CYBERSECURITY

PRESENTATION TO THE UNIVERSITY SYSTEM OF MARYLAND'S BOARD OF REGENTS

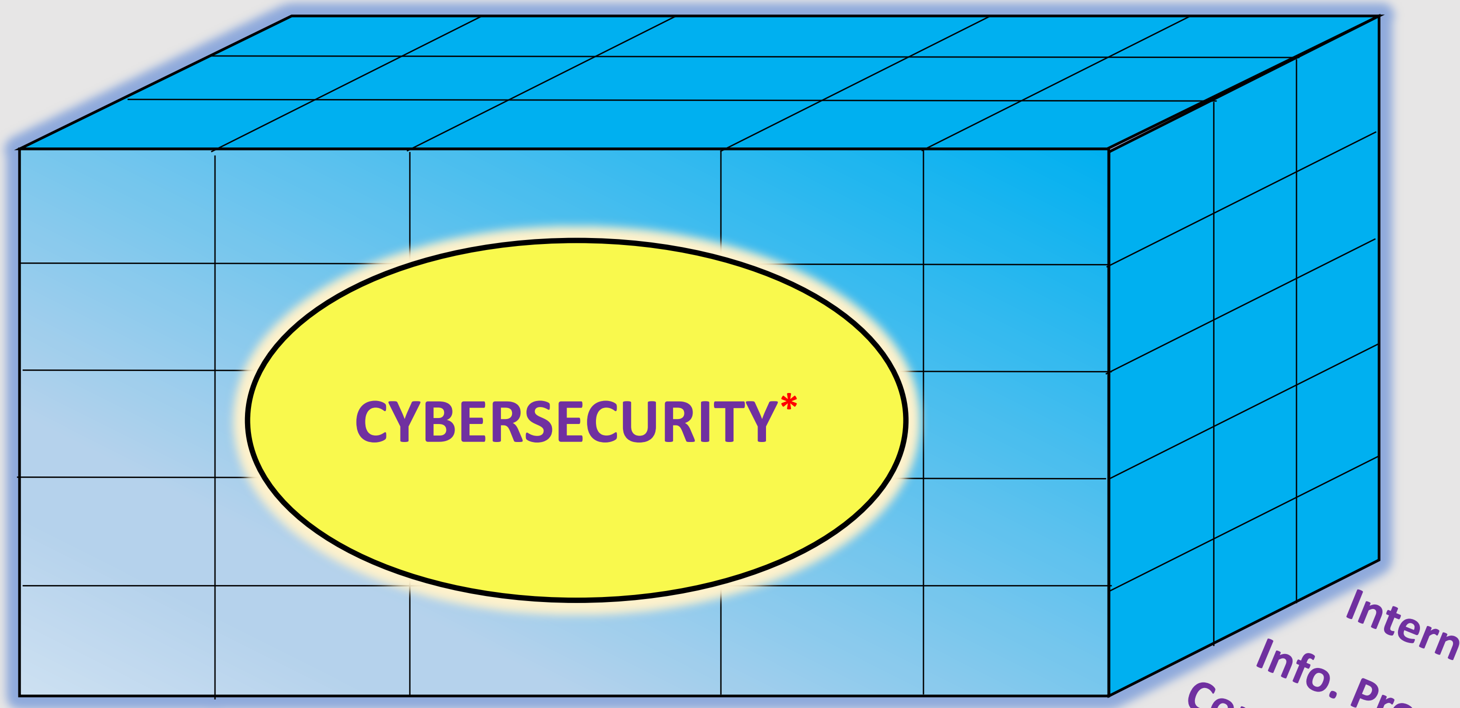
by

Dr. Lawrence A. Gordon (Lgordon@rhsmith.umd.edu)
EY Professor of Managerial Accounting and Information Assurance
Affiliate Professor in University of Maryland Institute for Advanced Computer Studies
Robert H. Smith School of Business, University of Maryland, College Park, MD

The "cyber threat is one of the most serious *economic* and *national* security challenges we face as a nation" and "America's economic prosperity in the 21st century will depend on cybersecurity" (from: Foreign Policy, the White House, President Barack Obama, see: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity, italics added)

April 11, 2014

FRAMEWORK FOR VIEWING CYBERSECURITY



CYBERSECURITY*

Sources of Threats

- Hackers
- Terrorists
- Cyber Criminals
- Insiders
- Nation States

Key Disciplines Impacting Cybersecurity

- Psychology
- Public Policy
- Economics
- CS & ECE
- Law

Attributes of Cyberspace & Computer Networks

- Internet
- Info. Processing
- Comp. Software/ Hardware

***Cybersecurity** = Protection of information transmitted via computer networks, including the Internet. Cybersecurity objectives are: "(1) to protect the *confidentiality* of private information, (2) assure the *availability* of information to authorized users on a timely basis, and (3) protect the *integrity* (i.e., accuracy, reliability and validity) of information" (Gordon, L. A. and M. P. Loeb, MANAGING CYBERSECURITY REOURCES: A Cost-Benefit Analysis, McGraw-Hill, Inc., 2006, p. 10). *Authentication* and *nonrepudiation* are considered subsets of availability.

EXAMPLES OF CYBERSECURITY TACTICS USED BY SOURCES OF THREATS

1. Malware Attacks (i.e., malicious software, that includes viruses, worms, spyware, etc.)
2. Spear Phishing (message that appears to be coming from a known firm or friend, trying to get unauthorized access to confidential information)
3. Social Engineering (tricking people into revealing confidential information, such as a password)
4. Hijacking Domain Name System-DNS is like an Internet phone book changing the comp. hostname into an IP address (i.e., numerical label)
5. Theft of Intellectual Data or Property
6. Theft of Desktop & Laptop Computers
7. Theft of Mobile Devices

SECURITY PROCESSES TO PREVENT AND DETECT CYBERSECURITY BREACHES

1. Annual cybersecurity training for employees
2. Anti-malware systems for prevention and detection
3. Network segmentation with use of firewalls
4. Encryption Techniques
5. Behavioral network analysis and monitoring
6. Access controls (e.g., 2-factor authentication for remote access)
7. Tokenization to protect information stored in system
8. Intrusion detection systems

Above processes were all in place at Neiman Marcus prior to security breach, as noted by Michael Kingston, firm's Senior VP & CIO (see: http://www.c-span.org/video/?317614-1/HouseEnergy)

QUESTIONS for John Mulligan (TARGET'S EXECUTIVE VP & CFO) & Michael Kingston (Neiman Marcus' Senior VP & CIO) at CONGRESSIONAL TESTIMONY (2/5/14)

1. How Much Does Your Company Invest in Cybersecurity?

   Answer: Hundreds of Millions and Tens of Millions over past several years.

   Comment: No discussion on how these amounts were determined.

2. How Much Did the Recent Cybersecurity Breach Cost the Company?

   Answer: Too early to tell. Comment: Full economic cost of a breach needs to consider implicit, as well as explicit, private costs and externalities.

3. What Security Processes Were in Place Prior to Recent Security Breach?

   See previous slide. Comment: 100% security is not possible.

4. How much Information Sharing of Cybersecurity Issues Takes Place in Industry? Answer: Some, but no ISAC for Retail Industry. Comment: There should be an ISAC for the Retail Industry.

MARYLAND's PRIORITIES AND RECOMMENDATIONS (see: CYBERMARYLAND at: http://www.choosemaryland.org/aboutdbed/documents/finalcyberreport.pdf)

Priority I: Support the Creation and Growth of Innovative Cyber Security Technologies

Priority II: Develop a Maryland Pipeline for New Cyber Security Talent and Workforce Development

Priority III: Advance Cyber Security Policies to Position Maryland for Enhanced National Leadership

Priority IV: Ensure the Sustained Growth and Future Competitiveness of Maryland's Cyber Security Industry

POWERING MARYLAND FORWARD: USM's 2020 Plan for More Degrees, A Stronger Innovation Economy*, A Higher Quality of Life (http://www.usmd.edu/10yrplan/)

1. **Helping Maryland achieve its goal of 55-percent college degree completion…;**
2. **Advancing Maryland's competitiveness in the innovation economy** by building on existing levels of research funding and more successfully translating that research in economic activity. The plan calls for the creation of 325 new companies, five internationally recognized research centers of excellence by 2020, and a culture of innovation and entrepreneurship throughout the USM;
3. **Transforming the academic model with course redesign strategies** that help students understand material, complete their degrees, and become better-qualified for the workforce;
4. **Identifying new ways to build on more than $200 million in direct cost savings** already achieved through USM's existing efficiency efforts, pledges, & federated capital campaign, …;
5. **Achieving and sustaining national eminence through the quality of USM's programs, people, and facilities.**

*An *Innovation Economy* focuses on Knowledge, technology, entrepreneurship, and innovation" (http://en.wikipedia.org/wiki/Innovation_economics).

ACTIONS USM's Board of Regents Could Take to Facilitate Maryland Being Viewed as the Epicenter of the Cybersecurity Industry

1. Establish *USM CYBERSECURITY EDUCATION AND RESEARCH PROJECT* (USM CER Project). Goals of USM CER Project:

(a) encourage innovative interdisciplinary, and inter-institutional, cybersecurity education and research programs at USM, emphasizing partnerships among businesses, government agencies, and academia,

(b) facilitate the transfer and commercialization of USM cybersecurity research,

(c) identify "best cybersecurity programs" and encourage the adoption of similar programs throughout USM,

(d) establish semester long *cybersecurity executive-in-residence*, and *cybersecurity faculty-in-residence*, programs among USM institutions and major corporations/government institutions.

2. Establish A *CYBERSECURITY BUSINESS CLINIC* (see Clinics at Law & Medical Schools) to:

(a) provide services to facilitate growth of small and medium size cybersecurity businesses in MD (including assistance with business plan, obtaining venture capital, legal issues, technical issues, etc.),

(b) assist MD organizations with decisions regarding the cost-benefit aspects of cybersecurity investments,

(c) assist MD organizations with cybersecurity risk management.

CYBERSECURITY ECONOMICS (Questions Underlying Gordon/Loeb Research)

1. What is the economic impact of cybersecurity breaches on firms?
2. How much should a corporation invest in cybersecurity activities & how should it be allocated?
3. What economic incentives/regulations are required to encourage firms to invest in cybersecurity and to share cybersecurity related information?
4. What Is the best way to conduct Cybersecurity Risk Management?
5. What are the effects of the Sarbanes-Oxley Act of 2002, and the 2011 SEC's Disclosure Guidance on Cybersecurity Risks and Cyber Incidents, on the cybersecurity activities of corporations?
6. How can we develop a vibrant cybersecurity insurance market?
7. What is the economic process for cybersecurity technology transfer and commercialization?

APPENDIX: NATIONAL STRATEGY FOR COMBATING THREATS

NATIONAL STRATEGY FOR HOMELAND SECURITY (see: http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf)

1. Prevent and Disrupt Terrorist Attacks
2. Protect the American People, Critical Infrastructure, and Key Resources (see President Obama's February 12, 2013, Executive Order 13636)
3. Respond to and Recover from Incidents
4. Ensuring Long-Term Success

U.S. International Strategy for Cybersecurity (May 2011, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/international_strategy_for_cyberspace_US.pdf)

Policy Priorities

1. Economy: Promoting International Standards and Innovative, Open Markets
2. Protecting our Networks: Enhancing Security, Reliability and Resiliency
3. Law Enforcement: Extending Collaboration and the Rule of Law
4. Military: Preparing for 21st Century Security Challenges
5. Internet Governance: Promoting Effective and Inclusive Structures International Development: Building Capacity, Security, and Prosperity
6. International Development: Building Capacity, Security, and Prosperity
7. Internet Freedom: Supporting Fundamental Freedoms and Privacy