



InfraGard & Cyber Response



Cyber News is Scary

Cyber crime costs the world almost **\$600 billion** annually, according to a report published earlier this year by the think tank Center for Strategic and International Studies and the cyber security company McAfee. That's a potential hole of around 0.7 percent in global gross

One in Four Americans Have Experienced Cybercrime

BY RJ REINHART

Why the US thinks Huawei has been a massive national security threat for years

Andrea Miller | Jordan Smith | 12:38 PM ET Mon, 17 Dec 2018



Cyber security: Hackers step out of the shadows with bigger, bolder attacks

Successful hacking campaigns used to be all about keeping under the radar, but now more important than lurking in the shadows.



By Danny Palmer | December 4, 2018 -- 10:56 GMT (02:56 PST) | Topic: Security

The Divide Between Silicon Valley and Washington Is a National-Security Threat

Cybercrime a \$2 trillion threat for business

This is sponsored content for KPMG Enterprise

HOME | COVERING COLORADO, NEWS, SEEN ON 5

More money made in cyber crime than in drug trafficking



Alaska Isn't Immune

The cyber-attack that sent an Alaskan community back in time

City of Valdez, Alaska admits to paying off ransomware infection

Crime & Justice

\$3.8M in Alaska Native corp. money sent to offshore account in cyberfraud attack

✍ Author: Laurel Andrews ⌚ Updated: September 28, 2016 📅 Published May 6, 2015

Chinese hackers targeted U.S. firms, government after trade mission: researchers

Top-secret intelligence requested by President Barack Obama in his last weeks in office identified seven states where analysts – synthesizing months of work – had reason to believe [Russian operatives](#) had compromised state websites or databases.

Price tag for cyberattack on Mat-Su Borough now tops \$2 million

Three senior intelligence officials told NBC News that the intelligence community believed the states as of January 2017 were [Alaska](#), Arizona, California, Florida, Illinois, Texas and Wisconsin.



Cyber Emergency Threats



- Top Trending Schemes
 - Ransomware
 - BEC / Online Fraud
 - DDOS Attacks
 - PII Data Breaches



- Additional Threats
 - Insider Threat
 - Cyber Swatting
 - Cyberterrorism
 - Banking Trojans





It All Starts with a Phish



- Phishing emails involved in 65-90% of cyber crime
- Leads to:
 - Malicious Link
 - Attached Doc
 - **MACROS!**





Attacks on Infrastructure

Baltimore's 911 emergency system hit by cyberattack

Two US power plants infected with malware spread via USB drive

Investigators find no up-to-date antivirus, system backups for control systems.

Hardin Memorial Recovering from Cyberattack, EHR Downtime

The Kentucky hospital was experienced IT disturbance and EHR downtime over the weekend, after hackers launched a cyberattack on several servers.

\$10 Million Cyber Attack Hits New York Hospital

ANDY GREENBERG SECURITY 06.12.17 08:00 AM

'CRASH OVERRIDE': THE MALWARE THAT TOOK DOWN A POWER GRID

DDoS Attack Takes Down Central Heating System Amidst Winter In Finland



The Ransomware Threat

Imperial County Government Website Down After Ryuk Malware Hacking, Ransom Demands

POSTED 1:03 PM, APRIL 19, 2019, BY LOS ANGELES TIMES

Albany, N.Y. hit with ransomware attack, mayor says

April 12, 2019

Garfield County, Utah falls victim to ransomware, pays attackers

Genesee County computer networks attacked by ransomware

April 11, 2019

**Ransomware knocks Greenville, N.C. offline
Augusta city offices hit by computer virus**

City of Stuart computer virus a ransomware attack



Enter.....FBI



**KEEP
CALM
WE'RE
HERE TO
HELP**





When You Call, ... We Won't



- Swoop in with black helicopters, heavy artillery and SWAT gear
- Take all your devices and leave a tumbleweed
- Go on the evening news to talk about what happened
- Produce a report blaming the victim for allowing the crime
- Share your proprietary data with anyone
- Stop your recovery so we can take what we need
- Give you orders on how to proceed



When You Call, ... We Will



- Set a time that works for you to have a conversation
- Plan with you how to retain key evidence
- Schedule time to collect evidence as unobtrusively as possible
- Share any intel/tools we have related to the threat
- Relate other victims experiences
- Try to take only copies of data
- Return any device as soon as possible



Alaskan Success



FOR IMMEDIATE RELEASE

Wednesday, December 13, 2017

Justice Department Announces Charges and Guilty Pleas in Three Computer Crime Cases Involving Significant DDoS Attacks

Defendants Responsible for Creating “Mirai” and Clickfraud Botnets, Infecting Hundreds of Thousands of IoT Devices with Malicious Software

The Justice Department announced today the guilty pleas in three cybercrime cases. In the District of Alaska, defendants pleaded guilty to creating and operating two botnets, which targeted “Internet of Things” (IoT) devices, and in the District of New Jersey, one of the defendants also pleaded guilty to launching a cyber attack on the Rutgers University computer network.

FOR IMMEDIATE RELEASE

Thursday, April 12, 2018

Former Airline Employee Sentenced For Hacking PenAir’s Ticketing And Reservations System

Anchorage, Alaska – U.S. Attorney Bryan Schroder announced today that a former airline employee has been sentenced in federal court for hacking PenAir’s ticketing and reservation system between April and May 2017.

FOR IMMEDIATE RELEASE

Thursday, December 20, 2018

Criminal Charges Filed in Los Angeles and Alaska in Conjunction with Seizures Of 15 Websites Offering DDoS-For-Hire Services



Dynamic Support



- Industry or segment specific briefings
- Presentations to businesses/associations
- Sharing of best practices:
 - Basics
 - Passwords
 - Backups
 - Advanced
 - Incident Handling
 - Forensic Processes



Resources Available



- IC3.gov
 - Online intake of cyber crime reporting
- CyWatch
 - 24 command center for intrusion reporting and response
- InfraGard
 - iGuardian for detailed reporting
 - Malware Analyzer
- Financial Fraud Kill Chain





Public Outreach



- FBI Citizen's Academy
- FBI Teen Academy
- Participation in various Cyber Task Forces
- **InfraGard**





InfraGard



- The **mission** of the InfraGard Program is to foster collaboration sharing that enhances our collective ability to address threats to the United States' critical infrastructure through a robust private-sector/government partnership.
- **Membership** includes business executives, entrepreneurs, military and government officials, IT professionals, academia, representing the designated critical sectors, state and local law enforcement and concerned citizens





16 Critical Sectors



1. Agriculture & Food
2. Banking & Finance
3. Chemical
4. Commercial Facilities
5. Communications
6. Critical Manufacturing
7. Dams
8. Defense Industrial Base
9. Emergency Services
10. Energy
11. Government Facilities
12. Healthcare and Public Health
13. Information Technology
14. Nuclear Reactors/Materials/Waste
15. Transportation
16. Water Supply





InfraGard History

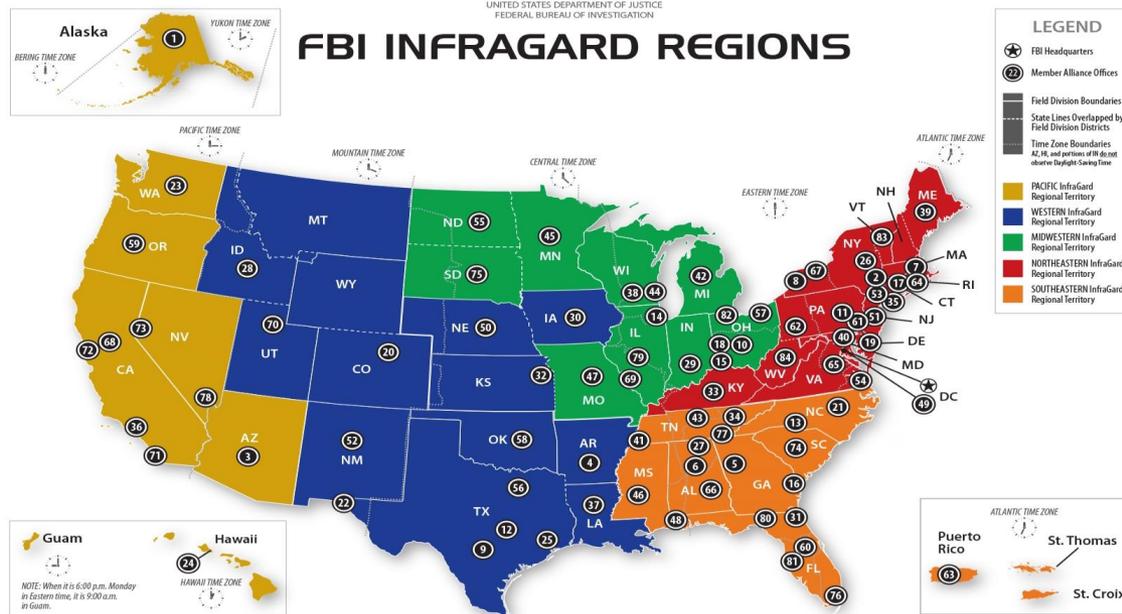


- Began in 1996, in Cleveland, Ohio as a collaborative effort between FBI, Cleveland Division and subject matter experts in local industries and academia
- Designed to harness private sector expertise for investigative efforts in cyber security
- Immediately successful and quickly expanded nationwide to all 56 FBI field offices
- InfraGard today is comprised of more than **55,000** members and has **84 InfraGard Chapters** throughout the United States.





InfraGard Regions



INFRAGARD MEMBER ALLIANCES

1 Alaska	9 San Antonio	17 Connecticut	24 Honolulu	32 Kansas City	40 Maryland	48 Mobile	56 North Texas	64 Rhode Island	72 San Francisco Bay Area	80 Tallahassee
2 Albany	10 Central Ohio	18 Dayton	25 Houston	33 Kentucky	41 Memphis	49 National Capital Region	57 Northern Ohio	65 Richmond	73 Sierra Nevada	81 Tampa Bay Area
3 Arizona	11 Central Pennsylvania	19 Delaware	26 Hudson Valley	34 Knoxville	42 Michigan	50 Nebraska	58 Oklahoma	66 River Region	74 South Carolina	82 Toledo
4 Arkansas	12 Capital of Texas	20 Denver	27 Huntsville	35 Long Island	43 Middle Tennessee	51 New Jersey	59 Oregon	67 Rochester	75 South Dakota	83 Vermont
5 Atlanta	13 Charlotte	21 Eastern Carolina	28 Idaho	36 Los Angeles	44 Milwaukee	52 New Mexico	60 Orlando	68 Sacramento	76 South Florida	84 West Virginia
6 Birmingham	14 Chicago	22 El Paso	29 Indiana	37 Louisiana	45 Minnesota	53 New York City Metro	61 Philadelphia	69 Saint Louis	77 Southeast Tennessee	
7 Boston	15 Cincinnati	23 Evergreen State	30 Iowa	38 Madison	46 Mississippi	54 Norfolk	62 Pittsburgh	70 Salt Lake City	78 South	
8 Buffalo	16 Coastal Empire	Ⓜ Headquarters	31 Jacksonville	39 Maine	47 Missouri	55 North Dakota	63 Puerto Rico	71 San Diego	79 Spring	





Benefits to the Member



- Providing access to a secure suite of numerous unclassified intelligence bulletins
 - Enabling them to play a key role in securing infrastructure
 - Improving understanding of the threatscape
- Opportunities to attend training events and briefings held by the FBI and its law enforcement partners
- Valuable networking/collaboration opportunities
- Establishes relationship with FBI ***before an incident***





Benefits to the FBI



- **Prevent, detect, and investigate threats impacting critical infrastructure and/or national security**
- Better understand emerging trends
- Foster crime prevention initiatives
- Promote the exchange of ideas
- **Build key contacts within local communities and the public and private sectors**
- Alert citizens to threats and vulnerabilities
- **Facilitate peer-to-peer collaboration and information sharing**





Member: Intelligence Info



Flash Message

- FBI Liaison Alert System
- Actionable intelligence for victims/potential victims

Threat Briefings

- FBI analysts (general/specific)

PIN/PSA

- Private Industry Notification
- Private Sector Advisory

JIB

- Joint Intelligence Bulletin
- Advisory disseminated based on current threat analysis





Member: Online Portal



- Access to InfraGard's secure web portal: www.infragard.org
- Comprehensive suite of sensitive but unclassified FBI, DHS and other federal, state and local threat intelligence products and daily news feeds
- Access to webinars and presentations from around the country concerning cyber security
- Access to iGuardian, the FBI's cyber incident reporting tool designed specifically to the private sector
- Access to Malware Analyzer online sandbox
- Future access to InfraGard U – Training and certification opportunities





Member: Training Opportunities



- Free or discounted seminars and conferences
- Access to government agency training programs from FBI, DHS and others
- Training discounts from SANS, the Center for Information Security Awareness (CFISA) and others
- InfraGard U: coming in Fall of 2019





How to Join



- Individual
- FREE
- Requirements:
 - 18 years or Older
 - U.S. Citizen
 - Pass Periodic Criminal Background Checks
 - Have Association with 1 of 16 Critical Sectors
 - Agree to Adhere to the IG Code of Ethics
- Apply Online at <https://www.infragard.org>





Questions??



Special Agent Kevin Hinrichs

FBI Anchorage – Cyber Squad
Alaska InfraGard Coordinator

101 East 6th Ave
Anchorage, AK 99501
907-276-4441