January 21, 2015

Is International Collaboration vital to assure Cybersecurity?

Access and Security in an Interconnected World

Dr. Karl V Steiner

Vice President for Research

Professor, Mechanical Engineering

UMBC

steinerk@umbc.edu

Opening Cyber Security Center Symposium

Kyushu University

January 21-23, 2015

UMBC
AN HONORS UNIVERSITY IN MARYLAND

九州大学
KYUSHU UNIVERSITY

Cybersecurity – Changing Global Priorities

UMBC
AN HONORS UNIVERSITY IN MARYLAND

Kevin "KAL" Kallaugher, The Economist – May 11, 2009

Stuxnet Attack

- **August 2010 –** virus attack on Bushehr nuclear power plant in southern Iran.
- Stuxnet reportedly infected 100,000 computers worldwide and ruined almost one-fifth of Iran's nuclear centrifuges
- Sophisticated design targeting previously unknown weaknesses in Windows, known as zero-day exploits, and alter the operation of Siemens Simatic process logic controller computers.
- Virus was capable of masking its presence while controlling and monitoring the systems it infected.

UMBC
AN HONORS UNIVERSITY IN MARYLAND

Kim Zetter, Wired.com – Nov 15, 2010

Shamoon Attack

- **August 15, 2012** – *Lailat al Qadr* (Night of Power)
- Over 30,000 Windows-based computers infected at Saudi Aramco
- Shamoon virus destroyed the hard drives of more than up to 85% of Saudi Aramco's computers
- Wiped out data on the company's servers, including the domain management servers that were the heart of the corporate network.

UMBC
AN HONORS UNIVERSITY IN MARYLAND

Nicole Perlroth, New York Times – Oct 23, 2012

Sony Pictures Entertainment

- **November 24, 2014**
- Over 100 Terabytes of confidential data stolen from SONY servers
  - Personnel information of 6,000 SONY employees
  - Several movies leaked online, including Brad Pitt's *"Fury"*
  - Release of "*The Interview*" movie delayed
  - *Snapchat* business plan revealed
- Responsibility claimed by *"Guardians of Peace (GOP)"*
- Alleged international link to North Korea

Pocket-lint.com – Dec 23, 2014

DDOS Attack on Playstation and Xbox Networks

- **December 25, 2014**
- Distributed Denial of Service Attack (DDOS) on Playstation and Xbox servers between Christmas and New Year 2014
- Sony's PlayStation system has about 110 million users and Microsoft's Xbox Live has 48 million subscribers.
- Both systems suffered long outages over Christmas
  - Busiest season for videogames
- Responsibility claimed by *"Lizard Squad"*
- 18-year old man arrested in Southport, UK – Jan 14, 2015

UMBC
AN HONORS UNIVERSITY IN MARYLAND

BBC.com and Reuters.com – Jan 16, 2015

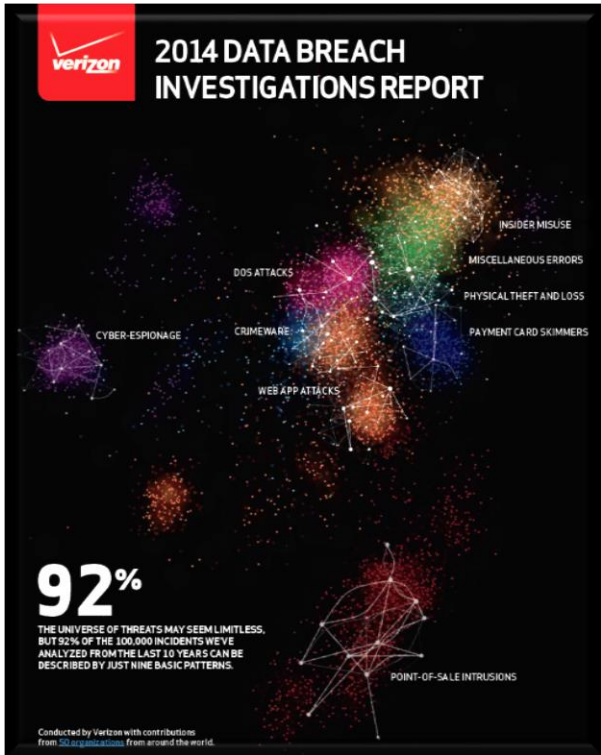
Increase in Cyber Attacks

The rise in successful cyber attacks is staggering

- 2012 saw a *single* data breach exposing over 10 Million identities.
- In 2013, there were *eight* such data breaches.

Types of information breached

- Real Names
- Birth Dates
- Medical Records
- Financial Information
- User Names & Passwords
- Government ID Numbers

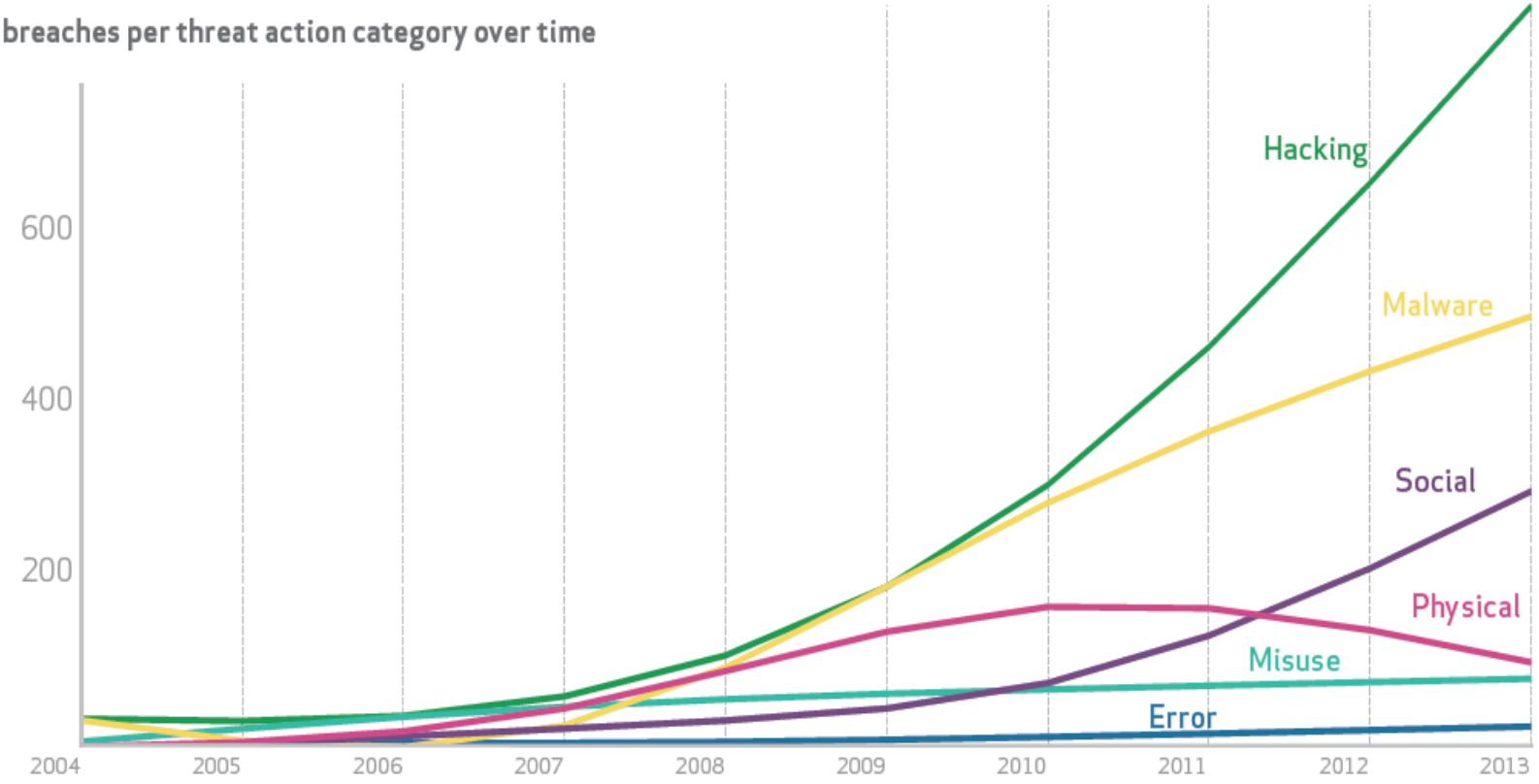


UMBC
AN HONORS UNIVERSITY IN MARYLAND

Exponential Increase in Cyber Attacks

- **Hacking and malware dominate cyber breaches**

Figure 8.
Number of breaches per threat action category over time

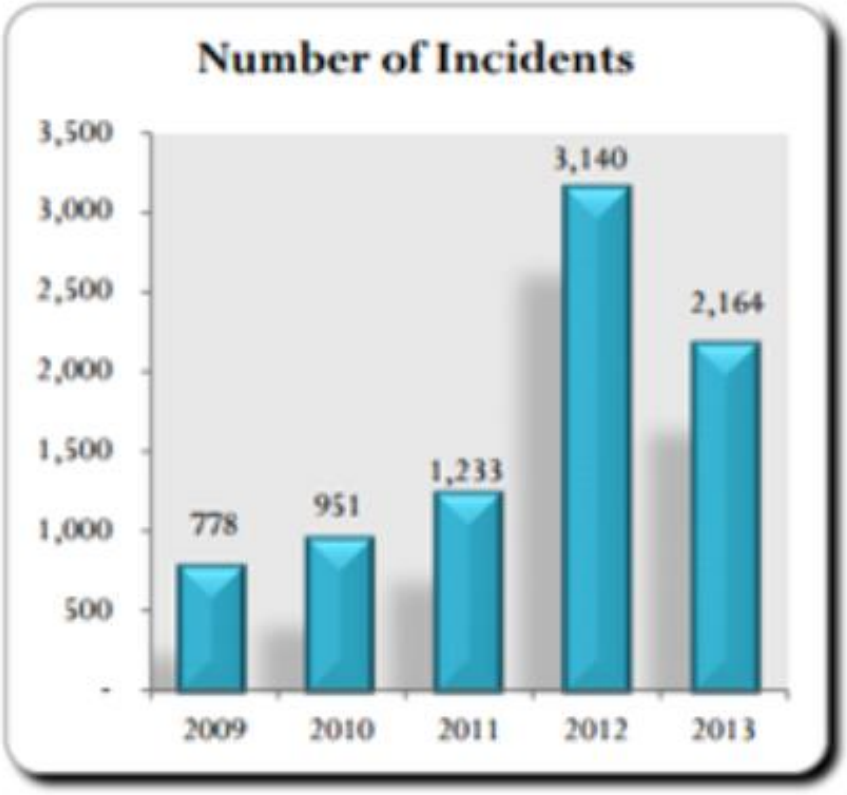


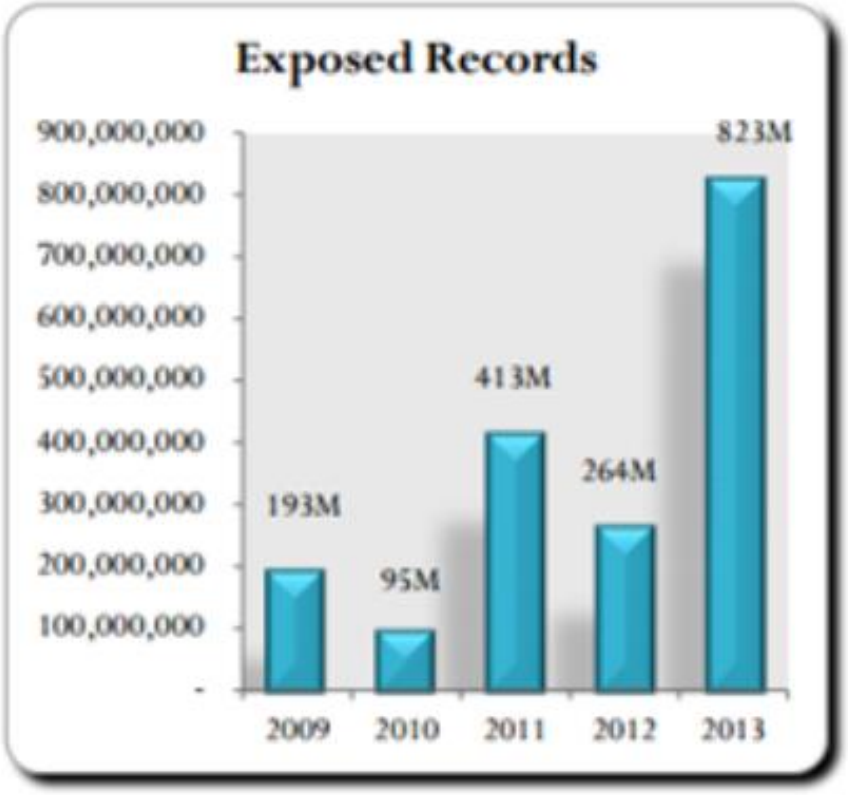
UMBC
AN HONORS UNIVERSITY IN MARYLAND

2014 Verizon Data Breach Investigations Report

Increase in Cyber Attacks

- **Increases in incidents and exposed records**



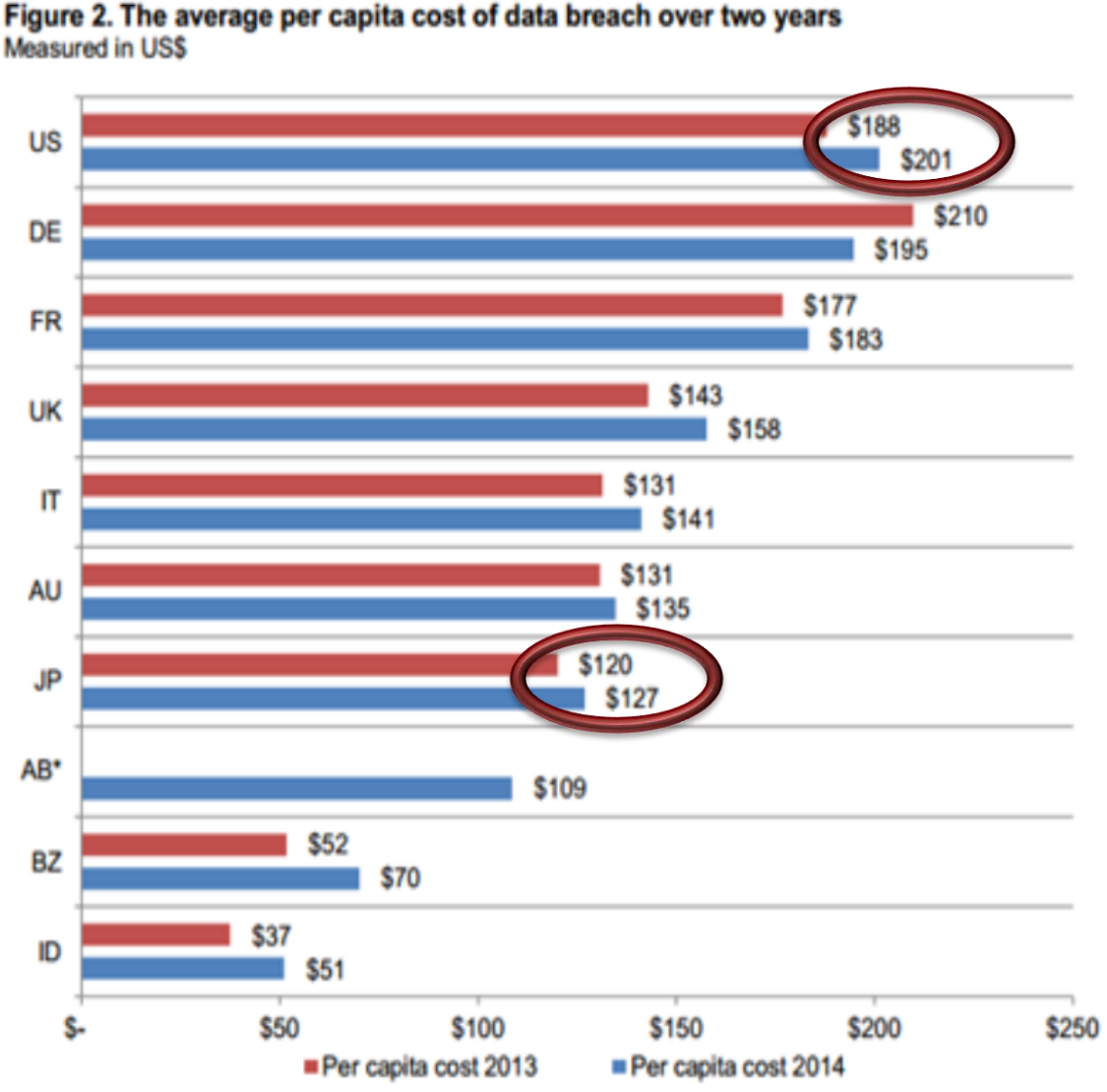


UMBC
AN HONORS UNIVERSITY IN MARYLAND

2014 Verizon Data Breach Investigations Report

Rising Cost of Data Breaches

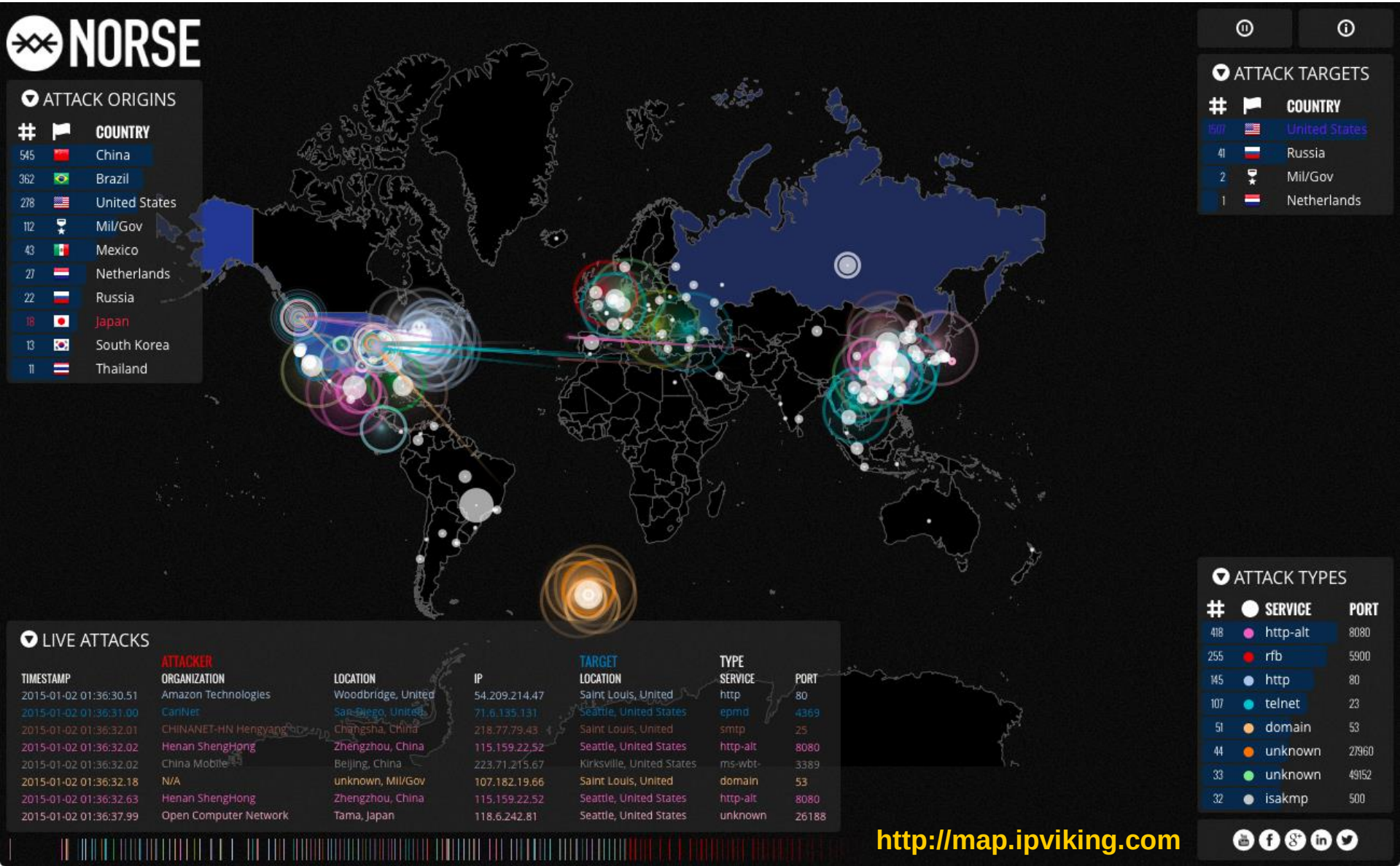
The average cost of data breaches has surpassed $200 per capita in the US and over $125 per capita in Japan



2014 Verizon Data Breach Investigations Report

UMBC
AN HONORS UNIVERSITY IN MARYLAND

International Map of Global Cyber Attacks

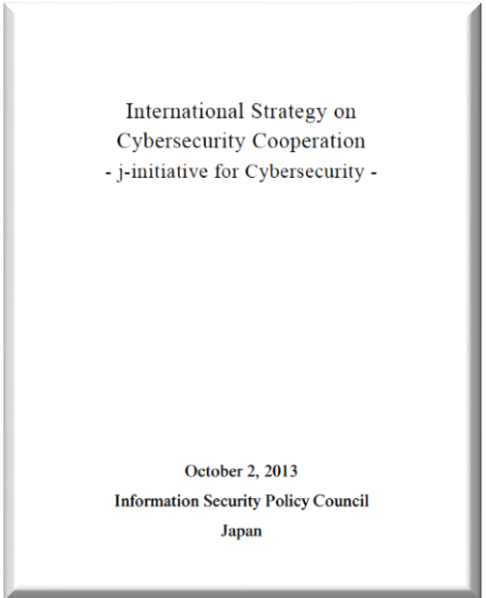


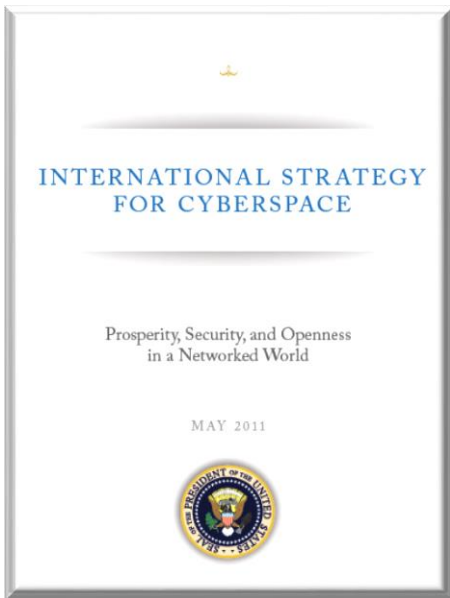
International Cybersecurity Policies

- ***"International Strategy for Cyberspace – Prosperity, Security, and Openness in a Networked World,"*** The White House, United States of America May 2011

- ***"Cybersecurity Strategy for the European Union – An Open, Safe and Secure Cyberspace,"*** European Commission, February 2013

- ***"International Strategy on Cybersecurity Cooperation – j-initiative for Cybersecurity,"*** Information Security Policy Council, Japan, October 2013





UMBC
AN HONORS UNIVERSITY IN MARYLAND

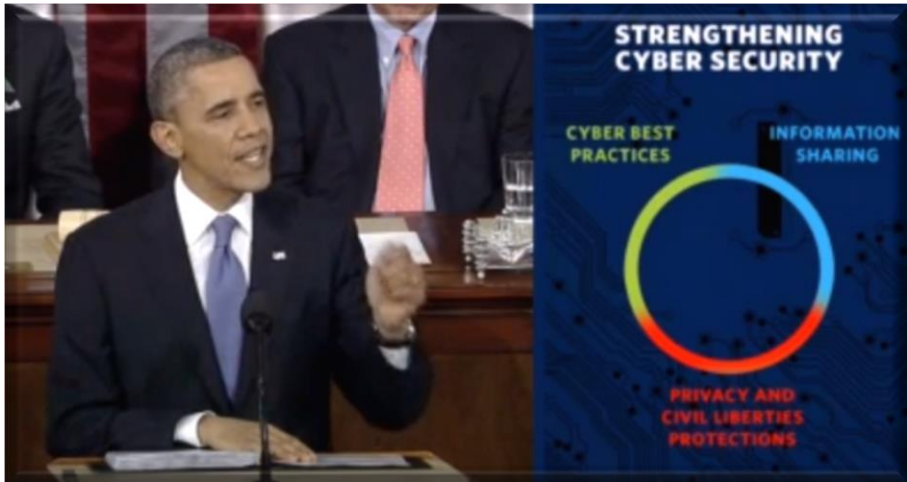
Cyberspace and Cybersecurity

This World – Cyberspace – is a world that we depend on every single day… [it] has made us more interconnected than at any time in human history.

President Barack Obama, May 2009

Cybersecurity is not an end unto itself; it is instead an obligation that our governments and societies must take on willingly, to ensure that innovation continues to flourish, drive markets, and improve lives.

President Barack Obama, May 2011



Comprehensive National Cybersecurity (CNC) Initiative

CNC Initiative Details

- Manage the Federal Enterprise Network as a single network enterprise with trusted internet connections.
- Deploy an intrusion detection system of sensors across the Federal enterprise.
- Pursue deployment of intrusion prevention systems across the Federal enterprise.
- Coordinate and redirect research and development (R&D) efforts.
- Connect current cyber ops centers to enhance situational awareness.
- Develop and implement a government-wide cyber counterintelligence (CI) plan.
- Increase the security of our classified networks.
- Expand cyber education.
- Define and develop enduring deterrence strategies and programs.
- Develop a multi-pronged approach for global supply chain risk management.
- Define the Federal role for extending cybersecurity into critical infrastructure domains.

UMBC
AN HONORS UNIVERSITY IN MARYLAND

THE WHITE HOUSE
WASHINGTON

Basis for Cybersecurity Norms

- **Open and Interoperable**
- **Secure and Reliable**
  - Uphold Fundamental Freedoms
  - Respect for Property
  - Value Privacy
  - Protect from Crime
  - Right of Self-Defense
- **Stability through Norms**
  - Global Interoperability
  - Network Stability
  - Reliable Access
  - Multi-Stakeholder Governance

International Strategy for Cyberspace, White House May 2011

US Cybersecurity Legislative Proposal

- **Introduced January 15, 2015**
  - National Cybersecurity and Communications Integration Center (NCCIC).
- **Enabling Cybersecurity Information Sharing**
  - Better cybersecurity information sharing between the private sector and government, and enhanced collaboration and information sharing amongst the private sector.
- **Modernizing Law Enforcement Authorities to Combat Cyber Crime**
  - Prosecution of the sale of botnets, would criminalize the overseas sale of stolen U.S. financial information like credit card and bank account numbers, would expand federal law enforcement authority to deter the sale of spyware used to stalk or commit ID theft, and would give courts the authority to shut down botnets engaged in distributed denial of service attacks and other criminal activity.
- **National Data Breach Reporting**
  - Simplify and standardize existing patchwork among States into one federal statute.

whitehouse.gov – Jan 15, 2015

International Strategies – Europe

- For cyberspace to remain open and free, the same norms, principles and values that the European Union (EU) upholds offline, should also apply online.
- Cyberspace should be protected from incidents, malicious activities and misuse
- Governments have a significant role in ensuring a free and safe cyberspace.
- By completing the *Digital Single Market*, Europe could boost its GDP by almost €500 billion a year; an average of €1000 per person
- But – a 2012 *Eurobarometer* survey showed that almost a third of Europeans are not confident in their ability to use the Internet for banking or purchases.
- European Network and Information Security Agency (ENISA)
  - Established 2004


EUROPEAN COMMISSION

HIGH REPRESENTATIVE OF THE EUROPEAN UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY

Brussels, 7.2.2013
JOIN(2013) 1 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Cybersecurity Strategy of the European Union:

An Open, Safe and Secure Cyberspace

UMBC
AN HONORS UNIVERSITY IN MARYLAND

"Cybersecurity Strategy for the European Union – An Open, Safe and Secure Cyberspace" European Commission, February 2013

Strategic Priority Areas – Europe

I. Achieve cyber resilience

II. Drastically reduce cybercrime

III. Develop cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)

IV. Develop industrial and technological resources for cybersecurity

V. Establish a coherent international cyberspace policy for the European Union and promote core EU values

"Cybersecurity Strategy for the European Union – An Open, Safe and Secure Cyberspace"
European Commission, February 2013

Strategic Priority Areas – Europe (II)

I. **Achieve cyber resilience**
- Establish common minimum requirements for Network & Information Security (NIS)
- Set up coordinated prevention, detection, migration and response mechanisms
- Improve preparedness and engagement in the private sector
- Raise awareness among end users
  - *European Cybersecurity Month*

II. **Drastically reduce cybercrime**
- Strong and effective legislation
- Enhanced operational capability to combat cybercrime
- Improved coordination at EU level

"Cybersecurity Strategy for the European Union – An Open, Safe and Secure Cyberspace"
European Commission, February 2013

Strategic Priority Areas – Europe (III)

III. Develop cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)

- Assess operation of EU cyberdefence mechanisms
- Develop EU cyberdefence policy framework
- Promote dialog and coordination between civilian and military actors in EU
- Ensure dialog with international partners

IV. Develop industrial and technological resources for cybersecurity

- Promote a single market for cybersecurity products
- Foster R&D investments and innovation

"Cybersecurity Strategy for the European Union – An Open, Safe and Secure Cyberspace"
European Commission, February 2013

Strategic Priority Areas – Europe (IV)

V. Establish a coherent International Cyberspace Policy for the European Union and promote core EU values

- Mainstream cyberspace issues into EU external relations and common foreign foreign security policy.

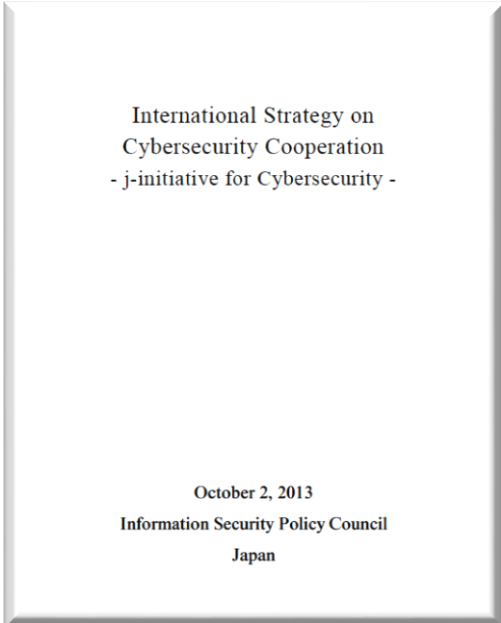
The EU does not call for the creation of new international legal instruments for cyber issues

- The *Budapest Convention* is an instrument open for adoption by third countries and serves as a basis for international cooperation in this field.

**"Cybersecurity Strategy for the European Union – An Open, Safe and Secure Cyberspace"
European Commission, February 2013**

International Strategies – Japan

- **Japan has developed the world's top-level telecommunications infrastructure containing fiber-optic networks and high-speed wireless networks nationwide, which led to increase in the use and application of cyberspace by various entities of all generations.**
- **Consequently, Japan has faced frequently serious cybersecurity issues ahead of many other countries.**
- **International Cybersecurity Strategy based on**
  - Japan Revitalization Strategy and
  - Japan Cybersecurity Strategy – June 2013.



International Strategy on Cybersecurity Cooperation
Information Security Policy Council, Japan, October 2013

ISPC Basic Principles and Priorities

- **Principles**
  - Ensure free flow of information
  - Respond to increasingly serious risks
  - Enhance risk-based approach
  - Act in partnership based on social responsibilities
- **Policies**
  - Incremental fostering of common global understanding
  - Japan's contribution to the global community
  - Expansion of the technological frontier at the global level

ISPC Cyber Priority Areas

- **Implementation of dynamic responses to cyber incidents**
  - Enhance multi-layered mechanisms for information sharing
  - Develop appropriate responses to cybercrime
  - Establish framework of cooperation for international security in cyberspace
- **Building up fundamentals for dynamic responses**
  - Support building a global framework for cyber hygiene
  - Promote awareness-raising activities
  - Enhance research and development through international cooperation
- **International rulemaking for cybersecurity**
  - Formulate international standards of technology
  - Foster international rulemaking

UMBC and Kyushu University Cyber Partnership

- **June 2014 – Kyushu University Delegation, led by President *Setsuo Arikawa*, visited UMBC to establish formal relationships with an initial focus on cybersecurity curriculum development between both institutions.**
- **January 2015 – UMBC Delegation is participating in Opening Symposium of the Kyushu University Cyber Security Center.**

九州大学
KYUSHU UNIVERSITY

UMBC
AN HONORS UNIVERSITY IN MARYLAND

Cybersecurity in Maryland

Maryland is a Hub of National Cyber Initiatives

- **National Security Agency (NSA)**
- **U.S. Cyber Command**
- **Intelligence Advanced Research Projects Agency (IARPA)**
- **Defense Information Systems Agency Headquarters (DISA)**
- **NIST – National Cybersecurity Center of Excellence (NCCoE)**

UMBC
AN HONORS UNIVERSITY IN MARYLAND

UMBC Center for Cybersecurity

- **Anupam Joshi, Director**
- **http://cybersecurity.umbc.edu**

UMBC
AN HONORS UNIVERSITY IN MARYLAND

NIST-NCCoE FFRDC in Cybersecurity

In 2014, UMBC and University of Maryland, College Park (UMCP) teamed with MITRE on successful bid for the NIST NCCoE *Federally Funded Research & Development Center (FFRDC*) in Cybersecurity

- **25-year, $5 Billion Indefinite Delivery / Indefinite Quantity (IDIQ) Contract awarded to MITRE/USM Team.**
- **Awarded – October 2014**
- **FFRDC Home will be between USM's Shady Grove Campus & NIST**
- **Academic Affiliates Council Leadership by UMBC & UMCP**
  - Anupam Joshi and Joseph JaJa

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

UNIVERSITY SYSTEM OF MARYLAND

MITRE

FFRDC Stakeholders

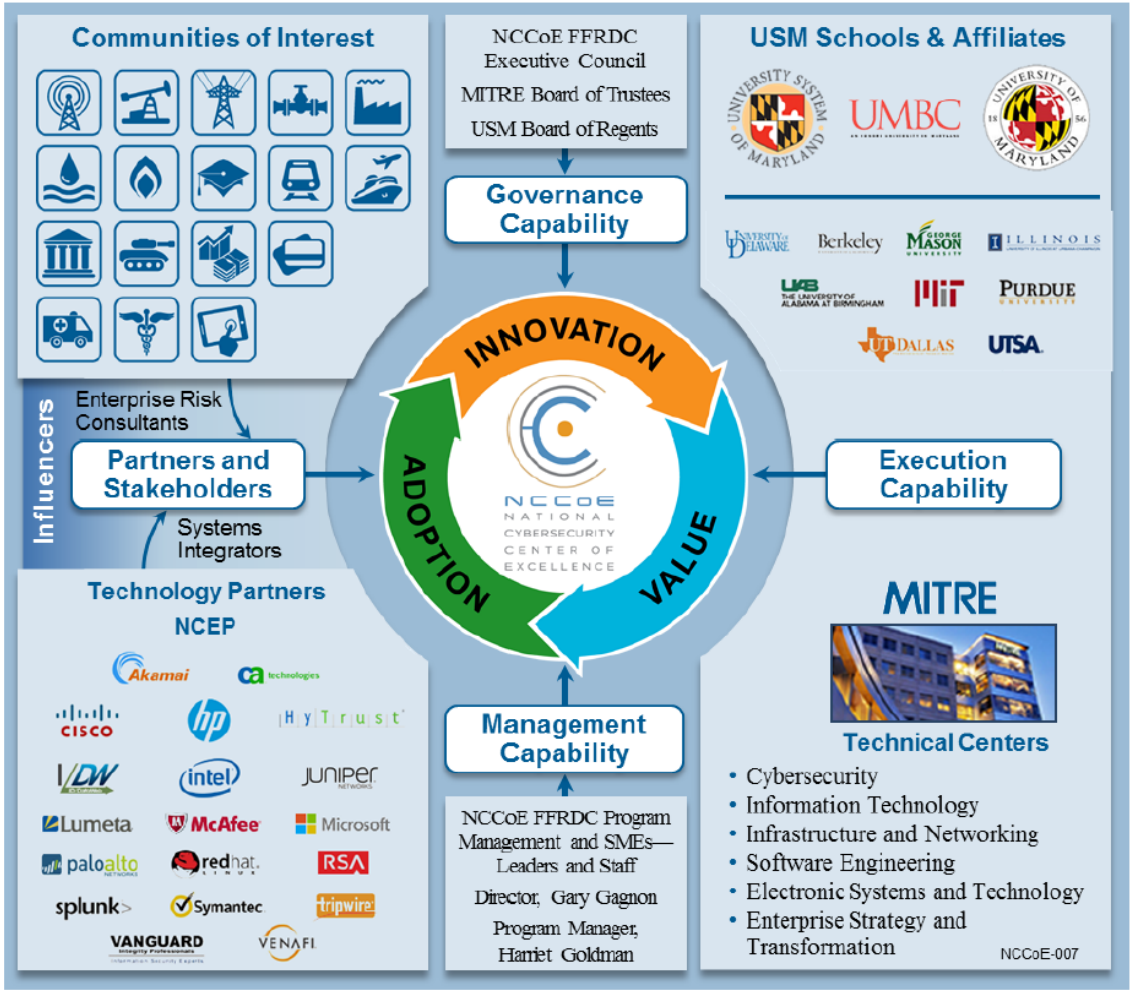


Figure 2-2. An Ecosystem of Stakeholders Working in Partnership to Achieve Innovation, Adoption and Value

UMBC
AN HONORS UNIVERSITY IN MARYLAND

MITRE

Academic Affiliates Council

- **USM Institutions**
- George Mason University
- Massachusetts Institute of Technology
- Purdue University
- University of Alabama – Birmingham
- University of California – Berkeley
- University of Delaware
- University of Illinois at Urbana-Champaign
- University of Texas – Dallas
- University of Texas – San Antonio

USM Member Institutions and Affiliate Partners

UMBC
AN HONORS UNIVERSITY IN MARYLAND

MITRE

Conclusions

- **Cybersecurity is a global responsibility**
  - Economic and national security implications
  - Governments have a significant role in ensuring a free and safe cyberspace
- **International collaborations are key to meeting the growing challenges**
  - Public, private and academic partnerships
  - A need for international standards
  - Enhanced research and development through international cooperation
  - Public awareness campaigns

Congratulations to Kyushu University's new Cyber Security Center (CSC)

UMBC
AN HONORS UNIVERSITY IN MARYLAND

The Price of Progress…

UMBC
AN HONORS UNIVERSITY IN MARYLAND

Kevin "KAL" Kallaugher, The Economist – Jun 9, 2012

Goseicho Arigatou Gozaimashita

ご静聴ありがとうございました。

Dr. Karl V. Steiner

Vice President for Research

steinerk@umbc.edu

UMBC
AN HONORS UNIVERSITY IN MARYLAND

九州大学
KYUSHU UNIVERSITY