning his doctorate, David worked as a consultant in the Philadelphia area. His specialty was network administration and end-user support in large organizations. He has consulted for GlaxoSmithKline, Comcast Cellular Communications (now AT&T Wireless), JP Morgan, and Air Products and Chemicals. Before he became a consultant, David worked for CoreStates Bank (now Wells Fargo).

The IBIT Report

The IBIT Report is a publication for the members of the Fox School's Institute for Business and Information Technology. IBIT reports provide actionable knowledge to industry based on rigorous academic research and vendor neutral analysis. Each report focuses on an important topic of interest to our members.

Learn more at ibit.temple.edu

Fox School of Business
TEMPLE UNIVERSITY®