CYBERSECURITY CHALLENGES FOR CORPORATE COUNSEL OPERATING GLOBALLY

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

JENNER&BLOCK

comSCORE

NAVIGANT

IT'S BEEN A BUSY FEW YEARS

CYBER THREATS

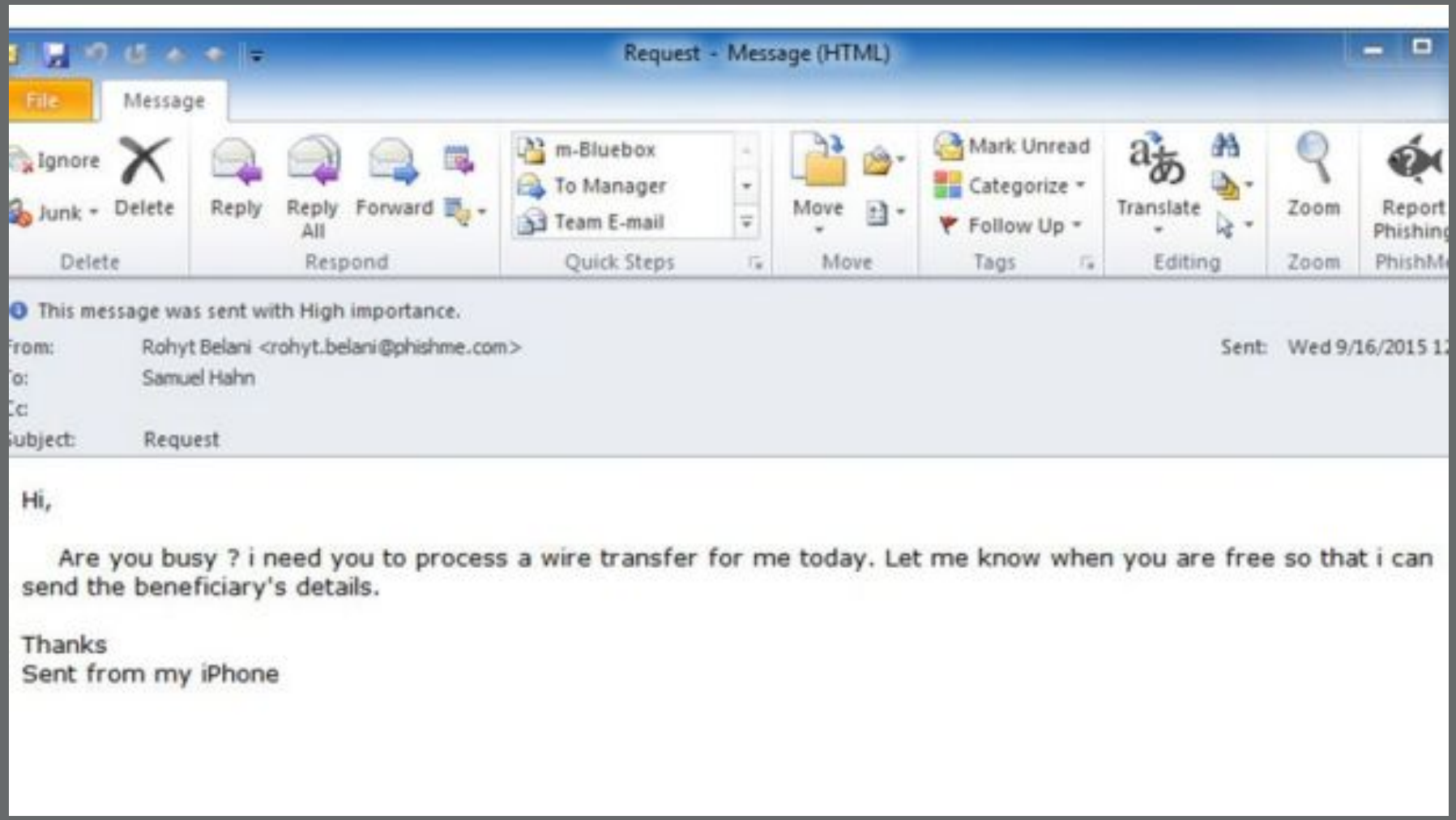
- Hacktivists
- Criminal Groups
- Insider
- Nation State
- Terrorism

MOST COMMON ATTACKS/VECTORS

- Office 365 Compromise
- Business Email Compromise
- Ransomware
- Employee Created
- Vulnerabilities
- Vendor Vulnerabilities
- PHISHING

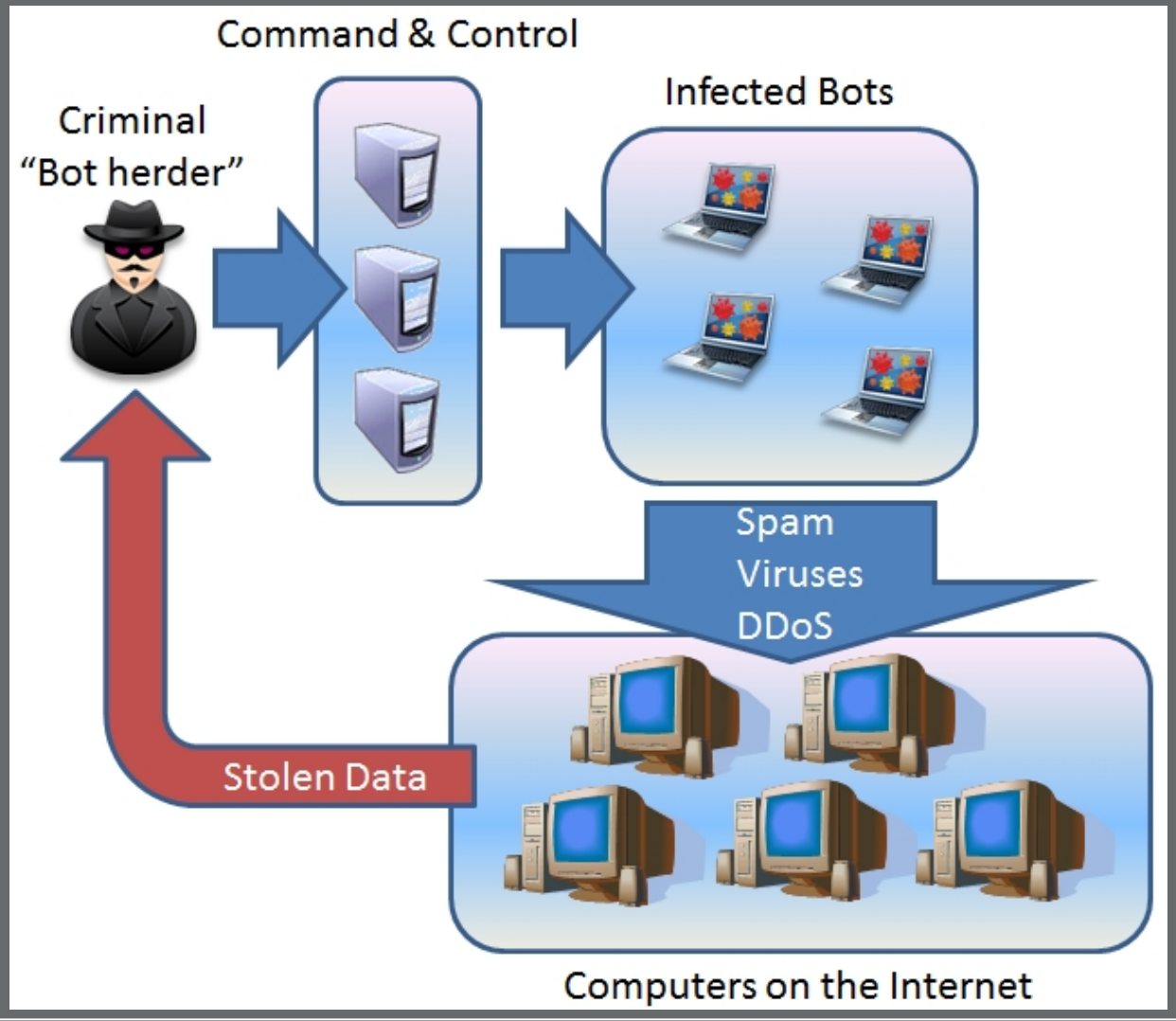
NAVIGANT

BUSINESS EMAIL COMPROMISE/CEO SCAM



NAVIGANT

BOTNETS AND THE EVOLUTION OF CYBER CRIME



NAVIGANT

NATION STATE ACTORS

NAVIGANT

NOT IF. WHEN.

- 59% of employees steal proprietary corporate data when they quit or are fired
- 28% of organizations have experienced an advanced persistent threat attack, and three-quarters have failed to update their third-party vendor contracts to include better protection against APTs
- 63% of businesses don't have a ‘fully mature’ method to track and control sensitive data
- 63% of confirmed data breaches leverage a weak, default, or stolen password
- 30% of phishing emails are opened. 12% of targets go on to click the link or attachment
- Only 38% of global organizations feel prepared for a sophisticated cyberattack
- 68% of funds lost as a result of a cyber attack were declared unrecoverable

“The cyber insurance market—mainly a U.S. market—has grown from $1 billion to $2.5 billion over the past two years, and it is expected to grow dramatically and expand globally over the next five years.”

MITIGATE THE RISK

- Identify and segregate the crown jewels
- Update and Patch
- Back-up data regularly and segregate the backups
- Maintain log files for a minimum of 6 months, preferably 12
- Layered defense to isolate protected data from internet or customer facing systems
- Data Encryption, at rest and in motion
- Implement Multi Factor Authentication
- Enforce “Policy of Least Privilege”
- Know Your Customer and have a robust vendor management program
- Retain outside counsel with cyber expertise
- Develop relationships with law enforcement before the attack

- Plan for a breach and prepare your response
- Know what data you have and where it is – network mapping
- Consider cyber insurance, but know what your policy covers and **what it doesn’t**

ETHICAL OBLIGATIONS RE: PROTECTION OF CLIENT INFORMATION

- American Bar Association (ABA) Rules of Professional Conduct impose a DUTY OF CONFIDENTIALITY:

  "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." ABA Model Rule 1.6(a).

  - Factors to be considered in determining whether counsel used "reasonable efforts": sensitivity of information, safeguards, cost of safeguards, effect on client. ABA Model Rule 1.6(a), Comment 18.
  - Client may require lawyer to implement special security measures not required by the Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. ABA Model Rule 1.6(a), Comment 19.

- ABA Rules also impose a DUTY OF COMPETENCE, requiring lawyers to keep up-to-date regarding technology. ABA Rule 1.1 (a lawyer must stay "abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology").

ETHICAL OBLIGATIONS OF OUTSIDE COUNSEL RE: CYBERSECURITY

- ABA Formal Opinion 477 – Describes how a lawyer's duties of CONFIDENTIALITY and COMPETENCE intersect with cybersecurity
- Duty of Competence requires lawyers to keep "abreast of knowledge of the benefits and risks associated with relevant technology" (Comment [8] to ABA Model Rule 1.1; Formal Opinion 477)
- Duty of Confidentiality requires lawyers to exercise reasonable efforts to prevent inadvertent or unauthorized disclosure of, or access to, client information when using technology (Formal Opinion 477)
- Considerations outlined in Formal Opinion 477:
  - Understand the nature of the threat
  - Understand how client information is transmitted and where it is stored
  - Understand and use reasonable electronic security measures
  - Determine how electronic communications about client matters should be protected
  - Label client confidential information
  - Train lawyers and non-lawyer assistants in technology and information security
  - Conduct due diligence on vendors that provide communications technology
- Formal Opinion 477: https://www.americanbar.org/content/dam/aba/administrative/law_national_security/ABA%20Formal%20Opinion%20477.authcheckdam.pdf

GENERAL DATA PROTECTION REGULATION (GDPR)

- GDPR
- Effective May 25, 2018

- Article 32 - Security of Processing
- Controller and processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate

- Article 33 - Breach Notification to the Supervisory Authority
- Notification to Supervisory Authority required within 72 hours unless it's unlikely to result in risk to "rights and freedoms of natural persons."

- Article 34 - Breach Notification to Data Subject
- Notification to data subject is not required if Controller "implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach"

CALIFORNIA CONSUMER PRIVACY ACT OF 2018, AB-375

- CA Consumer Privacy Act of 2018
- Signed into law June 28, 2018, effective January 1, 2020 and acknowledged as one of the strictest privacy laws in U.S. history
- Broad definitions of “Personal Information” and “Sale”
- Creates access and opt-out rights for consumers
- Specific steps for companies to take to provide consumers with notice of their rights
- Provides a private right of action for consumers to recover statutory damages and injunctive relief if personal information is stolen and not encrypted or redacted
- CA Attorney General enforcement
- The CA Attorney General is required to solicit public participation to adopt regulations to further the law.

CORPORATE COUNSEL BEST PRACTICES

- Create and maintain a strong relationship with Information Security team
- Work with IT, HR, Marketing to limit the type and amount of data collected to only what is necessary for business purposes
- Cybersecurity training for employees – reinforce importance of privacy and security in one on one interactions with business clients
- Identify buckets of data collected by company that are the most sensitive. Learn and stay current on the regulations that govern that type of data. Will be different for different industries and different geographies (i.e. retailers – PCI, healthcare companies – HIPAA, etc.)
- Data retention policy – keep the minimum amount of data needed for the shortest amount of time possible
- Cyber insurance - review policy and know when an incident needs to be reported for policy to kick in; be involved in renewal process
- Perform data privacy and cybersecurity due diligence on any acquisitions

Make sure people across your organization know who you are and that you are the point of contact for any transactions involving the collection or sharing of data

CORPORATE COUNSEL BEST PRACTICES IN EVENT OF SECURITY INCIDENT

- Determine whether disclosure of information warrants implementation of incident response plan (i.e., email accidentally sent to one person outside the organization v. threat actor identified in your environment)
- If necessary, initiate incident response plan
  - Organize internal stakeholders
  - Contact outside experts, which may include:
    - Outside counsel with cyber expertise
    - Forensics consultants (one or more)
    - Crisis management firm
- Educate business clients on importance of attorney/client privilege and how to maintain it
- Be careful with terminology – “data breach” is a term of art
- Learn your company’s technology
- Assist IT stakeholders with creation of remediation plan
- Determine if/when incident needs to be reported to affected individuals, regulators, cyber insurance carriers
- Deep dive post incident to discuss lessons learned and update incident response plan accordingly

TRENDS IN THE NEAR TERM

- Outsourcing IT
- Wireless payment systems
- Rapid Connectivity Growth in Developing Nations
- Bring Your Own Device/Telecommuting
- Internet of Things

CONTACT INFORMATION

Nancy C. Libin
Partner
Jenner & Block LLP
Phone: +1 202-639-6086
Email: NLibin@jenner.com

Jennifer Mailander
Associate General Counsel, Privacy and Compliance
comScore, Inc.
Phone: +1 571-306-6416
Email: jmailander@comscore.com

James Bickley
Director
Navigant Consulting
Phone: +1 202-973-3282
Email: James.bickley@navigant.com

