

National Defense University The *i*College



***Better LATE than NEVER; educating the non-IT executives
on THEIR cyber security responsibilities***

IEEE STC Conference

Professor Mike Donohoe

Professor Russ Mattern

October 15, 2015



“The views expressed in this presentation/article are those of the authors and do not reflect the official policy or position of the National Defense University, the Department of Defense, or the U.S. Government.”

“The global hub for educating, informing, and connecting Information Age leaders.”

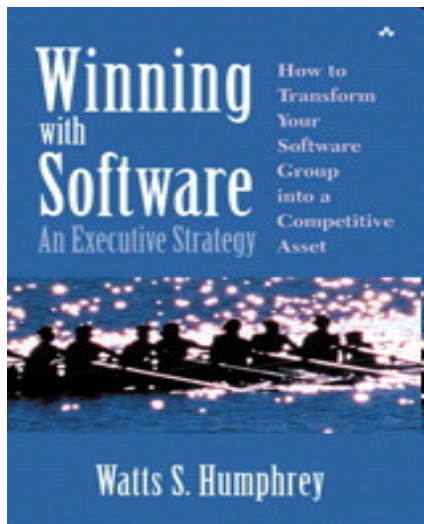


- **What's the problem (or challenge)?**
 - to advance the non-IT executives awareness of cyber security to influence decisions, reduce risk, and improve planning.
 - Why does it exist and how do we fix it?
- **Attention Step (what's in it for me) with non-IT Executives**
 - How did we get here / background of IT in business
 - the shift from evolutionary to transformational
 - Nexus of Forces / Internet of Things
 - Global attacks (wicked problem): new domain, real-time, nowhere to hide, and expanding (evolving & 3Vs)
- **Management's Role & Responsibility**
 - Shift from 'Blind Spot(s)' to a 360-degree cyber security vision
 - Provide managerial oversight towards projects prioritization and eliminate resource constraints towards cyber security activities
 - lead executive level discussions on strategic cyber security integration, resource planning, and talent develop at the enterprise level
- **Data Breach Erodes Public Trust (Cyber-attack is Imminent)**
- **Seek & Share Cyber Security Knowledge**
- **Summary / Q & A**



"The global hub for educating, informing, and connecting Information Age leaders."

Why Every Business Is a Software Business



- A senior vice president of Citibank once told me that “***we are a software business masquerading as a bank.***” He explained that they could not run the bank without software. I see this situation in business after business: software is now a critical part of running many businesses.
- Some executives recognize it, but many others do not.
 - Watts S. Humphrey

(Awarded the National Medal of Technology, 2005)



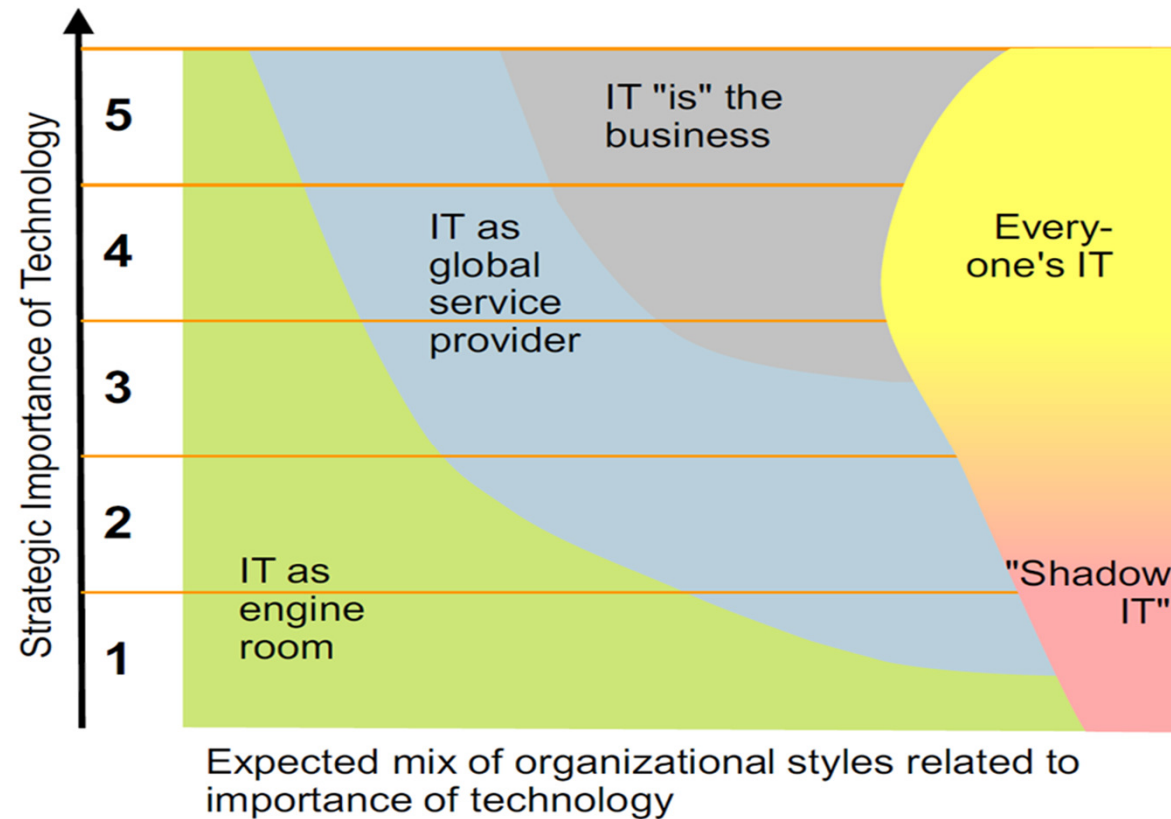
“The global hub for educating, informing, and connecting Information Age leaders.”

Management's View of Information Technology (and Cybersecurity) is Evolving



- Information Systems are the Engine of Business
- Information Systems are valued accelerators of Business Strategy
- Reality (***Ugly Truth***), companies are extremely dependent upon Information Systems and are “***All In – Like it or Not***”; therefore a comprehensive cybersecurity approach across the enterprise is imperative for the company’s ***success*** and ***survival***.

All Business Information System Applications are NOT Used and Managed the Same



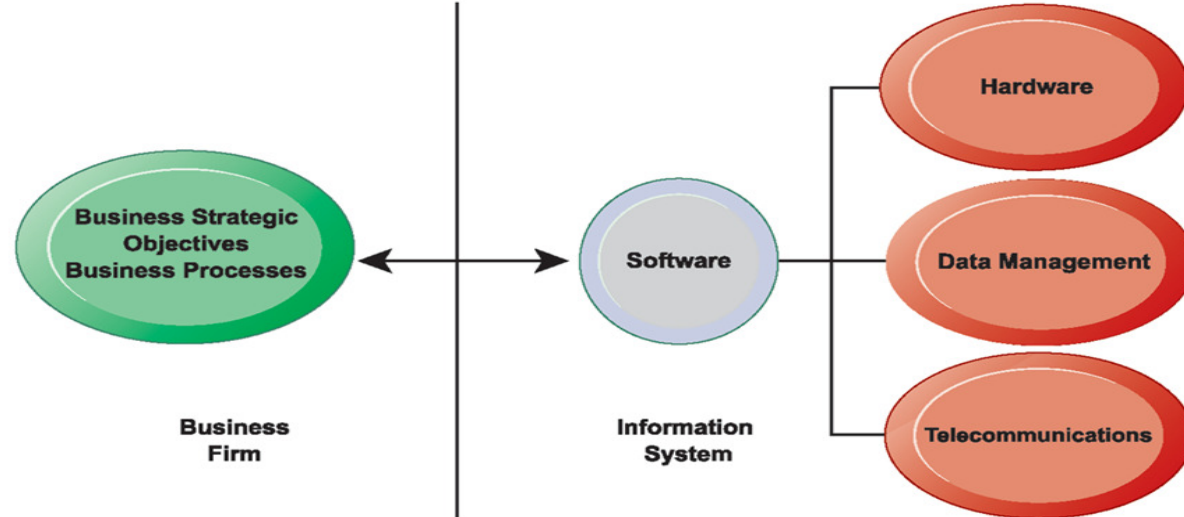
Source: Gartner (March 2013)



"The global hub for educating, informing, and connecting Information Age leaders."

Today's Business Runs on (ICT) Information Communications and Technology

“The successful companies of the next decade will be the ones that use digital tools to reinvent the way they work.” ~ Bill Gates,
[Business @ the Speed of Thought: Succeeding in the Digital Economy, 1999](#)



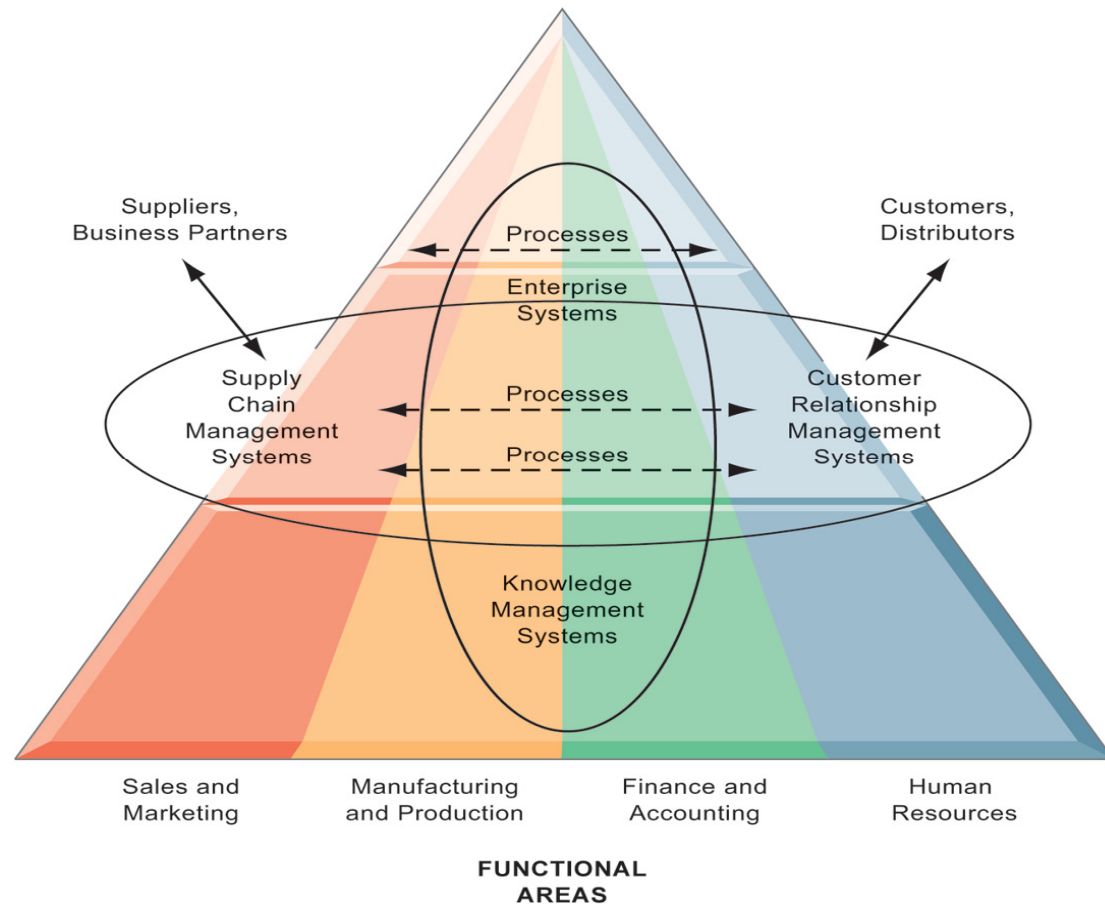
Source: [Management Information Systems: Managing the Digital Firm](#), 13th Edition, by Laudon & Laudon



“The global hub for educating, informing, and connecting Information Age leaders.”

Enterprise Application Architecture

Enterprise applications automate processes that span multiple business functions and organizational levels and may extend outside the organization.

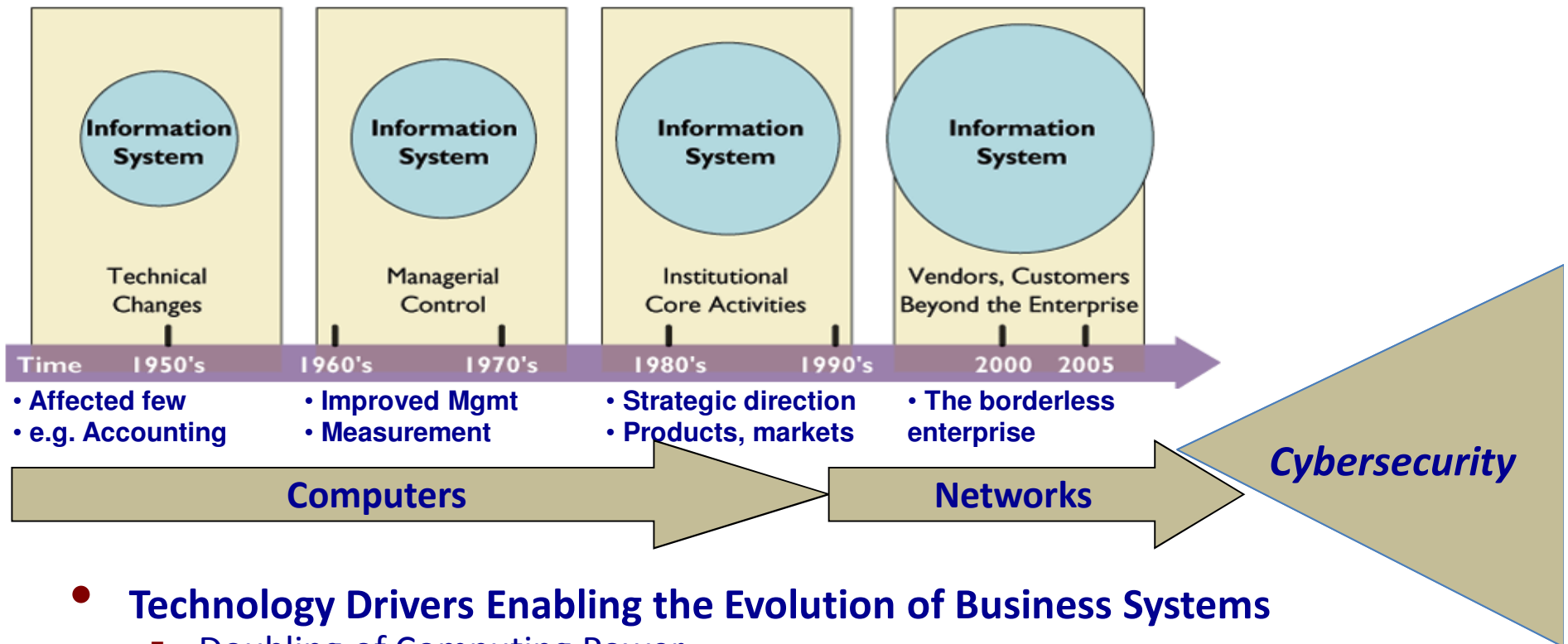


Source: *Management Information Systems: Managing the Digital Firm*, 13th Edition, by Laudon & Laudon



"The global hub for educating, informing, and connecting Information Age leaders."

The Changing ICT Landscape Both Incremental & Evolutionary (*More Pervasive than Ever*)



- **Technology Drivers Enabling the Evolution of Business Systems**

- Doubling of Computing Power
- Advances in Network and Internet
- Data Storage Costs Declining

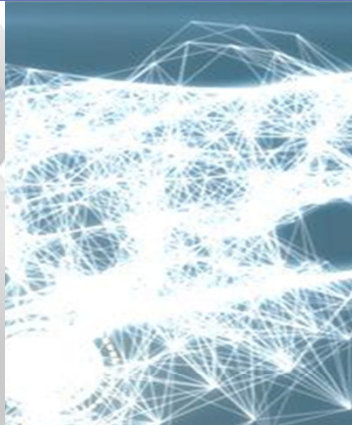
Big Data Demands and Security Risks

- Large organizations are collecting more information than they keep up with, while legacy security processes and analytic tools are applied.
- **44%** of the companies consider actual data collection/analyze as big data, and **44%** consider that it will become in the next 2 years
- Business process improvements are requiring greater data analysis & increased processing performance; yet, while data architecture evolves, security risks and liabilities are after thoughts.



"The global hub for educating, informing, and connecting Information Age leaders."

Nexus of Forces Shaping Business Technology Strategy



HD Camera

- "Kinect" type gesture sensing
- Facial expressions reading and interpretation
- 2D to 3D to Holograms to 4D

Micro-electro mechanical systems

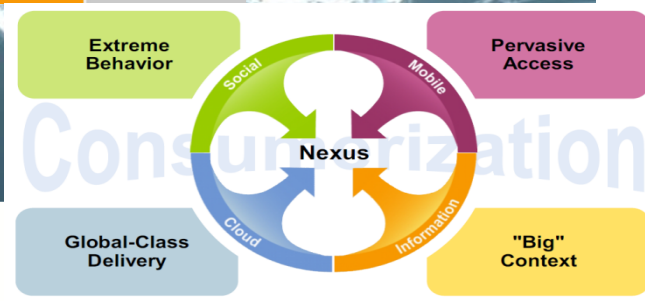
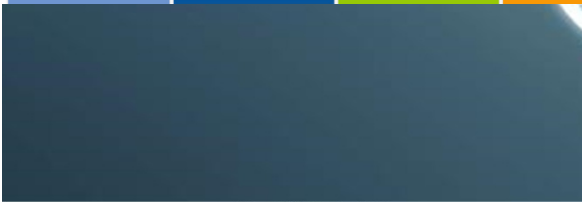
- Accelerometer
- Compass
- GPS (not a MEMS)
- Gyroscopes
- Sensors (i.e. Pressure & Temperature)

Biometric Authentication

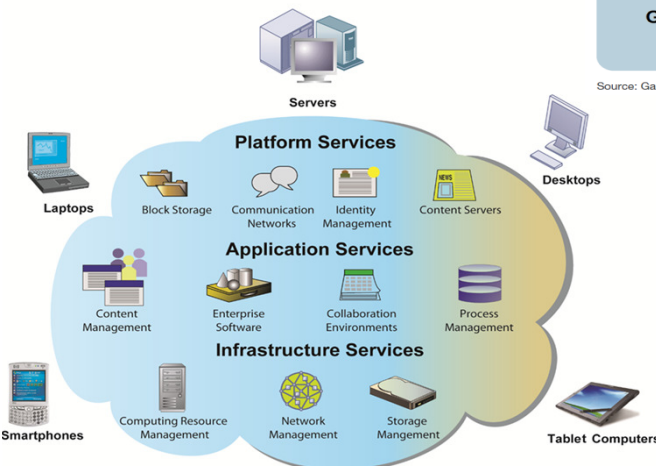
- Fingerprint
- Vein pattern (in the palm)
- Retina scan
- Voice authentication
- Heartbeat pattern

Information Exchange

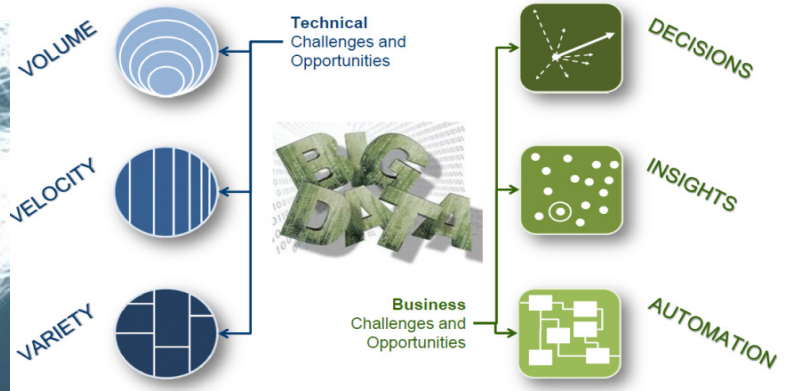
- Machine sensors (IoT)
- NFC
- New Bluetooth
- Wi-Fi Direct data transfer
- Device Pairing with multiple devices
- Information extraction from picture/video
- Augmented Reality (visual contextual info)
- Location-aware to activity-aware (i.e. smart VM)
- Active to Passive Computing



Cloud Computing



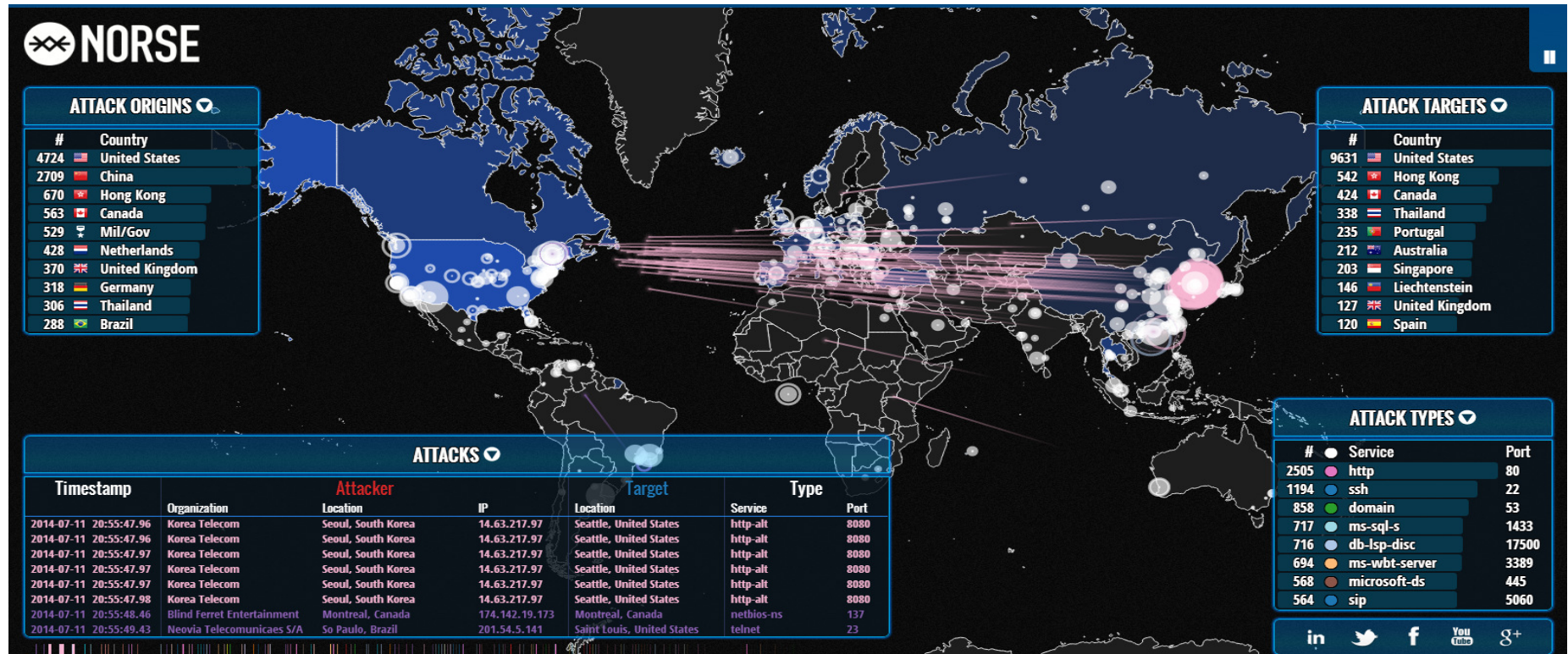
Source: Gartner (September 2013)



The Ugly Truth; Nowhere to Hide...

Cyber Attacks occur 24x7x365 "A Picture is Worth a Thousand Words" ~ Napoleon Bonaparte

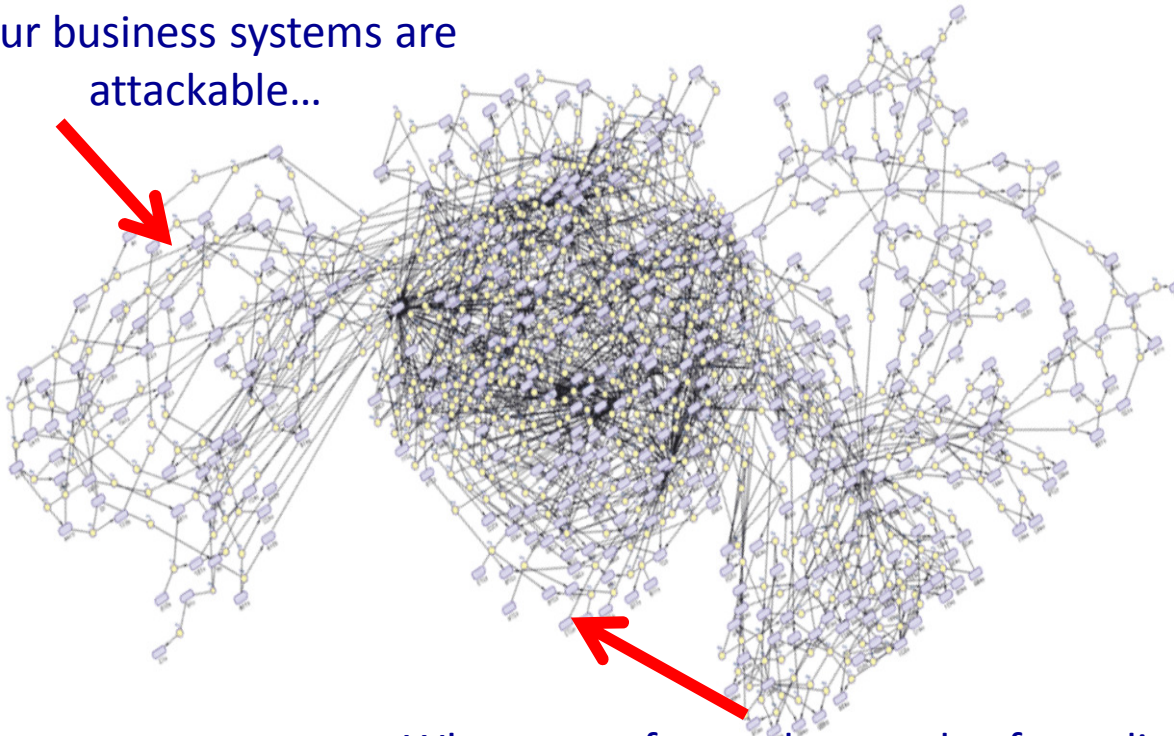
Source: <http://map.ipviking.com/>



"The global hub for educating, informing, and connecting Information Age leaders."

Today Everything's Connected

Your business systems are attackable...



When one of your thousands of suppliers (or customers) allow the 'bad actors' access through a system (or application) weakness or failed process.

"The global hub for educating, informing, and connecting Information Age leaders."



The IT Organization's Purpose and Service

- IT organizations deliver services to their businesses at the based on:
 - Their team's (and contractors) skills, knowledge, and capabilities.
 - the alignment to the organizational strategy and task prioritization, driven by management/executive leadership.
- Firms differ in their IT activities because of:
 - their organizational size & goals.
 - their structure and level of maturity.
 - resource availability.

"The global hub for educating, informing, and connecting Information Age leaders."



Who Owns the Responsibility of Cybersecurity?

- When managers are asked “***who owns the cybersecurity responsibilities***” most respond that it is the (CIO) Chief Information Officer or contracted IT Service Provider
- Traditionally cyber security was relegated to a few people within the company IT department (if that) or an additional duty when a problem occurred.
 - The cybersecurity group (if designated) was often viewed as a barrier to fully optimizing the enterprise Information systems and very resistant to change
 - Often reactive, operational, and resource challenged



“The global hub for educating, informing, and connecting Information Age leaders.”

Who Owns the Responsible of Cybersecurity?

- Cyber security is NOT a technical responsibility; it is a management responsibility that directs and provides guidance to a technical function and operation.
- Effective cyber security in an organization starts at the top; not Stops at the CIO/CISO, data center managers, firewalls, IDS, shielded cables or Smart-Cards.
- Shifting from CIO to CISO with C-Level visibility and reporting; active management leadership role with focus on enterprise cybersecurity strategy
- Senior Leadership drives the commitment to cybersecurity into the organization, by making it visible, education across the enterprise, demonstration (walking the talk), and treating it as a continuous dynamic challenge and imperative for the survival of the company.



"The global hub for educating, informing, and connecting Information Age leaders."

Who Owns the Responsibility of Cybersecurity?

“Corporations must successfully deal with cybersecurity threats, because such threats can have direct impacts on business and reputations... Businesses must own the problem to successfully carry out their mission.” ~
Mike Rogers, Admiral, National Security Agency (NSA) Chief & Commander of United States Cyber Command, 2014

“The loss of intellectual property due to cyber attacks amounts to the greatest transfer of wealth in human history.” ~ General Keith Alexander, Commander, United States Cyber Command, 2012

- Symantec placed the cost of IP theft to US Companies at \$250 Billion
- Global cybercrime at \$114 Billion – nearly \$388 with downtime
- McAfee estimates that \$1 Trillion was spent globally on remediation

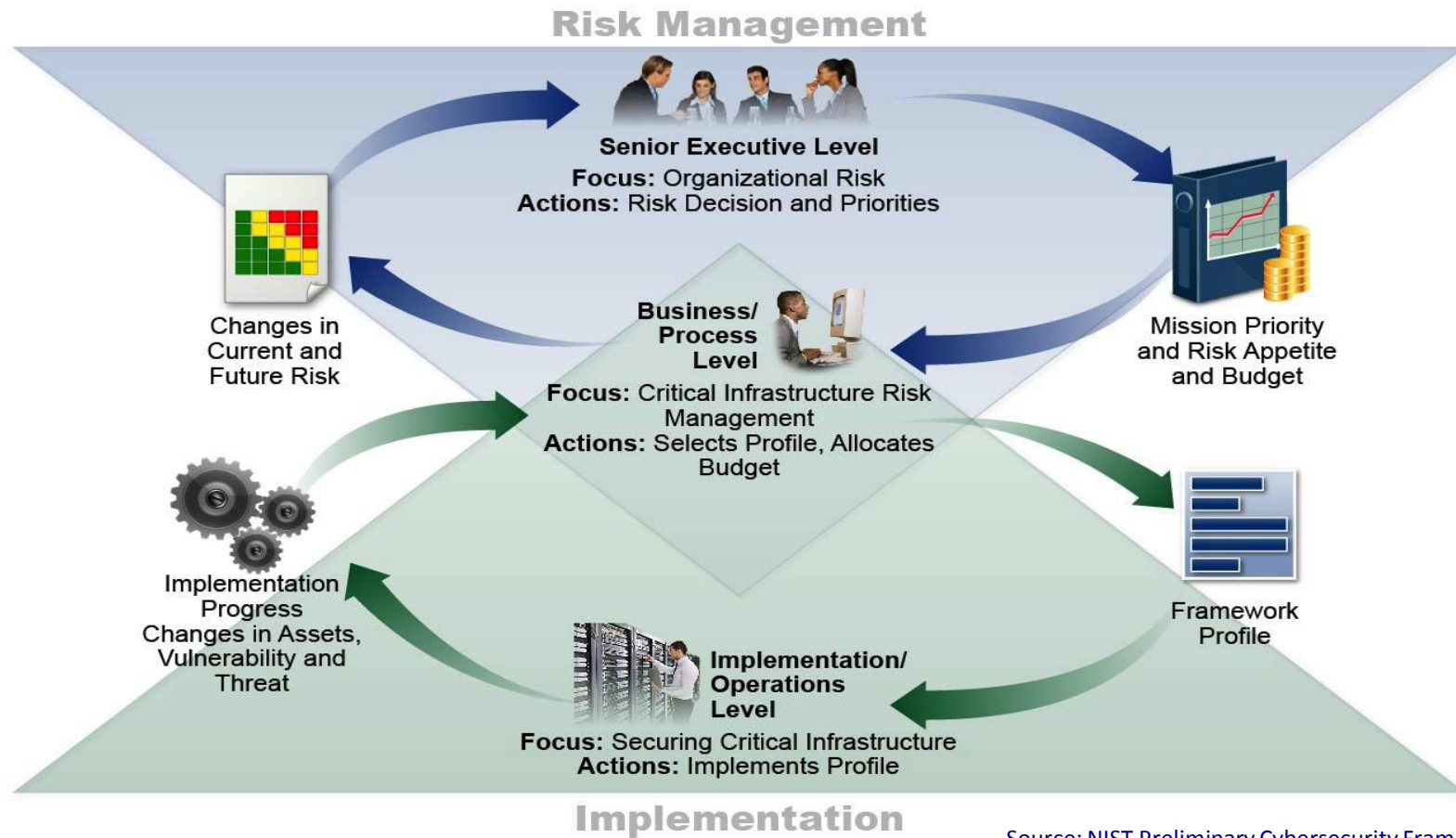


Source: <http://www.infosecisland.com/blogview/21876-Cyber-Espionage-and-the-Greatest-Transfer-of-Wealth-in-History.html>



“The global hub for educating, informing, and connecting Information Age leaders.”

Management's Visibility, Understanding, & Knowledge of All Things Cyber



Source: NIST Preliminary Cybersecurity Framework



"The global hub for educating, informing, and connecting Information Age leaders."

Information Systems Vulnerability

- Failed computer systems can lead to compromised or catastrophic loss of business capabilities
- Business vulnerabilities
 - Market value loss in event of security breach
 - Confidential personal and financial data
 - Trade secrets, new products, strategies
- Inadequate security and controls expose liability challenges



"The global hub for educating, informing, and connecting Information Age leaders."

Information Systems Vulnerability

- Disruption or loss of network Connectivity to Suppliers and Customers
- Hardware problems (breakdowns, configuration errors, damage from improper use or crime)
- Software problems (programming errors, installation errors, and unauthorized changes)
- Loss and theft of portable devices
- Use of networks/computers outside of firm' s control
 - **Suppliers, Customers, Partners...ROW**
 - **BYOD & BYOC**
- Disasters



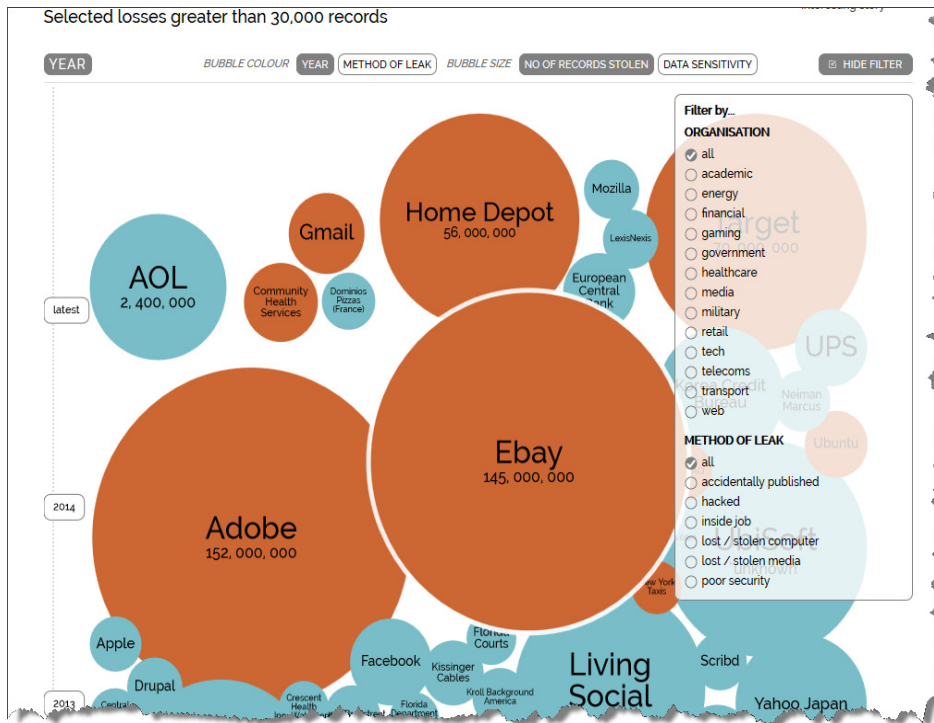
"The global hub for educating, informing, and connecting Information Age leaders."

- Internal threats: Employees
 - Security threats often originate inside an organization
 - Inside knowledge ***“The Snowden Effect”***
 - Sloppy security procedures
 - User lack of knowledge
 - Social engineering:
 - employees not trained and compromise key company information to unauthorized people

“The global hub for educating, informing, and connecting Information Age leaders.”



Data Breach Erodes Public Trust



Source: <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

From: "The Home Depot" <HomeDepotCustomerCare@email.homedepot.com>
 Date: November 7, 2014 at 5:04:32 PM EST
 To: [REDACTED]
 Subject: Notice to Our Customers from The Home Depot
 Reply-To: "The Home Depot" <reply-fe87167706c0c7a76-21178_HTML-131611896-10174489-1275@email.homedepot.com>

More saving. More doing.

Dear Valued Customer,

The Home Depot has discovered that a file containing your email address may have been taken during the payment card breach we announced in September. The file contained email addresses, but it did not contain passwords, payment card information, or other sensitive personal information. We apologize for this incident and for the inconvenience and frustration this may cause you.

In all likelihood this event will not impact you, but we recommend that you be on the alert for phony emails requesting personal or sensitive information. If you have any questions or would like additional information on how to protect yourself from email scams, please visit our website or call 1-800-HOMEDEPOT.

Again, we apologize for the frustration and inconvenience this incident may have caused. Thank you for your continued support.

Sincerely,

The Home Depot

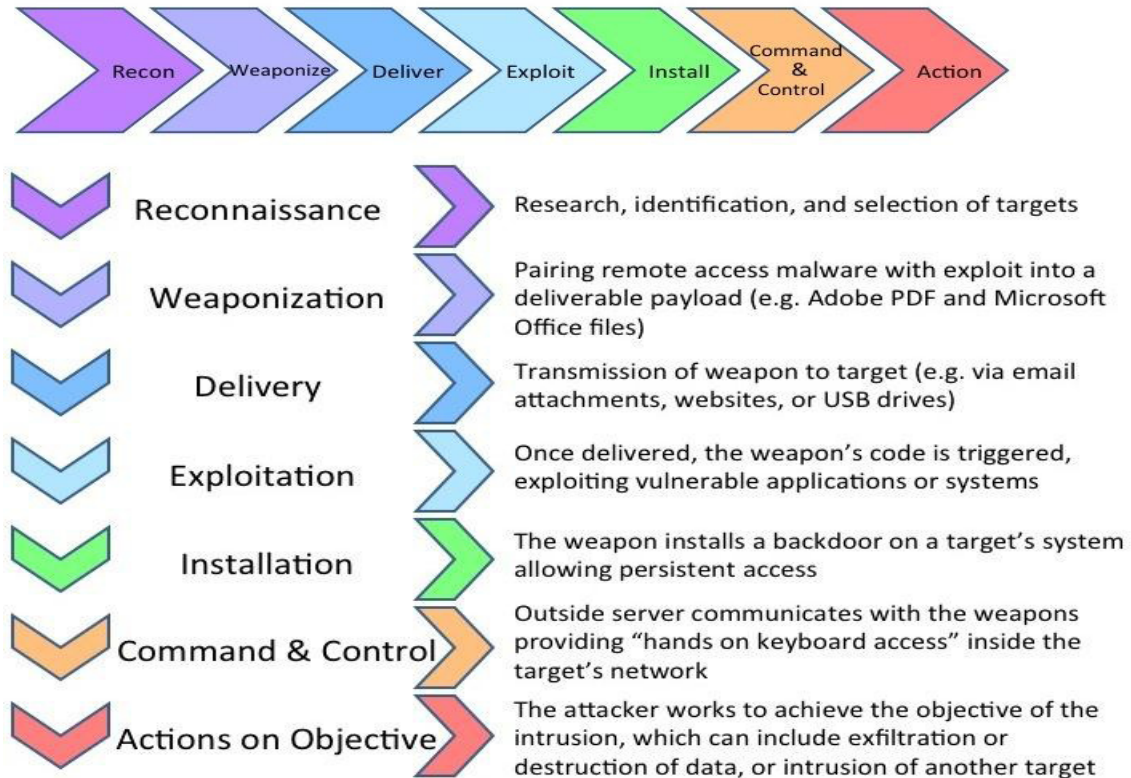
Please do not reply to this email. To contact us call 1-800-HOMEDEPOT, or contact us at The Home Depot, Attn: Privacy Official, 2455 Paces Ferry Road, N.W., Atlanta, GA 30339-4824, USA.



"The global hub for educating, informing, and connecting Information Age leaders."

Educating the non-IT Manager on What is at Risk

Phases of Cyber Intrusion Kill Chain



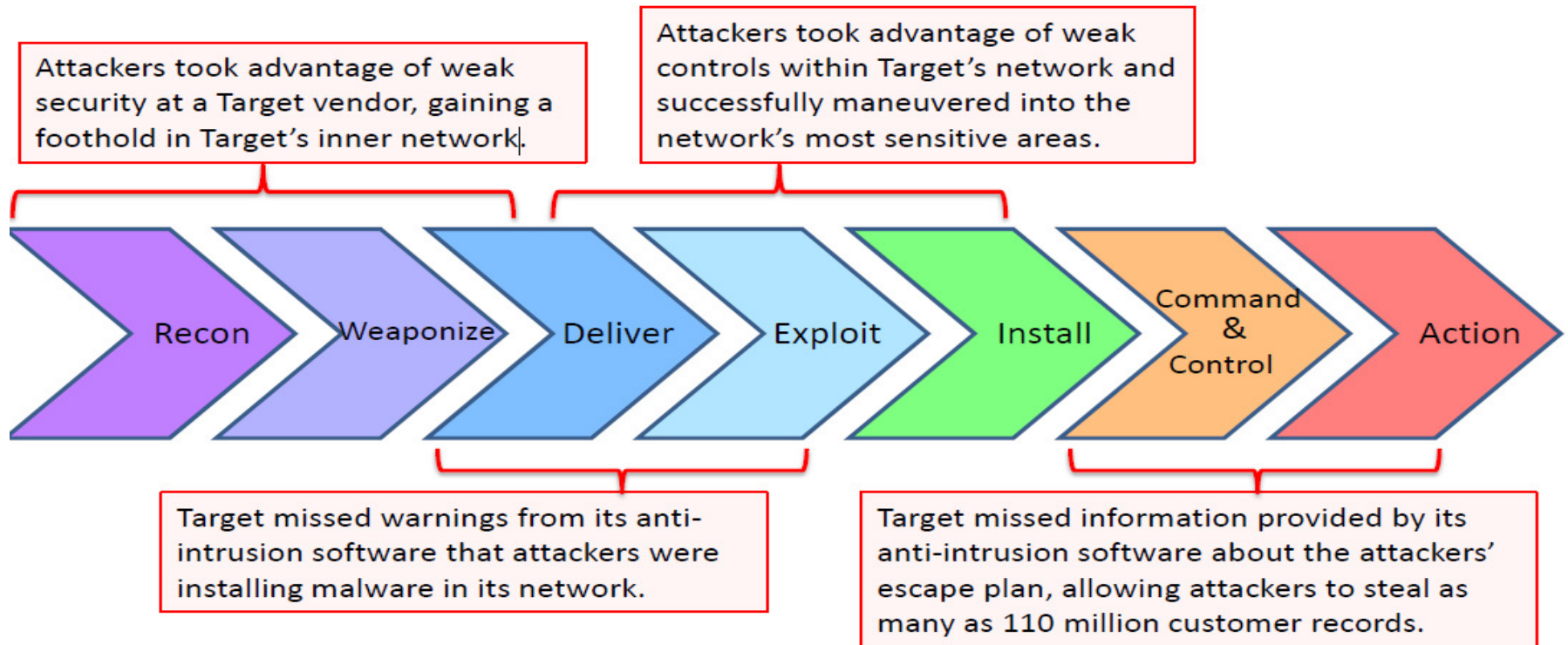
Source: Lockheed Martin Paper – Intelligence-Driven Computer Network Defense by Informed Analysis



"The global hub for educating, informing, and connecting Information Age leaders."

Target's Data Breach

Missed Opportunities to Protect and Defend

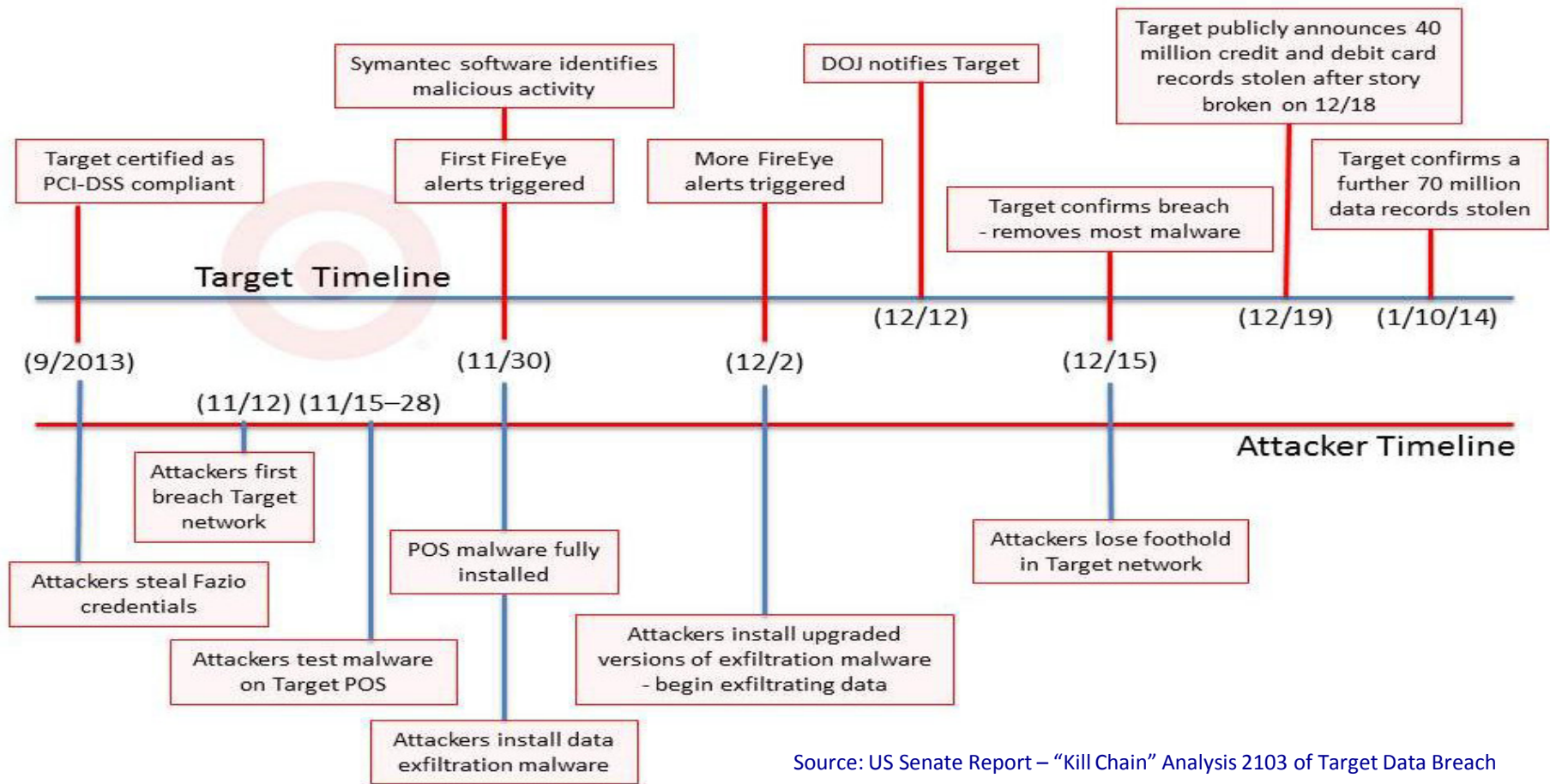


Source: US Senate Report – "Kill Chain" Analysis 2103 of Target Data Breach



"The global hub for educating, informing, and connecting Information Age leaders."

Target's Data Breach Timeline

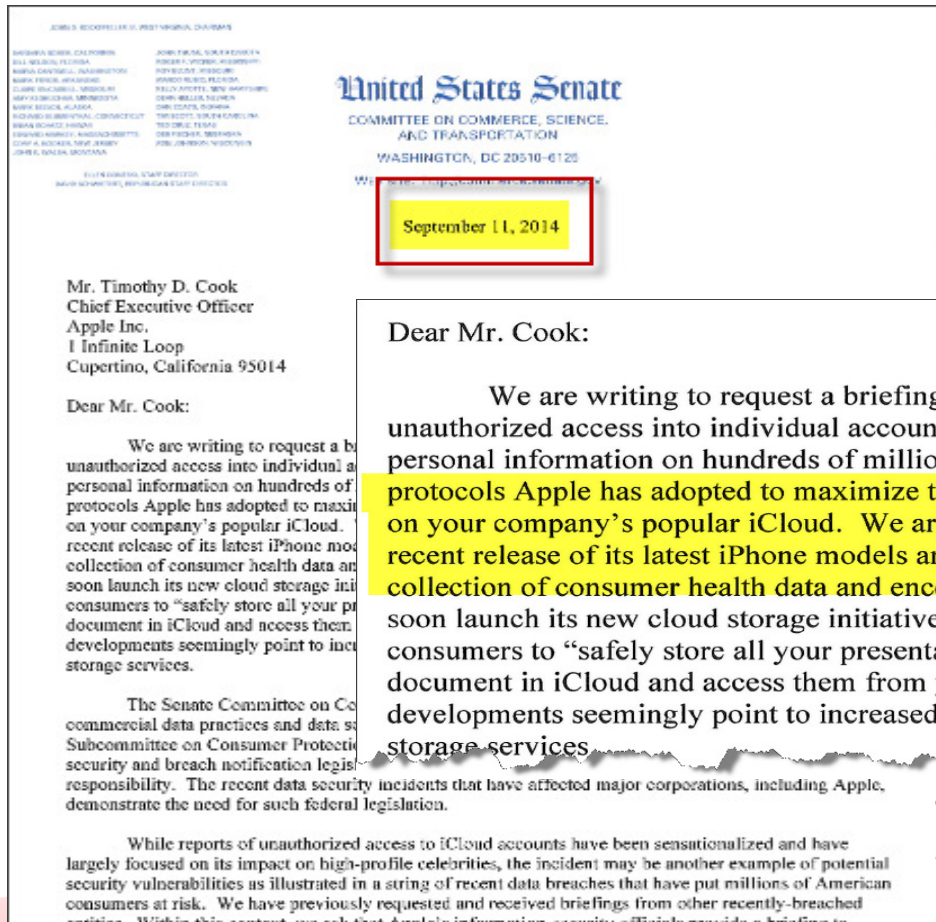


Source: US Senate Report – “Kill Chain” Analysis 2103 of Target Data Breach

“The global hub for educating, informing, and connecting Information Age leaders.”



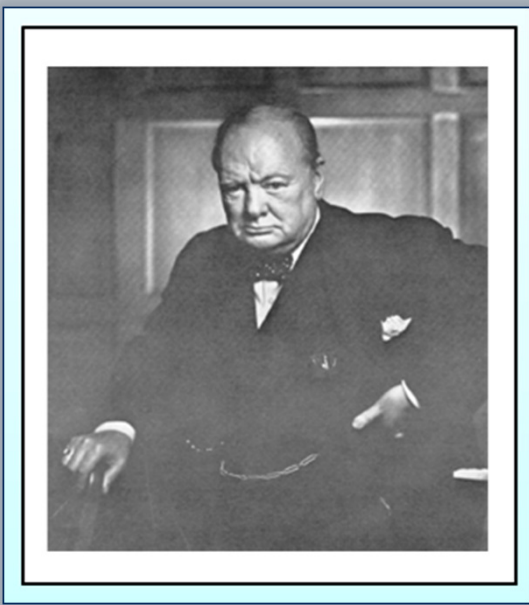
Regulatory Oversight – Cyber Security Ownership to the Top of the Organization



"The global hub for educating, informing, and connecting Information Age leaders."

Educating the non-IT Manager – Call to Action

*“Gentlemen, We Have Run Out of Money;
Now We Must Think.”* ~ Sir Winston Churchill



Why Winston Churchill?

In today's world of budget constraints, people tend to say that they don't have the money for areas such as cyber security...but it is not just a matter of money, it is also a matter of management understanding the complexities of the problem, to lead the necessary level of work required to ensure effective/continuous cybersecurity.



“The global hub for educating, informing, and connecting Information Age leaders.”

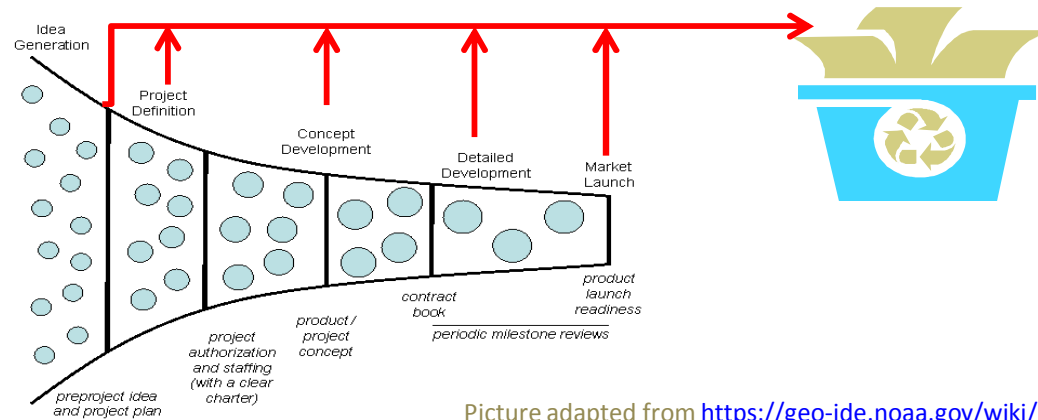
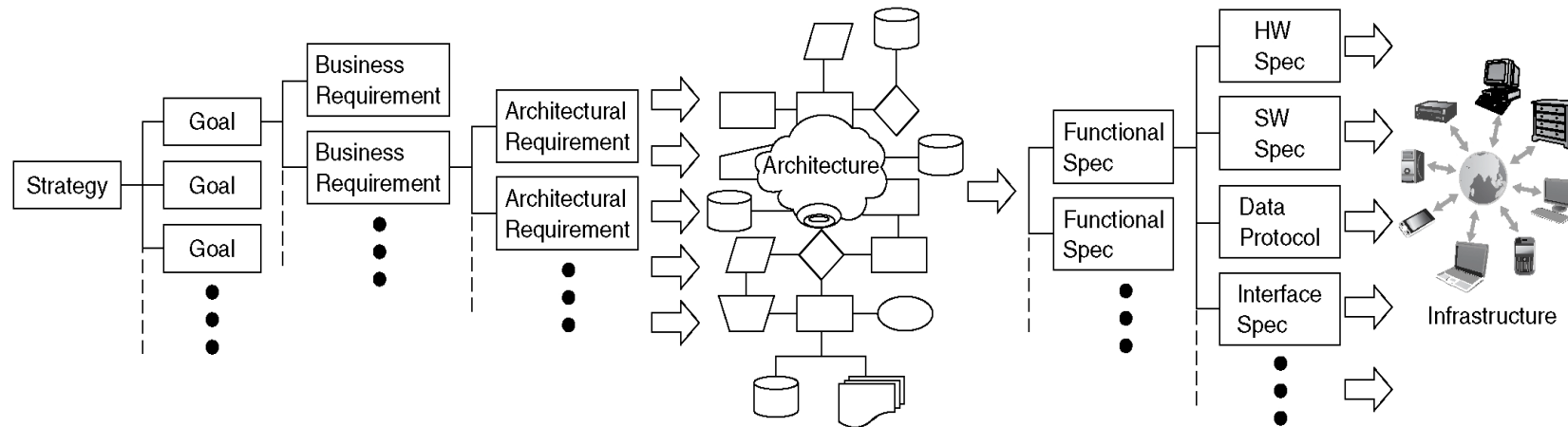
Developing a Cyber Security Business Strategy

- Questions to initiate a senior leadership discussion about cybersecurity if no strategy is in place:
 - Is your industry a key target (Financial)?
 - Do you maintain personal or credit card data on your systems?
 - Do you have valuable IP?
 - Do you have computer systems connected to the internet?
 - What are the potential costs & liabilities of a breach in cybersecurity (customers and suppliers)?
 - How much money do you have to spend on the problem?



"The global hub for educating, informing, and connecting Information Age leaders."

Build-in Cyber Security into Strategic Planning



Picture adapted from <https://geo-ide.noaa.gov/wiki/images/c/ca/Funnel.gif>

"The global hub for educating, informing, and connecting Information Age leaders."



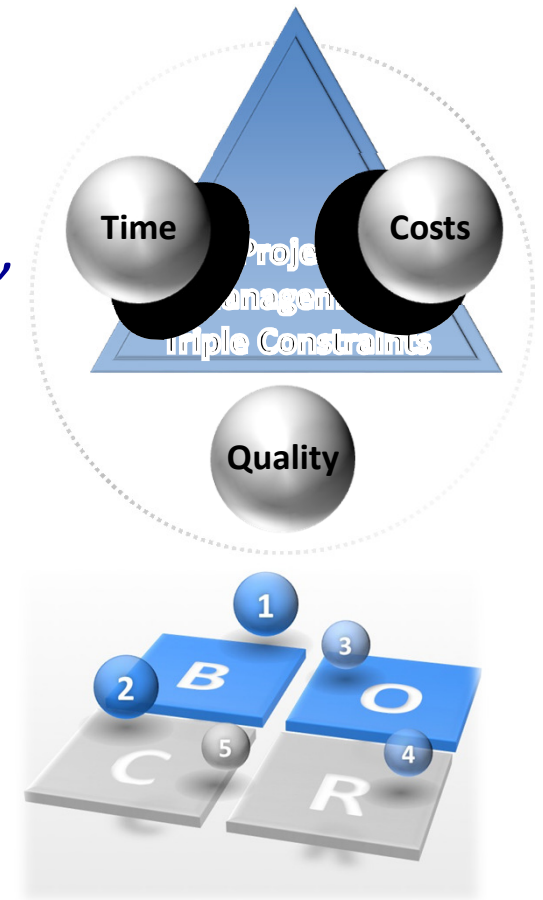
Build-In Cyber Security into your Project Management Processes

- Cobb's Paradox

“We know why projects fail; we know how to prevent their failure – so why do they still fail?”

- All Projects Are Risky
- Most Projects Include Unmanageable Risk
- Risk Management is Not Always Done Well
- Project Charters Often Omit Risk Thresholds
- Projects Should Exist in Risk-Balanced Portfolios
- Innovation is Built on Failure

Source: <http://pmworldjournal.net/wp-content/uploads/2013/01/PMWJ6-Jan2013-HILLSON-Resolving-Cobbs-Paradox-SeriesArticle.pdf>



Seek and Share Cybersecurity Knowledge

Government Guidance & Best Practices (FBI, DHS, & NIST)

FBI LIAISON ALERT SYSTEM
#M-000024-BT

(U) The following information was obtained through FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in **42 USC § 10607**.

(U) The FBI is providing the following information with **high confidence**:

SUMMARY

(U) Since September 2012, US financial institutions have been under coordinated and timed DDoS attacks. In total, **50 U.S. financial institutions** have been targeted in over 350 separate DDoS attacks with varying effects. The botnets used in the attacks, identified as "Brobrot" and "Kamikaze/Toxin" consist of compromised high bandwidth web servers with vulnerable content management systems. The compromised bots are infected through a vulnerable customer account. Once the customer account is accessed, attack scripts are uploaded to a hidden directory on the customer web site.

TECHNICAL DETAILS

(U) The FBI is providing 4,631 URLs (510 CONUS and 4,121 OCONUS), which have been observed receiving status updates or have participated in previous attacks. These URLs are located within the United States and worldwide. The FBI is distributing these indicators to enable network defense activities and reduce the risk of similar attacks in the future. The FBI has **high confidence** that these indicators were involved in past DDoS attacks or will be used in future attacks. The FBI recommends that your organization help victims identify and remove the malicious code.

URL	IP	LAST S	COUN	STATE	CITY	ISP
1 http://bradcoates.com/components/com_portfolio/includes/iphumb/	50.62.63.1	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
2 http://disher.net/components/com_portfolio/includes/iphumb/mo	50.63.123.1	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
3 http://www.cisaeo.com/ni/images/stories/semi.php	50.63.46.1	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
4 http://www.militarycontractorservices.com/iphumb/	208.109.46.127	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
5 http://www.paperjetika.com/components/com_portfolio/includes/	173.201.1.1	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
6 http://www.randellcompanies.com/components/com_portfolio/in	72.167.232.202	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
7 http://www.cisaeo.com/ni/images/stories/paginfo.php	50.63.46.1	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
8 http://www.cisaeo.com/ni/images/stories/paginfo.php	50.63.46.1	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
9 http://www.the3stopshop.com/images/stories/paginfo.php	97.74.144.119	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
10 http://www.the3stopshop.com/images/stories/paginfo.php	97.74.144.119	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
11 http://www.fu.ca/images/stories/paginfo.php	97.74.144.151	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
12 http://www.fu.ca/images/stories/paginfo.php	97.74.144.151	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
13 http://www.fu.ca/images/stories/paginfo.php	97.74.144.151	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
14 http://www.fu.ca/images/stories/paginfo.php	97.74.144.151	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
15 http://www.davidgwatercolors.com/images/stories/paginfo.php	50.62.100.1	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
16 http://www.genesalox.com/images/stories/paginfo.php	50.63.39.1	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
17 http://www.dakajw.com/ni/images/stories/paginfo.php	65.163.180.218	2014-01-21	US	AZ	Phoenix	Brinkster Communications Corporation
18 http://www.redsvetpa.org/images/stories/paginfo.php	72.167.232.143	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
19 http://www.seznetworld.com/images/stories/paginfo.php	72.167.232.188	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
20 http://www.crea.com/ni/images/stories/paginfo.php	72.167.232.188	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
21 http://www.charlievetliner.com/images/stories/paginfo.php	72.167.232.190	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
22 http://www.charlievetliner.com/images/stories/paginfo.php	72.167.232.190	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
23 http://www.charlievetliner.com/images/stories/paginfo.php	72.167.232.190	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
24 http://www.charlievetliner.com/images/stories/paginfo.php	72.167.232.190	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
25 http://www.charlievetliner.com/images/stories/paginfo.php	72.167.232.190	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
26 http://www.charlievetliner.com/images/stories/paginfo.php	72.167.232.190	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
27 http://www.charlievetliner.com/images/stories/paginfo.php	72.167.232.190	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
28 http://www.charlievetliner.com/images/stories/paginfo.php	72.167.232.190	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
29 http://www.charlievetliner.com/images/stories/paginfo.php	72.167.232.190	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
30 http://www.charlievetliner.com/images/stories/paginfo.php	72.167.232.190	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
31 http://www.charlievetliner.com/images/stories/paginfo.php	72.167.232.190	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
32 http://www.charlievetliner.com/images/stories/paginfo.php	72.167.232.190	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC
33 http://www.charlievetliner.com/images/stories/paginfo.php	72.167.232.190	2014-01-21	US	AZ	Scottsdale	GoDaddy.com, LLC

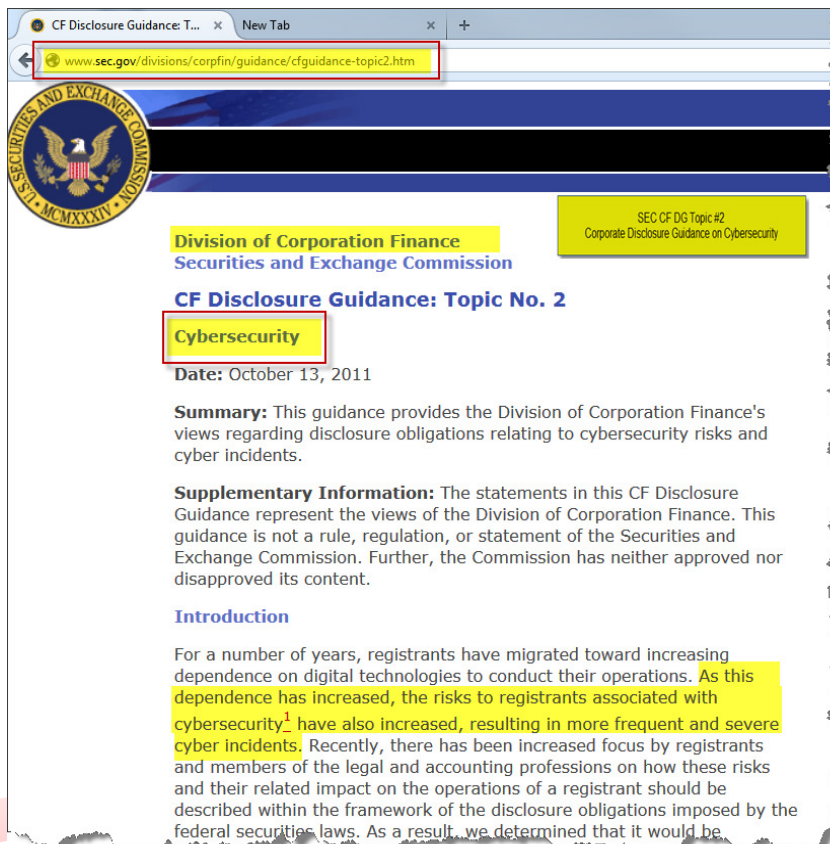
"The global hub for educating, informing, and connecting Information Age leaders."



SEC Recommendations of Cybersecurity

Risk Communications

SEC CF DG 2: *This guidance is not a rule”...but it is applied as if it were*



The screenshot shows a web browser window with the URL www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. The page header includes the SEC logo and the text "Division of Corporation Finance Securities and Exchange Commission". The main heading is "CF Disclosure Guidance: Topic No. 2 Cybersecurity", dated October 13, 2011. The summary states: "This guidance provides the Division of Corporation Finance's views regarding disclosure obligations relating to cybersecurity risks and cyber incidents." The supplementary information notes that the guidance is not a rule and that the Commission has neither approved nor disapproved its content. The introduction begins with: "For a number of years, registrants have migrated toward increasing dependence on digital technologies to conduct their operations. As this dependence has increased, the risks to registrants associated with cybersecurity¹ have also increased, resulting in more frequent and severe cyber incidents." The text continues: "Recently, there has been increased focus by registrants and members of the legal and accounting professions on how these risks and their related impact on the operations of a registrant should be described within the framework of the disclosure obligations imposed by the federal securities laws. As a result, we determined that it would be..."

Recommends Disclosures in Six Areas:

- Management’s Discussion and Analysis of financial conditions and results of operations
- Description of Business
- Legal Proceedings
- Financial statements disclosures
- Disclosures controls and procedures
- Mechanisms: Annual report Form 10-K | Quarterly report 10-Q | Current report 8-K



“The global hub for educating, informing, and connecting Information Age leaders.”

(COBIT) - Control Objectives for Information and Related Technology



- COBIT is an IT governance framework that:
 - focus on making sure that IT provides the systematic rigor needed for external compliance.
 - provide a framework for linking IT processes, IT resources, and IT information to a company's strategies and objectives.
- Information Systems **A**udit & **C**ontrol **A**ssociation (ISACA) issued COBIT in 1996 (Strong IT Auditing Guidance).
- COBIT provides a set of process goals, metrics, and practices.
 - Risk categorized into four major domains: planning and organization, acquisition and implementation, delivery and support, or monitoring.
 - The company determines the processes that are the most susceptible to the **risks** that it chooses to manage.



"The global hub for educating, informing, and connecting Information Age leaders."

Develop an Organizing a Cybersecurity Strategy National Institute of Standards and Technology Framework

NIST Framework of Core Functions

- Five High-Level Functions—Identify, Protect, Detect, Respond, Recover.
- When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risks.

Functions Defined

- Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event
- Respond – Develop and implement the appropriate activities to take action regarding a detected cyber security event.
- Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.



Source: <http://www.nist.gov/cyberframework/>



"The global hub for educating, informing, and connecting Information Age leaders."

Skills Gap = Talent (People) Shortage



- *“At the pace we’re training our digital soldiers, government and the private sector won’t be working together to secure the country – they will be too busy fighting each other for what little manpower’s coming out of the university system.” ~ Brian Fung, National Journal, May 2013*

UNITED STATES SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 8-K

CURRENT REPORT
Pursuant to Section 13 or 15(d)
of the Securities Exchange Act of 1934

Date of Report (date of earliest event reported): October 2, 2014

JPMorgan Chase & Co.
(Name of registrant as specified in its charter)

270 Park Avenue, New York, New York 10022
JPMorgan Chase & Co. (NYSE:JPM)

- (WSJ - October 2014) J.P. Morgan Chase & Co. Chairman and Chief Executive, James Dimon, the *“the bank would double spending on cyber security over the next five years.”*

Form 8-K

Item 7.01 Regulation FD Disclosure.

On October 2, 2014, JPMorgan Chase & Co. (“JPMorgan Chase” or the “Firm”) updated information for its customers, on its Chase.com and JPMorganOnline websites and on the Chase and J.P. Morgan mobile applications, about the previously disclosed cyberattack against the Firm. The Firm disclosed that:

- User contact information – name, address, phone number and email address – and internal JPMorgan Chase information relating to such users have been compromised.
- The compromised data impacts approximately 76 million households and 7 million small businesses.
- However, there is no evidence that account information for such affected customers – account numbers, passwords, user IDs, dates of birth or Social Security numbers – was compromised during this attack.
- As of such date, the Firm continues not to have seen any unusual customer fraud related to this incident.
- JPMorgan Chase customers are not liable for unauthorized transactions on their account that they promptly alert the Firm to.

The Firm continues to vigilantly monitor the situation and is continuing to investigate the matter. In addition, the Firm is fully cooperating with government agencies in connection with their investigations.

This Current Report on Form 8-K contains forward-looking statements within the meaning of the Private Securities Litigation Reform Act of 1995. These statements are based on the current beliefs and expectations of JPMorgan Chase & Co.’s management and are subject to significant risks and uncertainties. Actual results may differ from those set forth in the forward-looking statements. Factors that could cause JPMorgan Chase and Co.’s actual results to differ materially from those described in the forward-looking statements can be found in JPMorgan Chase & Co.’s Annual Report on Form 10-K for the year ended December 31, 2013, and Quarterly Reports on Form 10-Q for the quarters ended March 31, 2014 and June 30, 2014, which have been filed with the Securities and Exchange Commission and are available on JPMorgan Chase’s website (<http://investor.shareholder.com/jpmorganchase>) and on the Securities and Exchange Commission’s website (www.sec.gov). JPMorgan Chase & Co. is not providing any assurance that the information disclosed in this Current Report on Form 8-K is accurate, complete or current.

“The global hub for educating, informing, and connecting Information Age leaders.”

Questions?

Dr. Mike Donohoe

DonohoeDSc@Pitt.edu

Dr. Russ Mattern

matternr@ndu.edu



"The global hub for educating, informing, and connecting Information Age leaders."