Cyber DIVISION
FEDERAL BUREAU OF INVESTIGATION

FBI Salt Lake City Cyber Task Force

October 13, 2017

James Lamadrid

Supervisory Special Agent

2017 Utah Area Chapter CFE White Collar Crime Conference

Agenda

1. FBI Priorities
2. Salt Lake City CTF
3. Cyber Threat Actors
4. Cyber Crimes
5. InfraGard
6. Resources
7. Q & A

FBI top 3 Priorities

1. Protect the United States from Terrorist Attack.

2. Protect the United States against foreign intelligence operations and espionage.

3. Protect the United States against cyber based attacks and high technology crimes.

FEDERAL BUREAU OF INVESTIGATION
PROTECTING AMERICA
COUNTERTERRORISM DIVISION

PROTECT • PARTNER • PROSPER
PREVENT
FBI CI STRATEGIC PARTNERSHIPS

FBI CYBER DIVISION
IDENTIFY • PURSUE • DEFEAT

FBI Salt Lake City Field Office

FBI Salt Lake City

5425 West Amelia Earhart Drive
Salt Lake City, UT 84116
Phone: (801) 579-1400
Fax: (801) 579-6000
E-mail: SaltLakeCity@ic.fbi.gov

The Salt Lake City Division covers 135 counties throughout Utah, Idaho, and Montana.

Resident Agencies
Along with our main office in Salt Lake City, we have 19 satellite offices, known as resident agencies, throughout our tri-state territory.

FBI – Salt Lake City Cyber Task Force

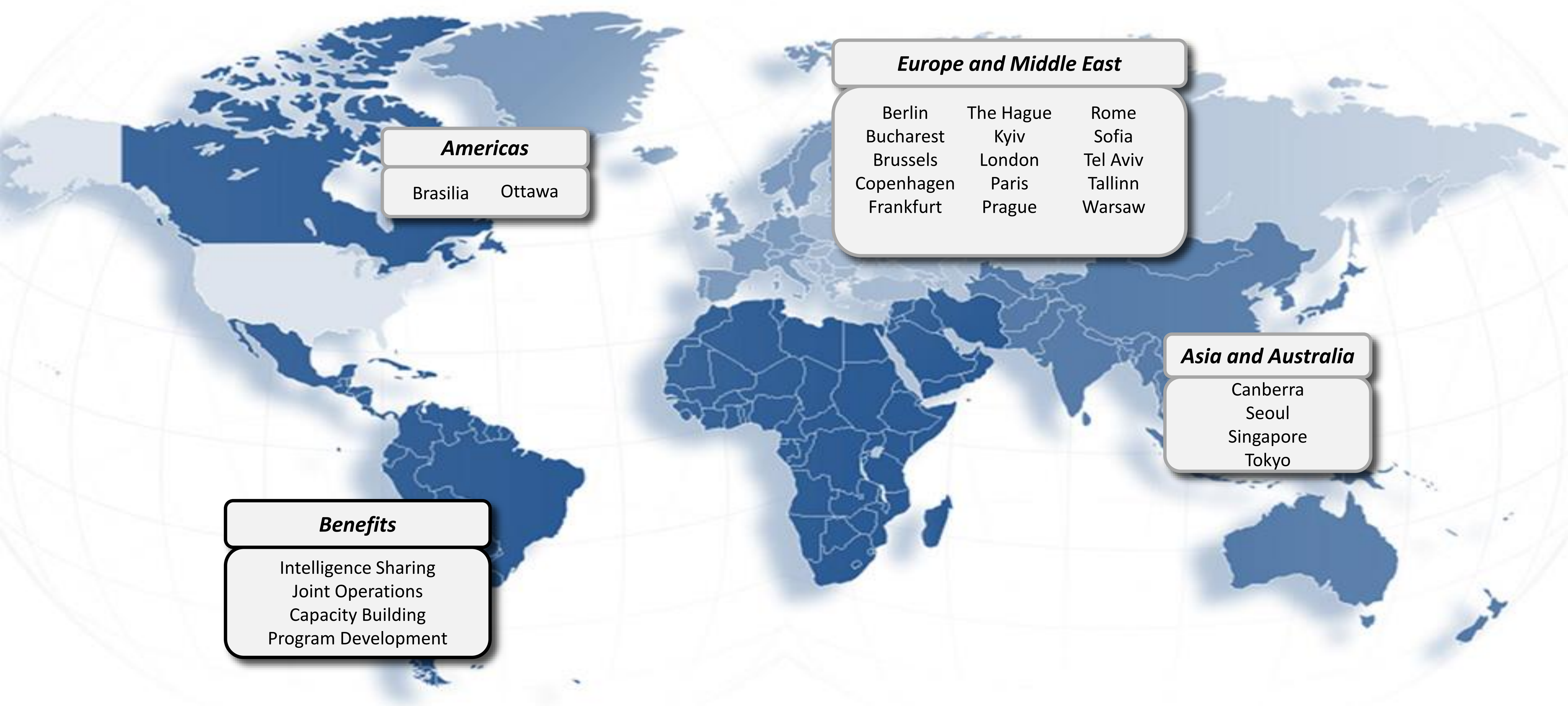
Cyber Task Force (CTF)

- FBI Special Agents
- FBI Intelligence Analysts
- FBI Computer Scientist
- FBI Staff Operation Specialist
- ATF/HSI/DCIS/FPS
- CART personnel (forensics)
- Utah Department of Public Safety
- Utah Statewide Information and Analysis Center (SIAC)
- SIAC Analyst
- Room for growth!

FBI’s Cyber Mission

Identify, **pursue**, and **defeat** cyber adversaries targeting global U.S. interests through collaborative partnerships and our unique combination of national security and law enforcement authorities.

Cyber Assistant Legal Attaché Program



Americas

Brasilia
Ottawa

Europe and Middle East

Berlin
Bucharest
Brussels
Copenhagen
Frankfurt
The Hague
Kyiv
London
Paris
Prague
Rome
Sofia
Tel Aviv
Tallinn
Warsaw

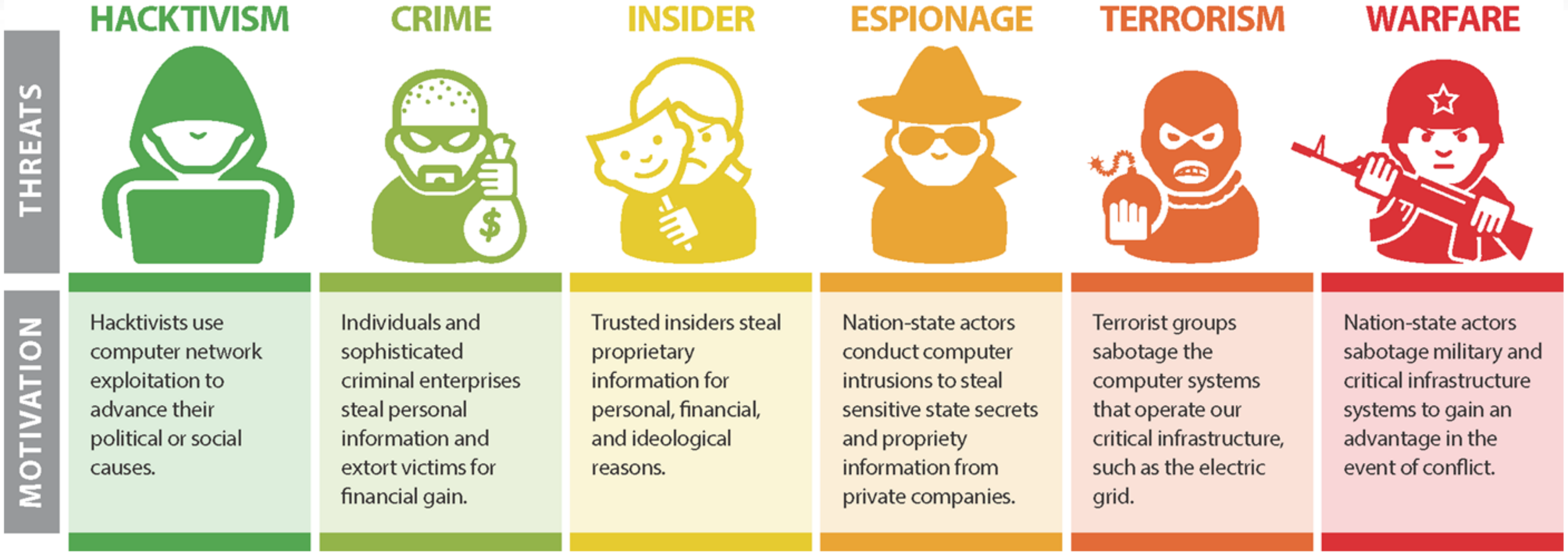
Asia and Australia

Canberra
Seoul
Singapore
Tokyo

Benefits

Intelligence Sharing
Joint Operations
Capacity Building
Program Development

Who Is Doing The Hacking?



THREATS	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
MOTIVATION	Hacktivists use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Trusted insiders steal proprietary information for personal, financial, and ideological reasons.	Nation-state actors conduct computer intrusions to steal sensitive state secrets and propriety information from private companies.	Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.	Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

Personal Information Available Online

Healthcare Sector

Patient Name
Date of Birth
Blood Type
Policy Numbers
Billing Information
Diagnoses Codes

Financial Sector

Credit/Debit Card
Banking Information
Home Address
Phone Number
PINs

Government Database

Social Security Number
Payroll Information
Salary
Email Address
Work Function

Valued by Every Cyber Adversary

IBM and Ponemon Institute 2016 Report

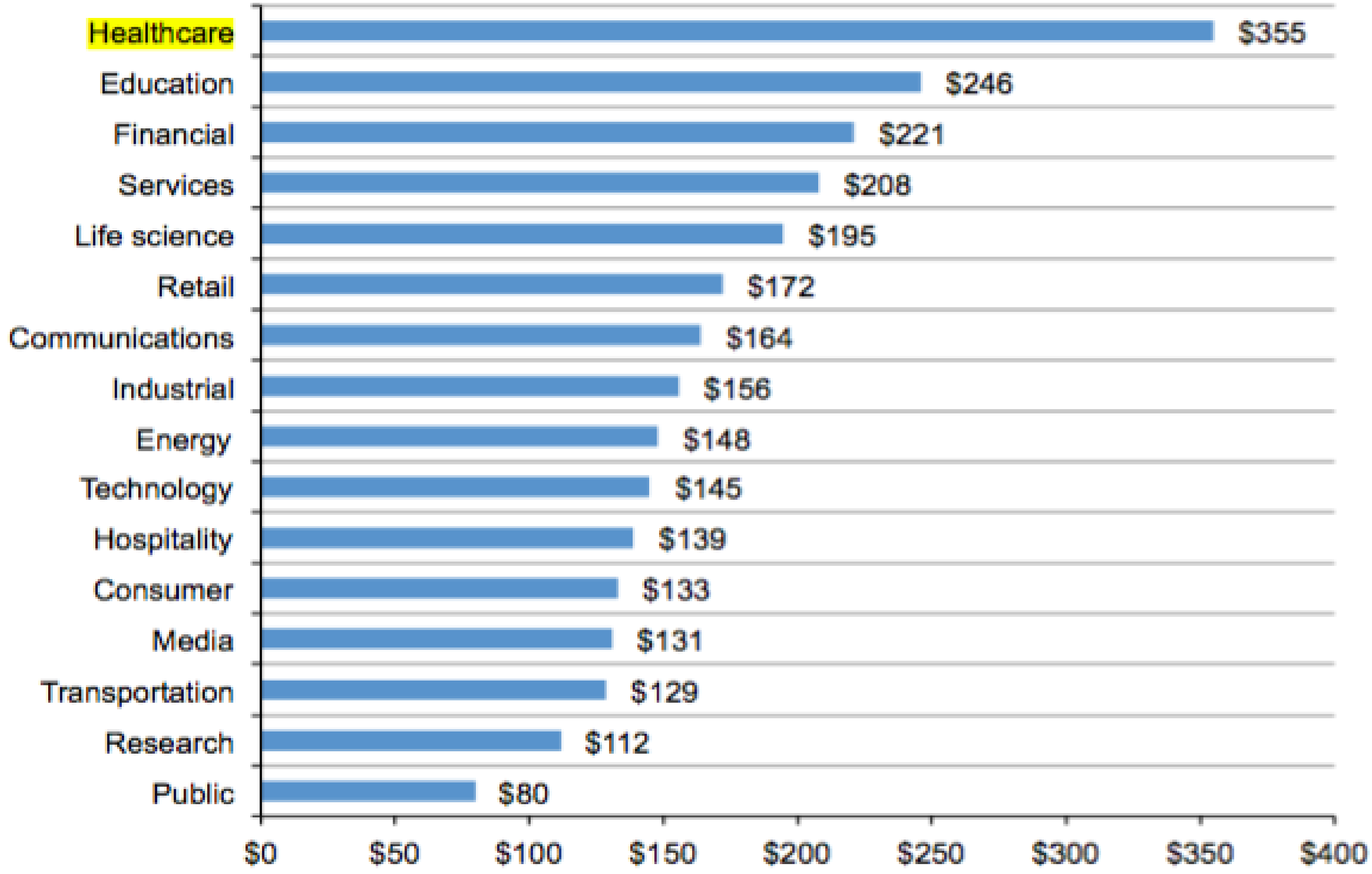
Global study at a glance

- 383 companies in 12 countries
- $4 million is the average total coast of the data breach
- 29% increase in total cost of data breach since 2013
- $158 is the average cost per lost or stolen record
- 15% percent increase in per capita cost since 2013

Average Cost of Breach Per Capita

Figure 4. Per capita cost by industry classification

Consolidated view (n=383), measured in US$



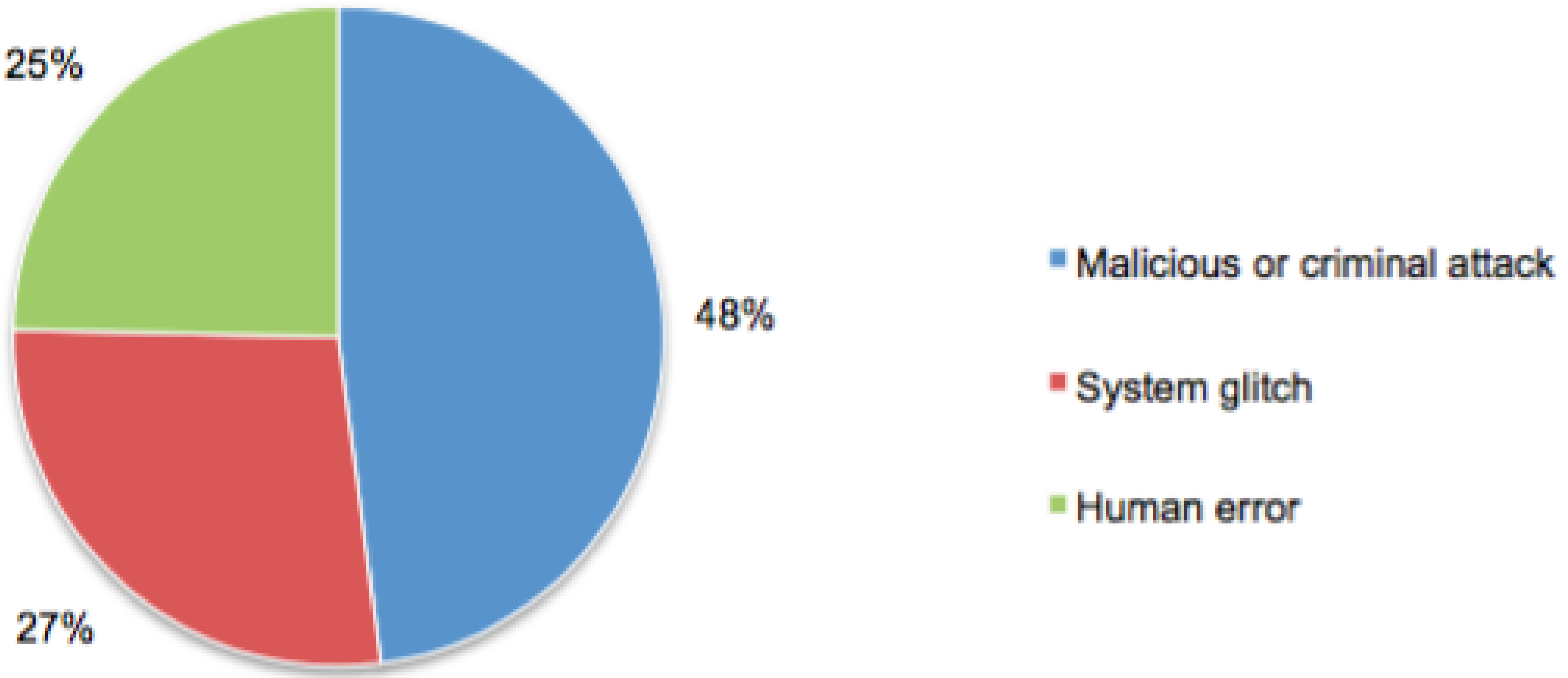
Source:

IBM and Ponemon Institute

2016 Cost of Data Breach Study: Global Analysis

Root Cause of Data Breach

Pie Chart 2. Distribution of the benchmark sample by root cause of the data breach
Consolidated view (n=383)



Types of Attack

- DDoS
- Doxing
- Theft of IP
- Theft of PII, PHI
- Point of Sale Breaches

- False Tax Return Filings
- Network Destruction Attacks
- Ransomware and Extortion ★
- Business E-mail Compromise ★
- Website Defacements

Computer Fraud and Abuse Act

- Computer Fraud and Abuse Act (CFAA)
  - Outlaws conduct that victimizes computer systems.
  - Cyber security law.
  - Protects federal computers, bank computers, and computers connected to the Internet.
  - Shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of Fraud.

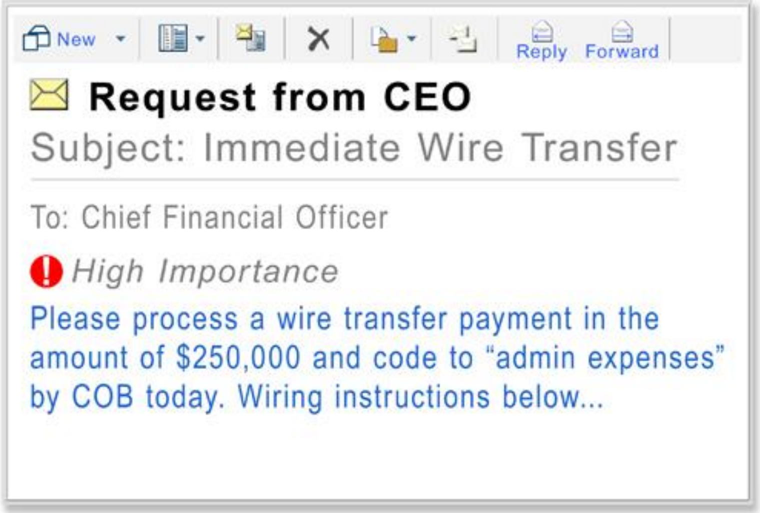
- As of January 2015, at least 47 states have passed database breach notification laws requiring companies to notify customers whose data is compromised by an intrusion; however, many data breach reporting laws allow a covered organization to delay notification if LE concludes that such notification would impede an investigation.

Title 18 U.S.C. § 1030

Ransomware

Business Email Compromise

- Sophisticated scam targeting businesses that regularly perform wire transfer payments
- Targets CEO, CFO, CTO or other executive
- Compromise via social engineering or computer intrusion techniques
- BOTH suppliers and their customers are victims of this scam
- Formerly known as the man-in-the-email



Request from CEO

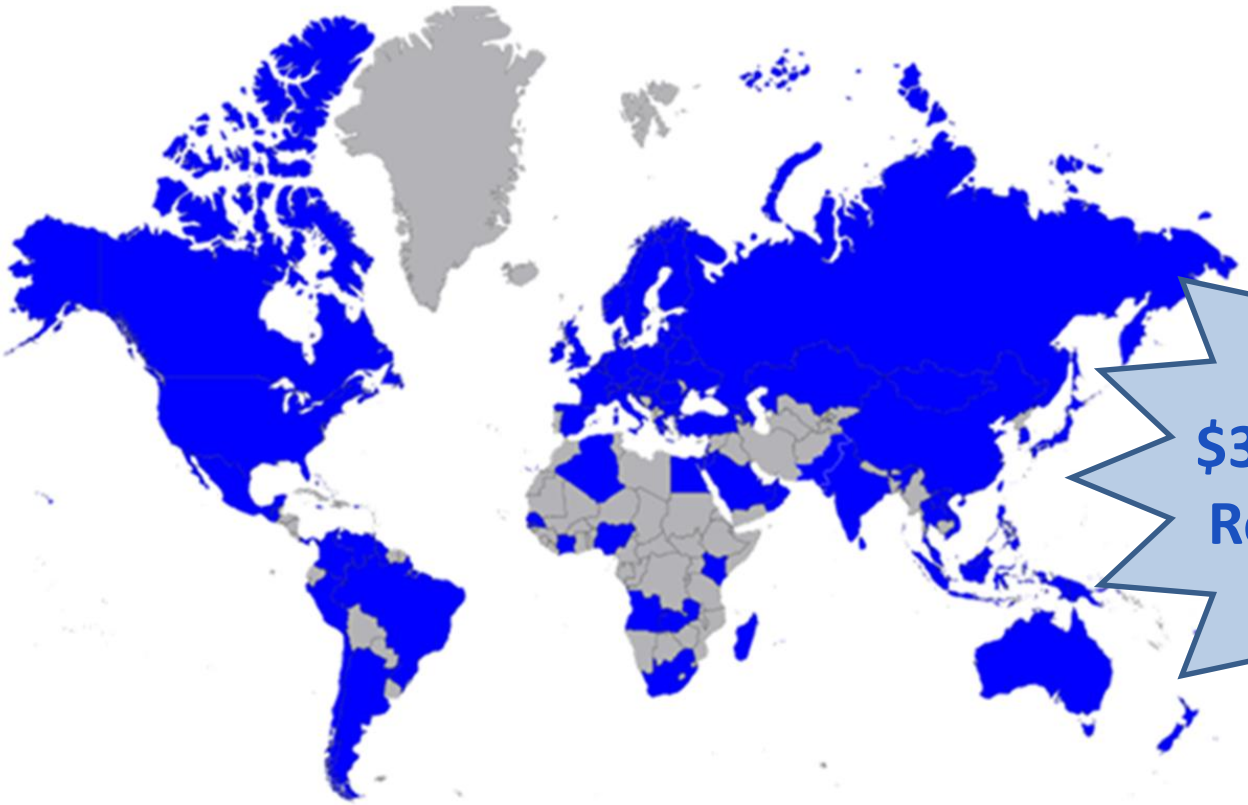
Subject: Immediate Wire Transfer

To: Chief Financial Officer

High Importance

Please process a wire transfer payment in the amount of $250,000 and code to “admin expenses” by COB today. Wiring instructions below...

Business Email Compromise

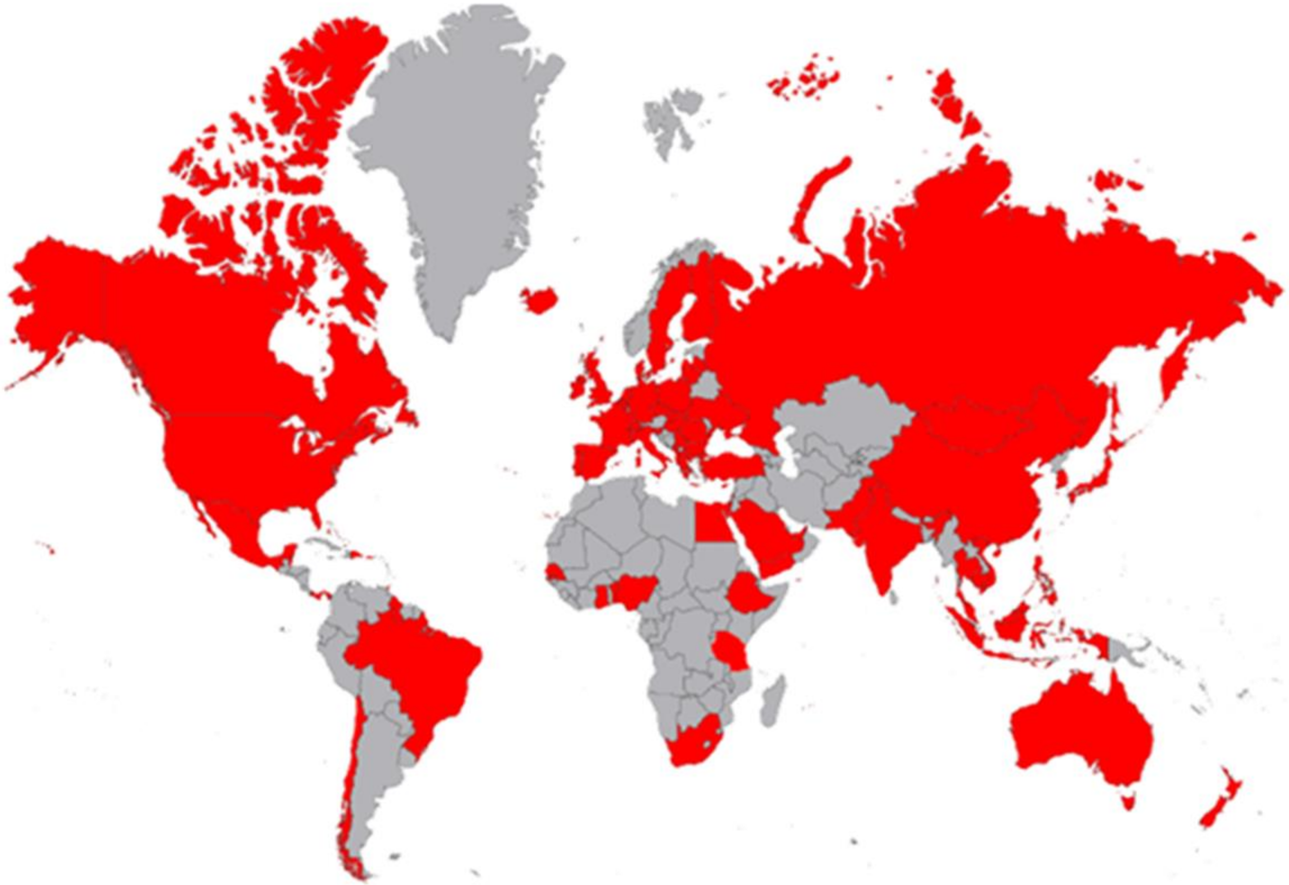


*95 COUNTRIES WITH VICTIMS

$360 Million losses Reported to IC3 in 2016.

Destinations of Fraudulent Wire Transfers

1. Hong Kong
2. China
3. Malaysia
4. Taiwan
5. Korea
6. Nigeria
7. UAE
8. Japan
9. Indonesia



*77 COUNTRIES WITH SUBJECTS

ATM Skimming Investigation

Alexandru Stefan

Ionela Stefan

Charged with access device fraud (18 U.S. Code § 1029)

Obtained people's bank card information data using skimmer.

ATM at a Credit Union in Sandy, UT. (May 2015)

Equifax Breach Exposed data for 143 Million Consumers

OPEN SOURCE REPORTING

- Hacked occurred between mid-May and July 2017
- Equifax discovered breach on 29 July 2017
- Included names, SSNs, DOB, some Driver's License numbers
- Equifax stated information form British and Canadian consumers were also stolen
- Lenders rely on information collected by credit bureaus for finance approvals
  - Eclipsed 2015 hack of health insurer Anthem Inc, SSN of 80 Million accounts.

Consumer Credit Bureaus

- Freezing your credit.
  - Online, phone, or in writing. A fee may be required.
  - Each bureau will provide a unique personal identification number (PIN) that you can use to unfreeze your account.
  - There are four consumer credit bureaus

EQUIFAX

Experian

TransUnion

Innovis

Internet Crimes Complaint Center www.ic3.gov

- Partnership between the FBI and National White Collar Crime Center
- Analyze Internet crime trends
- Triage Internet complaints
- Develop and refer investigative packets to appropriate agency.
- Ally with the National Cyber-Forensics and Training Alliance (NCFTA)

Partnership For Protection

Network with representatives from other companies that help maintain our national infrastructure.

350 of our nation’s Fortune 500 have a representative in InfraGard.

Gain access to an FBI secure communication network complete with VPN encrypted website, webmail, listservs, message boards and much more.

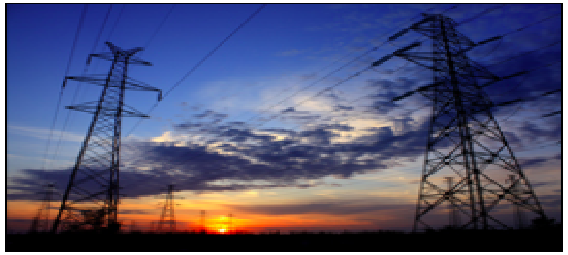
Learn time-sensitive, infrastructure related security information from government sources such as the FBI and DHS.

Get invitations and discounts to important training seminars and conferences.

Best of all, there is no cost to join InfraGard.

InfraGard
Partnership for Protection

SERVICES



CRITICAL INFRASTRUCTURES

Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

+ MORE INFO

CHAPTERS

InfraGard has 84 chapters with more than 54,000 members nationwide helping to protect and defend critical infrastructures. At the chapter level, members meet to discuss threats and other matters that impact their companies. The meetings—led by a local governing board and an FBI agent who serves as InfraGard coordinator—give everyone an opportunity to share experiences and best practices.

+ MORE INFO

FBI NEWS FEED

When you subscribe to a feed, it is added to the Common Feed List. Updated information from the feed can be viewed on your computer

- Press Releases
- National Press Releases
- News
- Cyber Crimes
- Cyber Crimes Fugitives

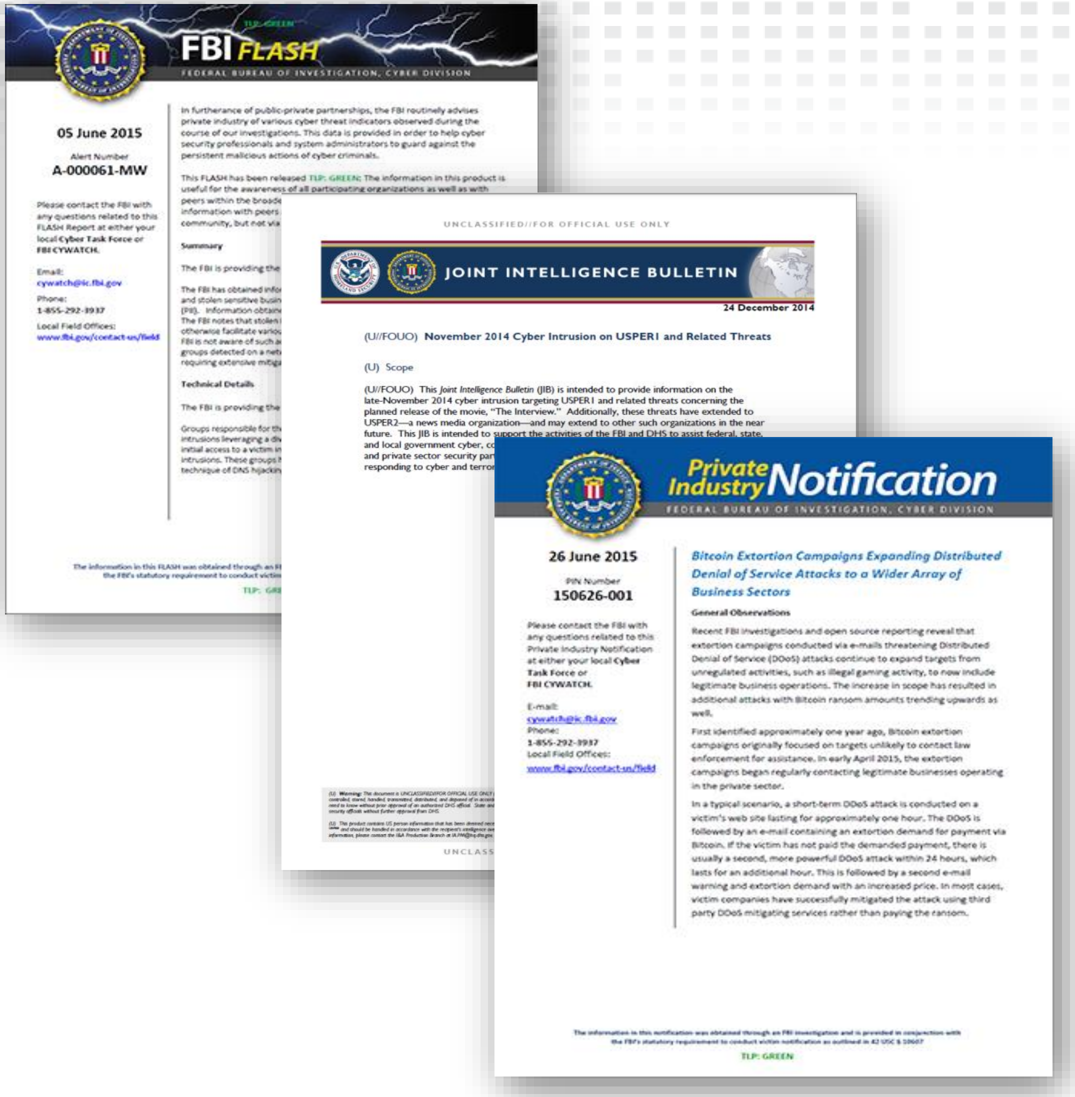
+ MORE INFO

FORTUNE 500

More than 400 of our nation's Fortune 500 have a representative in InfraGard. Network with representatives from other organizations and agencies that help maintain our national infrastructure.

+ MORE INFO

Information Sharing Methods



TLP: GREEN

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

05 June 2015

Alert Number
A-000061-MW

Please contact the FBI with any questions related to this FLASH Report at either your local **Cyber Task Force** or **FBI CYWATCH**.

Email:
cywatch@ic.fbi.gov

Phone:
1-855-292-3937

Local Field Offices:
www.fbi.gov/contact-us/field

In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been released TLP: GREEN: The information in this product is useful for the awareness of all participating organizations as well as with peers within the broade
information with peers
community, but not via

Summary

The FBI is providing the

The FBI has obtained infor
and stolen sensitive busin
(PII). Information obtaine
The FBI notes that stolen
otherwise facilitate variou
FBI is not aware of such a
groups detected on a netw
requiring extensive mitiga

Technical Details

The FBI is providing the

Groups responsible for th
intrusions leveraging a div
initial access to a victim in
intrusions. These groups h
technique of DNS hijackin

The information in this FLASH was obtained through an FI
the FBI's statutory requirement to conduct victim

TLP: GRE

UNCLASSIFIED//FOR OFFICIAL USE ONLY

JOINT INTELLIGENCE BULLETIN

24 December 2014

(U//FOUO) **November 2014 Cyber Intrusion on USPER1 and Related Threats**

(U) Scope

(U//FOUO) This *Joint Intelligence Bulletin* (JIB) is intended to provide information on the late-November 2014 cyber intrusion targeting USPER1 and related threats concerning the planned release of the movie, "The Interview." Additionally, these threats have extended to USPER2—a news media organization—and may extend to other such organizations in the near future. This JIB is intended to support the activities of the FBI and DHS to assist federal, state, and local government cyber, co
and private sector security par
responding to cyber and terror

*(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY*
controlled, stored, handled, transmitted, distributed, and disposed of in accord
need to know without prior approval of an authorized DHS official. State and
security officials without further approval from DHS.

(U) This product contains US person information that has been deemed nece
and should be handled in accordance with the recipient's intelligence ove
information, please contact the I&A Production Branch at IA.PM@hq.dhs.gov

UNCLASS

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

26 June 2015

PIN Number
150626-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CYWATCH**.

E-mail:
cywatch@ic.fbi.gov
Phone:
1-855-292-3937
Local Field Offices:
www.fbi.gov/contact-us/field

Bitcoin Extortion Campaigns Expanding Distributed Denial of Service Attacks to a Wider Array of Business Sectors

General Observations

Recent FBI investigations and open source reporting reveal that extortion campaigns conducted via e-mails threatening Distributed Denial of Service (DDoS) attacks continue to expand targets from unregulated activities, such as illegal gaming activity, to now include legitimate business operations. The increase in scope has resulted in additional attacks with Bitcoin ransom amounts trending upwards as well.

First identified approximately one year ago, Bitcoin extortion campaigns originally focused on targets unlikely to contact law enforcement for assistance. In early April 2015, the extortion campaigns began regularly contacting legitimate businesses operating in the private sector.

In a typical scenario, a short-term DDoS attack is conducted on a victim's web site lasting for approximately one hour. The DDoS is followed by an e-mail containing an extortion demand for payment via Bitcoin. If the victim has not paid the demanded payment, there is usually a second, more powerful DDoS attack within 24 hours, which lasts for an additional hour. This is followed by a second e-mail warning and extortion demand with an increased price. In most cases, victim companies have successfully mitigated the attack using third party DDoS mitigating services rather than paying the ransom.

The information in this notification was obtained through an FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in 42 USC § 10607

TLP: GREEN

✓Actionable intelligence for victims/potential victims

✓Any classification, generally UNCLASSIFIED//FOR OFFICIAL USE ONLY

✓Advisories disseminated to private sector partners based on current threat analysis

✓Collaboration with IC3, DHS, Secret Service

- **16 Critical Infrastructures**

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Defense Industrial Base Sector
- Dams Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector

Seven Tips for Small Business Security

1. Identify and minimize information assets.

2. Keep sensitive data off the network as much as possible.

3. Provision a separate PC for sensitive business functions, like banking.

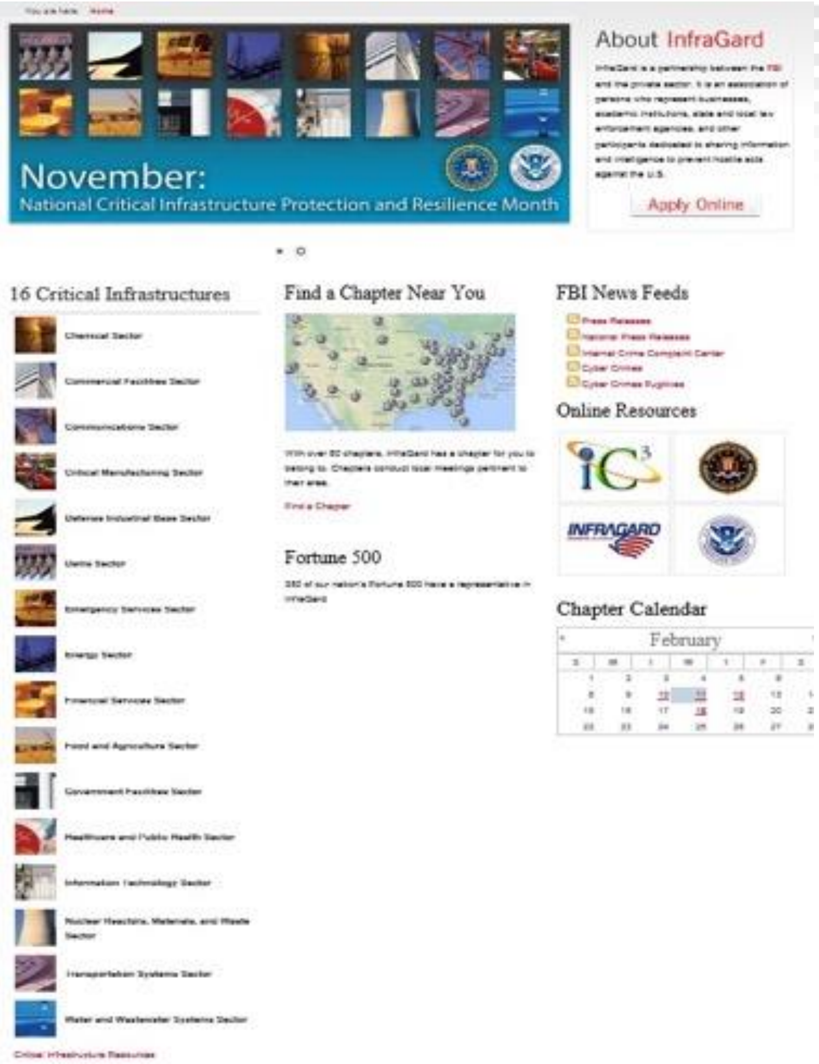
4. Enable two-factor authentication (2FA) wherever possible.

5. Leverage trustworthy cloud solutions.

6. Join Infragard. Infragard is a non-profit organization run by the Federal Bureau of Investigation.

7. Treat cyber security as a business problem, not a technical problem.

Source: Huffington Post, Richard Bejtlich, FireEye
Date: June 18, 2014



You are here: Home

November:
National Critical Infrastructure Protection and Resilience Month

About InfraGard

InfraGard is a partnership between the FBI and the private sector. It is an association of persons who represent businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the U.S.

Apply Online

16 Critical Infrastructures

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Defense Industrial Base Sector
- Dams Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector

Critical Infrastructure Resources

Find a Chapter Near You

With over 80 chapters, InfraGard has a chapter for you to belong to. Chapters conduct local meetings pertinent to their area.

Find a Chapter

Fortune 500

350 of our nation's Fortune 500 have a representative in InfraGard

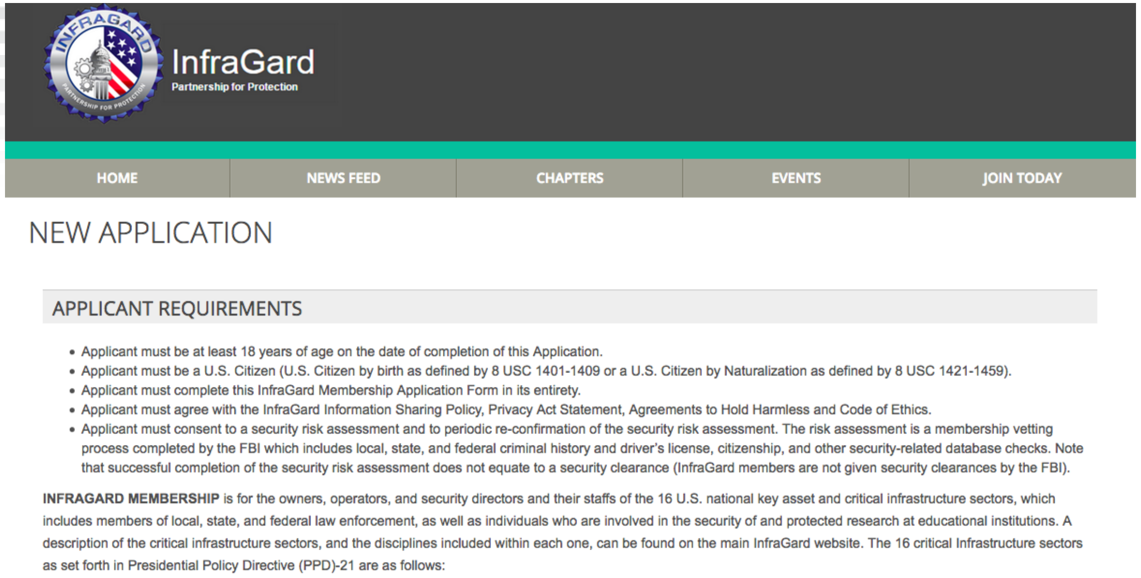
FBI News Feeds

- Press Releases
- National Press Releases
- Internet Crime Complaint Center
- Cyber Crimes
- Cyber Crimes Fugitives

Online Resources

Chapter Calendar

February



InfraGard
Partnership for Protection

NEW APPLICATION

APPLICANT REQUIREMENTS

- Applicant must be at least 18 years of age on the date of completion of this Application.
- Applicant must be a U.S. Citizen (U.S. Citizen by birth as defined by 8 USC 1401-1409 or a U.S. Citizen by Naturalization as defined by 8 USC 1421-1459).
- Applicant must complete this InfraGard Membership Application Form in its entirety.
- Applicant must agree with the InfraGard Information Sharing Policy, Privacy Act Statement, Agreements to Hold Harmless and Code of Ethics.
- Applicant must consent to a security risk assessment and to periodic re-confirmation of the security risk assessment. The risk assessment is a membership vetting process completed by the FBI which includes local, state, and federal criminal history and driver's license, citizenship, and other security-related database checks. Note that successful completion of the security risk assessment does not equate to a security clearance (InfraGard members are not given security clearances by the FBI).

INFRAGARD MEMBERSHIP is for the owners, operators, and security directors and their staffs of the 16 U.S. national key asset and critical infrastructure sectors, which includes members of local, state, and federal law enforcement, as well as individuals who are involved in the security of and protected research at educational institutions. A description of the critical infrastructure sectors, and the disciplines included within each one, can be found on the main InfraGard website. The 16 critical Infrastructure sectors as set forth in Presidential Policy Directive (PPD)-21 are as follows:

DOJ Best Practices for Cyber Incidents

I. Steps to Take BEFORE a Cyber Intrusion or Attack Occurs

✓ Identify Your “Crown Jewels”

✓ Have an Actionable Plan Before a Breach Occurs

✓ Have Appropriate Technology and Services in Place

✓ Have Appropriate Authorization in Place to Permit Network Monitoring

✓ Brief Legal Counsel with Technology and Cyber Incident Management

✓ Ensure Organization Policies Align with Cyber Incident Response Plan

✓ Engage with Law Enforcement Before an Incident

✓ Establish Relationships with Cyber Information Sharing Organizations ISAC/ISAO

Information Sharing and Analysis Center (ISAC)

Information Sharing and Analysis Organizations (ISAO)

Breaches Happen: Do You Have an Incident Response Plan?

DOJ Best Practices for Cyber Incidents

II. Responding to a Computer Intrusion: Executing Your Incident Response Plan

- ✓ Make an Initial Assessment (malicious act or technological glitch)
- ✓ Implement Measures to Minimize Continuing Damage
- ✓ Record and Collect Information
- ✓ Notify (Internal personnel/Law Enforcement/DHS/Other Victims)

DOJ Best Practices for Cyber Incidents

III. <u>What Not to Do Following a Cyber Incident</u>

- ✓ Do Not Use the Compromise Systems to Communicate
- ✓ Do Not Hack Into or Damage Another Network
- ✓ Continue to Monitor the Network
- ✓ Conduct a post-incident review to identify deficiencies (AAR)

Recommendations for Protecting Your Systems

- ✓ Focus on awareness and training
- ✓ Dual-Factor / Multi-Factor Authentication
- ✓ Password Management
- ✓ Keep patches updated
- ✓ Manage privileged (Administrator) accounts.
- ✓ Data Back-up and Recovery Plans
- ✓ Encryption of Sensitive Data
- ✓ Social Media Habits

Questions?

Contacting the FBI

CyWatch
24/7 Operation
(855) 292-3937
cywatch@ic.fbi.gov

Cyber Task Force
Located within 56 local field offices

Focused on cyber security threats

Internet Crime Complaint Center
www.ic3.gov

FBI Salt Lake City Field Office

FBI Salt Lake City

Cyber Task Force

SSA James E Lamadrid

(801) 570-1400