Center for Applied Economics
Indian River State College

On the Economics of Cybersecurity

Samuel Mikhail, Ph.D.

November 8th, 2017
5:30 p.m.
V-110

"The views expressed here do not necessarily reflect the views of the IRSC College, the faculty or the staff."

Cybersecurity

"Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace."

https://www.dhs.gov/topic/cybersecurity

The economics of cybersecurity applies the principles of economics to the analysis of cybersecurity problems.

Cybersecurity

Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace.

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services.

Cybersecurity Overview

Strengthening the security and resilience of cyberspace has become an important homeland security

Combating Cyber Crime

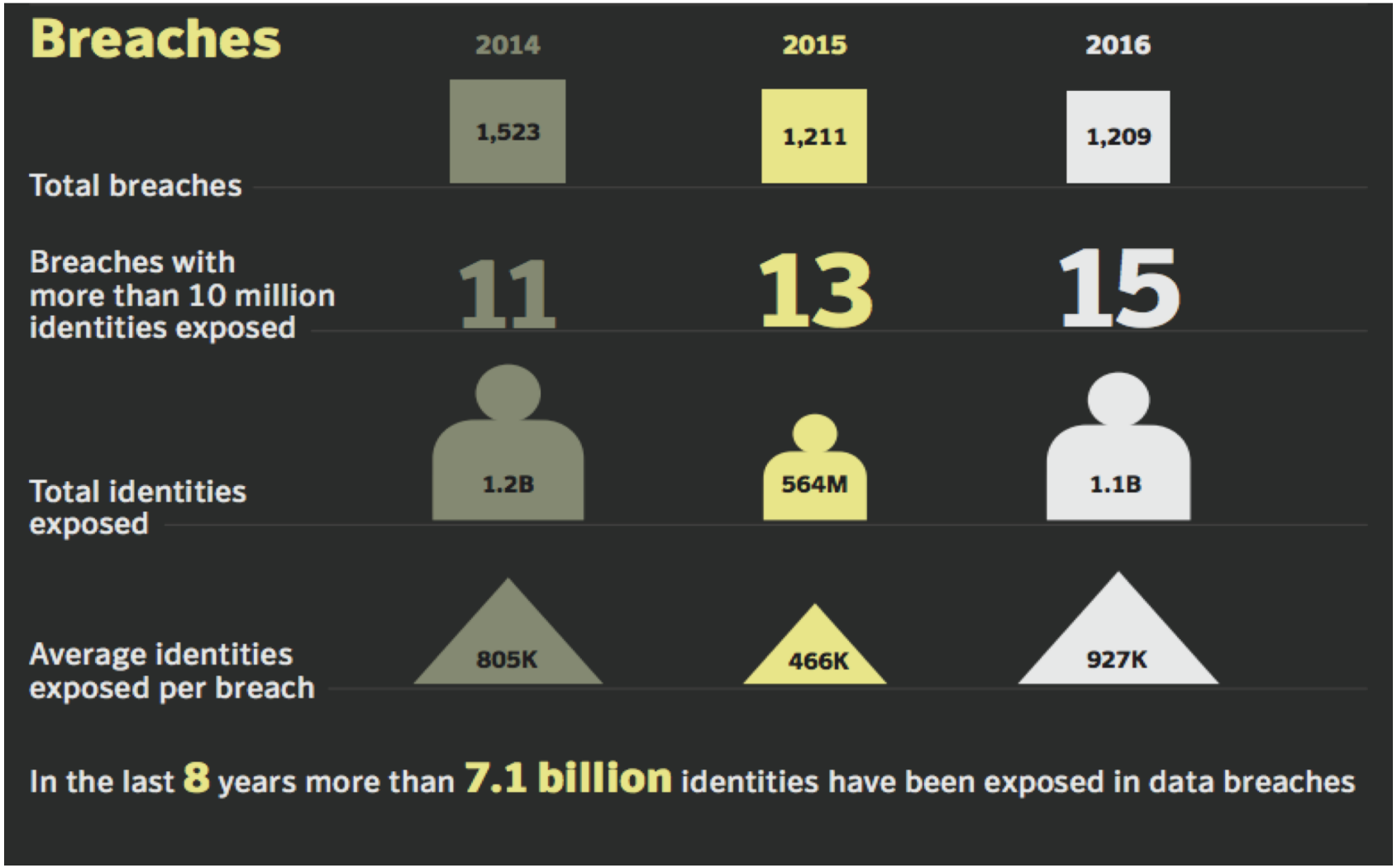
Today's world is more interconnected than ever before. Yet, for all its advantages, increased connectivity

Cybercrimes

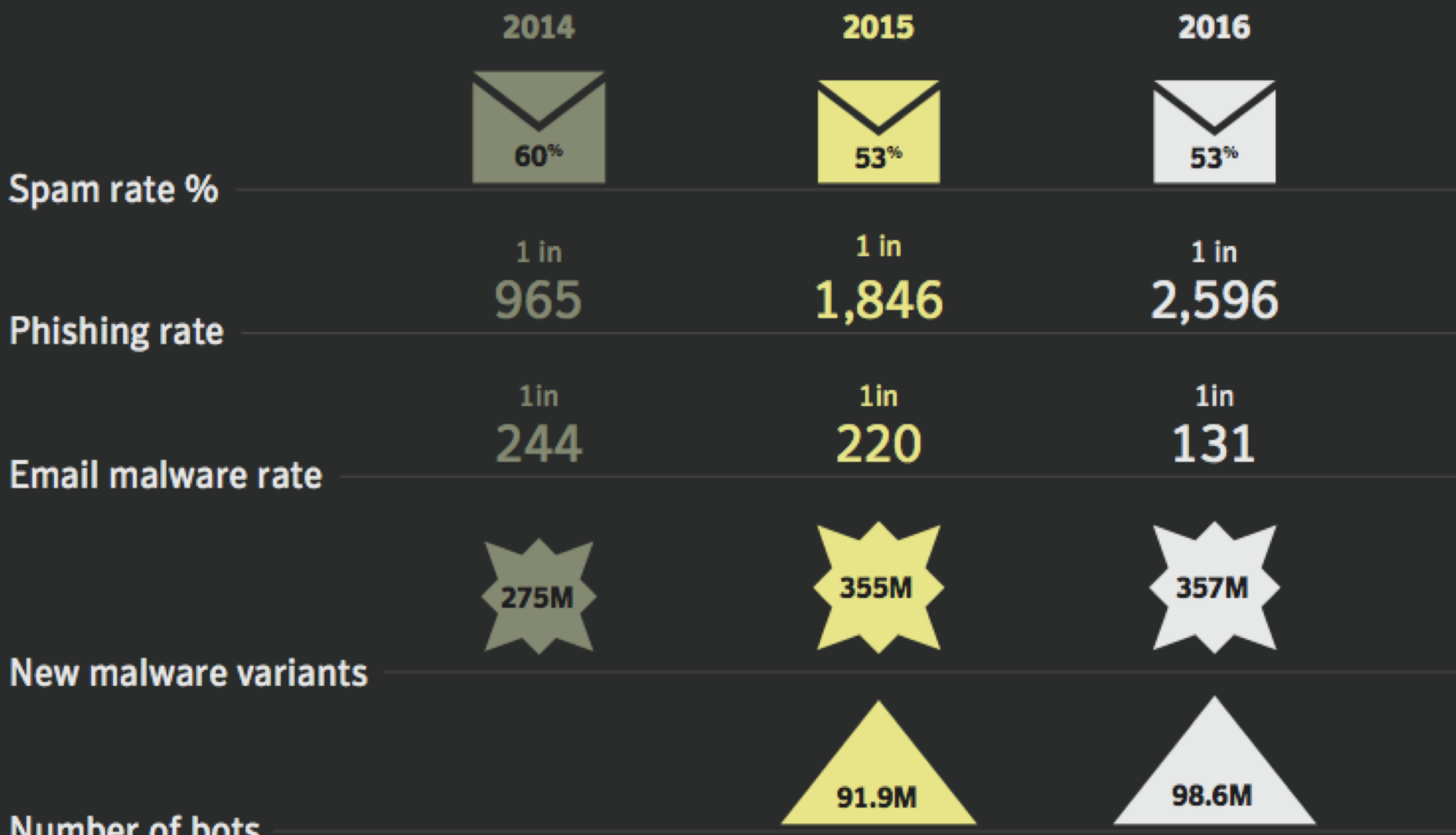
- IT is becoming integrated with critical physical infrastructure operations,
- Banking/Financial fraud,
- Intellectual property violations,
- Online identity theft,
- Industrial cyber espionage, and
- Botnets (robots+network).

- Considerable human and economic consequences.

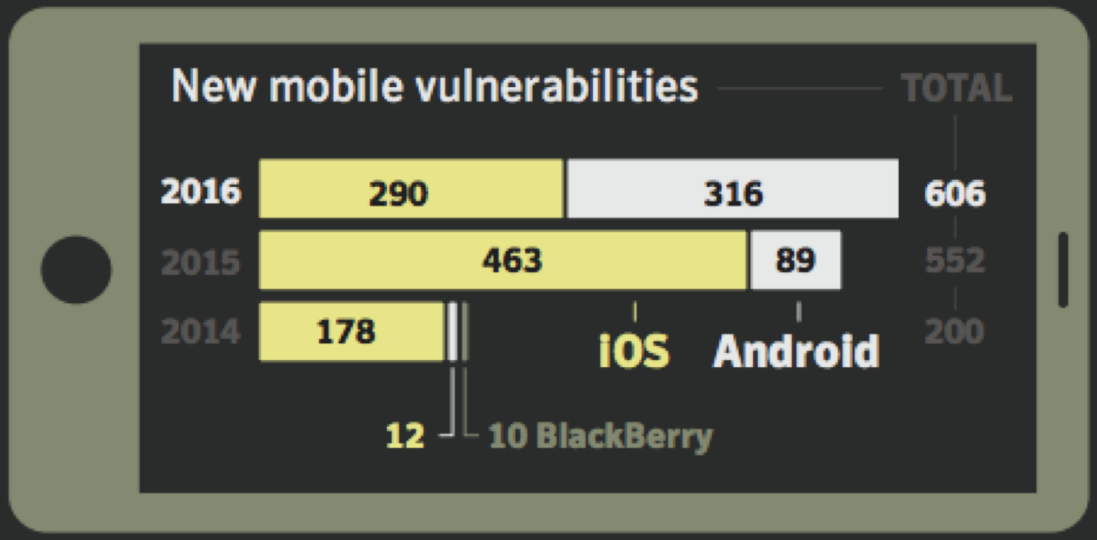
Global


Breaches
2014
2015
2016
1,523
1,211
1,209
Total breaches
Breaches with more than 10 million identities exposed
11
13
15
1.2B
564M
1.1B
Total identities exposed
805K
466K
927K
Average identities exposed per breach
In the last 8 years more than 7.1 billion identities have been exposed in data breaches

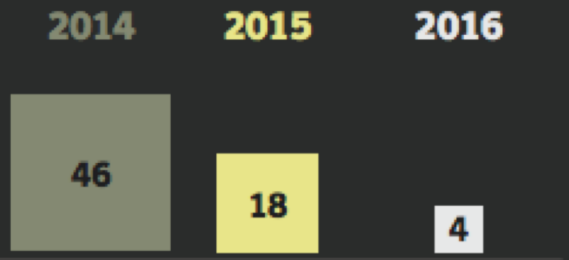
Email threats, malware, and bots



Mobile

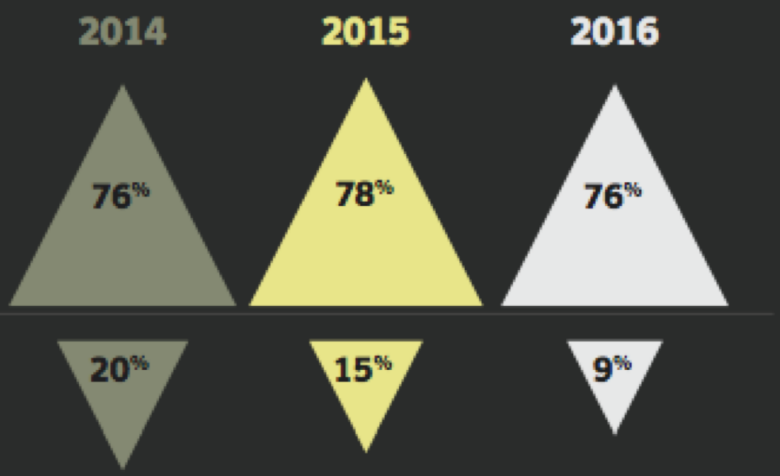


New Android mobile malware families

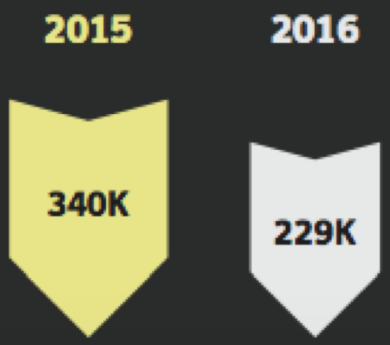


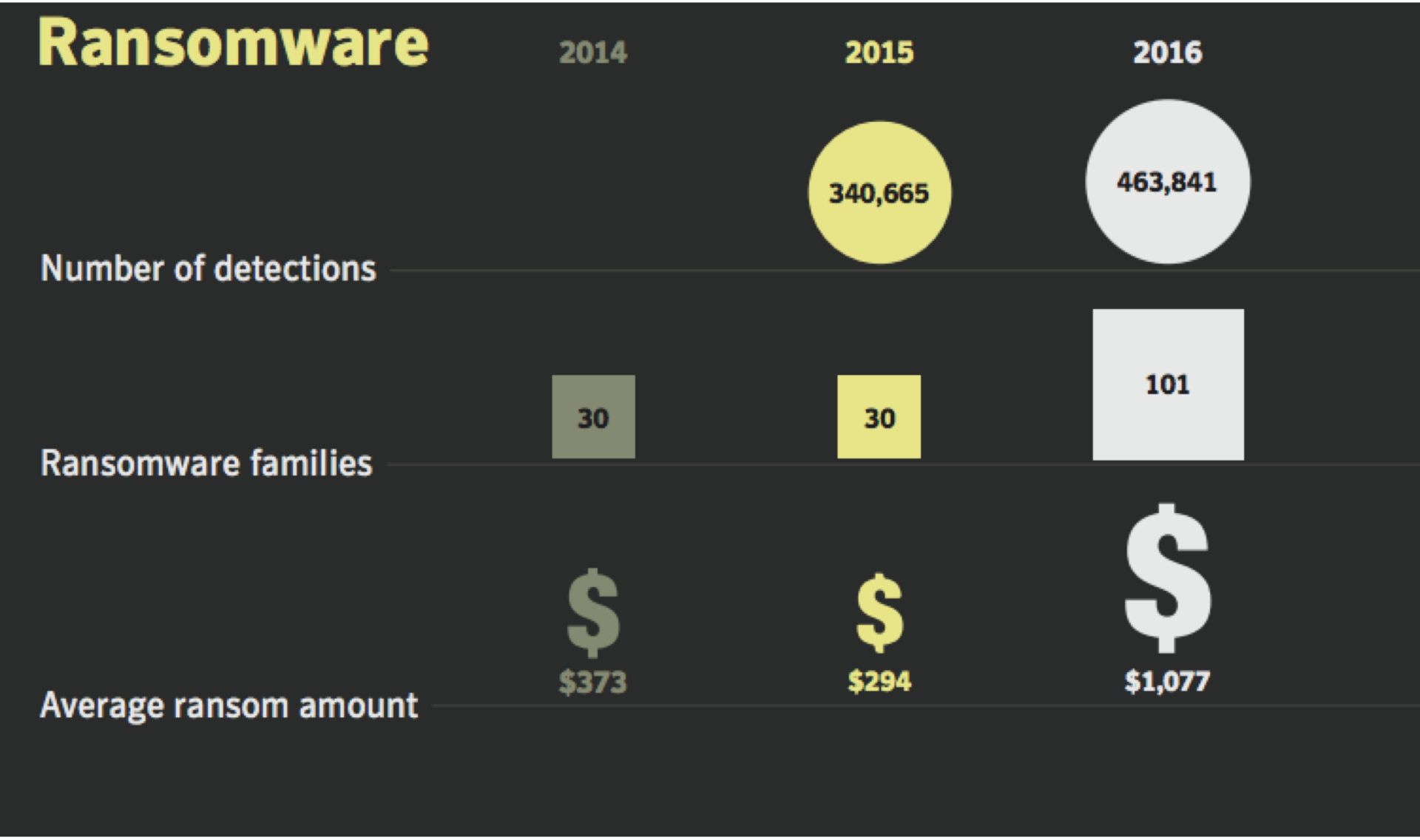
New Android mobile malware variants

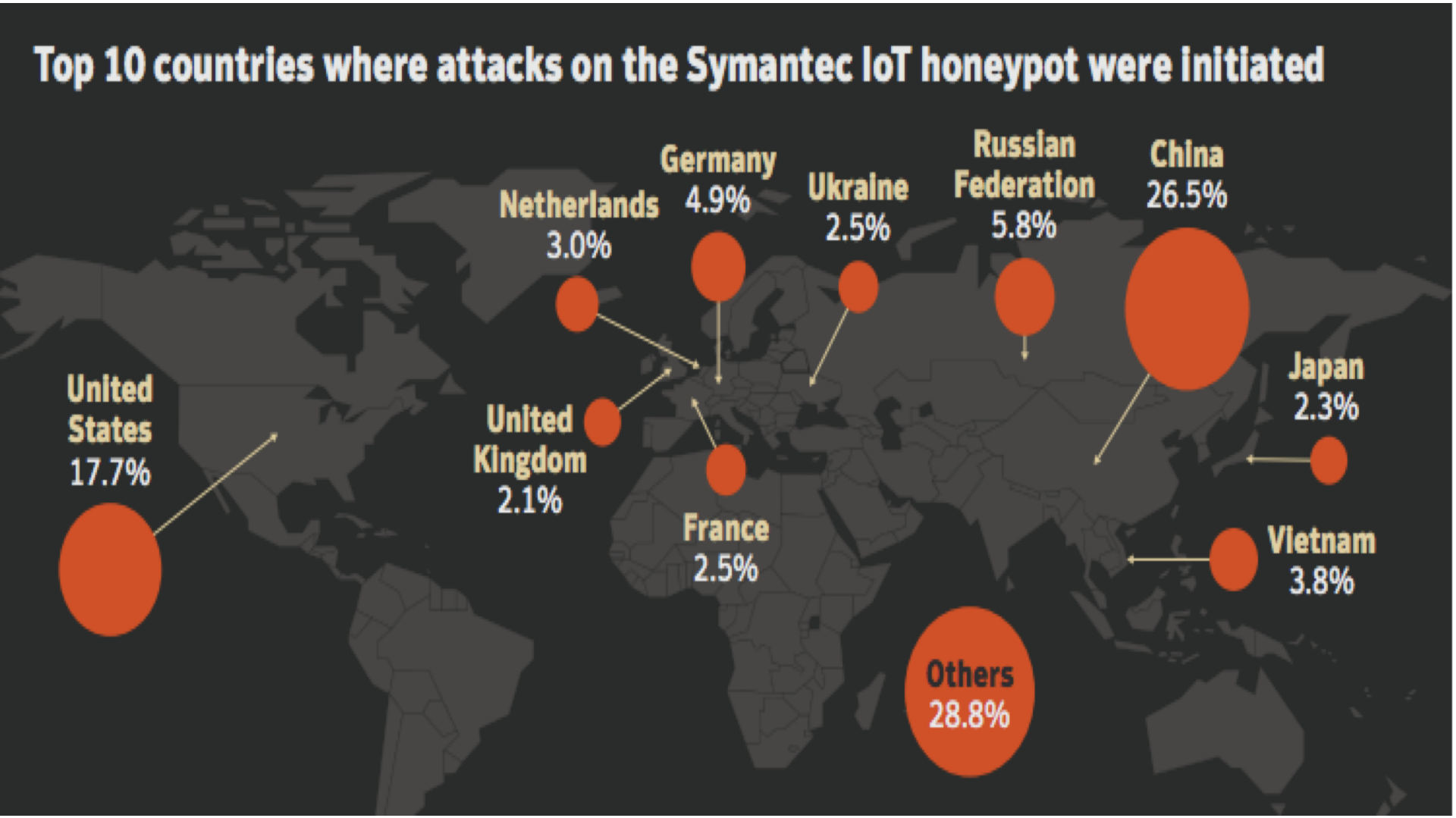
Web



Average number of web attacks blocked per day




Ransomware
2014
2015
2016
340,665
463,841
Number of detections
30
30
101
Ransomware families
$
$
$
$373
$294
$1,077
Average ransom amount



ISTR April 2017 Symantec Volume 22

The U.S.

- Catalyst to spend: breach resulting in loss of intellectual property
- **$15 billion** is spent each year by organizations in the United States to provide security for communications and information systems. [Market Research 2013; Gartner 2013]
- In 2009, President Obama estimated the economic impact of cyberattacks at over **$1 trillion/year or about 6% of the Gross Domestic Product (GDP)** of the United States. [Reference: Friedman 2011; Gorman 2013; Obama 2009]
- US DoD Defense Security Service (DSS) conference: a multinational firm invested more than $100M in cybersecurity over the past two years.

Dimensions

- Economics.
- Strategy, Policy and Doctrine.
- Law and Regulations.
- Psychology.
- Organization of Government.
- Privacy and Civil Rights.

Questions

- Investment in Cybersecurity does not generate money, it does prevent (money) losses.
- Organizations: **how much** to invest in cybersecurity as well as **where** these investments should be made.
- Is the investment by the United States in cybersecurity being appropriately applied?
- Invest more or less in order to provide adequate security?
- Where should organizations invest to gain the biggest economic return? (Air Force 2005-2006 automated updates for 500000 desktops/laptops, operating cost reduction versus cost of project implementation)

Economics of Cybersecurity

- Market for Cybersecurity.
- The return to Research & Development for producers.
- Return on Investment (ROI) for organizations.
- Quantitative Analysis – decision theory – operations research.
- Cybersecurity: is it a public good? Free-rider problem? Does the security depends on the weakest link in the chain?
- Cybersecurity: Does the market display externalities: + network externality, - botnet externality? Role for the Government?
- Asymmetric Information: Market for lemons (Akerlof 1970) buyers have no intention to pay a premium for a quality that they can't measure. Market for secured software is a market for lemons (Anderson 2001).

Economics of Cybersecurity

- Game Theory: Aligning incentives / principal-agent problem / one responsible for protecting system does not suffer a cost when it fails (hospital admins / banks admins).
- The Economics of network convergence: Phone, video and data over a single network. Used to be on distinct and incompatible networks — SS7 managed the phone system, SCADA controlled electrical grids. Cheaper to train engineers in Transmission Control Protocol/Internet Protocol (TCP/IP).
- Optimization Algorithms: Efficiency versus Security trade-off. What is the optimal level of security?

Models of investment in cybersecurity

- Models to help guide investment by organizations in cybersecurity.
- Data about cyber attacks (lag time in discovery, unreported: impact on stock valuation and brand name.)
- Models: measurements versus metrics.
- Optimal Metrics are: Specific, Measurable, and Time/Technology-dependent.

- V : Vulnerability = error or weakness in design
- T: Threat = intrusive behavior to access, change or destroy system (virus)
- Risk = Pr(breach|threat)
- L: Potential loss
- I : Investment in *preventive* maintenance.
- Types of security technologies: preventive, detective and recovery.
- Assess risk by the expected loss (similar to the B<PL rule in law and economics, harm could be avoided for *less* than the cost of the harm) leads to optimal allocation of resources.

Gordon-Loeb Investment Model

- Professors Lawrence Gordon and Vernon Loeb.
- Gold Standard of Cybereconomics Models.
- 1) Incremental additional investment in security provides additional benefit by reducing the potential of successful attack up to a point. Beyond this point, there is diminishing (or no) additional benefit for additional investment. **Investment is weakly increasing in vulnerability**.
- 2) Assuming a security breach probability (Class I power function or class II exponential function) **An organization should not invest more in cybersecurity protection measures than 37% of the expected potential loss without any protection**.
- Limitations and sensitivity to assumptions made: parametric functions and constant probability of threat. Model considers only preventive technology.

- Pr(breach) = Pr(breach|threat). Pr(threat) = f(I,V).Pr(T)
- Expected Loss = L.Pr(breach) = L. f(I,V).Pr(T)
- Optimal I* is from min [L. f(I,V).Pr(T) + I]

For a Class II function

Pr(breach) = Pr(breach|threat). Pr(threat)
= Lambda t S(z,v)
I = z
Optimal z* is from
min [Lambda t S(z,v) + z]

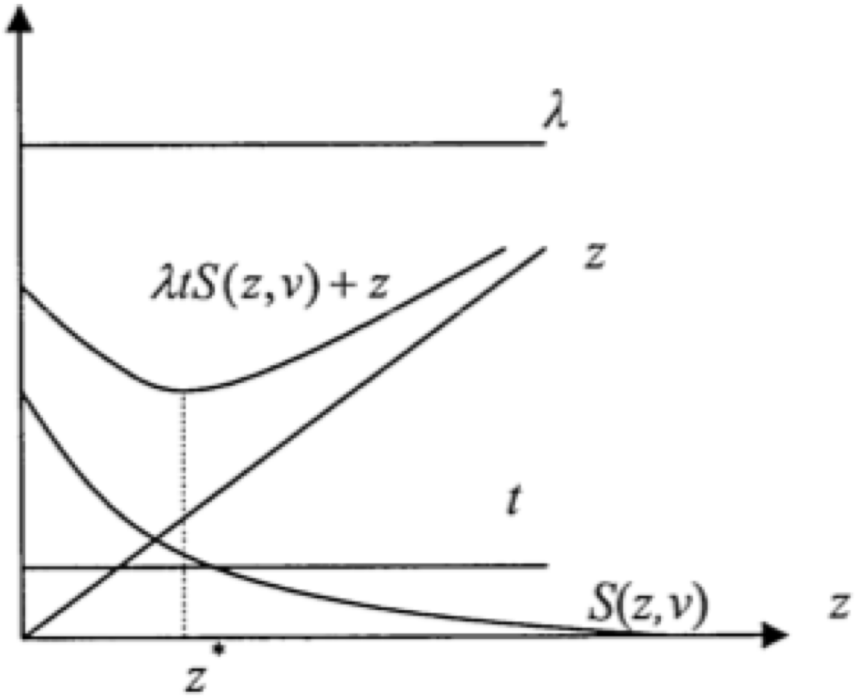


Figure 1. Objective Function

NIST Risk Management Framework

- The National Institute for Standards and Technology (NIST), the United States government organization responsible for providing standards and guidance in the area of cyber security.
- "800 Series" publications. NIST Special Publication 800-37 [NIST2010] and 800-53 [NIST2009; NIST 2010(2)] define the cybersecurity Risk Management Framework (RMF) including a method for assessing the implementation of controls to mitigate risk.
- Process to guide federal organizations on appropriate security controls, in non-economic terms.
- Optional but recommended for non-federal.
- Residual risk (R) is calculated as a function of threats (T) exploiting cyber vulnerabilities (V) offset by countermeasures (C) or $R = (T \times V) - C$
- Comprehensive, implementation issues because of a well defined T and/or V.

Private Investment Strategies

- A number of private sector organizations have independently developed cyber investment strategies. These are **proprietary** and not available outside the company.

Regulations

- *Proactive Ex ante* safety regulation - Gramm-Leach-Bliley Act 1999 – forces banks to "protect the security and confidentiality."
- **United States Cyber Command** (**USCYBERCOM**).
- Ex post liability- FTC Act section 5, grants the FTC authority to take action against unfair or deceptive acts and practices that affect commerce.
- The Federal Information Security Management Act (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA was signed into law part of the Electronic Government Act of 2002.

- Data: The volunteer website http://www.datalossdb.org

Recommendations

- (Moore 2010)
- mitigating malware infections via ISPs by subsidized cleanup,

- Data reporting:
- mandatory disclosure of fraud losses and security incidents,
- mandatory disclosure of control system incidents and intrusions,

- Asymmetric Information: develop a Market for Cyberinsurance.

References

- Gartner 2013: "Gartner reveals Top 10 Security Myths", by Ellen Messmer, NetworkWorld, June 11, 2013.
- Obama 2009: Remarks by the President on Securing our Nation's Cyber Infrastructure, The White House East Room, May 30, 2009.
- Friedman 2011: Economic and Policy Frameworks for Cybersecurity Risks, Allan Friedman, Center for Technology Innovation at Brookings, July 21, 2011. Gorman 2013: "Cybercrime Costs Put at $100 Billion", Siobhan Gorman, The Wall Street Journal, July 23, 2013, p. A4.
- Symantec 2012: Symantec Intelligence Report, 2012 Updated June 25, 2013.
- Gordon 2002: The Economics of Information Security Investment, Lawrence Gordon and Martin Loeb, University of Maryland, ACM Transactions on Information and Systems Security, November 2002.
- NIST 2010: SP 800-37 Rev. 1. Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010.
  NIST 2009: SP 800-53, Rev 3. Recommended Security Controls for Federal Information Systems and Organizations. August 2009.
- NIST 2010(2): SP 800-53 A, Rev 1. Guide for Assessing the Security Controls of Federal Information Systems and Organizations, Building Effective Security Assessment Plans.
- Gilligan, John (2013) "A Practical Framework for Cybersecurity Investment." AFCEA International Cyber Committee.
- Tyler Moore (2010) Introducing the Economics of Cybersecurity: Principles and Policy Options. Proceedings of a Workshop on Deterring Cyberattacks.

Thank You