Keynote Address
Tuesday, January 14, 2020
9:05 a.m. – 9:45 a.m.

Speaker: Michael Driscoll
Special Agent in Charge
Federal Bureau of Investigation (FBI)

Speaker Biography:

In June 2019, Director Christopher Wray named **Michael J. Driscoll** as a Special Agent in Charge in the New York Office where he currently oversees the Counterintelligence/Cyber Division. SAC Driscoll previously recently served as a Section Chief in the Criminal Investigative Division at FBI Headquarters in Washington, D.C. SAC Driscoll began his career as an FBI Special Agent in 1996, when he was assigned to the New York Office to work counterterrorism matters. He was part of the team that investigated al Qaeda conspirators, including those responsible for the 1998 bombings of United States Embassies in Kenya and Tanzania and the attacks on 9/11. SAC Driscoll was transferred to FBI Headquarters in 2003 to work as the FBI's representative to the al Qaeda Department of the CIA's Counterterrorism Center. In 2005, SAC Driscoll was promoted to Supervisor and returned to the New York Office, where he was in charge of the squad responsible for extraterritorial investigations in Africa. He also led the FBI's counterterrorism efforts in the New York Hudson Valley region and was later promoted to the Coordinating Supervisory Special Agent for New York's Counterterrorism Program. SAC Driscoll was named Assistant Legal Attaché for London in 2013, overseeing the Cyber Program and working closely with United Kingdom law enforcement and intelligence services. In 2016, he was appointed Assistant Special Agent in Charge of the Philadelphia Field Office's Cyber and Counterintelligence Programs. He returned to FBI Headquarters in 2018 as the chief of the Violent Crime Section, which leads the FBI's Crimes Against Children Program, as well as efforts to reduce violent crime and gang-related violence. Prior to joining the FBI, SAC Driscoll was an attorney working in commercial litigation. He graduated from the State University of New York in Albany and received his law degree from Hofstra University School of Law in Hempstead, New York. He earned an Attorney General's Award for Distinguished Service in 2002 for his work investigating al Qaeda and the 1998 embassy bombings.

Cyber DIVISION
FEDERAL BUREAU OF INVESTIGATION

Cyber Threats, Response, and Collaboration

Michael J. Driscoll
Special Agent in Charge
Cyber and Counterintelligence Division
New York Office

Hello

Me

What we are concerned about?

National Priorities

Tools

2 Requests

National Priorities

- Counterterrorism
- Counterintelligence
- Cyber
- Criminal

- Hybrid Threats
- Universal Threats
- Common Modus Operandi

The changing threat of Hostile Nation States

Spies

Economic espionage now dominates our counterintelligence program.

Non-traditional collectors

Investors

Business partners

University Professors and Staff

Students

Researchers

Consultants

RUSSIA

Fifteen largest companies in each country, according to Forbes Global 2000 list (2018):

	China	Russia	USA
1	Industrial & Commercial Bank of China	Gazprom	Berkshire Hathaway
2	China Construction Bank	Sberbank	JPMorgan Chase
3	Agricultural Bank of China	Rosneft	Wells Fargo
4	Bank of China	Lukoil	Bank of America
5	Ping An Insurance Group	Surgutneftegas	Apple
6	Sinopec	VTB Bank	AT&T
7	Bank of Communications	Novatek	Citigroup
8	China Merchants Bank	Norilsk Nickel	ExxonMobil
9	China Life Insurance	Transneft	General Electric
10	Postal Savings Bank of China	Tatneft	Wal-Mart
11	Industrial Bank	Rosseti	Verizon
12	Shanghai Pudong Development Bank	Magnit	Microsoft
13	China State Construction Engineering	Rusal	Alphabet
14	China Minsheng Banking	Novolipetsk Steel	Comcast
15	China CITIC Bank	Severstal	Johnson & Johnson

- IRAN
- NORTH KOREA
- Others?

Hostile Nation States are our most serious source of Cyber related threats.

They will target your network, your people, and your supply chain.

Criminal Threats

DDOS and the IOT

Ransomware

- More focused attacks on companies or parts of companies
- Increasing focus on State and Local government offices

BEC

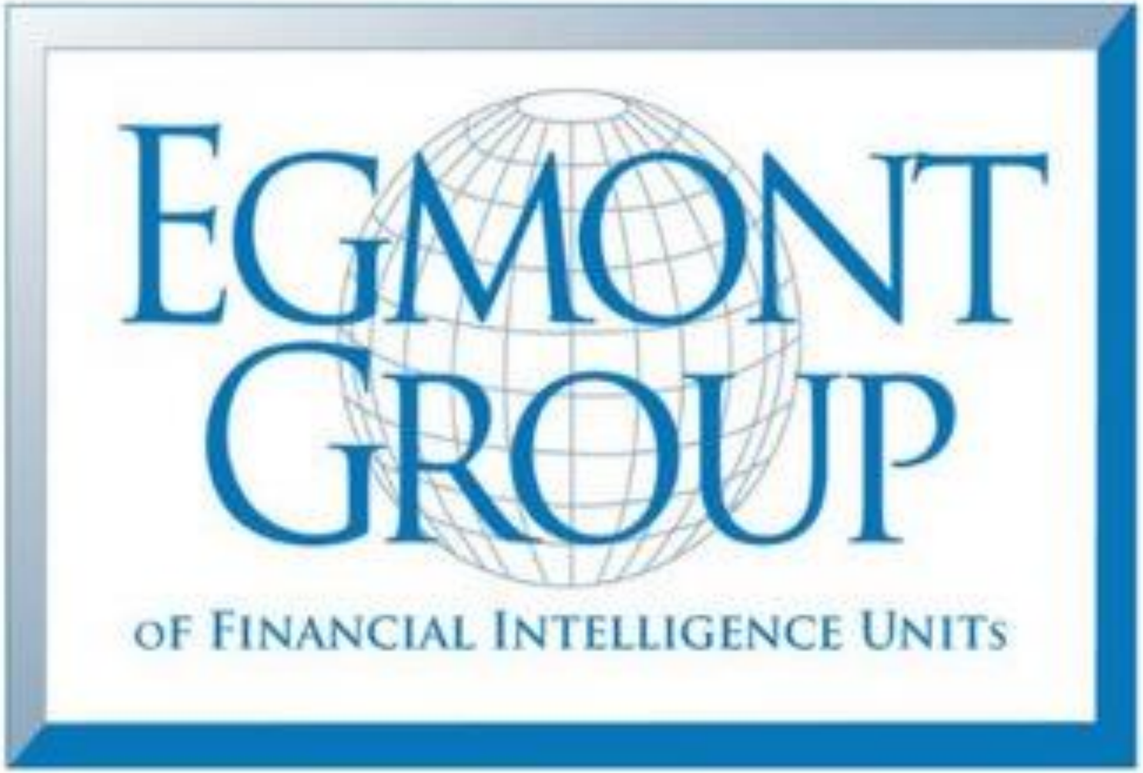
- Attackers are getting better at targeting the right people in your organization.

- Other Cyber Threats, like Malware, are being used to better understand your business processes.

Once you have been the victim of a BEC….

…the clock is ticking.

Financial Intelligence Units


EGMONT
GROUP
OF FINANCIAL INTELLIGENCE UNITS

155

Members

FINANCIAL CRIMES
ENFORCEMENT NETWORK

Bank Secrecy Act information

7

- CTR
- 8300
- CMIR
- DoEP
- FBAR
- RMSB
- SAR

- SARs

Identifying Criminal Actors

Low-level Structures

Facilitators

Serial Fraudsters

Typology Frequency

SARs tell a story !

Details are important…but what is your story?

Accuracy is important…

particularly with names !!

Outside the norm??

Fraud

Terrorist Financing

Human Trafficking

Your reporting can also help identify Cyber threats!

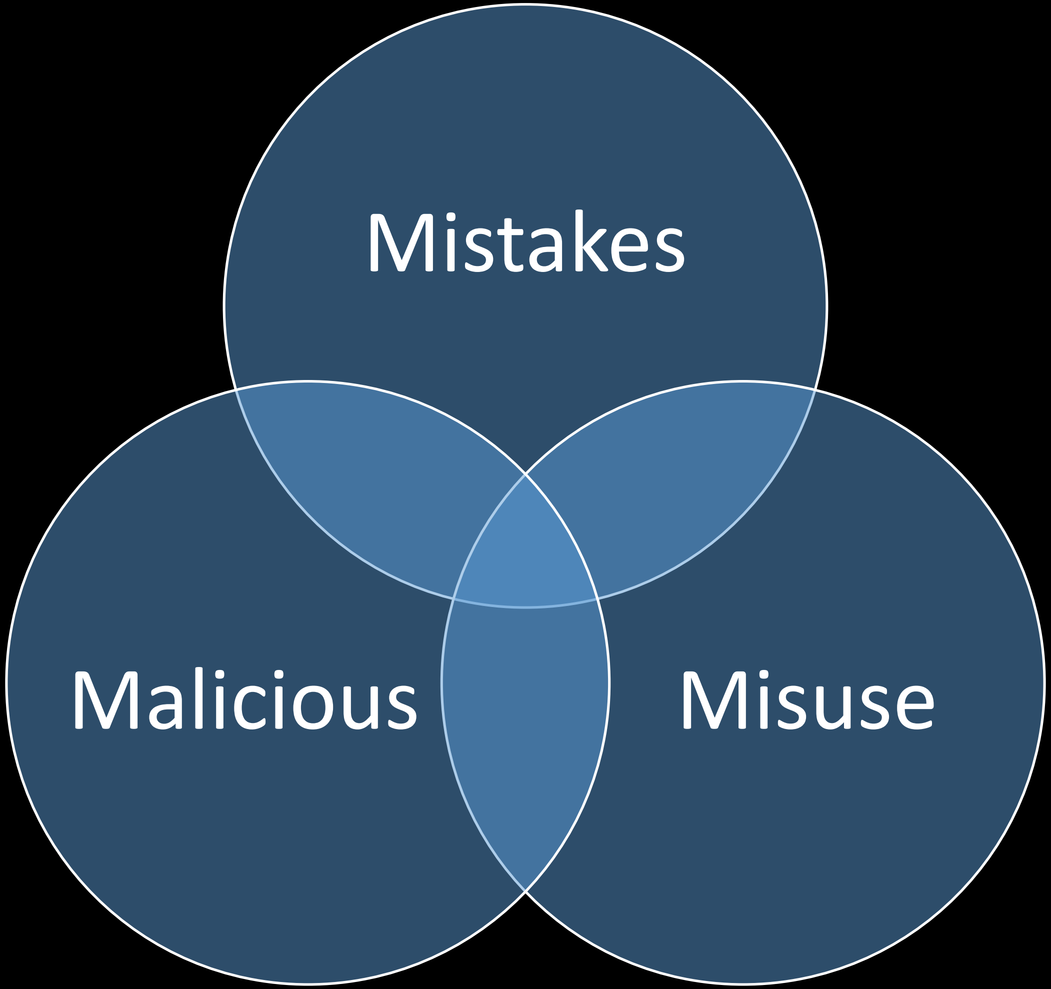
Elder Fraud

Elder Fraud Task Force

Early Adopters of Dark Web Tools

The Insider Threat

THREE TYPES OF INSIDER THREATS



Indicators

- Irregular Work Hours
- Accessing more that the position requires
- Repeated policy violations
- Financial difficulty or unexplained wealth
- Undisclosed foreign contacts
- Undisclosed foreign travel
- Destructive behaviors
- Ego

Indicators of Insiders for the Financial Sector

- Unexplained affluence
- Attempts to access information or accounts…The Dormant Account!!
- Avoids vacations
- Repeated policy violations

The Insider Threat can lead to serious Cyber vulnerabilities!

What happens when you leave the door open??

Consider how your efforts to combat money laundering, identify cyber threats, or address issues of fraud might also be used to identify the insider threat for your organization.

Best Practices for Individuals

- Remember: The Internet was not designed for security
- Limit personal information you post on the web and social media
- Manage your privacy/security settings on social media
- Do not use easy-to-guess passwords or reuse passwords. Consider using a password manager.
- Use two-factor authentication when possible
- Be suspicious of any e-mails you did not expect, especially those containing links or attachments
- Never provide personal information after clicking on a link
- Avoid public Wi-Fi spots and never conduct personal or sensitive business using public Wi-Fi
- Use secure browsing (HTTPS) when possible

  https://
- Keep antivirus tools up to date
- Only install software from trusted sources
- Do not ignore software update warnings, updates often include critical security fixes
- Remove software you do not use

BEST PRACTICES FOR THE ENTERPRISE

- Utilize legal banners
- Establish enforceable security policies and an employee handbook
- Implement employee training and awareness programs
- Maintain network topography maps
- Maintain lists of internal and external IP addresses and hosts
- Maintain inventory of network devices (switches, routers, etc)
- Maintain adequate incident logs
- Archive network traffic
- Perform regular backups of critical systems and data
- Ensure all patches and anti-virus software are up-to-date
- Obtain forensic images of compromised hosts (live memory captures)
- Maintain physical access logs (video cameras, key cards, etc)
- Contact the FBI as soon as possible following an incident

Good Logs!!

Patching!!

What are you protecting??

Don’t trust email!!

Cyber Security Frameworks

www.IC3.gov

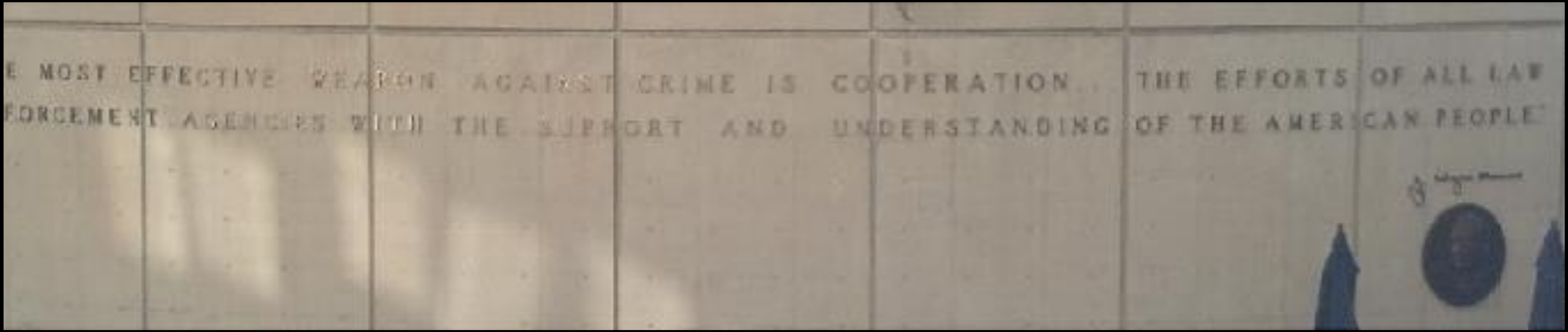
FEDERAL BUREAU OF INVESTIGATION
IC3
INTERNET CRIME COMPLAINT CENTER

https://www.ncfta.net/

www.ncfta.net

www.infragardnational.org

2nd Request



E MOST EFFECTIVE WEAPON AGAINST CRIME IS COOPERATION ... THE EFFORTS OF ALL LAW
FORCEMENT AGENCIES WITH THE SUPPORT AND UNDERSTANDING OF THE AMERICAN PEOPLE"

“The most effective weapon against crime is cooperation… the efforts of all law enforcement agencies with the support and understanding of the American people.”