24th ANNUAL WEST COAST AML CONFERENCE MAY 4 – 6, 2016

THE IMPORTANCE OF CYBER SECURITY

CYBER CRIME VS VIRTUAL CRIME

- **David Griesbach**, Google
- **John Riggi**, Section Chief, Cyber Division, Federal Bureau of Investigation
- **Greg Ruppert**, Senior Vice President, Charles Schwab Corporation

Why is Cyber Security Relevant to the AML Compliance Professional?

- Regulatory priority
- Overlap between multiple disciplines within the firm as well as criminal world
- Downstream ramifications of cyber enabled criminal activity
- Impact to financial firms and their clients
- Related regulatory responsibility

FinCEN's Cyber-Related SAR Definitions

Intrusion

- For purposes of the FinCEN SAR, the term "computer intrusion" has been replaced by the term "unauthorized electronic intrusion". The new term continues to be defined as gaining access to a computer system of a financial institution, to:

  a. Remove, steal, procure, or otherwise affect funds of the institution or the institution's customers;

  b. Remove, steal, procure or otherwise affect critical information of the institution including customer account information; and

  c. Damage, disable or otherwise affect critical systems of the institution.

Account takeover

- "Account takeover" activity differs from other forms of computer intrusion, as the customer, rather than the financial institution maintaining the account, is the primary target.
- In an account takeover, at least one of the targets is a customer holding an account at the financial institution and the ultimate goal is to remove, steal, procure or otherwise affect funds of the targeted customer.

Key Components of Cyber Security

- Information Technology
- Access and Entitlements
- Fraud Prevention
- Fraud Detection
- Risk Assessments
- Testing
- Training
- Technology Development
- Transaction Monitoring
- Audit

- Regulatory Interaction
- Law Enforcement Engagement
- Intelligence Collection
- Threat Reporting
- Background Checks
- Vendor Management
- Internal Investigation/Insider Threat

Areas of Overlapping Responsibility

- CyberSecurity
- Information Technology
- Compliance
- Fraud Prevention
- Fraud Investigation
- Privacy
- Risk Management

- AML
- Legal
- Physical Security
- Internal Investigation
- Human Resources
- Audit
- Customer Service

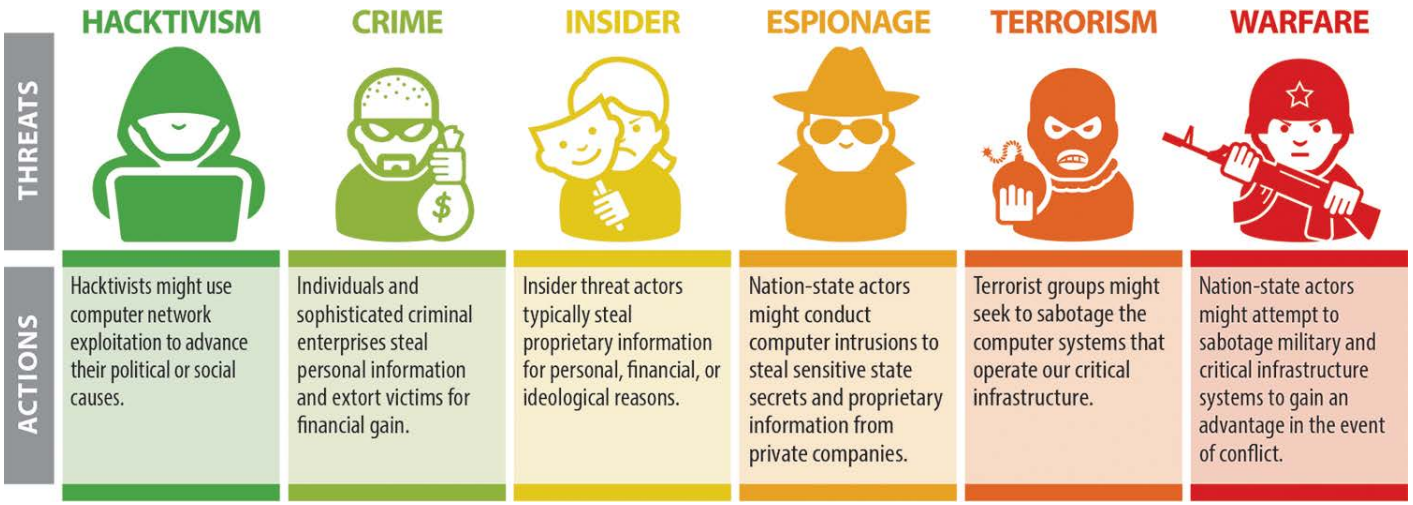
CyberCrime vs Virtual Crimes

Cyber Intrusions	**Cyber Enabled**
• Spear Phishing • Malware • Password Attacks • SEO Attacks	• Account Take-Overs • Business E-Mail Compromise • Ransomware • Romance/Lottery Scams

Mission

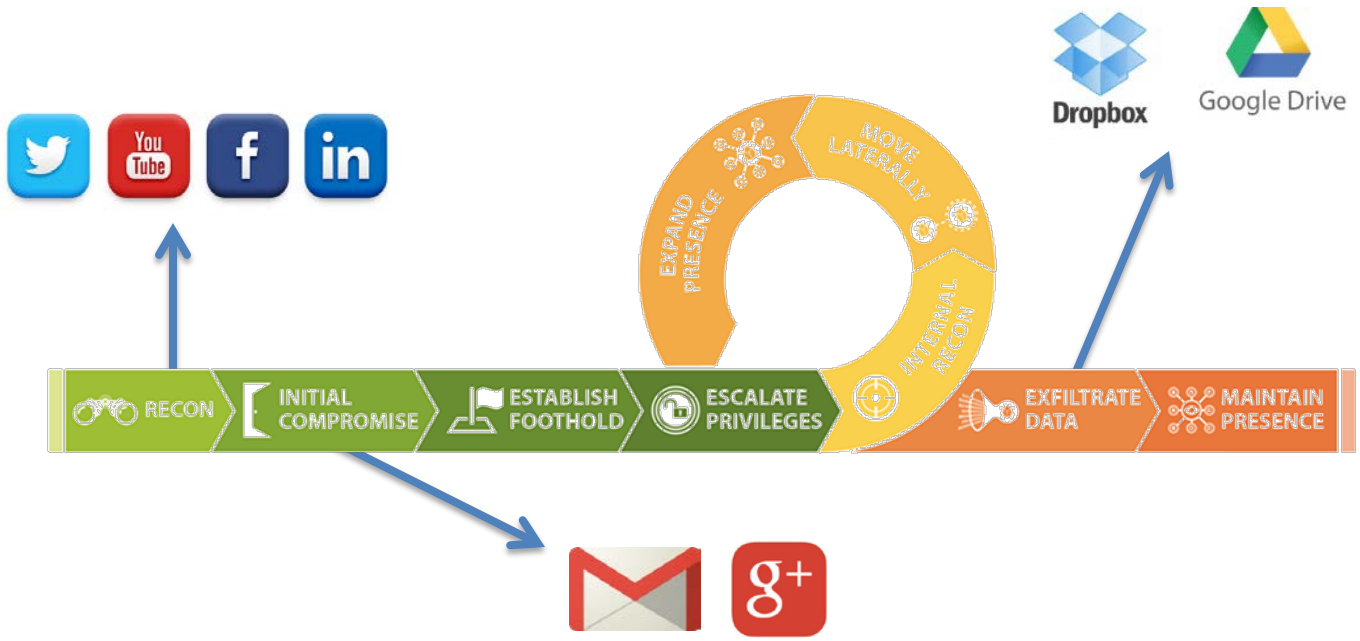
Identify, **pursue**, and **defeat** cyber adversaries targeting global U.S. interests through *collaborative partnerships* and our unique combination of *national security* and law enforcement authorities.

Who May Be Doing the Hacking?



Anatomy of a Hack

Companies with Legitimate Services that Could Be Used for Illicit Cyber Acts



Major Takeaways

- Rapidly Evolving Threat Environment
- Two Factor Authentication
- Security Controls/ Patching
- Speed Matters
- Relationship & Trust
- Information Security Culture
- Computer networks, customer data and YOU are targets
- Privacy vs. Info Sharing
- Media & Legal
- Third Party Vendors
- Whole of Government
- Whole of Nation Approach

Cyber Enabled (Virtual Crimes)

- Account Take-Overs
- Business E-Mail Compromise
- Ransomware
- Romance/Lottery Scams
- Credit/Debit/ATM Card
- Elder Abuse
- SPAM

Law Enforcement's Use of SAR Intelligence

The Financial Crimes Enforcement Network (FinCEN) 2014 Advisory highlighting the importance of the Board and senior management's role in establishing a "strong culture of BSA/AML compliance" across a financial institution, including that:

- its leadership and staff understand the purpose of its BSA/AML efforts and how its reporting is used

Law Enforcement has increased use of and reliance on SAR information well beyond money-laundering.

FinCEN Director Jennifer Shasky Calvery stated at a December 9, 2015 cybersecurity forum that FinCEN "is strongly encouraging financial institutions to include cyber-derived information (such as IP addresses on bitcoin wallet addresses) in suspicious activity reports."

Regulatory Notification to Industry

Federal Financial Institutions Examination Council (Ongoing)

- A number of initiatives to raise the awareness of financial institutions and their critical third-party service providers have been implemented.

FDIC's Supervisory Insights (2015 Winter)

- On February 1st, the *Federal Deposit Insurance Corporation (FDIC)* published "A Framework for Cybersecurity," an article that appears in the Winter 2015 issue of *Supervisory Insights*.

OCC Thomas J. Curry, Comptroller of the Currency (December 16, 2015)

- [W] e can't lose sight of the continued risk associated with cybersecurity and compliance, including anti-money laundering requirements. We can't allow the federal banking system to be compromised by hackers or used by criminals or terrorists. We saw in the aftermath of the financial crisis that there is a price to be paid for ignoring compliance.

2016 Regulatory Exam Priorities (SEC and FINRA)

- AML
- Cybersecurity
- Microcap Securities
- Senior and Vulnerable Investors

Key Membership Groups

- ACAMS (http://www.acams.org/acams-chapters/northern-california/)
- Financial Services Information Sharing Analysis Center (FS-ISAC) (https://www.fsisac.com/)
- National Cyber Forensic Training Alliance (http://www.ncfta.net/)
- FBI InfraGard (https://www.infragard.org/) Public-Private Outreach
- USSS Electronic Task Force (http://www.secretservice.gov/investigation/)
- FBI Cyber Task Force (https://www.fbi.gov/about-us/investigate/cyber/cyber-task-forces-building-alliances-to-improve-the-nations-cybersecurity-1)
- DHS – US CERT (https://www.us-cert.gov/)
- US ICE: Homeland Security Investigations Cyber Crime Center (https://www.ice.gov/cyber-crimes)