COMMUNICATIONS & ADMINISTRATION WORKSHOP
Strategies for Success
MARCH 12-14, 2017 TAMPA, FLORIDA

IBTTA
TOLLING. MOVING SMARTER.

Cyber Security – Managing Threats to Customer Data and Privacy

Moderator: Rosa C. Rountree
Chief Executive Officer
Egis Projects, Inc.

Panelists

Adam C. Losey

Senior Counsel

Foley and Lardner LLP

Special Agent Andrew Lenzen

Federal Bureau of Investigation

Dr. Waseem Naqvi

Director Technology

Raytheon Highway Transportation Solutions

In 2017, are we better prepared than Target in 2013?

Hacker posed as HVAC vendor installed malware an access through the security and point-of-sales system designed to steal every credit card used at the company's 1,797 U.S. stores that were stored on Target's server.

U.S. Department of Justice notified the retailer of the breach on December 12. Target confirmed and eradicated the malware on December 15. In a press release at 6 a.m. on December 19 Target publicly confirmed, three (3) weeks after customer data was first scooped up on Black Friday.

Richard Blumenthal stated "it appears that Target may have failed to employ reasonable and appropriate security measures to protect personal information".

Results and Response

Debit and credit cards stolen from **40 million accounts and 70 million customers** names, addresses, phone numbers, and email addresses were also hacked

Target Chairman, President and CEO, Gregg Steinhafel issued an email statement – "Target was certified as meeting the standard for Payment Card Industry (PCI) in September 2013…"

Bloomberg - March 17, 2014

The cost for not managing customer data and privacy in 2013.

Target offered customers – free credit monitoring services, identity theft protection, set up a telephone hotline, and a 10% discount on selected days.

By February 1, 2014 Target has spent $61 million responding to breaches.

March 19, 2015 Target *settled to pay $10 million to victims.*

Target used a third-party forensics firm to investigate .. Recommendations included: designation of a Chief Information Security Officer and provide security training to its employees.

Breakdown in the organizational structure and workforce.

Six (6) months prior to the attack, Target installed $1.6 million in malware detection and monitoring. *Target ignored the alarms and warnings received around Thanksgiving pointing to the same server in Russia …*

FireEye's alerts occurred on Nov 30 and again on December 2, when hacker installed yet another version of malware prior to transmitting the stolen credit card data out of Target's network.

Bloomberg - March 17, 2014

Cyber attacks are growing.

Yahoo Reveals 32 Million Accounts Were Hacked Using 'Cookie Forging Attack' *…March 01, 2017* Mohit Kumar

The Hacker News

Yahoo has just revealed that around 32 million user accounts were accessed by hackers in the last two years using a sophisticated cookie forging attack without any password. These compromised accounts are in addition to the Yahoo accounts affected [...

Ransomware Crooks Demand $70,000 After Hacking San Francisco Transport System – UPDATED … *November 25, 2016* Thomas Fox-Brewster

Forbes

The Perfect Weapon: How Russian Cyber power Invaded the US ... *Dec 14, 2016* – The New York Times

An investigation reveals missed signals, slow responses and a continuing underestimation of the seriousness of a campaign to disrupt the ...

How A Simple Command Typo Took Down Amazon S3 and Big Chunk of the Internet *…March 02, 2017*

Swati Khandelwal

The Hacker News

The major internet outage across the United States earlier this week was not due to any virus or malware or state-sponsored cyber attack, rather it was the result of a simple TYPO. Amazon on Thursday admitted that an incorrectly typed command during [...]

Internet-Connected Teddy Bear Leaks Millions Of Voice Messages and Password … *February 27, 2017* Swati Khandelwal

The Hacker News

Every parent should think twice before handing out Internet-connected toys or smart toys to their children, as these creepy toys pose a different sort of danger: privacy and data security risks for kids who play with them. This same incident was happened [...

What Now

Friday evening, Nov. 25, 2016
SFMTA Infrastructure Manager Sean Cunningham receives an email

"**You Hacked, ALL Data Encrypted**." Muni was hit in a so-called "spray and pray" attack, *"We don't attention to interview and propagate news! Our software working completely automatically and we don't have targeted attack to anywhere! SFMTA network was Very Open and 2000 Server/PC infected by software! So we are waiting for contact any responsible person in SFMTA …"*

He claimed to have breached a Windows 2000 server at the Muni. In their broken English, the hackers said: "Company don't pay attention to Your safety! They give your money and everyday rich more! But they don't pay for IT security and using very old systems!"

The hacker said he had compromised thousands of computers at the SFMTA, scrambling the files on those systems with strong encryption. The files encrypted by his ransomware, he said, could only be decrypted with a special digital key, and that key would cost 100 Bitcoins, or approximately USD $73,000.

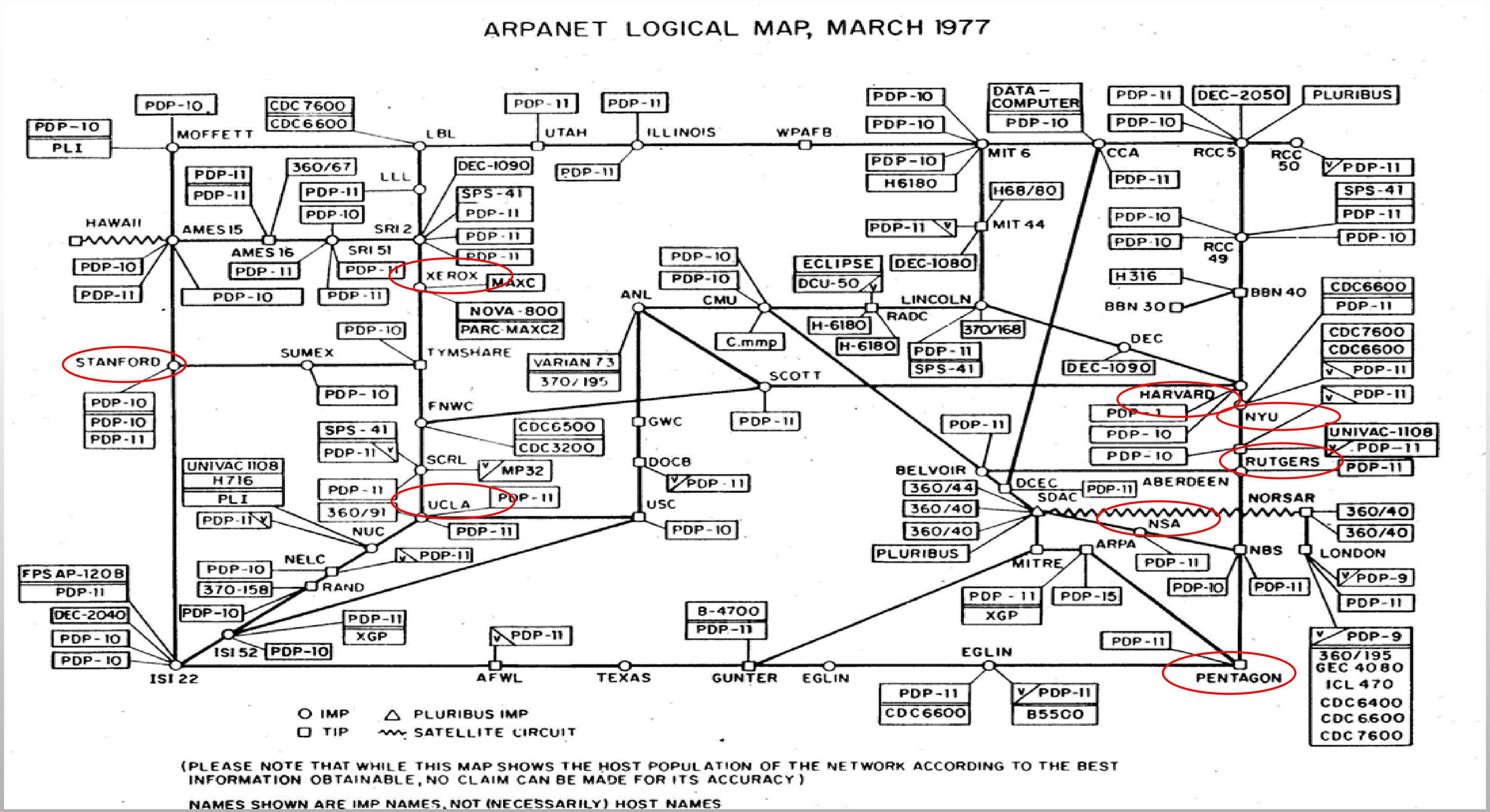
According to the Cryptom27 crew, all payment kiosks, internal automation systems and email were compromised. Signing off, they threatened to leak 30GB of the Municipal Transportation Agency's databases and documents, including "contracts, employees' data [and] customers, if the organization didn't accept the hackers' help in securing their systems.

San Francisco Metropolitan Transit Authority statements to the public.

"We can confirm a cyber attack. It disrupted some of our internal computer systems, such as email. Fare gates are again operational," a spokesperson from the Municipal Transportation Agency said over email. "We opened them on Friday and Saturday as a precaution to minimize any possible impacts to customers. There has been no impact to transit service, to our safety systems or to our customers' personal information. The incident remains under investigation, so it wouldn't be appropriate to provide any additional details at this point."

"The SFMTA has never considered paying the ransom. We have an information technology team in place that can restore our systems and that is what they are doing," said SFMTA spokesman Paul Rose. "Existing backup systems allowed us to get most affected computers up and running this morning, and our information technology team anticipates having the remaining computers functional in the next two days."

The Internet is slightly more complicated than it was in 1977.

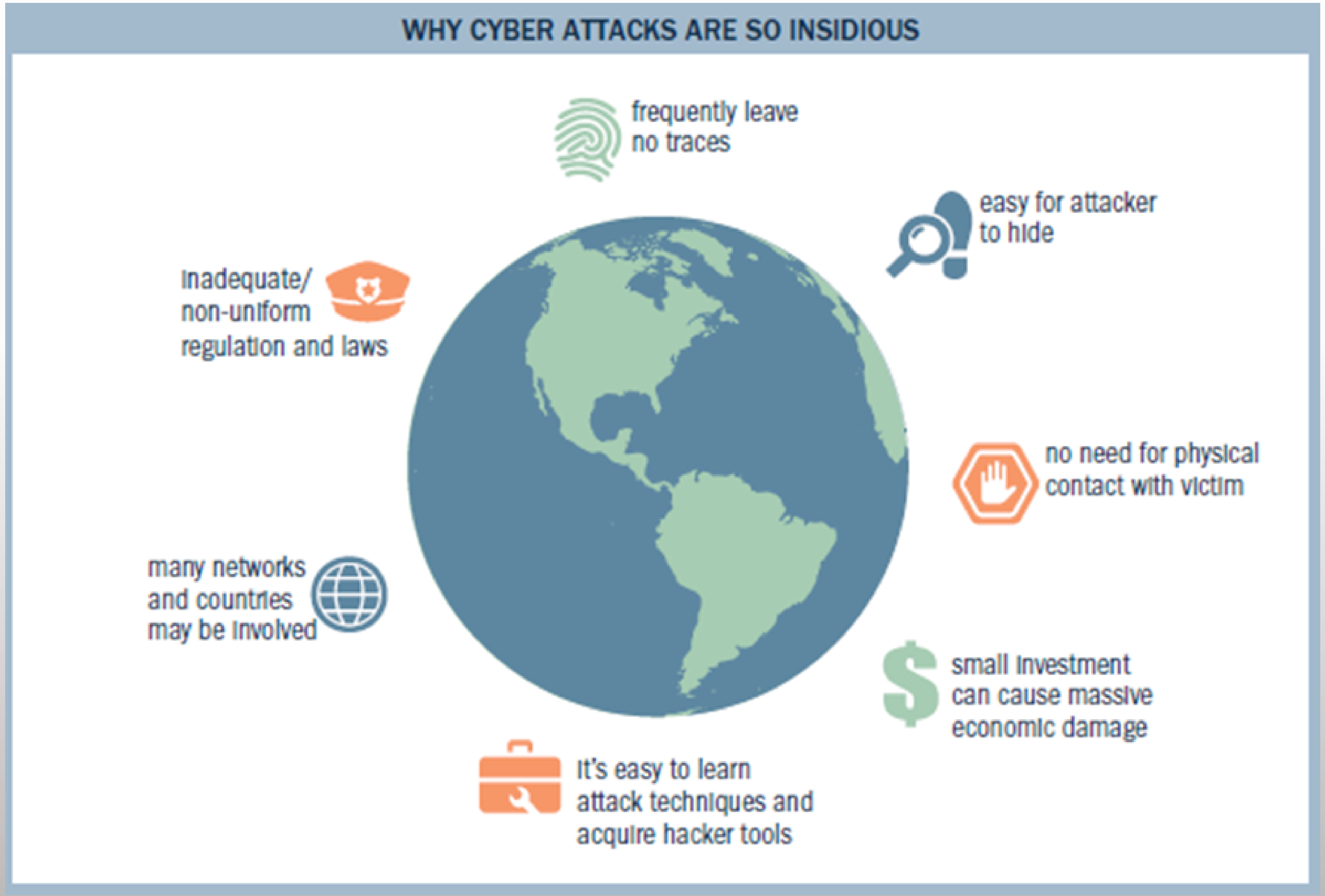


ARPANET LOGICAL MAP, MARCH 1977

(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)

NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

Why cyber threats are uniquely different.



WHY CYBER ATTACKS ARE SO INSIDIOUS

frequently leave no traces

easy for attacker to hide

no need for physical contact with victim

small investment can cause massive economic damage

it's easy to learn attack techniques and acquire hacker tools

many networks and countries may be involved

inadequate/ non-uniform regulation and laws

- The threat is incredibly serious—and growing. Cyber intrusions are becoming more commonplace, more dangerous, and more sophisticated.
- Our nation's critical infrastructure, including both private and public sector networks, are targeted by adversaries.
- The FBI is the lead federal agency for investigating cyber attacks by criminals, overseas adversaries, and terrorists.

Why cyber threats are uniquely different.

U.S. Senator John McCain opening statement on March 2, 2017 at a hearing on cyber strategy policy said “the threats to the U.S. in cyber space continue to grow in scope and severity”.

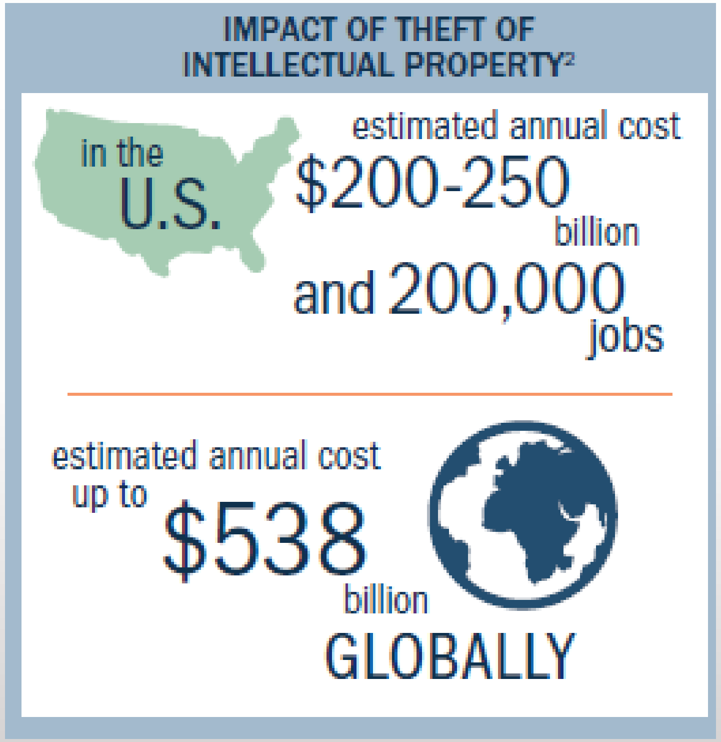
Cyber weapons are often deployed under a cloak of anonymity, making it difficult to figure out who is really responsible.

Cyber attacks can achieve a broad range of effects, most of which are disruptive and costly, but not catastrophic.

- “Dumps – credit card will make you rich!”
- Shopper can buy credit card individual card numbers or load up by the thousands and get a bulk discount.

Cybersecurity by the numbers

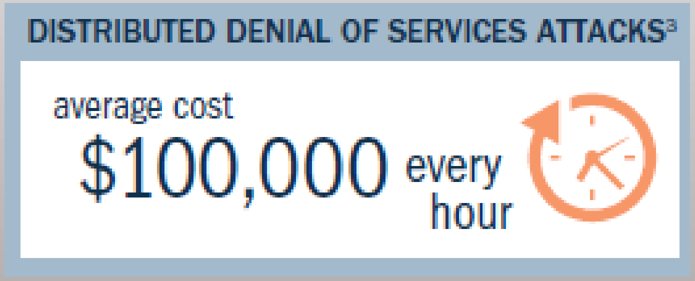
Transportation is an increasingly vulnerable sector for cyber attacks. The most common techniques involve DDOS attacks, ransomware based extortion, and malicious attachments and links.



IMPACT OF THEFT OF INTELLECTUAL PROPERTY[2]

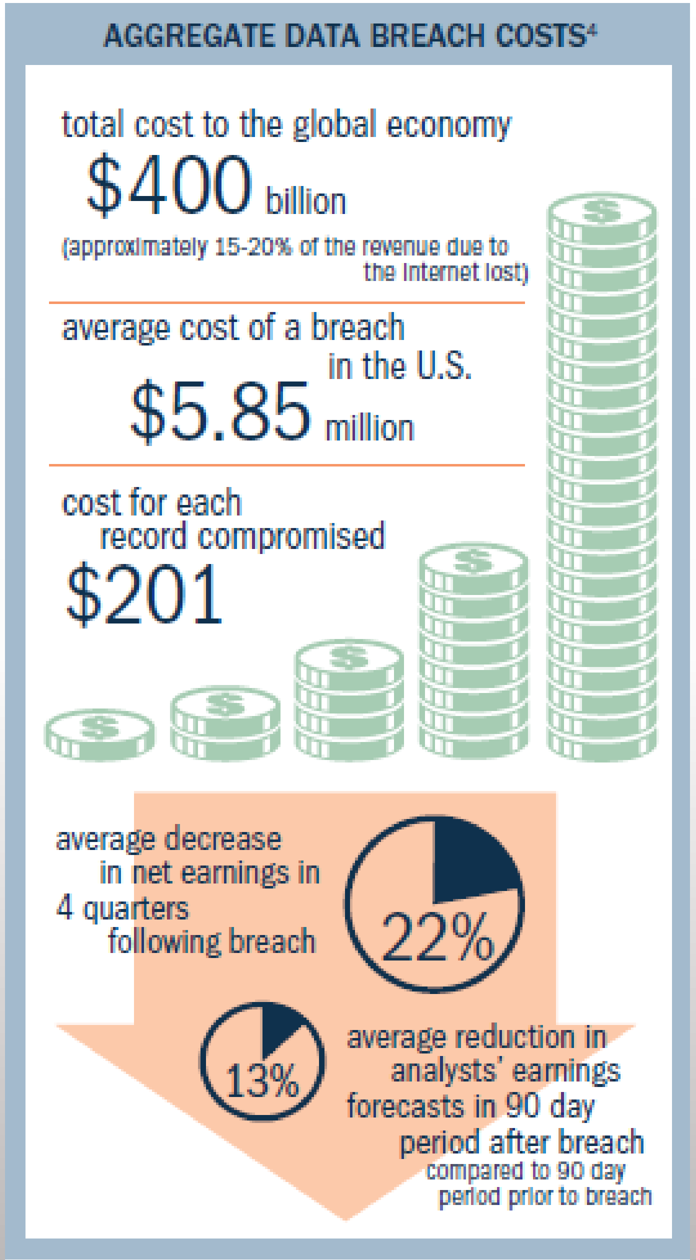
in the U.S. estimated annual cost $200-250 billion and 200,000 jobs

estimated annual cost up to $538 billion GLOBALLY



DISTRIBUTED DENIAL OF SERVICES ATTACKS[3]

average cost $100,000 every hour



AGGREGATE DATA BREACH COSTS[4]

total cost to the global economy $400 billion (approximately 15-20% of the revenue due to the Internet lost)

average cost of a breach in the U.S. $5.85 million

cost for each record compromised $201

average decrease in net earnings in 4 quarters following breach 22%

13% average reduction in analysts' earnings forecasts in 90 day period after breach compared to 90 day period prior to breach

[4] Research Report, *2014 Cost of Data Breach Study: Global Analysis*, Ponemon Institute (2014).

COMMUNICATIONS & ADMINISTRATION WORKSHOP
Strategies for Success
MARCH 12-14, 2017 TAMPA, FLORIDA

Raytheon

20,000 Customers Across Industries

BIO-TECH
Dow MONSANTO Celgene

ENERGY & NATURAL RESOURCES
BAKER HUGHES HESS ExxonMobil Anadarko Petroleum Corporation

FINANCIAL SERVICES
SallieMae M&T Bank FINANSBANK BB&T RBS KKR ZURICH

GOVERNMENT & DEFENSE
GENERAL DYNAMICS
UNITED STATES SENATE
Australian Government Department of Defence
Ministry of JUSTICE

FOOD SERVICES AND PRODUCTS
CHS SMUCKER'S Yum!

TECH & PROFESSIONAL SERVICES
accenture High performance. Delivered. cisco Adobe pwc Cloudpath Google

HEALTHCARE SERVICES
CENTENE corporation AmerisourceBergen American Red Cross UnitedHealth Group CVS CAREMARK

HOTELS, MOTELS AND RESORTS
Marriott HOTELS · RESORTS · SUITES starwood Hotels and Resorts WYNN RESORTS

INFORMATION TECHNOLOGY
DELL L3 communications Panasonic Canon United Technologies intel

MANUFACTURING
GM HARLEY-DAVIDSON MOTOR CYCLES 3M MATTEL EMERSON

MEDIA AND ENTERTAINMENT
FOX 21ST CENTURY FOX VIACOM Paramount

RETAIL AND WHOLESALE
ebay COACH Zappos RALPH LAUREN Walmart

TELECOMMUNICATIONS
at&t COX COMMUNICATIONS Charter COMMUNICATIONS QUALCOMM Comcast BROADCOM HARRIS

TRANSPORTATION
AVIS SOUTHWEST AIRLINES BRITISH AIRWAYS PENSKE CSX CORPORATION

UTILITY
PG&E Sempra Energy nrg

OEM
JUNIPER NETWORKS f5

FORCEPOINT POWERED BY Raytheon

Are Intelligent Transportation Systems Addressing Cyber as Aggressively as other Industries?

IBTTA TOLLING. MOVING SMARTER.

Waseem Naqvi - Cleared for publication under EXIM 2017-007-CON

Intelligent Transportation Systems

Connected Vehicles

Autonomous Vehicles

RFID

LIDAR

Image Capture

Video Stream

Localization

Mechanical

…

Sensors

Communications

Command & Control

Subway Ticketing

Highway Tolling

SPOOFING SNOOPING STEALING

Security and the Cloud

Essential Characteristics:

- Rapid elasticity
- Resource pooling
- Measured service
- Broad network access
- On-demand self-service

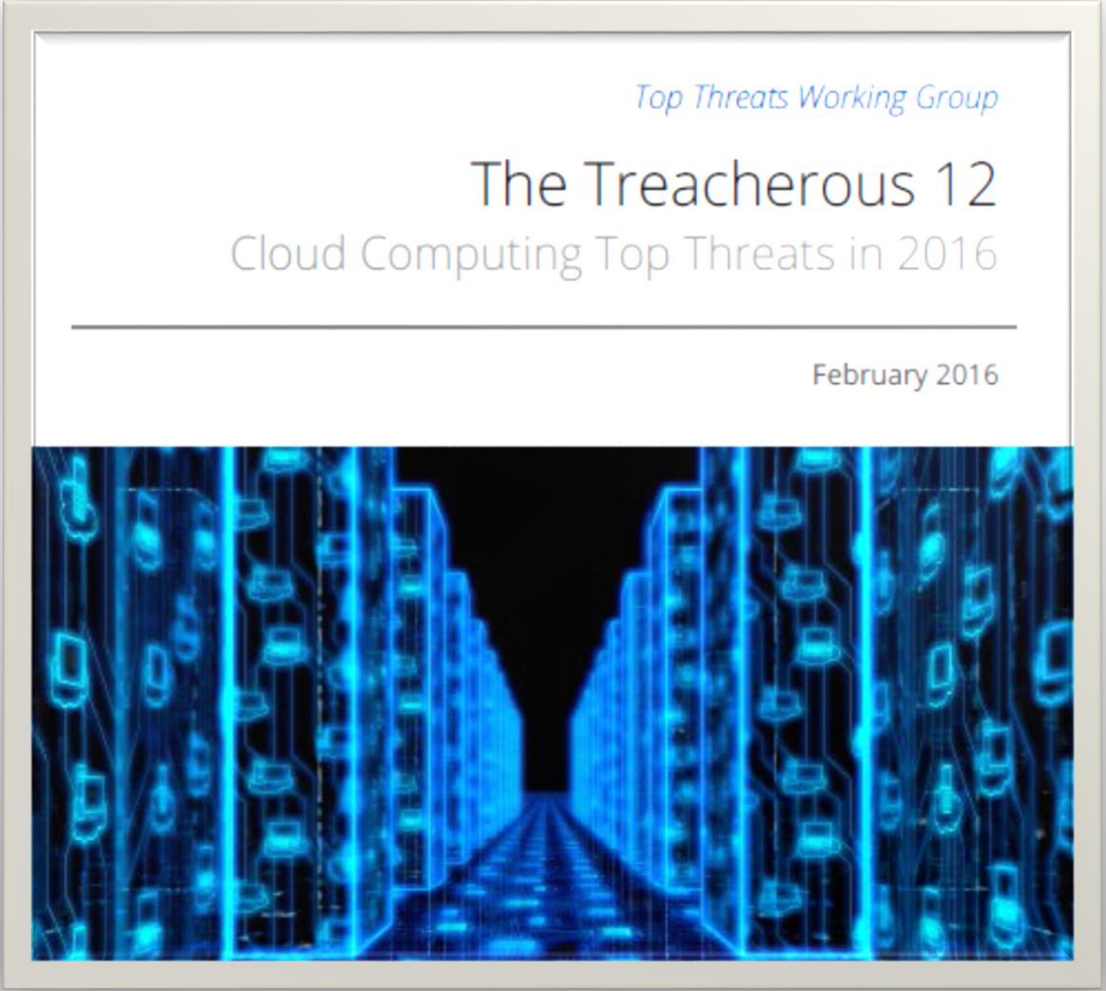
Image licensed from GlobeDevicesshutterstock_189001601_Cmpr.jpg

- **NIST SP 800-145, Mell and Grance, September 2011**
  - Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Cloud Based Utilities Enable Scaling at Cost of Control

The Treacherous 12

- Data Breaches
- Weak Identity, Credential and Access Management
- Insecure APIs
- System and Application Vulnerabilities
- Account Hijacking
- Malicious Insiders
- Advanced Persistent Threats (APTs)
- Data Loss
- Insufficient Due Diligence
- Abuse and Nefarious Use of Cloud Services
- Denial of Service
- Shared Technology Issues



Top Threats Working Group

The Treacherous 12

Cloud Computing Top Threats in 2016

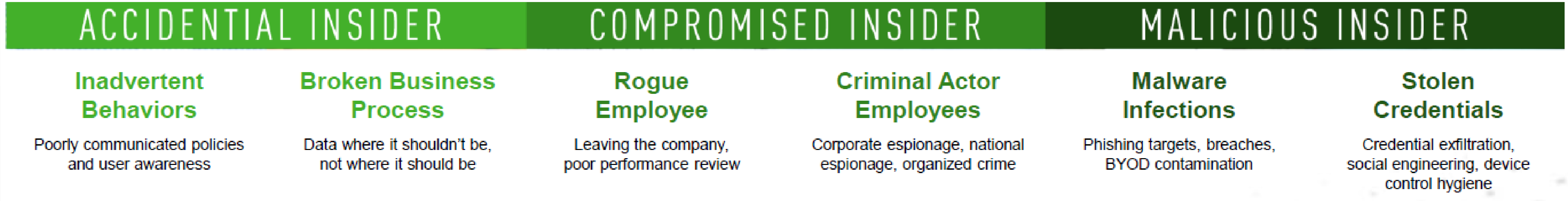
February 2016

www.cloudsecurityalliance.org

Loss of Control Enables Threats on the Cloud

Threats

Insider



ACCIDENTIAL INSIDER		COMPROMISED INSIDER		MALICIOUS INSIDER	
Inadvertent Behaviors	**Broken Business Process**	**Rogue Employee**	**Criminal Actor Employees**	**Malware Infections**	**Stolen Credentials**
Poorly communicated policies and user awareness	Data where it shouldn't be, not where it should be	Leaving the company, poor performance review	Corporate espionage, national espionage, organized crime	Phishing targets, breaches, BYOD contamination	Credential exfiltration, social engineering, device control hygiene

External

FINANCIAL	ESPIONAGE	MALICIOUS
Ransomware, Theft, User Information	Information, Secrets, Plans	Disruption Terrorism
Phishing, Insider Threat, Malware, USB	Phishing, Social Engineering Device Control Hygiene	Advanced Persistent Threats (APTs), Phishing, Social Engineering, Device Control Hygiene

Average US Corporation Actively Defend Against >100,000 Attacks Per Day

What should an agency do to prepare and respond to an incident?

Are my cyber policies documented?
Are they reasonable?
Are my employees actually following the policies?
Am I using tech that helps enforce these policies?
The user is the MOST IMPORTANT SECURITY MEASURE.

Prioritize Security Efforts!

According to the 2014 IBM Cyber Security Intelligence Index, over 95% of all threat incidents investigated involved human error. Malwarebytes LABS March 16, 2016

How to Think about Protecting Your System

- Risk Assessment
  - Vulnerability
  - Penetration Tests
- Operations
  - Prevention
  - Protection
  - Detection
  - Incident Response
- Engineering
  - Security Architecture
  - Access Control
  - Development

Educate yourself on information security and form a information security committee.

CYBERSECURITY AWARENESS

Stop.Think.Connect.™

- National public awareness campaign aimed at increasing the understanding of cybersecurity threats and empowering all Americans to be safer and more secure online. Resources are available at www.dhs.gov/stopthinkconnect
- October is National Cyber Security Awareness Month. Learn more at www.dhs.gov/national-cyber-security-awareness-month

CERTIFICATIONS

Visit NICCS for more information on certifications

- Payment Card Industry Data Security Standards (PCI DSS)
- Comp TIA SECURITY+
- Certified Information Systems Security Professional
- GIAC Security Essentials (GSEC)

Establish cybersecurity policies and processes.

Your cybersecurity policy should include specific on controls.

- Which security programs will be implemented *(Example: In a layered security environment, endpoints will be protected with antivirus, firewall, anti-malware, and anti-exploit software.)*
- How updates and patches will be applied *(Example: Set frequency for browser, OS, and other Internet-facing application updates.)*
- How data will be backed up *(Example: Automated backup to an encrypted cloud server with multi-factor authentication.)*

Your policy should identify roles and responsibilities.

- Who issued the policy and who is responsible for its maintenance
- Who is responsible for enforcing the policy
- Who will train users on security awareness
- Who responds to and resolves security incidents and how
- Which users have which admin rights and controls

COMMUNICATIONS & ADMINISTRATION WORKSHOP
Strategies for Success
MARCH 12-14, 2017 TAMPA, FLORIDA

Establishing acceptable use condition for employees.

Banning all Internet and social media usage would certainly keep your company safe from on-line attack, but it could be potentially counterproductive.

- Some guidelines might include:
  - How to detect social engineering statics and other scams
  - What is an acceptable internet usage
  - How remote workers should access the network
  - How social media use will be regulated
  - What password management system might be utilized
  - How to report security incidents

Be vigilant of suppliers and embed information security in new relationships.

Attackers increasingly exploit weaknesses in third-party suppliers' networks to access data and assets from target companies.

- Contract documentation should include meaningful cybersecurity provisions related to liability and indemnification for incidents and identify the security policies and procedures that the supplier will be expected to comply with during the term.
- Including adequate audit and risk assessment provisions for regular risk assessments and remediation plans (annual at a minimum), of the supplier's operations.

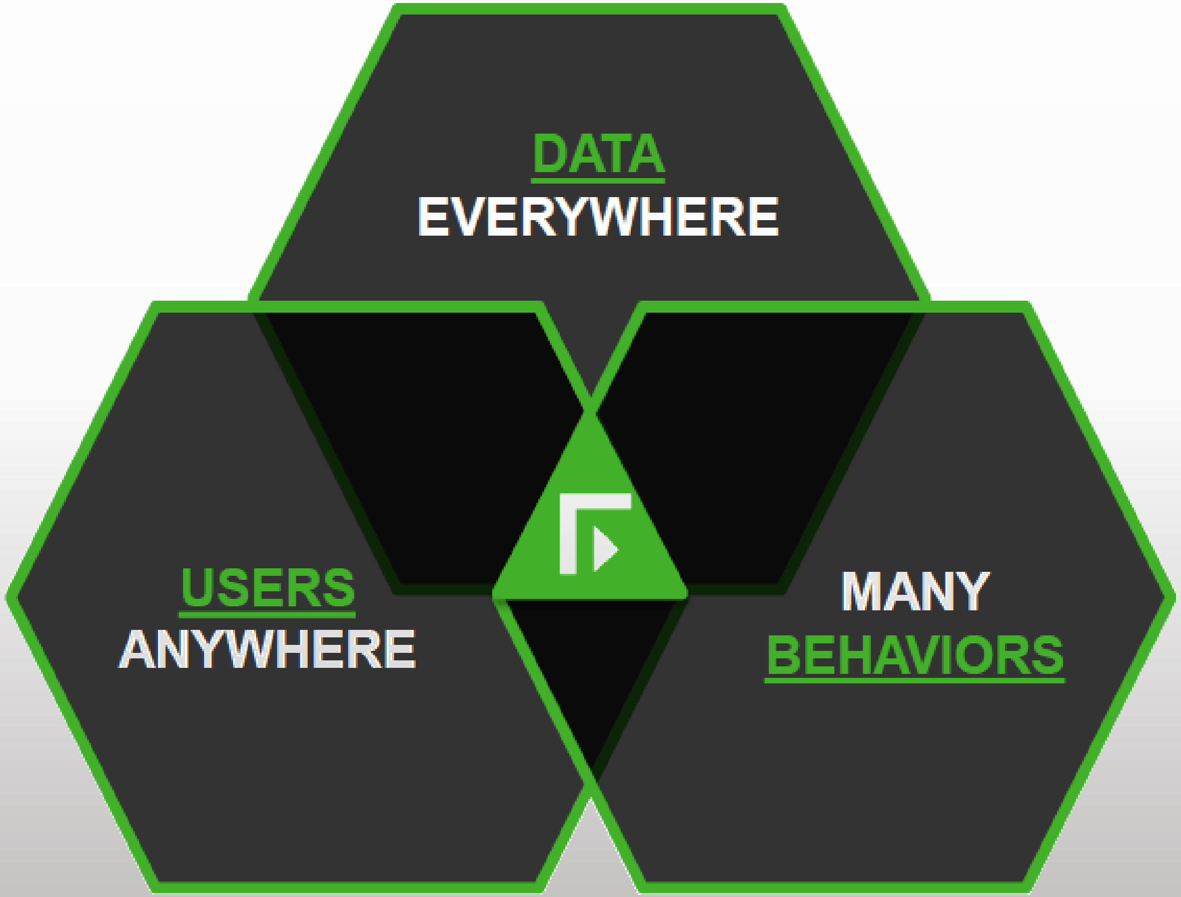
COMMUNICATIONS & ADMINISTRATION WORKSHOP
Strategies for Success
MARCH 12-14, 2017 TAMPA, FLORIDA

Next or first steps

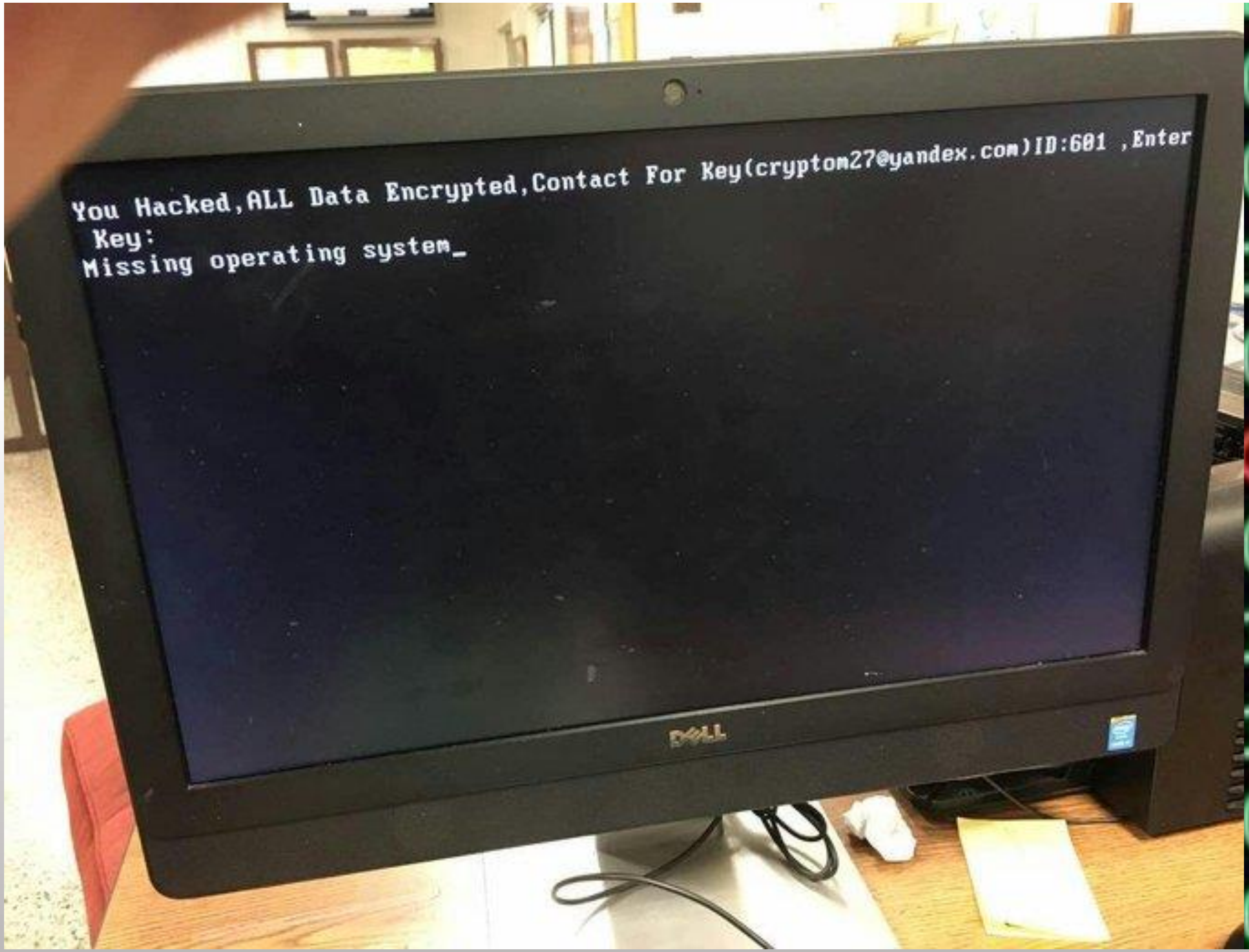
- Federal Bureau of Investigation Internet Crime Complaint Center: https://ic3.gov
- Building Your Cybersecurity Workforce: https://niccs.us-cert.gov/
- Cyber Security Self-Assessments: https://www.us-cert.gov/ccubedvp
- Protecting Critical Infrastructure from the Insider Threat: https://training.fema.gov/is/courseoverview.aspx?code=IS-915
- Stop, Think, Connect: https://www.dhs.gov/stopthinkconnect
- Cyber Security: https://www.dhs.gov/topic/cybersecurity
- Insider Threat (CERT.org): http://www.cert.org/searchresults.cfm?q=insider&x=0&y=0
- Resources for Application Security Training: https://training.safecode.org
- On-line security training: https://www.owasp.org/index.php/WebGoat_Installation

Summary

- ITS are Vulnerable to Cyber Security Threats
- Plan ahead
- Other industries have adopted cyber defense, is transportation ready



You have been hacked!



```
You Hacked,ALL Data Encrypted,Contact For Key(cryptom27@yandex.com)ID:601 ,Enter
 Key:
Missing operating system_
```