

womblebonddickinson.com



# Cybersecurity Law for Corporate Counsel

Allen O'Rourke

July 10, 2019



## Presentation Roadmap

---

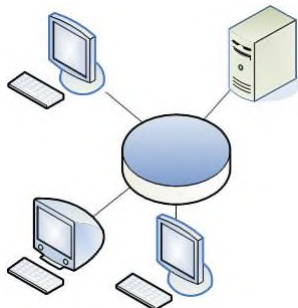
- A. Internet for Lawyers
- B. Cyber Incident Response
- C. Breach Notification
- D. Cybersecurity Law Trends



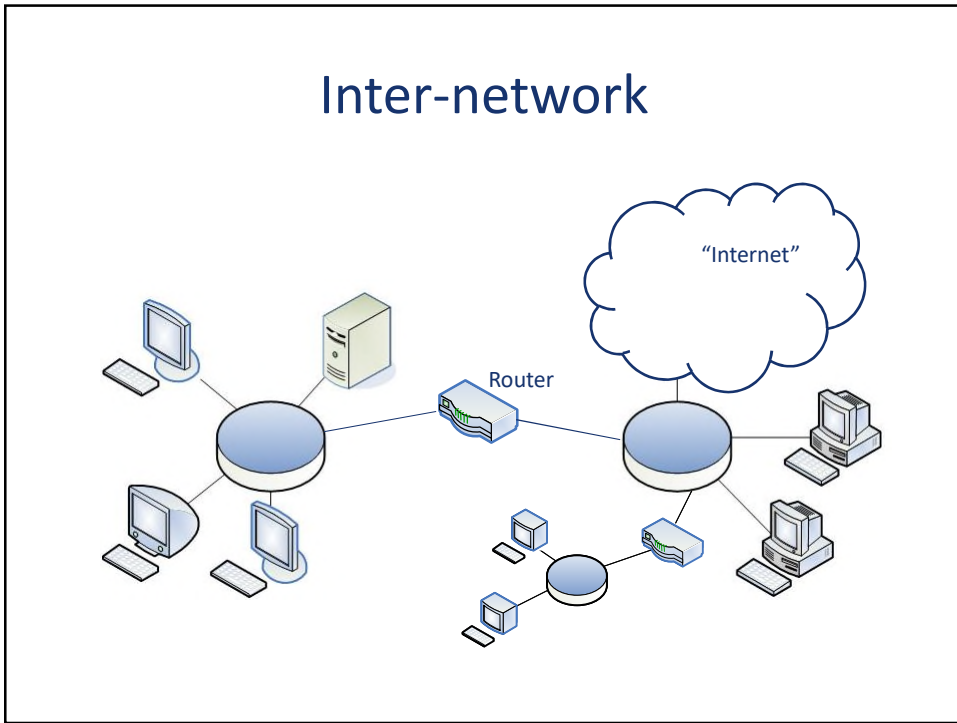
Confidential Attorney Work Product  
and Attorney-Client Privileged

66.57.3.106

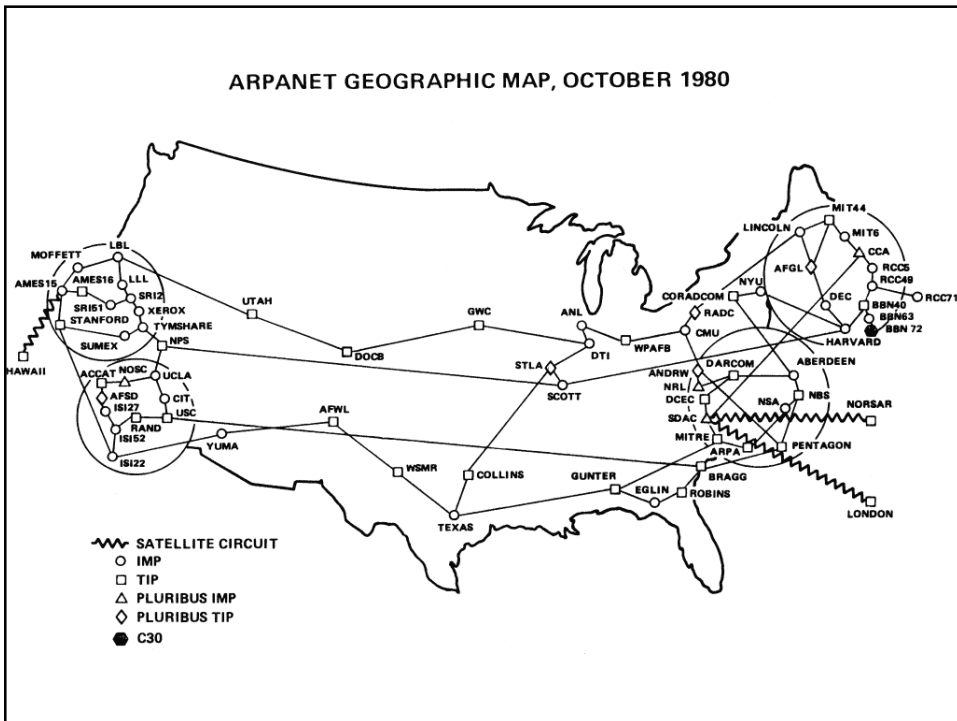
Network

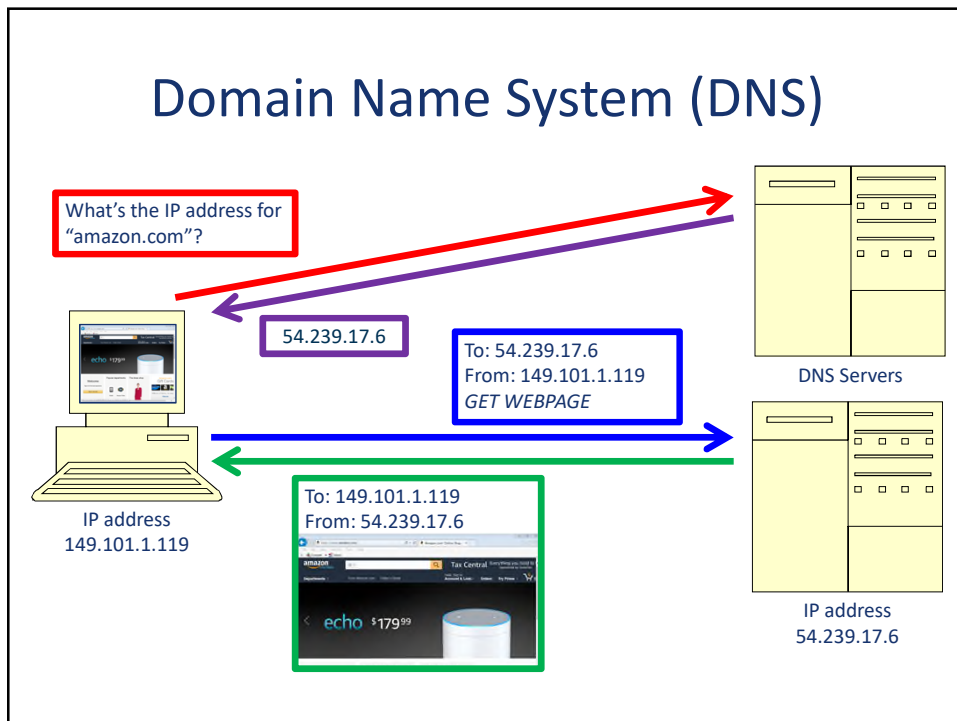
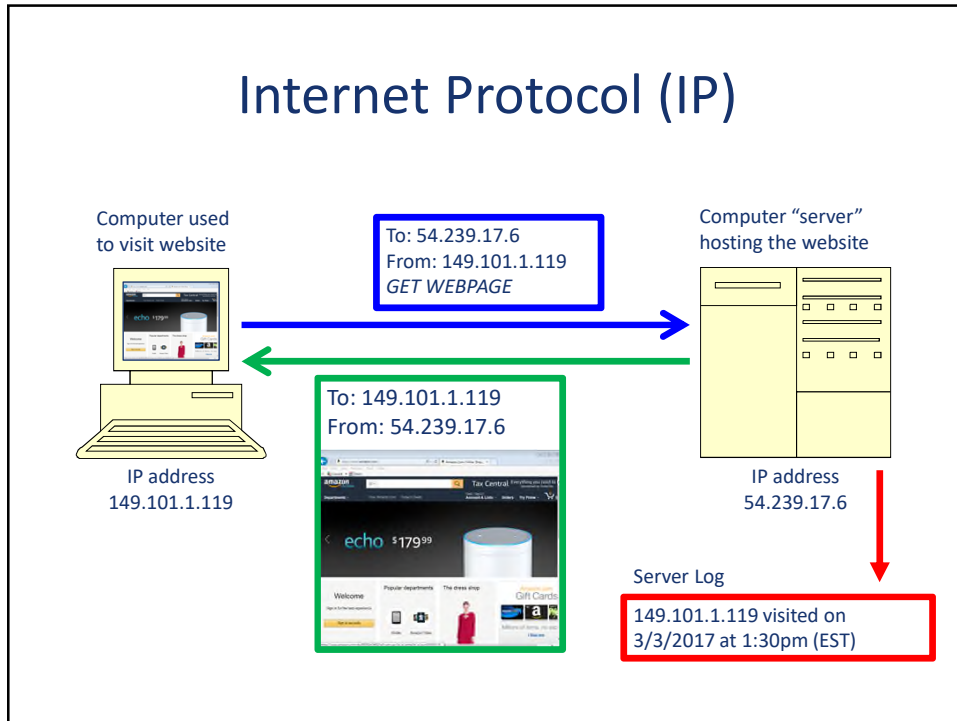


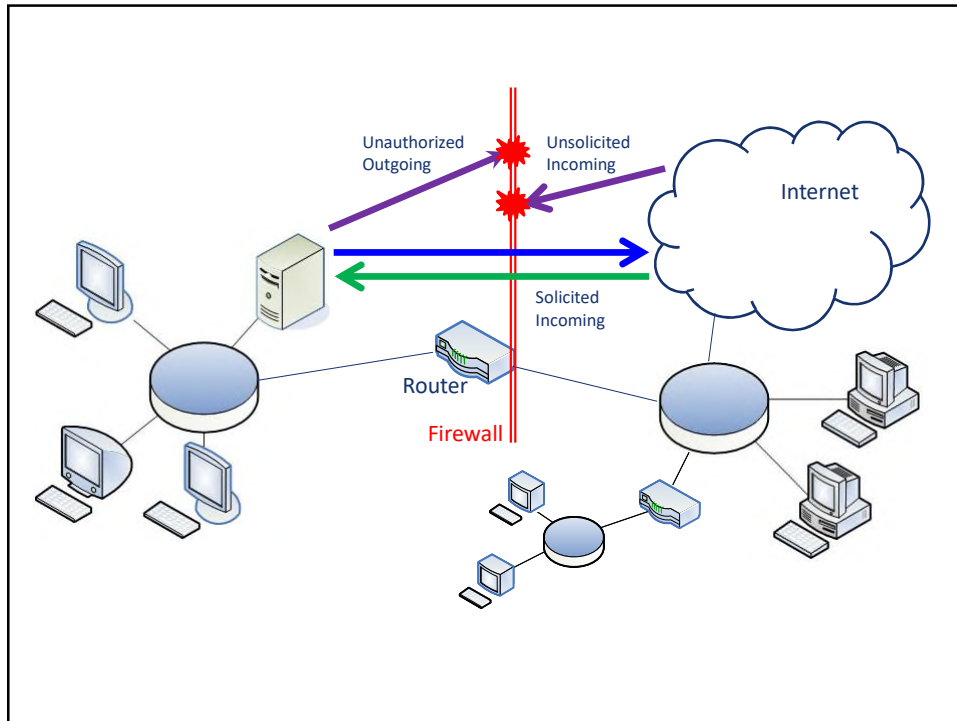
# Inter-network



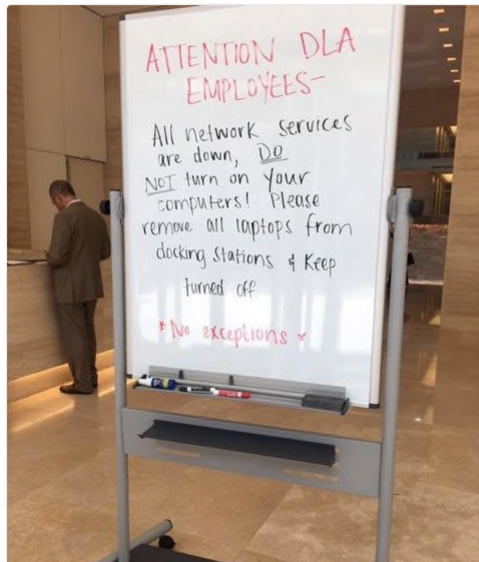
ARPANET GEOGRAPHIC MAP, OCTOBER 1980







A tipster sends along this photo taken outside DLA Piper's D.C. office around 10am.  
[#Petya](#)



9:30 AM - 27 Jun 2017

## Presentation Roadmap

---

- A. Internet for Lawyers
- B. Cyber Incident Response
- C. Breach Notification
- D. Cybersecurity Law Trends

## Company got a tip from the FBI ...

- We believe hackers got inside your network.
- Here are IP addresses for about 75 computers we think are infected.
- Can we have copies of some of your infected computer systems for our investigation?
- Watch what you say in your emails, since the hackers might be monitoring them now.



## But the FBI's tip got worse ...

- These are sophisticated foreign hackers that we've been tracking for a long time.
- From past experience, we think they're preparing to launch a "ransomware attack" that encrypts your computers until you pay a huge ransom.



## Incident Response (IR) Playbook



**Detect** and verify the incident.



**Analyze** applicable legal requirements and liability risk.



**Mitigate** any ongoing breach or cyberattack.



**Notify** people affected, law enforcement, and any others as required.



**Investigate** nature and cause of compromise, and data affected.



**Review** what went wrong and implement any lessons learned.

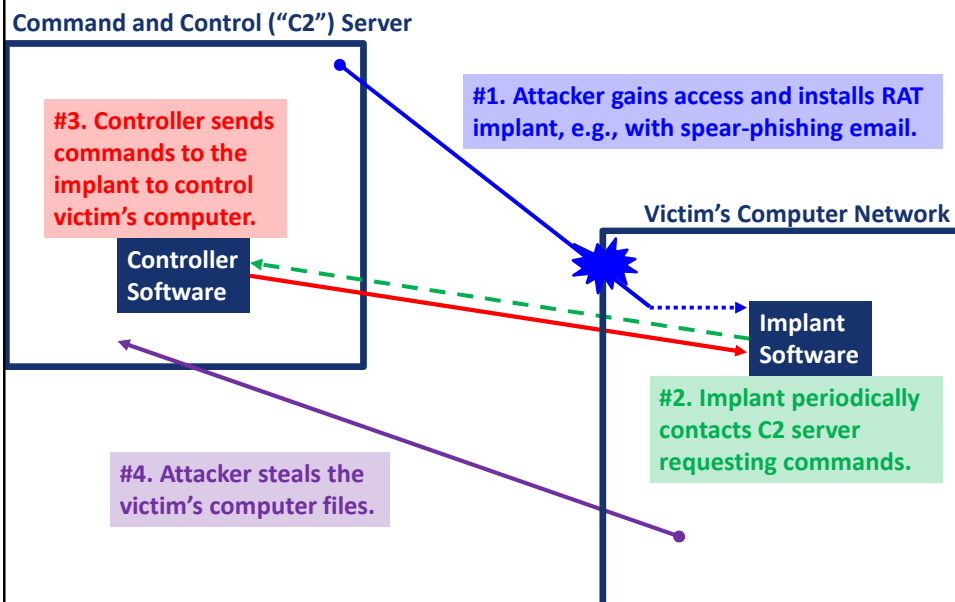
## Phase 1 – Detect & Verify

- Several types of remote access trojan (“RAT”) malware were found.
- This would enable remote access into the infected computer to execute commands – like to install and detonate ransomware.



15

## Remote Access Trojan (RAT)





## *Phase 2 – Mitigate*

- The team began right away (Day 1) using off-channel communications.
- Worked to locate malware files and determine the channels for “C2” communication.
- Successful counterstrike ended on Day 12 (e.g., quarantine malware, block C2 traffic, and reset passwords).
- This was done without setting off ransomware or significantly disrupting business operations.

17

## *Phase 3 – Investigate*

Data security firm did a forensic investigation into the nature and scope of compromise:

- First evidence of intrusion was 4 weeks earlier
- Initial point of entry was likely spear-phishing
- 100 computers of various types infected
- Ten sets of stolen credentials, mostly IT staff
- No evidence of data “exfiltration” or searches

18

## Challenges & Lessons

- Layers of evidence gathering
  - Router → Network monitoring
  - Endpoints → Endpoint monitoring
  - Files & emails → Audit logging
- Log management
- Data impact review
- Written incident response plan



19

## Presentation Roadmap

---

- A. Internet for Lawyers
- B. Cyber Incident Response
- C. Breach Notification
- D. Cybersecurity Law Trends

## *Phase 4 – Analyze*

- Breach notification obligations:
  - Assortment of state statutes
  - Federal sectoral requirements, e.g., GLBA
  - PCI-DSS for payment card data
  - Foreign laws, e.g., GDPR
  - Contract clauses, e.g., DFARS 252.204-7000
- Business impact and reputational harm
- Data security liability exposure

21

## Example: NC's Data Breach Law

- “‘Security breach’. — An incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer.”
- The business “shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach.”

N.C. Gen. Stat. §§ 75-61, 75-65

22

## Example: GLBA Guidelines

- “When a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused.”
- “If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible.”

12 C.F.R. § Pt. 30, App. B

23

## Example: Europe’s GDPR

- “[P]ersonal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.”
- “In the case of a personal data breach, the controller shall ... notify the personal data breach to the supervisory authority ... unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.”

Regulation (EU) 2016/679, Art. 4(12) and 33

24

## Challenges & Lessons

- Key questions for notification analysis:
  - Was the defined type of data compromised?
  - Did the compromise amount to a “breach”?
  - If required, was there risk of harm?
- Notifying law enforcement
- Contract review for breach notification and data security clauses
- Data mapping and management

25

## Presentation Roadmap

---

- A. Internet for Lawyers
- B. Cyber Incident Response
- C. Breach Notification
- D. Cybersecurity Law Trends

## Evolving Duty of Cybersecurity

- Affirmative data security obligations:
  - Growing number of state laws
  - Federal sectoral requirements, e.g., GLBA
  - PCI-DSS for payment card data
  - Foreign laws, e.g., GDPR
  - Contract requirements, e.g., NIST SP 800-171
- Common law torts, e.g., negligence
- “Unfair or deceptive acts or practices” (UDAP)

27

## FTC Enforcement: Wyndham Hotels (2015)

- In 2008-2009, Wyndham suffered three data breaches of over 600,000 customers’ records, leading to over \$10.6 million in fraud.
- In 2012, the FTC sued Wyndham for UDAP in violation of 15 U.S.C. § 45(a).
  - “Unfair” based on deficient cybersecurity
  - “Deceptive” based on Wyndham’s privacy policy overstating its cybersecurity

28

## FTC Enforcement: Wyndham Hotels (2015)

The alleged “unfair” cybersecurity included:

- Storing credit card data in clear text
- Allowing simple passwords for sensitive servers
- Failure to use basic network safeguards (firewalls)
- Failure to adequately oversee the cybersecurity of hotels connecting to Wyndham’s network
- Allowing vendors unnecessary system access
- Failure to take reasonable measures for security investigations or incident response

29

## FTC Enforcement: Wyndham Hotels (2015)

- Wyndham refused to settle, challenging the FTC’s authority to bring such actions.
- In 2015, the Third Circuit upheld the FTC’s interpretation of their § 45(a) authority, ruling that UDAP may include unfair or deceptive cybersecurity practices. *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015)

30

## SEC Enforcement: Altaba/Yahoo! (2018)

- In December 2014, Yahoo's information security team became aware that nation-state hackers stole personal data of 108 million users and gained access to 26 email accounts.
- The 26 users with compromised accounts were notified, and their passwords reset.
- Yahoo's senior management and legal teams received internal reports about the breach.





31

## SEC Enforcement: Altaba/Yahoo! (2018)

- In June 2016, Yahoo's new CISO concluded their entire user database had been compromised by the hacker group over several intrusions, including the 2014 breach.
- In September 2016, Yahoo finally disclosed the breach, having already negotiated their acquisition by Verizon. The disclosure led to a \$350 million reduction in the purchase price.

32



<p><b>WANTED BY THE FBI</b></p> <p><b>ALEXSEY BELAN</b></p> <p>Conspiring to Commit Computer Fraud and Abuse; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging a Computer Through the Transmission of Code and Commands; Economic Espionage; Theft of Trade Secrets; Access Device Fraud; Aggravated Identity Theft; Wire Fraud</p>  <p><b>DESCRIPTION</b></p> <p><small>Names: Alexsei Belan, Alexsey Belan, Alexsey Aleksandrovich Belan, Alexsey Aleksandrovich Belan, Alexsei Belan, Alex' Vasiliev, "Miyunov"</small></p>	<p><b>WANTED BY THE FBI</b></p> <p><b>DMITRY ALEKSANDROVICH DOKUCHAEV</b></p> <p>Conspiring to Commit Computer Fraud and Abuse; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging a Computer Through the Transmission of Code and Commands; Economic Espionage; Theft of Trade Secrets; Access Device Fraud; Aggravated Identity Theft; Wire Fraud</p> 
<p><b>KARIM BARATOV</b></p> 	<p><b>WANTED BY THE FBI</b></p> <p><b>IGOR ANATOLYEVICH SUSHCHIN</b></p> <p>Conspiring to Commit Computer Fraud and Abuse; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging a Computer Through the Transmission of Code and Commands; Economic Espionage; Theft of Trade Secrets; Access Device Fraud; Wire Fraud</p> 


## SEC Enforcement: Altaba/Yahoo! (2018)


- The SEC brought an action against Yahoo for Securities Act violations based on material omissions in SEC filings and failure to maintain adequate disclosure controls.
- As the SEC explained, “Yahoo senior management and relevant legal staff did not properly assess the scope, business impact, or legal implications of the [2014] breach ...”
- In 2018, Altaba/Yahoo settled for \$35 million.

## UK ICO Enforcement: British Airways (2019)


- In Summer 2018, British Airways suffered a cyberattack in which details from 380,000 booking transactions were stolen, including customer payment card data.
- On July 8, 2019, the UK Information Commissioner's Office (ICO) announced a penalty of about \$229 million under GDPR.
- This is the largest fine ever imposed for a data breach, and the first under GDPR.

35






**Allen T. O'Rourke**  
Womble Bond Dickinson (US) LLP



**WOMBLE  
BOND  
DICKINSON**

**Contact Information**  
Charlotte Office  
t: 704.350.6357  
e: allen.orourke@wbd-us.com

**Social Media**  
 [linkedin.com/in/allenorourke](https://www.linkedin.com/in/allenorourke)

Womble Bond Dickinson (US) LLP is a member of Womble Bond Dickinson (International) Limited, which consists of independent and autonomous law firms providing services in the US, the UK, and elsewhere around the world. Each Womble Bond Dickinson entity is a separate legal entity and is not responsible for the acts or omissions of, nor can bind or obligate, another Womble Bond Dickinson entity. Womble Bond Dickinson (International) Limited does not practice law. Please see [www.womblebonddickinson.com/us/legal-notice](http://www.womblebonddickinson.com/us/legal-notice) for further details.

Womble Bond Dickinson (US) LLP communications are intended to provide general information about significant legal developments and should not be construed as legal advice regarding any specific facts and circumstances, nor should they be construed as advertisements for legal services.

©2017 Womble Bond Dickinson (US) LLP