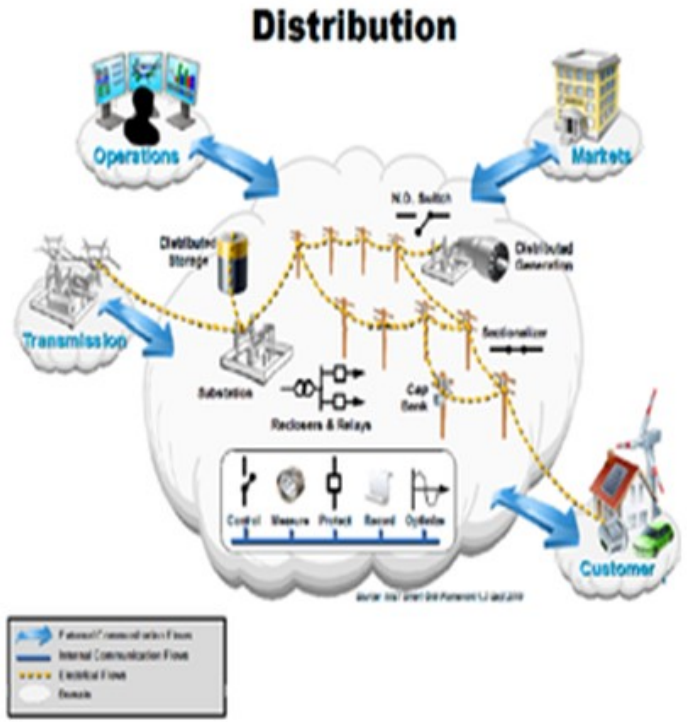
Mitigating and Managing the Risk of a Cyberphysical Cat (Event)

NECPUC Symposium, May 22nd, 2018
Samantha Kappagoda
RiskEcon® Lab @ NYU Courant of Mathematical Sciences
Numerati Partners LLC



Cyber Incidents by Sector: Fiscal Year 2012

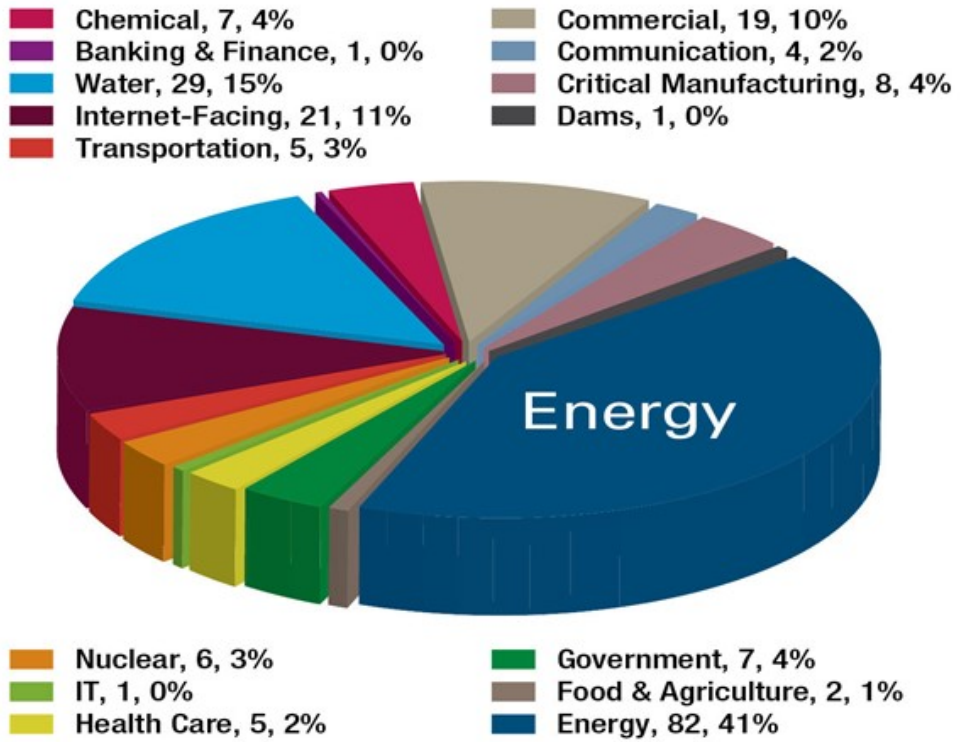
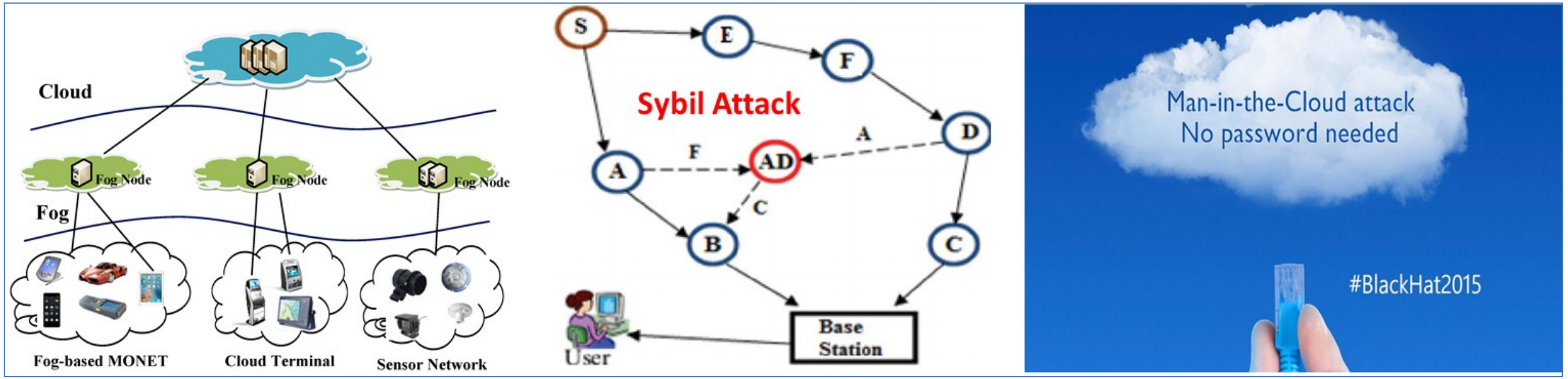


Image source: DHS Industrial Control Systems Cyber Emergency Response Team, ICS-CERT Monitor

Risk of a Cyberphysical Cat: Analogous Lessons and Cautionary Tales from Financial Crises

- Jevons: Economics of technology adoption drives these risks
  - Pandora's box: cannot put the genie back in the bottle
- Similar to contagion from propagated susceptibility (hardware, software defects) coupled with (ad hoc) network interconnectivity leading to cascading event (knock-on effects), i.e. fleets, electricity, water, telecom, …
- Result: Low-cost cyber exploits can cause devastating physical damage!!!

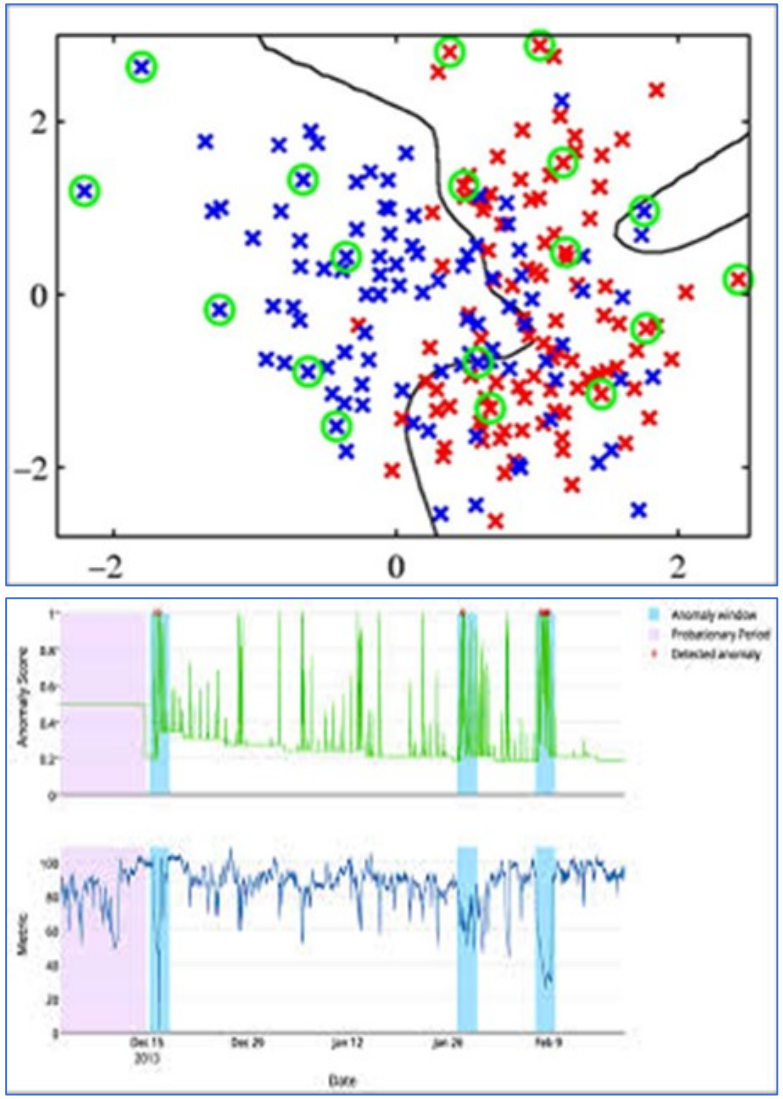


Mitigant (A) Enumeration: Analogous to Legal Entity Identification

- A *network enumerator* (or *network scanner*) is a program:
  - Retrieves usernames and info about groupings, sharing, and services of networked computers
  - Scans networks for vulnerabilities in the security of that network. If there is a vulnerability with the security of the network, it will send a report back to a hacker who may use this info to exploit that network glitch to gain entry to the network or for other malicious activities
- Ethical ("*white hat*") hackers often also use the information from enumeration to remove the glitches and strengthen their network, since malicious ("*black-hat*") hackers can, on entry of the network, employ enumeration to identify and access security-sensitive information or corrupt the network
- Enumeration and network analysis can be used to sterilize, immunize and quarantine code to reduce attack surfaces from redundant or dormant code
  - Example: Ford F-150 has 150 Million lines of code

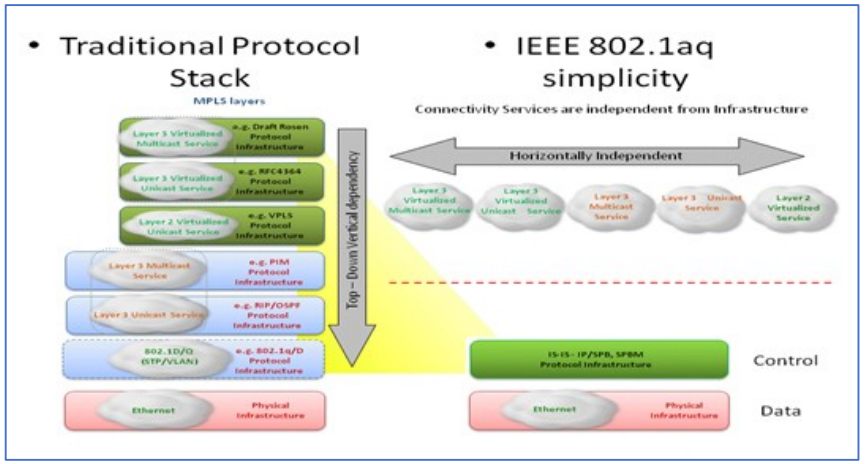
Mitigant (B) Anomaly Detection & Simulation: Analogous to “market watch”

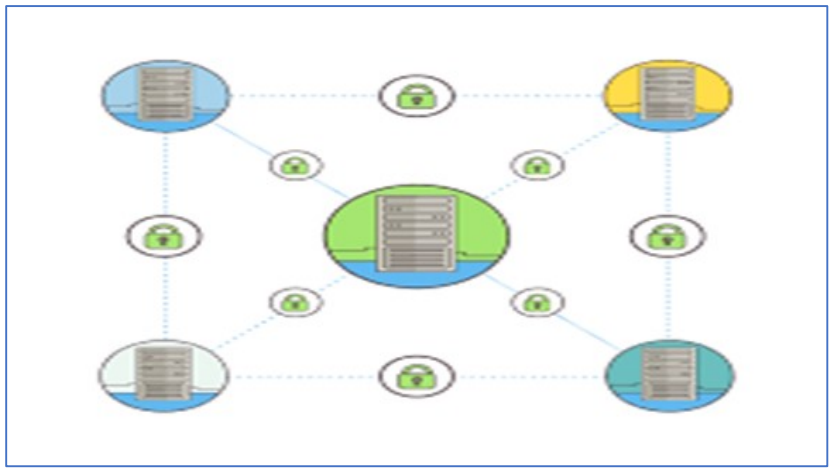
- Surveillance for Anomaly detection:
  - Pattern recognition
  - Classification
- Simulation of shocks to *ad hoc* network configuration
- Multi-purpose:
  - Adaptive system maintenance
  - Testing system reliability with changing conditions (e.g. system response to demand shocks and weather-related load imbalances)
  - Early-warning against system failures and exploitation



Mitigant (C) Iterative and Adaptive Encryption: Analogous to Dynamic Hedging

- Iteratively adapt encryption and actively employ key
  - Reduce availability of attack surfaces
  - Present a moving target
- Randomize and keep a low(er) profile:
  - Shortest Path Bridging (SPB) protocol (IEEE standard labeled 802.1aq) is increasingly being deployed to reduce the visibility of IP Addresses
  - Random rotation of proxy IP addresses might be adopted as a further countermeasure to mitigate attacks by reducing silhouette





Cost/Benefit Tradeoff: Is it Worth it?

- Given proliferation of M2M and IoT, Cyberphysical exposure is emerging to becoming the dominant, ubiquitous risk (e.g. product defect, interoperability failures, cyberterror)
  - Cyber Risk is already quite pervasive: by way of example, $23 Billion Premium vs $445 Billion Losses
  - Exploit frequency high and increasing
  - Potential likelihood and conditional loss:
    - Nontrivial likelihood
    - Catastrophic Exposure (comparable to EMP)

- US Cyber grid attack loss estimate: $71 Billion (Lloyds/Cambridge University)
- Cyber cloud attack estimate: >$13 Billion (Lloyds/AIR)

- Estimates likely too low: *ad hoc* networks and contagion
- Cascade failure dynamics similar to traffic and congestion
  - Endogeneity and mispricing of event risk
  - Cascades and externalities (feedback loops)
  - Ad hoc networks, imbalance, and instability

7

How to Price and Implement It?

- Given the likelihood and severity of cyberphysical risk similar to scope/scale of a pandemic or EMP
  - By way of illustration, risk of prolonged US infrastructure impairment (i.e., electricity, water, communication) similar to Puerto Rico, but on a regional, superregional or national scale
  - Compounded by weather/other environmental events

- Scalable system-level risk monitoring and mitigation services:
  - Active Surveillance (both hardware and software)
  - Adaptive Defensive Measures
  - Early-Warning Alerts (Anomaly Detection; Simulation)
  - Dynamic Redundancy (Mesh Network)
  - Rapid Response and Recovery Capabilities

- How to finance: Tolling for fixed and variable costs
  - Capacity-based: fixed tolling for overhead (installing and maintaining reserve capability)
  - Volume-based: variable tolling frequency, type and size of packet-flow
  - Other tolling: congestion-based, complexity and variability

Recent cyber attacks on Critical Infrastructure

Stuxnet Malware (2010-2012)

- Sophisticated attack on nuclear manufacturing facilities in Iran
- US/Israel malware exploits vulnerabilities in Microsoft Windows

Power Plant (2012)

- Plant shut down for three days after technician unknowingly inserts virus infected USB disk
- US Dept of Homeland Security declines to share additional information

Water Supply (2011)

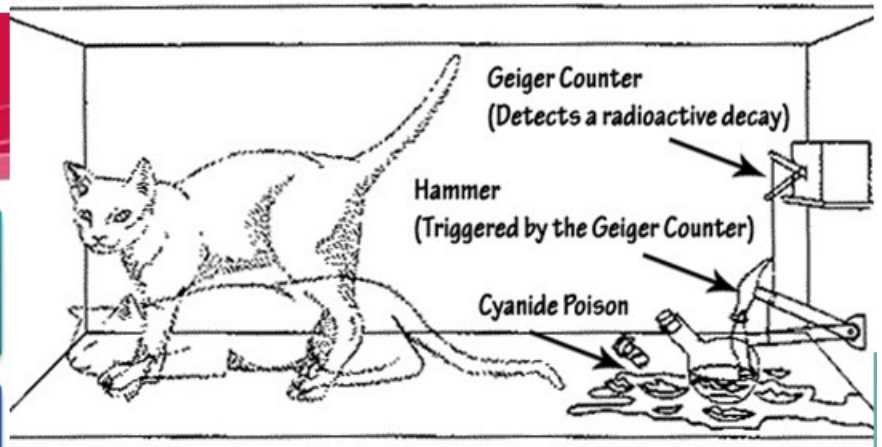
- Critical pump damaged by Russian hackers
- Cycled pump on/off until it burned out

Rail Network (2011)

- Hackers manipulated railway company computer systems
- Disrupted rail service – could have been much worse

Chemical Plant (2011)

- PoisonIvy malware infected systems at more than 48 chemical and defense companies
- Source of attack traced back to China



9

RiskEcon® Lab for Decision Metrics @ Courant

- The focus of RiskEcon® Lab @ Courant Institute of Mathematical Sciences, New York University (https://cims.nyu.edu/riskeconlab/), is to facilitate the development of software, analytics tools, and semantic libraries that employ high-dimensional datasets to integrate conventional data with web-enabled demographic, biometric, psychometric and sociometric data from innovative sources, by applying a range of computational and analytical methods to commercial, consumer and population-related societal trends, focusing primarily on research and development (R&D).
- Our goal is to integrate web-enabled crowdsourcing with machine learning, data-mining, and text-mining, in order to promote research fundamental to large-scale, real world questions, employing applied computational statistics, and robust and scalable data analytic solutions.
- RiskEcon® Lab for Decision Metrics was established in 2011 at Courant Institute of Mathematical Sciences, an independent division of New York University (NYU). Courant is considered to be one of the world's leading mathematics educational and scientific research centers, and has been ranked first in research in applied mathematics. RiskEcon® Lab is the cornerstone of the Computational Economics and Algorithmic Data Analytics (CEcADA) cooperative at New York University, established concurrently in 2011.

Numerati Partners LLC

The mission of Numerati® Partners LLC is to manage privately-held data analytics investment and development consortia in order to curate the next generation of scalable data-intensive risk and liability management enterprises, by providing resources critical to accelerating the development of nascent leading-edge inferential surveillance, monitoring, and cyberphysical distributed network analytics technologies for deployment in forensic domains of *RiskTech*, *LitTech* and *FinTech* (i.e. risk technology, litigation technology and financial technology).

Numerati-affiliated consortia curate and commercialize domain-specific use-case applications via systems integration and managed service provider platforms, by employing fully-integrated, risk technology-oriented domain-specific and customized data analytics-driven enterprise solutions, i.e. *Solutions-as-a-Service* (SolaaS) that implement and maintain use-case applications via proprietary value-added reseller arrangements of *Software-as-a-Service* (SaaS), *Infrastructure-as-a-Service* (IaaS), *Platform-as-a-Service* (PaaS) functionality.

RiskEcon® & Numerati® Eco-System

- RiskEcon® Lab for Decision Metrics @ New York University
- Courant Institute of Mathematical Sciences
- General descriptions of other participants:
  - Cyberphysical risk engineering (telematics) spinoff (CEO formerly engaged with Batelle, DARPA and other programs)
  - Global leader in economic regulatory analysis, liability, litigation-risk, causation and damages analysis
  - Social media surveillance and monitoring development teams
  - Wearable tech (telemetrics) monitoring development team
  - Remote-sensing platforms (cellular, satellite, etc.)
  - Leading global Technology Infrastructure-as-a-Service providers
  - AFL-CIO leadership
  - Governmental agencies (e.g. NOAA, NTSB, DOT, etc)
  - NGOs (agriculture, environmental and conservation science, etc.)
  - Other Academic Research Institutions, Financial and Technology Industry Participants …

Samantha Kappagoda
David K.A. Mordecai

RiskEcon® Lab for Decision Metrics @ NYU Courant
Numerati® Partners LLC
Risk Economics®, Inc.