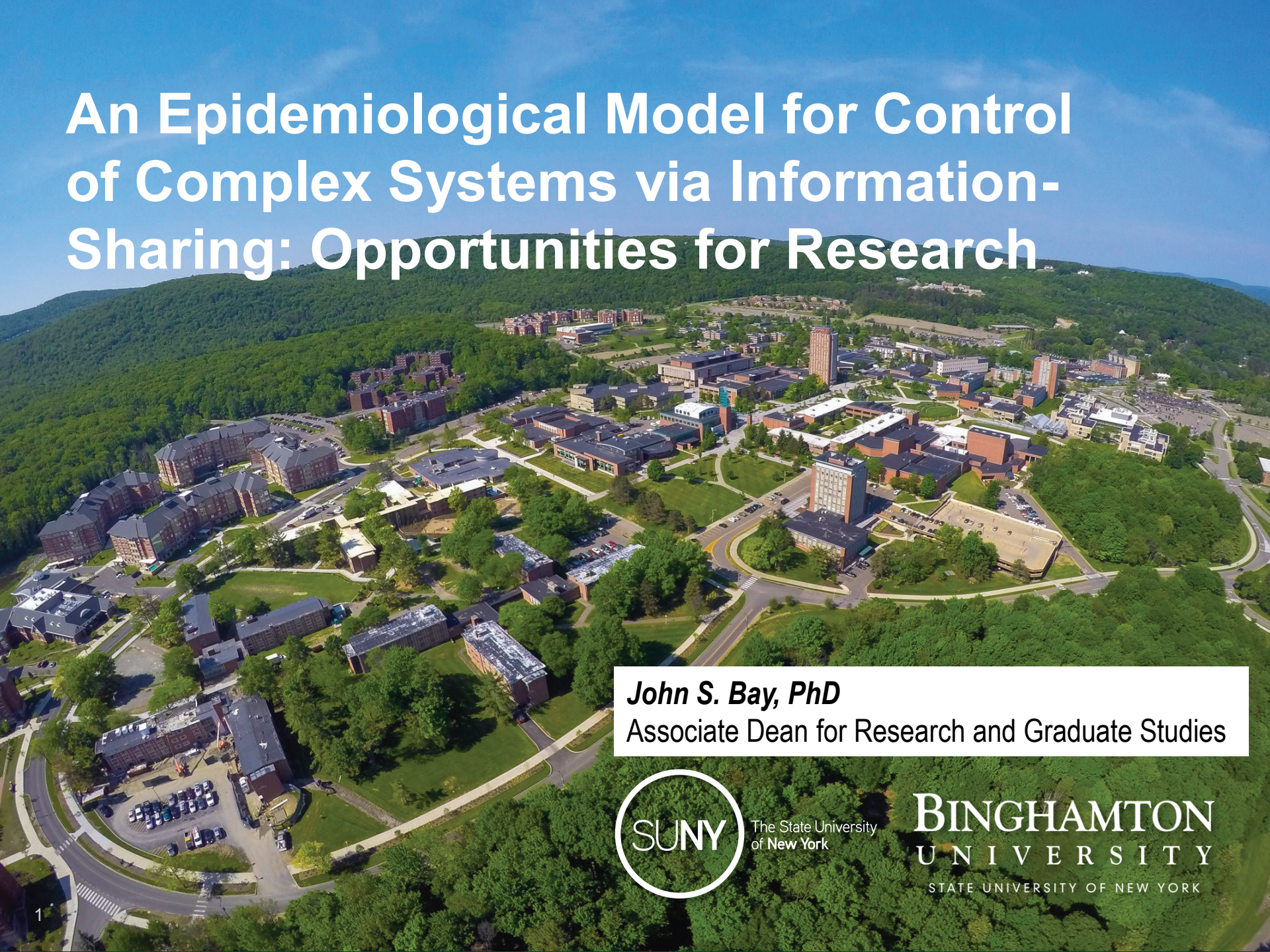
An Epidemiological Model for Control of Complex Systems via Information-Sharing: Opportunities for Research



John S. Bay, PhD
Associate Dean for Research and Graduate Studies

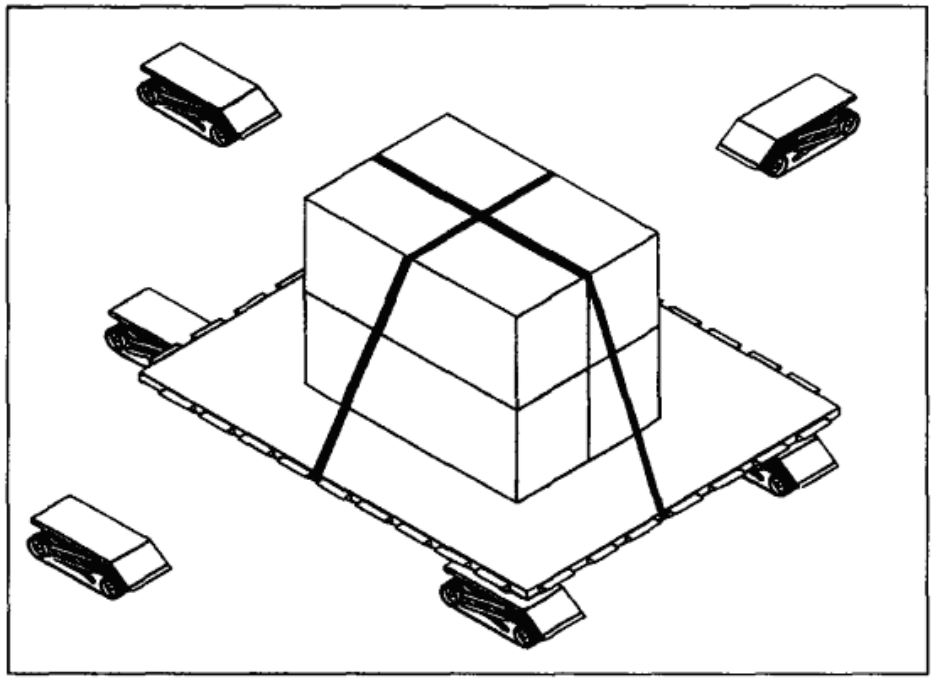
SUNY The State University of New York

BINGHAMTON UNIVERSITY
STATE UNIVERSITY OF NEW YORK

My Introduction to Complex Systems: 1990

The “Army Ant” Robot Concept

- Coordinated control through anonymous mechanical coupling
- Autonomous recruitment and collaboration
- No supervisory level
- Only broadcast communications
- Complex dynamics in both the physical and behavioral domains



In the News

Healthcare IT

SIGN UP MAIN MENU

Modern Healthcare

The leader in healthcare business news, research & data

Network Infrastructure Priv

2015 healt … long list

U.S., Canada issue ransomware warning for hospitals after three hit in a week

By Bernie Monegain | December 10, 2015 | 03:02 PM

SHARE 44

By Joseph Conn | April 04, 2016

MedStar Health still recovering from computer virus

By Modern Healthcare | April 02, 2016

Details of Anthem's massive cyberattack remain in the dark a year later

By Bob Herman | March 30, 2016

Criminal Attacks Are Now Leading Cause of Data Breach in Healthcare, According to New Ponemon Study

Hospital cyberattack highlights healthcare vulnerabilities

By Associated Press | March 30, 2016

Healthcare underspends on cybersecurity as attacks accelerate

By Beth Kutscher | March 03, 2016

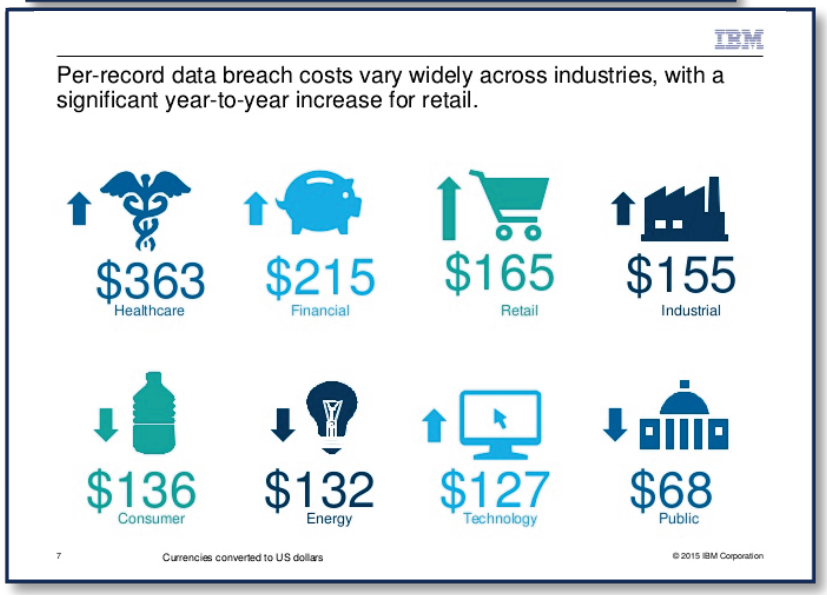
The Problem: Cybersecurity for Healthcare Records

- Data breaches in the health care industry have exposed the largest number of personal records of New Yorkers since 2006.
- Healthcare records are a primary target of malicious hackers
- Each personal compromised record costs an entity approximately $363
  - Much more than any other type of record

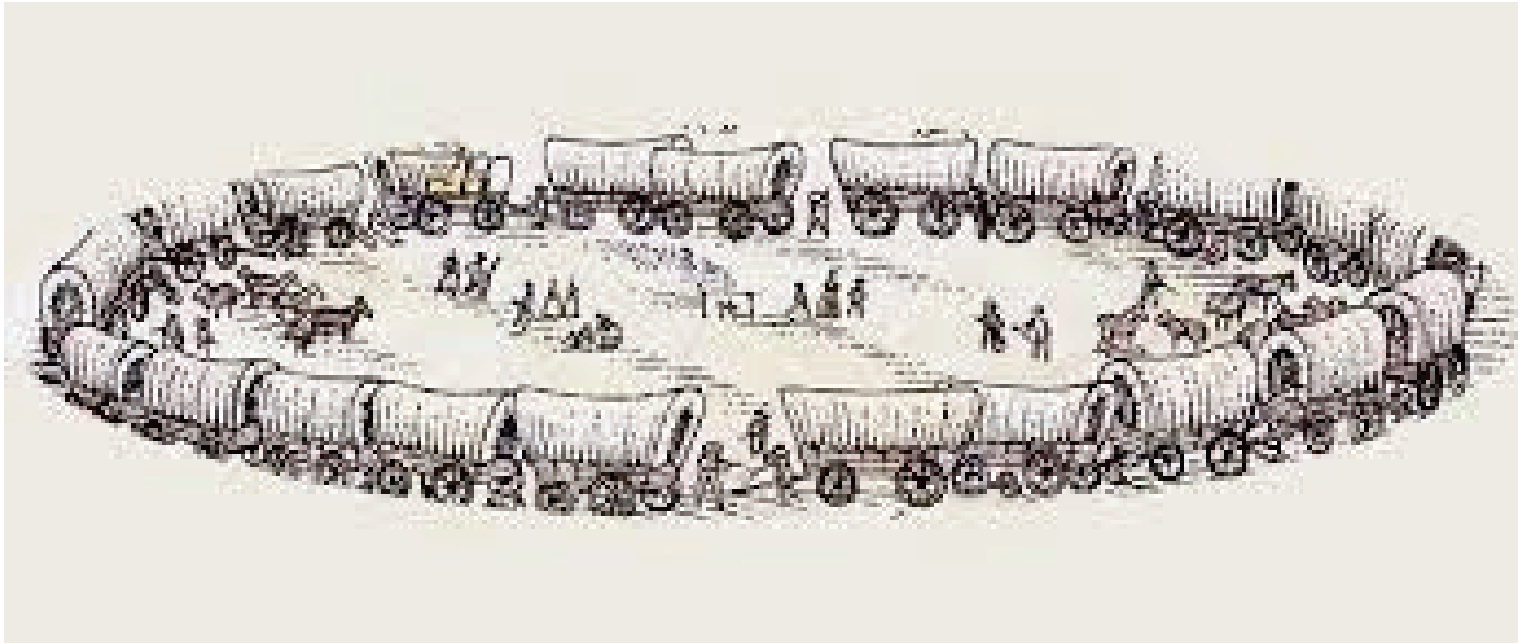
Many institutions and providers have no in-house security capabilities or resources

Industry Type	Entities With 3+ Breaches	Personal Records Exposed
Retail Services	54	163,319
Financial Services	31	624,000
Health Care	29	1,012,269
Banking	27	560,208
Insurance	20	72,138
Professional Services	16	788,280
Educational Inst.	15	103,787
Government Agency	14	86,548
Loan Services	9	133,866
Hospitality	8	16,091
Technology	7	13,195
Telecommunications	4	80,963
Credit Reporting	3	3,120
Credit Card Company	2	237,296
Nonprofit	1	507
Public Utility	1	50,456
Grand Total	**241**	**3,946,043**

Source: New York State Security Breach Reporting Forms (2006-2013)



The Idea: Create a *Security Cooperative*

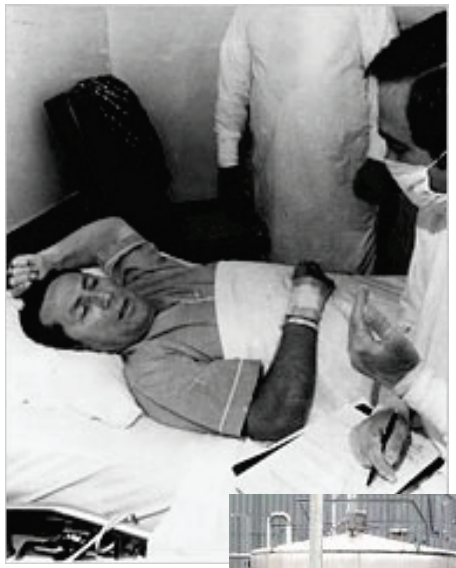


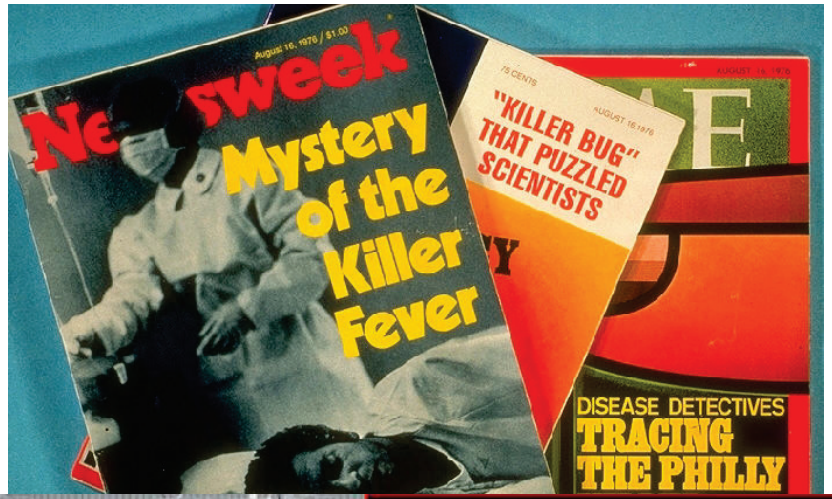
- Create a *social response*
- Use shared capabilities and services
- How would this work?? *Compare to epidemiology*

Ebola. 1976, Zaire

Not as virulently infectious; most deadly

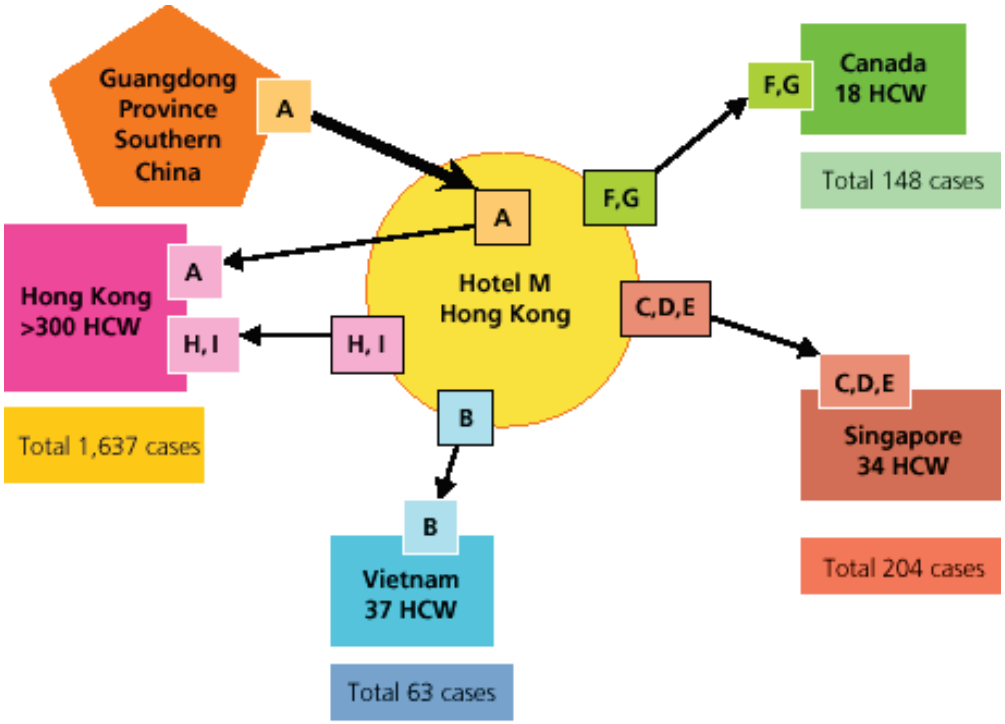
Legionnaire's Disease. 1976, Philadelphia

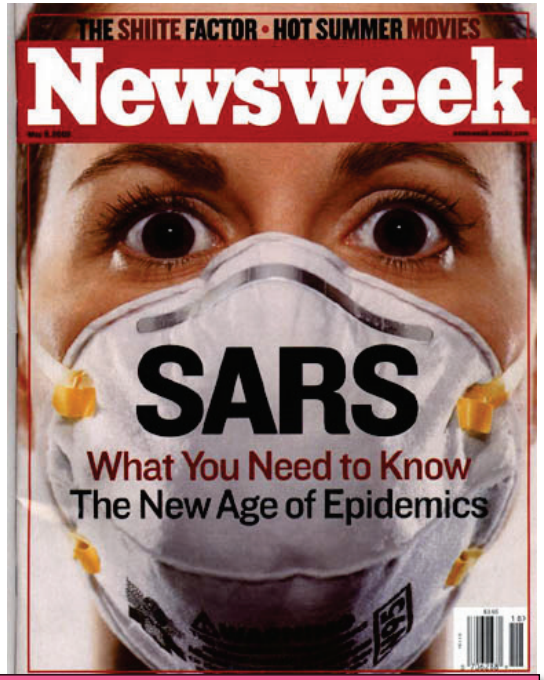




More virulently infectious; less deadly

SARS. Hong Kong 2003





Most virulently infectious; not as deadly

Extending an Epidemiology Model to Cybersecurity

WiFi networks and malware e

arXiv.org > cs > arXiv:1401.4208

Computer Science > Social and Information Network

Epidemiological modeling of online

John Cannarella, Joshua A. Spechler

(Submitted on 17 Jan 2014)

Online Promiscuity: Prophylactic Patching and the Spread of Computer Transmitted Infections

Timothy Kelley
Indiana University Bloomington
107 S. Indiana Ave.
Bloomington, IN, 47405
kelleyt@indiana.edu

L. Jean Camp
Indiana University Bloomington
107 S. Indiana Ave.
Bloomington, IN, 47405
ljcamp@indiana.edu

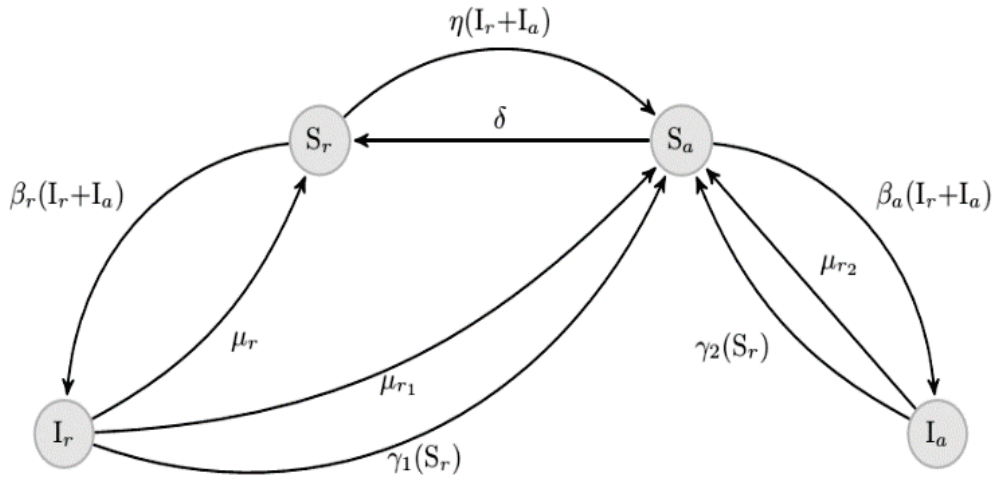


Figure 3: Two Population SIS model with Recovery and Social response.

Notation	Definition
S_r	Susceptible non-vigilant population
S_a	Susceptible vigilant population
I_r	Infected non-vigilant population
I_a	Infected vigilant population
η	Non-vigilant response to Infection
δ	Rate to return to non-vigilant population
β_r	Infection rate in non-vigilant population
β_a	Infection rate in vigilant population
μ_r	Non-vigilant recovery rate
μ_{a_1}	Non-vigilant to vigilant recovery rate
μ_{a_2}	Vigilant recovery rate
γ_{a_1}	Non-vigilant to vigilant social response rate
γ_{a_2}	Vigilant social response rate
R_∞	Equillibrium infected population
R_{∞_a}	Equillibrium infected vigilant population
R_{∞_r}	Equillibrium infected non-vigilant population

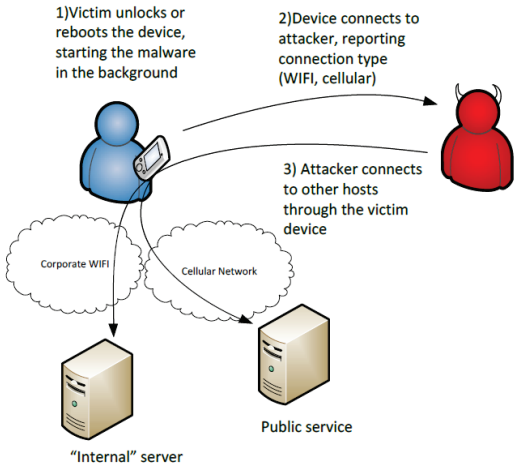
Table 1: Table Giving Definitions to included Symbols

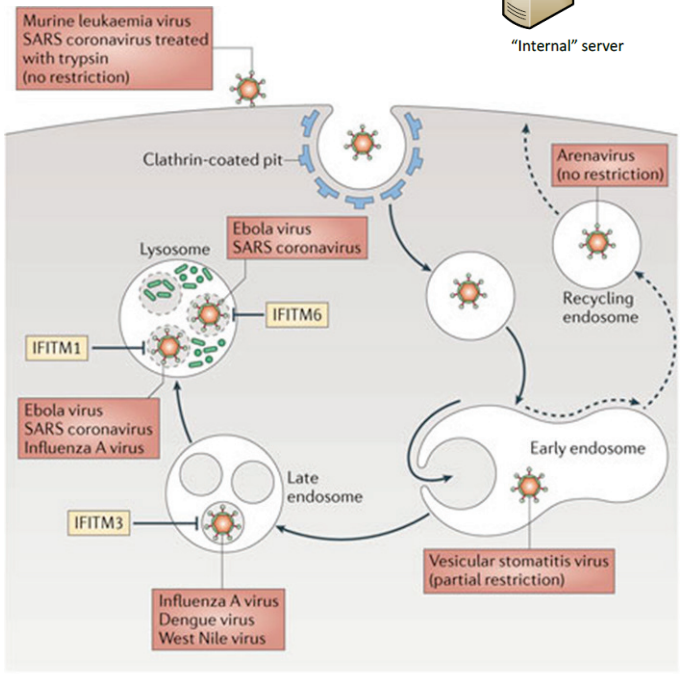
Timothy Kelly and L. Jean Camp, "Online Promiscuity: Prophylactic Patching and the Spread of Computer Transmitted Infections," *Workshop on the Economics of Information Security (WEIS)* 2012, June 25-26, Berlin, Germany.

Modeling the Spread of Infection

What are the key variables?

- Transmissibility
- Contact
- Preventative Measures
  - Costs to protect
  - Social response
- Elapsed Time
- Vigilance
- Recovery Rate





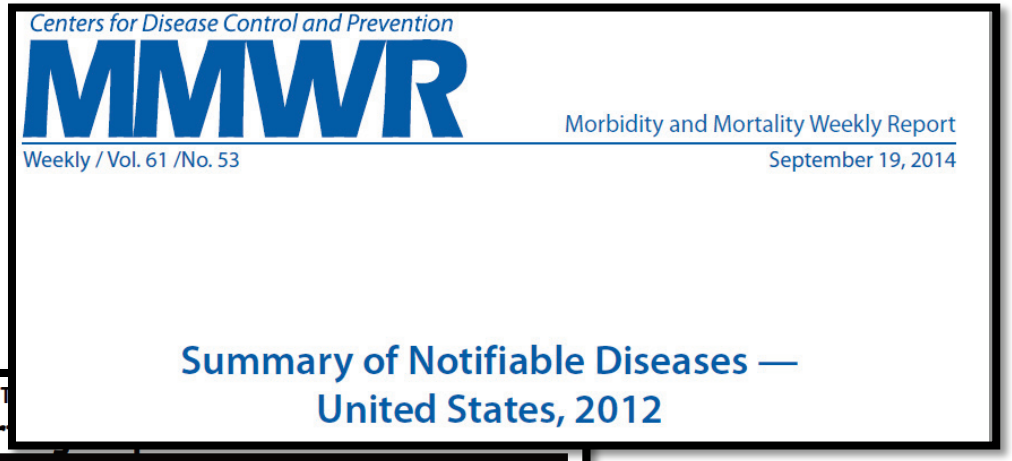
The Translation to Malware

Some Conclusions are Common to Both Healthcare and Malware

- "Risk Communication" is more effective than "Global Mandates" for actions
- Central reporting and incident response is important to containing the event
- Small groups of users engaging in risky behavior are a threat to the entire population
- Spread of infection can be arrested by
  - Immunization
  - Treatment (patching)
  - Awareness & active vigilance
  - Central reporting:
    a CDC for Malware?

Health Incident Reporting is Mandatory

- Centers for Disease Control
- World Health Organization
- State Health Departments



NEW YORK STATE DEPARTMENT

Communicable Disease Report

Reporting of suspected or confirmed communicable diseases is mandated under the New York State Sanitary Code (10NYCRR 2.10,2.14). The primary responsibility for reporting rests with the physician; moreover, laboratories (PHL 2102), school nurses (10NYCRR 2.12), day care center directors, nursing homes/hospitals (10NYCRR 405.3d) and state institutions (10NYCRR 2.10a) or other locations providing health services (10NYCRR 2.12) are also required to report the diseases listed below.

Anaplasmosis
Amebiasis
C Animal bites for which rabies prophylaxis is given[1]
C Anthrax[2]
C Arboviral infection[3]
Babesiosis
C Botulism[2]
C Brucellosis[2]
Campylobacteriosis
Chancroid
Chlamydia trachomatis infection
C Cholera
Cryptosporidiosis
Cyclosporiasis
C Diphtheria
E.coli O157:H7 infection[4]
Ehrlichiosis
C Encephalitis
C Foodborne Illness
Giardiasis
C Glanders[2]
Gonococcal infection
Haemophilus influenzae[5] (invasive disease)
C Hantavirus disease
Hemolytic uremic syndrome
Hepatitis A
C Hepatitis A in a food handler
Hepatitis B (specify acute or chronic)
Hepatitis C (specify acute or chronic)
Pregnant hepatitis B carrier
Herpes infection, infants aged 60 days or younger
Hospital associated infections (as defined in section 2.2 10NYCRR)
Influenza, laboratory-confirmed
Legionellosis
Listeriosis
Lyme disease
Lymphogranuloma venereum
Malaria
C Measles
C Melioidosis[2]
Meningitis
Aseptic or viral
C Haemophilus
C Meningococcal
Other (specify type)
C Meningococcemia
C Monkeypox
Mumps
Pertussis
C Plague[2]
C Poliomyelitis
Psittacosis
C Q Fever[2]
C Rabies[1]
Rocky Mountain spotted fever
C Rubella (including congenital rubella syndrome)
Salmonellosis
C Severe Acute Respiratory Syndrome (SARS)
Shigatoxin-producing E.coli[4] (STEC)
Shigellosis[4]
C Smallpox[2]
Staphylococcus aureus[6] (due to strains showing reduced susceptibility or resistance to vancomycin)
C Staphylococcal enterotoxin B poisoning[2]
Streptococcal infection (invasive disease)[5]
Group A beta-hemolytic strep
Group B strep
Streptococcus pneumoniae
C Syphilis, specify stage[7]
Tetanus
Toxic shock syndrome
Transmissable spongiform encephalopathies[8] (TSE)
Trichinosis
C Tuberculosis current disease (specify site)
C Tularemia[2]
C Typhoid
C Vaccinia disease[9]
Vibriosis[6]
C Viral hemorrhagic fever[2]
Yersiniosis

But Cyber Incident Reporting is NOT Mandatory!

What Is The Problem?

- Privacy protections
- Means of exchange
- Civilian vs. military control
- Limitations of use/disclosure
- Information accountability
- Monitoring authority
- Countermeasure authority
- Unfunded mandates
- Liabilities

ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

FEBRUARY 13, 2013 | BY RAINEY REITMAN

CISPA, the Privacy-Invading Cybersecurity Spying Bill, is Back in Congress

MARCH 19, 2015 | BY MARK JAYCOX

Senate Intelligence Committee Advances Terrible ~~"Cybersecurity" Bill~~ Surveillance Bill in Secret Session

Private entities are reluctant to share information that will be accessible to the government

Cyber Information Sharing: The Law

US Congress Passes a Cybersecurity Sharing Bill … on the 13th Attempt!

	H.R. 3674, the PRECISE Act of 2011, as reported from HHSC Subcmte on Cybersecurity (Lungren)	H.R. 3523, the Cyber Intelligence sharing and Protection Act of 2011, as reported from HPSCI (Rogers-Ruppersberger)	S. 2105, the Cybersecurity Act of 2012, as introduced (Lieberman-Feinstein)	S. 2151, the SECURE IT Act of 2012, as introduced (McCain)
WHAT INFORMATION MAY BE SHARED	-Notwithstanding any provision of law,	-Notwithstanding any provision of law,	-Notwithstanding any provision of law,	-Notwithstanding any provision of law
WHO MAY RECEIVE CYBERSECURIT Y RELATED INFORMATION	-New semi-private entity called the National Information Sharing Organization (NISO), which will be	-Any private or governmental entity if the protected entity gives consent, including military agencies such as the	- Any private entity (Sec. 3(a)), -DHS approved private exchanges	- Six existing federal 'cybersecurity centers' including the NSA, and offices at DHS, DoD,
HOW MAY INFORMATION BE USED / REDISTRIBUTED	-Federal government and private entities may use for CS purposes	-Federal government may use for any lawful purpose only if (A) not for	-Private entities can use, retain or further disclose in order to protect	-CTI given to a cybersecurity center may be disclosed to and
EXPANSION OF PRIVATE MONITORING/SURVEILLANCE and AUTHORIZATION TO TAKE COUNTERMEASURES	-Notwithstanding any other provision of law, CS providers with the express consent of a protected entity and self-protected entities may use 'CS systems to identify and obtain cyber threat information to protect the rights and property of	-'Notwithstanding any other provision of law, a CS provider, with the express consent of a protected entity for which such CS provider is providing goods or services for CS purposes, or self-protected entity may use 'CS systems to identify and obtain cyber	-Notwithstanding ECPA, FISA, or the Communications Act, any private entity may monitor its info systems and info that is stored on, processed by or transiting such info for cyber threats, and monitor 3rd party if it lawfully authorizes such	-'Notwithstanding any other provision of law, a private entity may, for the purpose of preventing, investigating or otherwise mitigating threats to information security on its own networks, or as authorized by
LIABILITY PROTECTION / IMMUNITY	-Provided against tort or criminal right of action in Fed or State court for failure to warn or disclose, provided the info is shared with NISO (sec. 248(b)(7) at p. 39),	-Against a CS provider or protected entity acting in good faith for 'using cybersecurity systems or sharing info' or 'for not acting on information obtained or shared in accordance with this section' (Sec. 2(b)(3) at p. 6).	-For monitoring (706(a)(1)), -For sharing with exchange, CI operators, customers of CS services or any other entity if an exchange is notified (706(a)(2)),	-For any entity for use, receipt or disclosure of cyber threat information or subsequent action or inaction of any lawful recipient of cyber threat information; (102(g)),

Cyber Information Sharing: The Communities

Even specialized sharing organizations have emerged

Now Reaching the Commercial Market

The OLD Way:

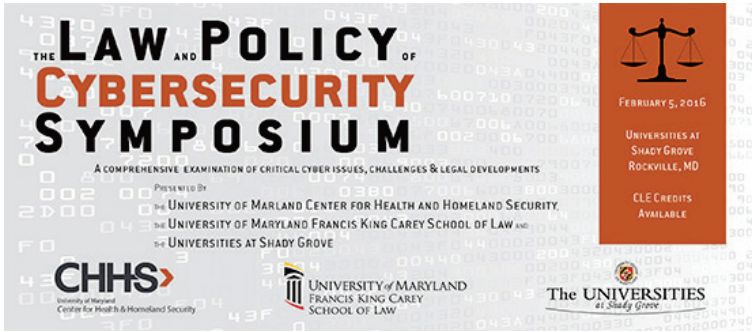
Pre-Execution	Execution	Post-Execution
▪ Hash-based - (semi) automated	▪ Memory-based (signature)	▪ IDS
▪ Human generics and heuristics (manual signature)	▪ IDS	▪ Memory analysis
▪ File reputation-based - cloud/local (late 2000s)	▪ Exploit detection	▪ Behavioral
▪ Policy (whitelist only) (late 2000s)		▪ SIEM (analytics)
▪ Machine learning-based models (2012)		▪ "Detect and respond" (ETDR)

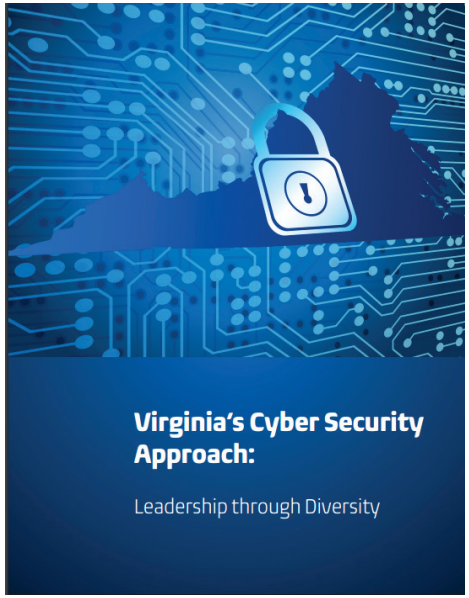
The NEW Way:

- Define a file ***genome***
- Learn patterns in good files and in malware
- Classification

Cybersecurity Law and Regulations

- CISA: Cyber Information Sharing Act
- Sector-Level Regulations (e.g. SEC, DoD, HHS)
- Corporate Board responsibilities
- Legal rulings
- Insurance Matters
- ***NY Data Security Act***





… and in Public Policy

Symbol	Type	Meaning	Constraint
x	choice variable	security investment	$x \geq 0$
t	choice variable	probability of truthful reporting	$t \in [0,1]$
a	choice variable	audit probability	$a \in [0,1]$
S	choice variable	sanction level	$S \geq 0$
q_2	parameter	security breach disclosure costs	$q_2 \geq 0$
γ	parameter	security interdependence	$\gamma \in [0,1]$
ϵ	parameter	error rate of detective controls	$\epsilon \in]0,1]$
b	parameter	effectiveness of an authority	$b \in [0,1]$
n	constant	number of firms	$n = 2$
q_1	constant	direct costs of a security breach	$q_1 = 1$
β	constant	security productivity	$\beta = 20$
L	function	sum of security breach related costs	
η	function	reduction of interdependence	
P	function	security breach probability	
c	function	expected costs due to security issues	
B	random variable	security breach	
D	random variable	security breach detection	
A	random variable	security audit	
α	realization	realization of B	
$\hat{\alpha}$	realization	realization of D	
$\tilde{\alpha}$	realization	choice on security breach reporting	
ψ	realization	realization of A	

The Economics of Mandatory Security Breach Reporting to Authorities

Stefan Laube*[1], Rainer Böhme[2]

[1] Department of Information Systems, University of Münster, Germany
Stefan.Laube@uni-muenster.de
[2] Institute of Computer Science, University of Innsbruck, Austria
Rainer.Boehme@uibk.ac.at

Information Systems Research
Vol. 16, No. 2, June 2005, pp. 186–208
ISSN 1047-7047 | EISSN 1526-5536 | 05 | 1602 | 0186

The Economic Incentives for Sharing Security Information

Esther Gal-Or
Katz Graduate School of Business, 368 A Mervis Hall, University of Pittsburgh, Pittsburgh, Pennsylvania 15260, esther@katz.pitt.edu
Anindya Ghose
Leonard Stern School of Business, New York University, New York, New York 10012, aghose@stern.nyu.edu

The first derivates of Eq. (9), w. r. t. t and x, are

$$\frac{\partial c}{\partial x} = [\gamma \cdot \eta(t^*) \cdot (1 - P(x)) + (1 - \gamma \cdot \eta(t^*) \cdot P(x))] \cdot L(t^*, 0) \cdot P'(x) + 1 \quad (18)$$

$$\frac{\partial c}{\partial t} = (1 - \epsilon) \cdot P(x^*) \cdot ((1 - P(x^*)) \cdot (\gamma \cdot q_2 \cdot \eta(t) - b \cdot \gamma \cdot L(t)) + q_2). \quad (19)$$

B.1 Optimal Security Investment

The root of the first-order condition $\partial c / \partial x = 0$ is

$$x^*(t^*) = -\frac{\log\left(\frac{\gamma \cdot \eta(t^*)+1}{4 \cdot \gamma \cdot \eta(t^*)} - \sqrt{\frac{(\gamma \cdot \eta(t^*)+1)^2}{16 \cdot \gamma^2 \cdot \eta(t^*)^2} - \frac{1}{2 \cdot \gamma \cdot \log(\beta) \cdot \eta(t^*) \cdot L(t^*,0)}}\right)}{\log(\beta)}. \quad (20)$$

[*Workshop on the Economics of Information Security (WEIS)* 2012, June 25-26, Berlin, Germany.]

Doing the Math …

- Security information sharing is almost always a good "social" policy, and can be shown to benefit companies individually as well – even competitors.
- Reporting policies are most effective in conjunction with
  - low "disclosure costs" (costs to report and remediate),
  - highly-effective "detective controls" (companies must have effective means to detect intrusions, or else they are unfairly punished for missing them)
  - highly effective dissemination of knowledge from the informed authority, and
  - firms that have a high degree of "security interdependence" (a breach in one company increases the probability of a breach at another company)
- Any effective policy will include a significant -- but not excessive -- probability of audit. Without this, even large sanctions/penalties will not increase the level of compliance

Opportunities

Business is good

And there are a lot of open questions:

- Generalization to generic “optimal policy” for government
- How to model and incorporate privacy

Awareness, Vigilance, Susceptibility