LOYOLA MARYMOUNT UNIVERSITY

Cyber Threats and Security

System Thinking
Eve Huang
April 2016

Agenda

I. Common Good
II. Define Problem
III. Unstructured & Structured Problem
IV. Define the System & Boundary
V. System Graphic
VI. Stakeholder Interaction
VII. Root Definition
VIII. Root Definition Graphic
IX. Conceptual Model
X. Unintended Consequences
XI. Big Questions

Introduction

- "Cyber threats cover a wide range of malicious activity that can occur through cyberspace," - Caitlin Hayden, spokeswoman for the White House National Security Council.
  - Such threats include web site defacement, espionage, theft of intellectual property, denial of service attacks, and destructive malware.

- Cybersecurity are measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack

Franzen, C. (2013, 02 14). *White House says 'cyber threats' include web site defacement, IP theft.* Retrieved 04 02, 2016, from The Verge: http://www.theverge.com/2013/2/14/3989686/white-house-says-cyber-threats-include-web-site-defacement-ip-theft

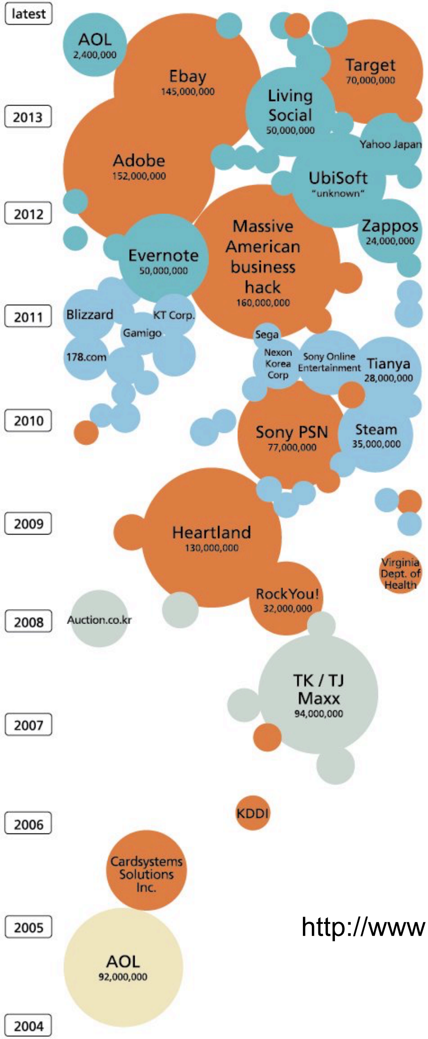
http://blog.willis.com/2015/07/us-industry-and-government-collaborate-to-address-cyber-risks/

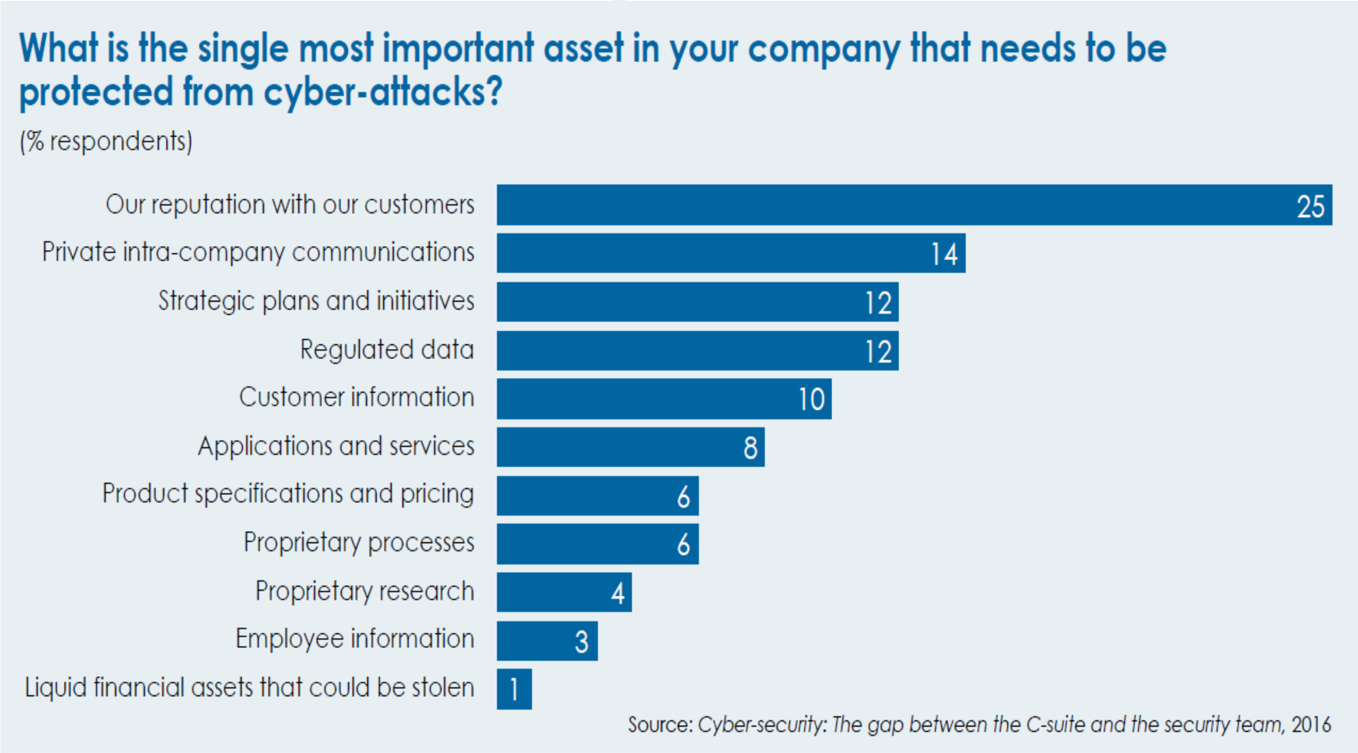
Introduction-Hacked History

- **The Morris Worm 1988:**
  - Robert Tappan Morris created the first computer worm transmitted through internet. Not intended to be harmful but morphed into a virus and infected 6000 computers. $10-$1000 million dollars in repair costs.
- **NASA & US Defense Department Hacked 1999**
  - Jonathan James was 15, installed a backdoor on US Defense system servers. He was able to retrieve emails, login names and passwords for high profile military computers. Shut down NASA computer systems after stealing classified information. Committed suicide in 2008
- **MafiaBoy 2000:**
  - 15 year old Michael Calce, unleashed a DDoS attack on Amazon, CNN, eBay and Yahoo. Estimated 1.2 Billion in damage costs.
- **The Internet Hack 2002:**
  - Cyber attack aimed at all 13 domain name system's in the United States. DDoS attack that lasted 1 hour. Described as the largest and most complex in history at the time. Would have literally stopped the internet if it lasted any longer.

Source: "Top 10 Most Notorious Cyber Attacks in History." *ARN*. N.p., n.d. Web.

Companies Affected



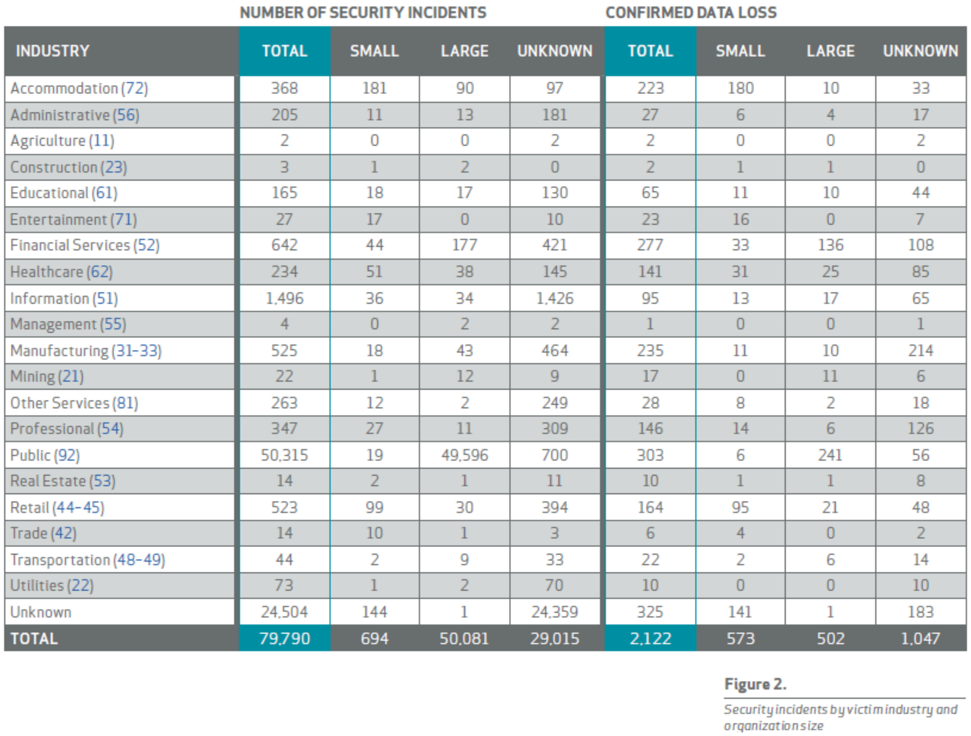


What is the single most important asset in your company that needs to be protected from cyber-attacks?

(% respondents)

Source: *Cyber-security: The gap between the C-suite and the security team*, 2016

http://www.businessinsider.com/heres-how-big-the-most-recent-hacking-data-breaches-have-been-2014-10



	NUMBER OF SECURITY INCIDENTS				CONFIRMED DATA LOSS			
INDUSTRY	TOTAL	SMALL	LARGE	UNKNOWN	TOTAL	SMALL	LARGE	UNKNOWN
Accommodation (72)	368	181	90	97	223	180	10	33
Administrative (56)	205	11	13	181	27	6	4	17
Agriculture (11)	2	0	0	2	2	0	0	2
Construction (23)	3	1	2	0	2	1	1	0
Educational (61)	165	18	17	130	65	11	10	44
Entertainment (71)	27	17	0	10	23	16	0	7
Financial Services (52)	642	44	177	421	277	33	136	108
Healthcare (62)	234	51	38	145	141	31	25	85
Information (51)	1,496	36	34	1,426	95	13	17	65
Management (55)	4	0	2	2	1	0	0	1
Manufacturing (31–33)	525	18	43	464	235	11	10	214
Mining (21)	22	1	12	9	17	0	11	6
Other Services (81)	263	12	2	249	28	8	2	18
Professional (54)	347	27	11	309	146	14	6	126
Public (92)	50,315	19	49,596	700	303	6	241	56
Real Estate (53)	14	2	1	11	10	1	1	8
Retail (44–45)	523	99	30	394	164	95	21	48
Trade (42)	14	10	1	3	6	4	0	2
Transportation (48–49)	44	2	9	33	22	2	6	14
Utilities (22)	73	1	2	70	10	0	0	10
Unknown	24,504	144	1	24,359	325	141	1	183
TOTAL	79,790	694	50,081	29,015	2,122	573	502	1,047

Figure 2.

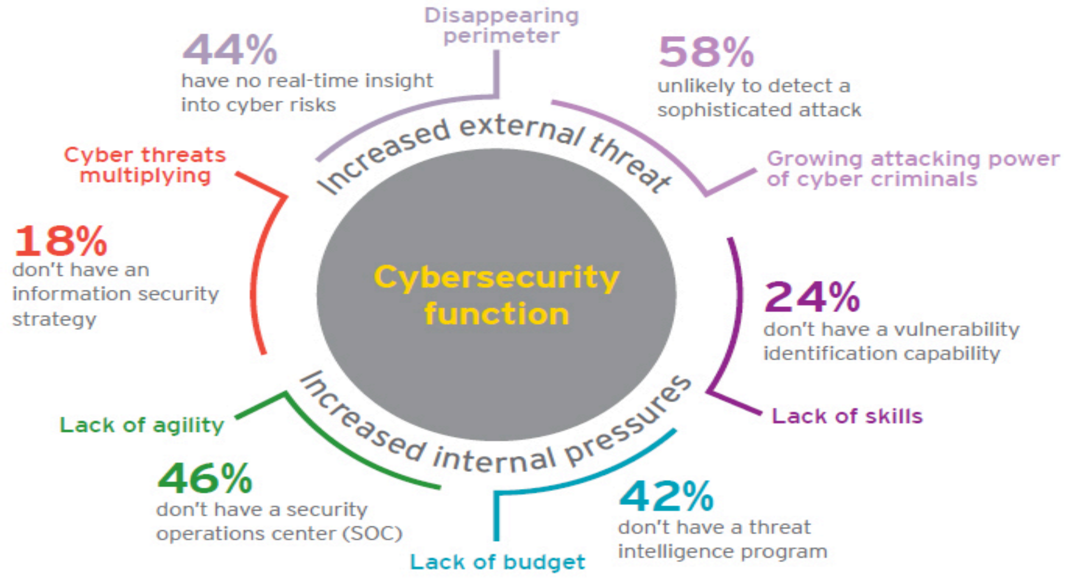
Security incidents by victim industry and organization size

- The top three industries affected in 2015 are the same as previous years:
  - Public
  - Information
  - Financial Services

Verizon Enterprise 2015 Data Breach Investigations Report: Explore related resources. http://www.verizonenterprise.com/DBIR/2015/resources/#Industry

Define Problem

The rapidly expanding cyber threat landscape

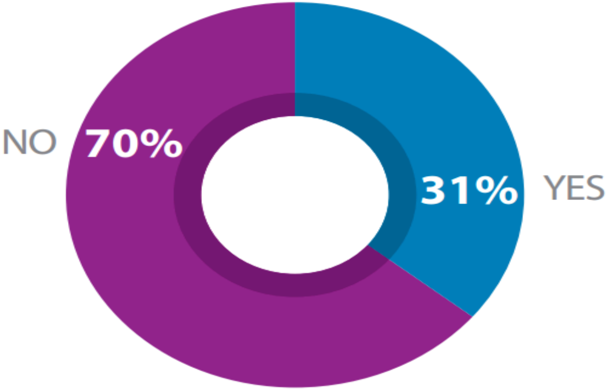

Disappearing perimeter
44%
have no real-time insight into cyber risks
58%
unlikely to detect a sophisticated attack
Increased external threat
Cyber threats multiplying
Growing attacking power of cyber criminals
18%
don't have an information security strategy
Cybersecurity function
24%
don't have a vulnerability identification capability
Increased internal pressures
Lack of agility
Lack of skills
46%
don't have a security operations center (SOC)
42%
don't have a threat intelligence program
Lack of budget

- An unavoidable problem.
- Threatens companies, individuals, and Government agencies
- Continually transforming
- Lack of funding towards security resources
- Results in huge financial damage
- Results in physical damage (hacked medical devices)
- Weak protection efforts

"Cyber-Security in Metals and Mining - Emerson Process Experts."*Emerson Process Experts RSS*. N.p., 20 July 2015.

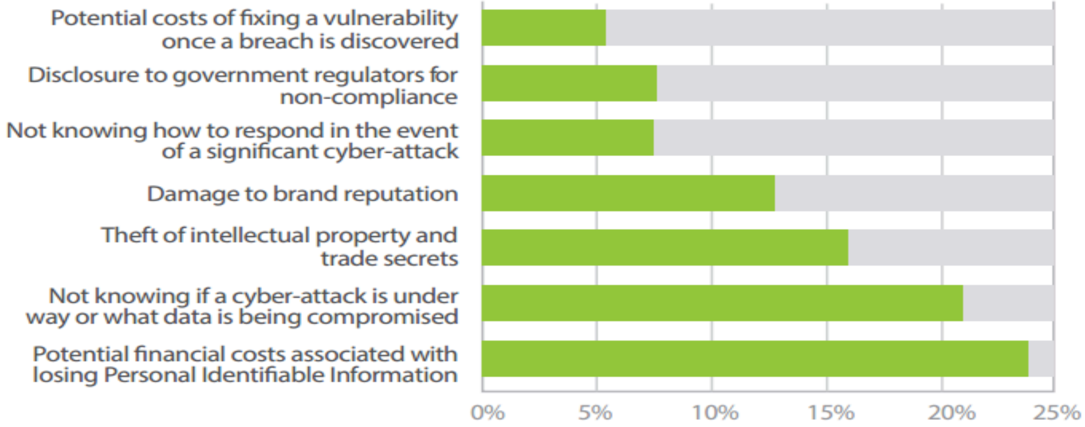
What the Public Thinks

DO ENTERPRISES DO ENOUGH?



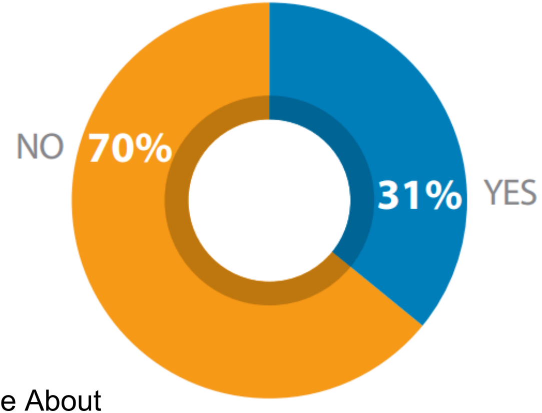
Consumers aren't confident that enterprises are adequately protecting their personal information.

TOP CYBER CONCERNS



The potential costs of losing customers' personal information in a data breach weighs heaviest on the minds of enterprise executives.

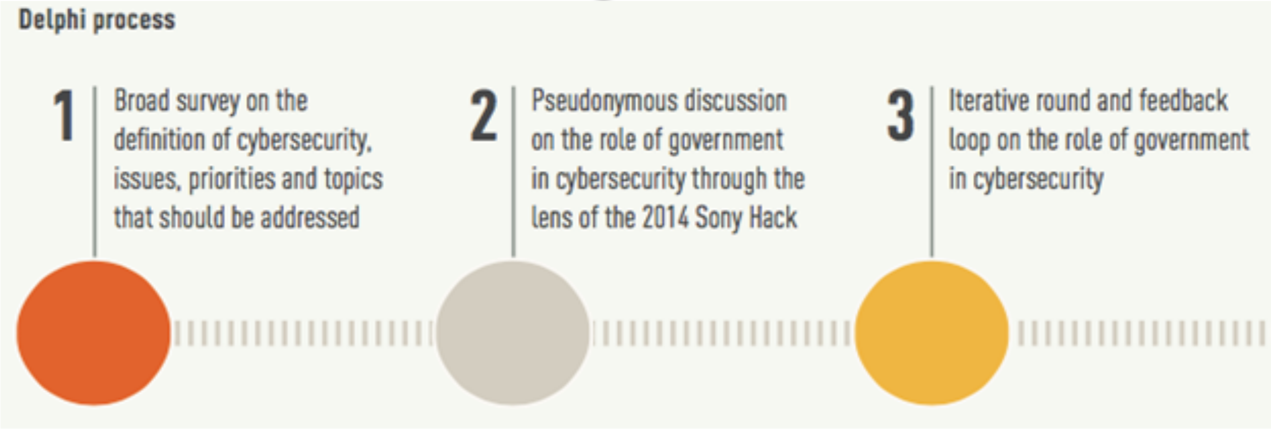
SHOULD THE GOVERNMENT TELL COMPANIES HOW TO HANDLE DATA?



Consumers don't want the government dictating how private enterprises store and control their data.

"Study: Enterprise Executives and Consumers Lack Confidence About Cybersecurity." *ThreatTrack Security*. N.p., n.d. Web.

Define Problem - Expert Recommendations on CybSecurity



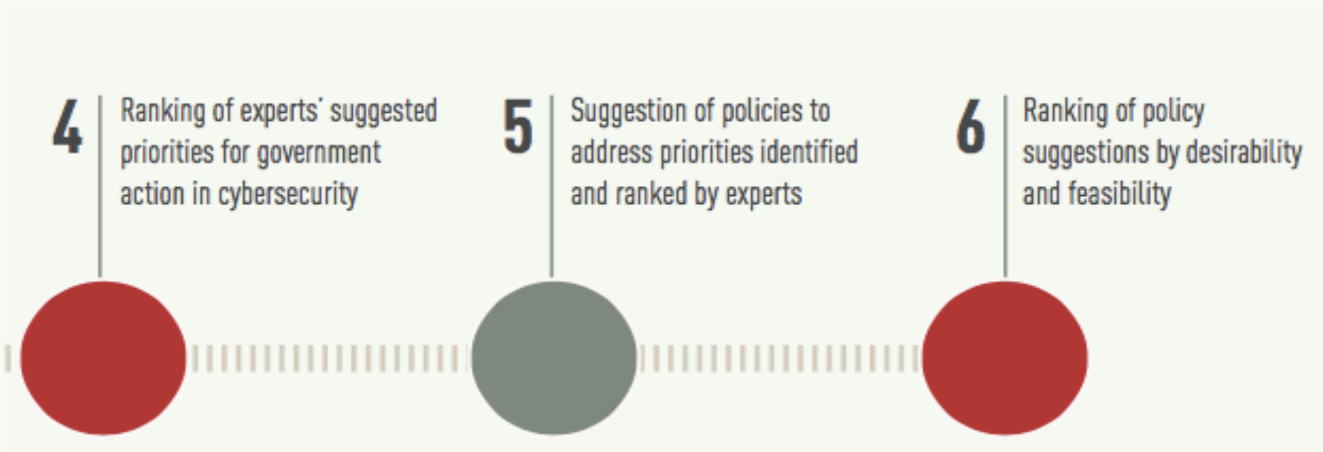
Delphi process

1 Broad survey on the definition of cybersecurity, issues, priorities and topics that should be addressed

2 Pseudonymous discussion on the role of government in cybersecurity through the lens of the 2014 Sony Hack

3 Iterative round and feedback loop on the role of government in cybersecurity

"Experts Develop Cybersecurity Recommendations." *Open Policy Advocacy RSS*. N.p., n.d. Web.

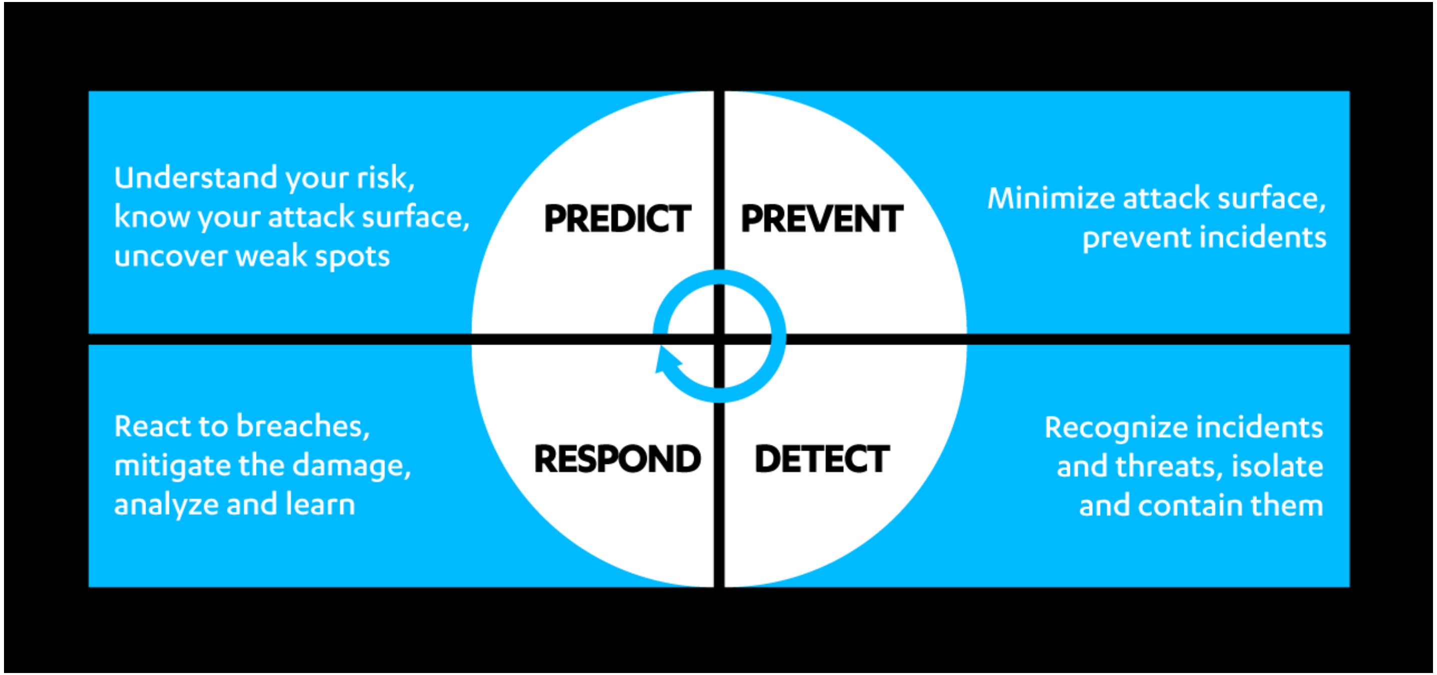


4 Ranking of experts' suggested priorities for government action in cybersecurity

5 Suggestion of policies to address priorities identified and ranked by experts

6 Ranking of policy suggestions by desirability and feasibility

Define Problem - Expert Recommendations on Cyber Security



Understand your risk, know your attack surface, uncover weak spots

PREDICT

PREVENT

Minimize attack surface, prevent incidents

React to breaches, mitigate the damage, analyze and learn

RESPOND

DETECT

Recognize incidents and threats, isolate and contain them

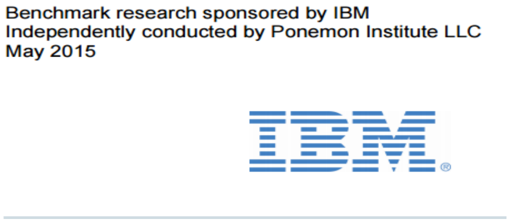
“There are 2 types of companies: those that have been breached and those who do not know it yet.”

- "The 360 Degree Approach to Cyber security." *Business Security Insider by FSecure*. N.p.,

Common Good

Cyber attacks are expensive,
Cyber threats affect a large population

- In 2014, 47% of american adults had personal information stolen
- Data breaches increased by 62% from 2012 to 2013
- Total added up to $18,000,000,000 in credit card fraud in 2013



Benchmark research sponsored by IBM
Independently conducted by Ponemon Institute LLC
May 2015

http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03053wwen/SEW03053WWEN.PDF?

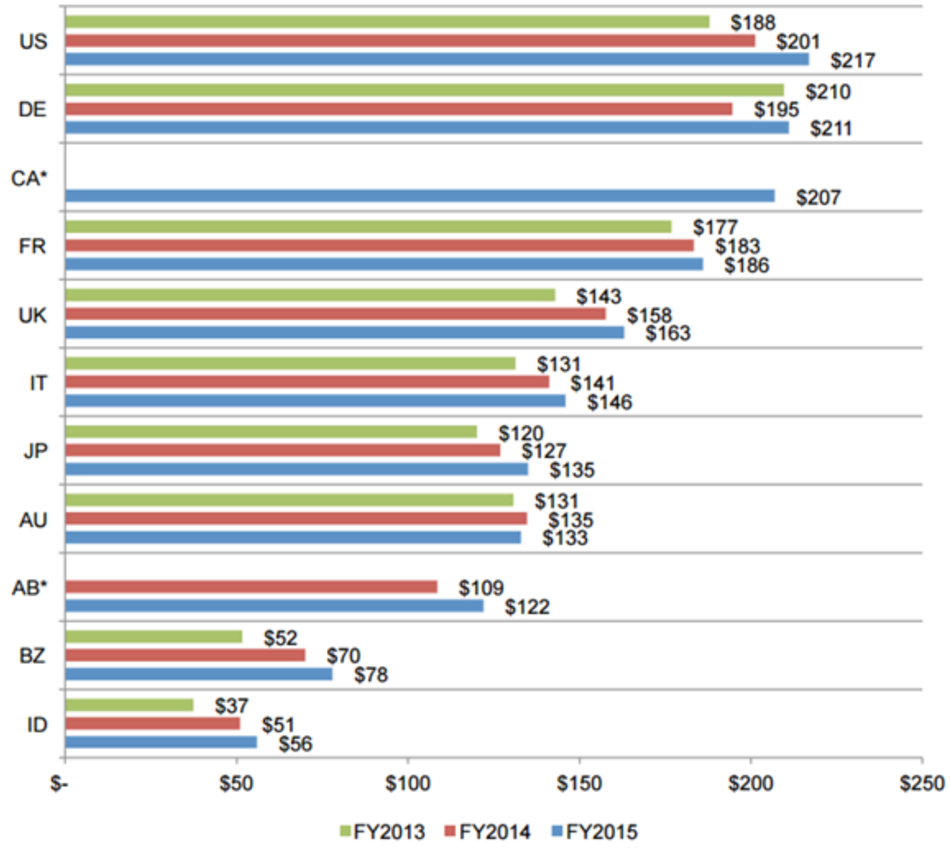
Common Good

- Study of 350 companies in 11 countries
- Cost is calculated from direct and indirect expenses
  - Loss of business, forensics cost

Data Breach: defined as an event where an individual’s name and medical/financial record or credit card is put at risk

- Data breaches cost the most in the US and Germany
  - Average per capita cost of data breach: $217 in the US, $211 in Germany
- The cost of data breach varies by industry
  - Average global cost is $154
  - Healthcare average cost is $363, Education is $300
- Hackers and criminal insiders cause the most data breaches
  - 47% of breaches are malicious or criminal attacks
- Certain countries are more likely to have a data breach
  - Brazil and France are most likely to have a data breach
  - Canada and Germany are least likely

Figure 1. The average per capita cost of data breach over three years
*Historical data is not available
Consolidated view (FY 2015 = 350, FY 2014 = 315, FY 2013 = 277)
Measured in US$



- Gradual cost increase
- Average in 2015: $154
- Average in 2014: $145

Unstructured & Structured Problem

Unstructured Problem

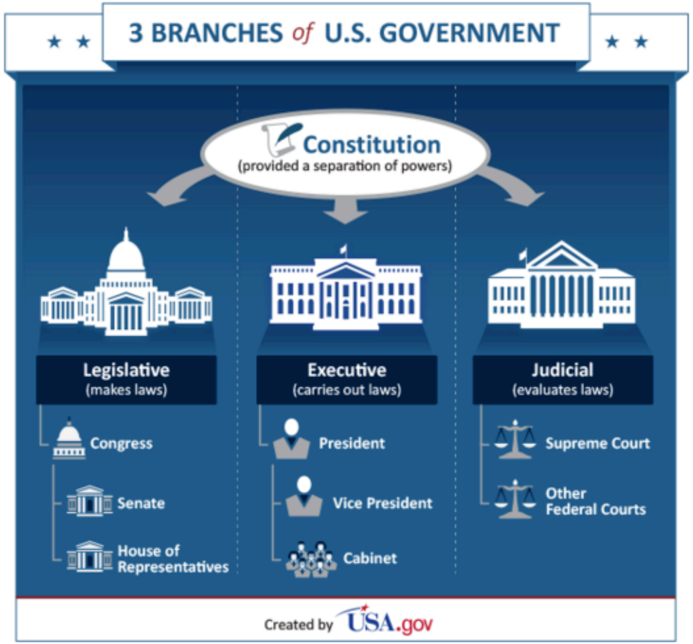
The United States is the country with the highest rate of cybercrime. Americans and other non-British English speakers still produce the most malware, more than a third of the world's total.

Structured Problem

The United States 2016 cybersecurity budget is $14 billion, but cybersecurity spending does not mean that all agencies have benefited equally. Experts say that, "the security industry needs to attract the attention of government authorities, educate users and encourage changes in basic operating systems," for everyone to benefit.

- http://www.forbes.com/2007/07/13/cybercrime-world-regions-tech-cx_ag_0716cybercrime.html

Define System and Boundary


3 BRANCHES of U.S. GOVERNMENT

Constitution
(provided a separation of powers)

Legislative
(makes laws)
- Congress
  - Senate
  - House of Representatives

Executive
(carries out laws)
- President
- Vice President
- Cabinet

Judicial
(evaluates laws)
- Supreme Court
- Other Federal Courts

Created by USA.gov

Boundary:

WHO:

- United States

WHAT:

- Hacking/Unauthorize
Systems & Database

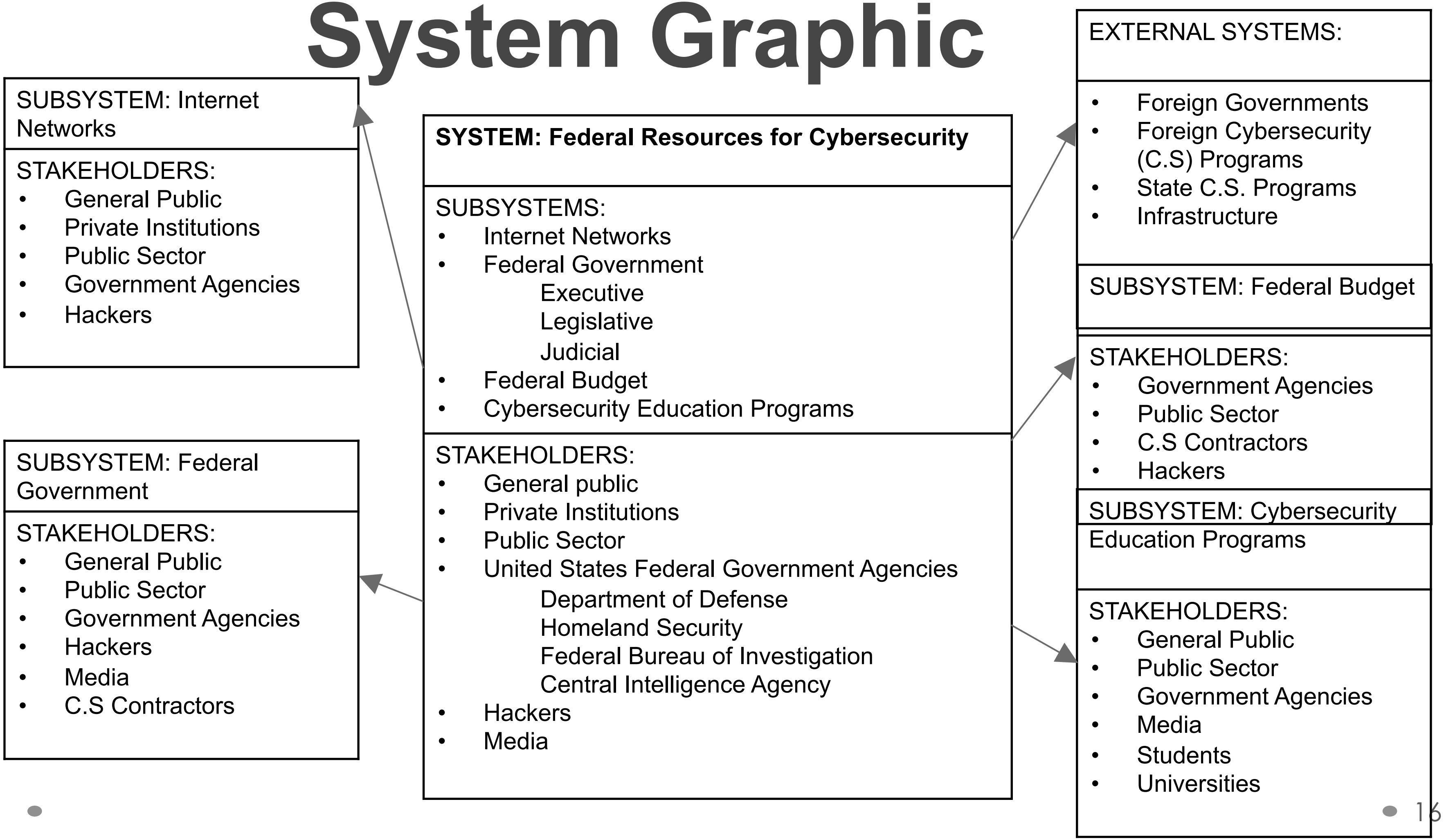
HOW:

- Funding
- Legislation
- Education
- Technical Resources

http://www.businessinsider.com/nsa-trained-snowden-to-hack-2013-7

System: Federal Resources for Cybersecurity

System Graphic



SUBSYSTEM: Internet Networks

STAKEHOLDERS:
- General Public
- Private Institutions
- Public Sector
- Government Agencies
- Hackers

SUBSYSTEM: Federal Government

STAKEHOLDERS:
- General Public
- Public Sector
- Government Agencies
- Hackers
- Media
- C.S Contractors

SYSTEM: Federal Resources for Cybersecurity

SUBSYSTEMS:
- Internet Networks
- Federal Government
  - Executive
  - Legislative
  - Judicial
- Federal Budget
- Cybersecurity Education Programs

STAKEHOLDERS:
- General public
- Private Institutions
- Public Sector
- United States Federal Government Agencies
  - Department of Defense
  - Homeland Security
  - Federal Bureau of Investigation
  - Central Intelligence Agency
- Hackers
- Media

EXTERNAL SYSTEMS:
- Foreign Governments
- Foreign Cybersecurity (C.S) Programs
- State C.S. Programs
- Infrastructure

SUBSYSTEM: Federal Budget

STAKEHOLDERS:
- Government Agencies
- Public Sector
- C.S Contractors
- Hackers

SUBSYSTEM: Cybersecurity Education Programs

STAKEHOLDERS:
- General Public
- Public Sector
- Government Agencies
- Media
- Students
- Universities

Stakeholder Interactions-U.S. Citizens

- Cyber Crime: Any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them
- The Patriot Act: Permits government surveillance through electronic records without notifying the suspect. Allows victims of hackers to receive government assistance.
- The current penalties for committing acts of cybercrime are 6 months in prison and $1,000 fine to 20 years in prison and $15,000 fine.

https://www.justice.gov/archive/ll/highlights.htm
https://www.cga.ct.gov/2012/rpt/2012-R-0254.htm
http://cybercrime.org.za/definition

Stakeholder Interactions: Government Agencies

- Department of Defense-must defend it's own network, system and info; defend the United States against cyber attacks; support military operations. Invests money in improving education and training for C.S
- Homeland Security-Works with other agencies to deal with cyber crimes
  - U.S Secret Service-focuses on cyber intrusions, bank fraud, data breaches, and other computer crimes
  - U.S Immigration and Customs Enforcement-focus on cyber crimes both domestic and international in cross-border crimes
- National Security Agency-in charge of domestic internet surveillance

- http://webpolicy.org/2015/06/04/nsa-cybersecurity/
https://www.dhs.gov/topic/combating-cyber-crime
http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Obama's Cyber Security National Action Plan

What can we do now?

- FY 2017 $19 billion budget for cybersecurity
- Dept. of Justice (including FBI) increasing funding for cybersecurity by 23%
- Cyber Mission Force
- Establish Commission on Enhancing National Security
- Educating Public

How do we better prepare for the future?

- Educating Next Generation of Cyber Warriors
  - CyberCorps Reserve program: scholarships for Americans who want a cybersecurity education and to work for the Federal govt
  - National Centers for Academic Excellence In Cybersecurity Program: Supports institutions that offer education in cybersecurity
  - Student loan forgiveness programs for cybersecurity experts joining Federal workforce

https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

Cybersecurity Funding Solutions

- Ballot Initiatives to Increase funds to Cybersecurity
  - Shifting funds from overspent military programs
  - (Increasing taxes)
  - Establish corporation tax for US Cybersecurity Administration
    - Protect Banking, Infrastructure
- Repurpose employees/ departments/ projects
  - Unneeded Departments of DOD, FBI, Homeland security etc.
  - E.g. F-35, Lockheed Martin Company; Tanker Programs
  - Many contracting companies have experience in cybersecurity services

https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

Solutions: Shifting Funds

DOD Budget $587 billion. $175.9 billion for other defense-related agencies and functions

The table below shows some of the areas the DOD budget goes towards.

Area/ Issue/ Projects	Budget
Counter Terrorism -Counter ISIL -ISIR air fleet	-$7.5 billion 50% increase from 2016 -$1.2 billion
Countering Russian aggression	- $3 billion, quadrupling from 2016
Cyberthreats	- $6.7 billion
F-35 (Lockheed Martin) http://useconomy.about.com/od/usfederalbudget/p/military_budget.htm	The budget includes $10.1 billion in FY 2017 for F-35s across the force The Air Force cut five F-35s in the FY 2017 budget approx $1 billion.

Solutions: Top Defense Contractors

2015	Company	Contracts	2014
1	Lockheed Martin	$11,700,962,000	1
2	Northrop Grumman	$6,893,607,000	2
3	Boeing Co.	$5,256,827,000	4
4	Raytheon	$4,815,472,000	3
5	General Dynamics	$4,071,992,000	5
6	Hewlett-Packard Co.	$3,866,791,000	6
7	Booz Allen Hamilton	$3,665,860,000	7
8	Science Applications International Corp.	$2,570,645,000	19
9	Harris Corp.	$2,552,193,000	12
10	Computer Sciences Corp.	$2,379,495,000	9
11	Verizon Communications	2,029,767,000	14
12	CACI International	$2,011,349,000	13

- Largest government contractors by their prime contract dollars in IT, systems integrations, telecommunications, engineering and professional services.
- 2015 Top 100 with aggregate of **$98.5 billion**
- Peaked in 2011 Top 100 with aggregate of **$132 billion**

https://washingtontechnology.com/toplists/top-100-lists/2015.aspx

Solutions:Defense Contractors

(e.g. Lockheed Martin Company)

- Already have experience in cybersecurity
- They already offer
  - Assessments
  - Products
  - Services e.g. cybersecurity consulting
  - Training
- Funds from the F-35 project could be diverted to their cybersecurity division
  - Provide training to employees for government organizations
  - Improve training programme to gain market competitiveness in education of cybersecurity

http://lockheedmartin.com

Solutions: Cybersecurity industry

- Fastest Growing Tech Sector
- Estimated $77 billion market (2015)
- Estimated to grow to $170 billion by 2020
- More than 200,000 US cybersecurity jobs are unfilled (2015)
- Shortage is expected to reach 1.5 million by 2019
- Corporate investors and VC firms have invested several hundred-million dollar plus funds for cybersecurity startups

http://www.forbes.com/sites/stevemorgan/2015/10/16/the-business-of-cybersecurity-2015-market-size-cyber-crime-employment-and-industry-statistics/#583b68aa10b2

Solutions: the Funds

- Campaigns increasing awareness and persuading people
- Educating
  - Individual protection
  - Training people in Cybersecurity
- Centralize main agency for Cybersecurity
- Cyber security departments
  - State level - "2014 Deloitte-NASCIO cybersecurity study, which found that nine of 10 state IT officials surveyed reported that the biggest barrier to attracting cybersecurity talent is salary, which generally can't match that offered by private industry."
  - Public organizations: FBI, Homeland Security, DOD
- Cyber Threats Emergency Response System
  - Creating team such as "Commission on Enhancing national security" to create a plan for the prevention of and response to cyber attacks. It is important that breaches are detected quickly and are responded to quickly. It is essential that the system can recover quickly.

http://www.govtech.com/security/Hiring-Cybersecurity-Staff-Is-Hard-for-States.html

Solutions: Media/ Campaigns/ Non-profits

- Needed to persuade people that increasing taxes is important
- Campaigning to individuals
  - Educating them about the risks
  - Increasing awareness about cybersecurity
  - Build actionable awareness
- Campaigning to institutions
  - Costs of cyberattacks/ hacks
  - SBA - offer training to over 1.4 million small businesses

https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

Solutions: Integration of Government, Public Sector and Private Sector

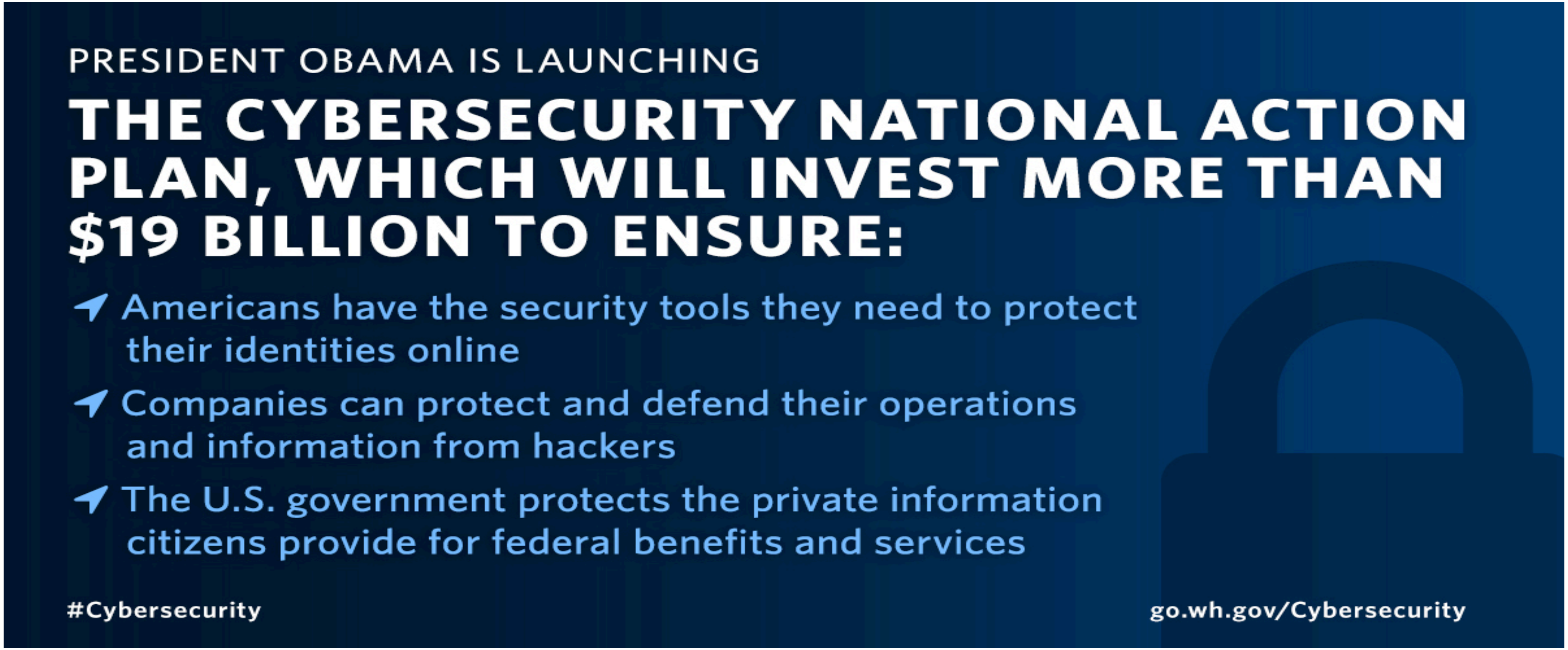
- Importance of communication e.g. Sony Hack
  - According to NY Times, government was warned of hack months before, but did not alert Sony
- Partnerships/ teams connecting people in government, public sector and private sector
- Implement more industry-to-government partnerships similar to InfraGard
  - Establish information database
  - Reduce liability sharing issues (reform laws)
  - Share information more timely

http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html

Root Definition

C = Customer: Beneficiaries and Victims

Beneficiaries: American Citizens/ Companies, Corporations/ The U.S government



PRESIDENT OBAMA IS LAUNCHING

THE CYBERSECURITY NATIONAL ACTION PLAN, WHICH WILL INVEST MORE THAN $19 BILLION TO ENSURE:

- Americans have the security tools they need to protect their identities online
- Companies can protect and defend their operations and information from hackers
- The U.S. government protects the private information citizens provide for federal benefits and services

#Cybersecurity

go.wh.gov/Cybersecurity

https://www.whitehouse.gov/blog/2016/02/09/presidents-national-cybersecurity-plan-what-you-need-know

Root Definition

C = Customer: Beneficiaries and Victims

Victims: Cyber Criminals/ Cyber Hackers/ The terrorist

http://nationalcybersecurity.com/hackers-double-their-attacks-against-south-africans/

WisdomTimes.com

http://blog.oureducation.in/cyber-crime/

Root Definition

A = Actors who make things happen

Actors: The U.S. government/ Cyber Security Organizations/ Cyber Security Experts/ Cyber Security Corporations/ Defense Contractors/ Schools, Institutions

CSS:
Central Security
Service

NSA:
National Security
Agency

United States
Cyber
Command

http://www.gettyimages.com/detail/news-photo/the-seals-of-the-u-s-cyber-command-the-national-secrity-news-photo/466108378

T = input - output transformation process

1. Input

1) Cyber Security Funding and Organizations

2) U.S Government establish Cyber actions, legislations

3) Cyber Security Educations

2 . Transformation

1) More secure databases

2) More Experts, Laws

3) Cyber Security Corporations, system

3. Improvement/ Output

1) A relatively perfect Cyber Legislations System

2) A stronger national Defense Cyber System

3) A Cyber Threats Emergency Response System

4) A cyber criminal Center: Cyber Police, Database, etc

5) Less Cyber Crimes, Threats, Criminals, Hackers, Terrorist

https://tawkster.att.com/conference/2013/

Root Definition

V = viewpoint, or aspect of common goods

Clean Cyber Environment

Less Cyber Crimes, Threats

Less Cyber Criminals, Terrorists

Less Economic Risk

Less Homeland Security Risk

V

O = system owners

The U.S government,

Cyber Security Organizations,

Cyber Security Corporations

O

E = environmental (external) constraints

Development of the Internet

Technology

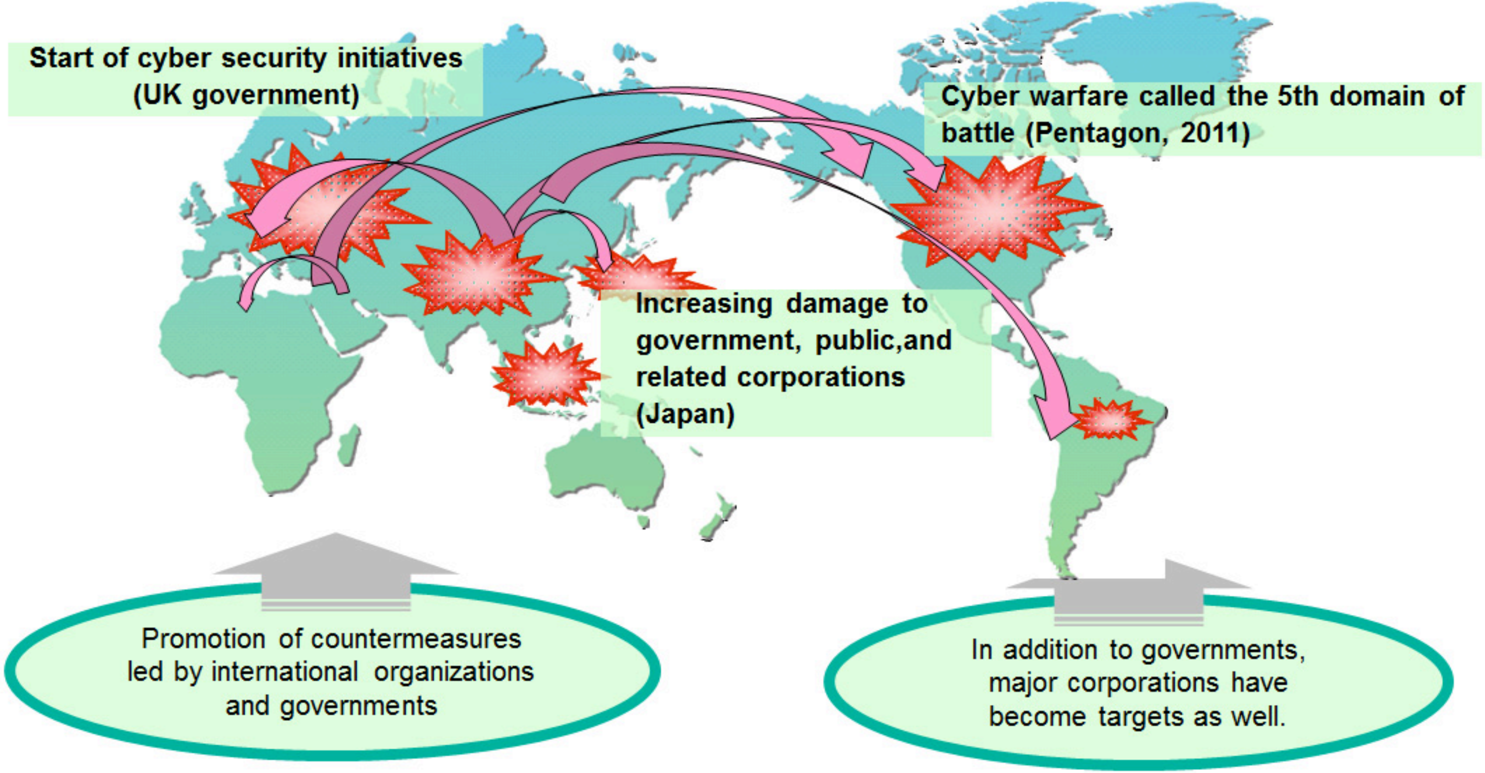
Relationships between Great-Power countries

Nation’s Economy

Politics

E

E = environmental (external): Relationships Between big Country



Start of cyber security initiatives (UK government)

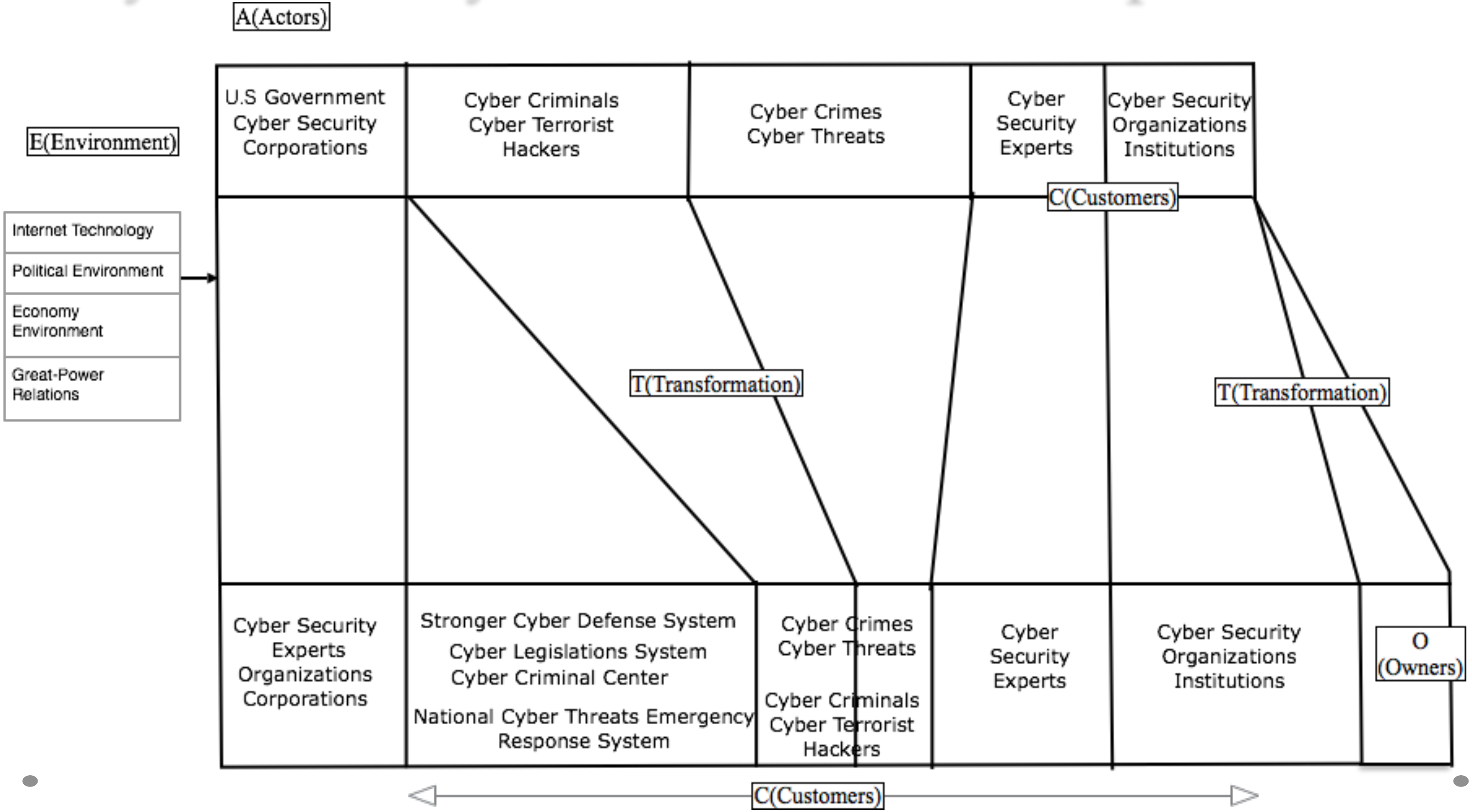
Cyber warfare called the 5th domain of battle (Pentagon, 2011)

Increasing damage to government, public,and related corporations (Japan)

Promotion of countermeasures led by international organizations and governments

In addition to governments, major corporations have become targets as well.

Cybersecurity Root Definition Graphic



A(Actors)

E(Environment)

Internet Technology

Political Environment

Economy Environment

Great-Power Relations

U.S Government
Cyber Security
Corporations

Cyber Criminals
Cyber Terrorist
Hackers

Cyber Crimes
Cyber Threats

Cyber
Security
Experts

Cyber Security
Organizations
Institutions

C(Customers)

T(Transformation)

T(Transformation)

Cyber Security
Experts
Organizations
Corporations

Stronger Cyber Defense System
Cyber Legislations System
Cyber Criminal Center
National Cyber Threats Emergency Response System

Cyber Crimes
Cyber Threats

Cyber Criminals
Cyber Terrorist
Hackers

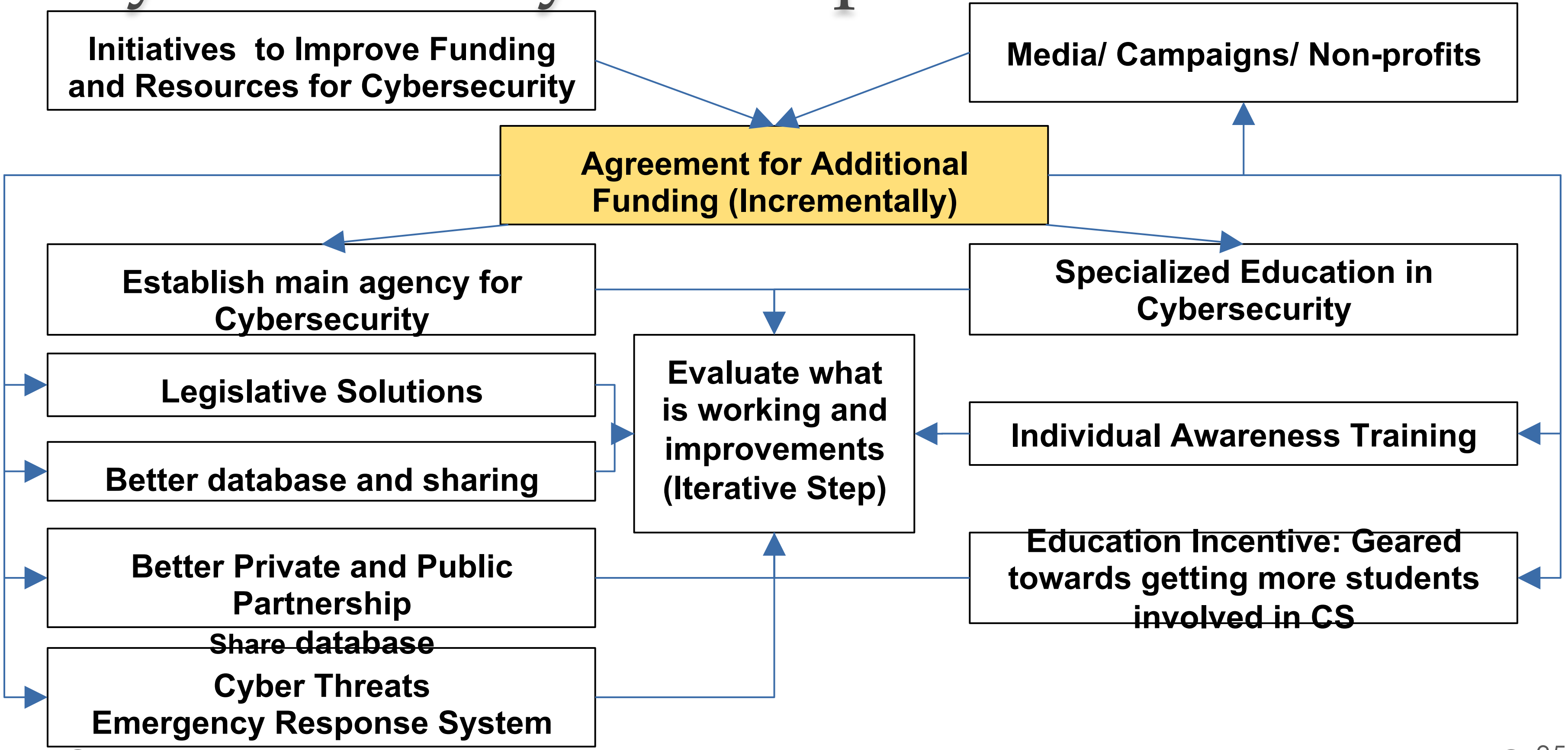
Cyber
Security
Experts

Cyber Security
Organizations
Institutions

O
(Owners)

C(Customers)

Cybersecurity Conceptual Model



Initiatives to Improve Funding and Resources for Cybersecurity

Media/ Campaigns/ Non-profits

Agreement for Additional Funding (Incrementally)

Establish main agency for Cybersecurity

Specialized Education in Cybersecurity

Legislative Solutions

Better database and sharing

Evaluate what is working and improvements (Iterative Step)

Individual Awareness Training

Better Private and Public Partnership

Education Incentive: Geared towards getting more students involved in CS

Share database

Cyber Threats Emergency Response System

Unintended Consequences

- Individual privacy vs. safety of nation
  - Increase of metadata and compilation/connection to citizens
  - Loss of privacy on browsing history
- Teaching people computer science, encryption decryption etc. gives them skills not only for cybersecurity but also for hacking
- Eventual government control over CS infrastructure for private companies
- The rise of new and more sophisticated threats

Big Questions: Feasibility - Things to Consider

- Political
  - Conflicting stakeholder views
- Technical
  - Virus possibility
- Economical
  - U.S. budget may not support our solutions
  - How much is needed for a significant impact?
- Social
  - Many stakeholders need to be persuaded
  - Will taxpayers be willing to increase taxes to support cybersecurity?