WILMERHALE®

WILMER CUTLER PICKERING HALE AND DORR LLP®

WEBINAR

Cybersecurity Updates and Trends

January 12, 2021

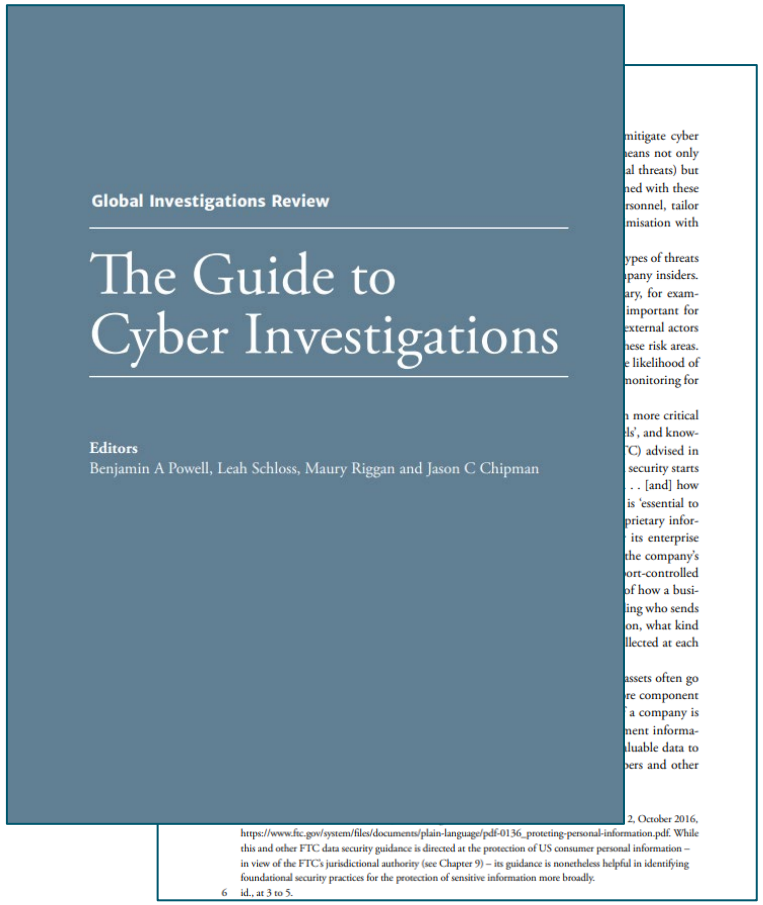
Speakers: Ben Powell, Jason Chipman, Martin Braun, Arianna Evers

Webinar Guidelines

- Participants are in listen-only mode
- Submit questions via the Q&A feature
- Questions will be answered as time permits
- Offering 1 CLE credit in California and New York*
- The webcast is being streamed through your computer, so there is no dial-in number. For the best quality, please make sure your volume is up and other applications are closed. If you experience a delay or get disconnected, press F5 to refresh your screen at any time
- For additional help with common technical issues, click on the question mark icon at the bottom of your screen

WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional credit in New York. This program, therefore, is being planned with the intention to offer CLE credit for experienced New York attorneys only. Attendees of this program may be able to claim England & Wales CPD for this program. WilmerHale has been approved as a Colorado Certified Provider, as recognized by the Colorado Supreme Court Continuing Legal and Judicial Education Committee. We will apply for Colorado CLE if requested. The type and amount of credit awarded will be determined solely by the Colorado Supreme Court. New Jersey grants reciprocal credit for programs that are approved in New York. We can also issue Connecticut credit for this program. All attendees, regardless of jurisdiction, will receive a uniform certificate of attendance that shows the states in which the program was approved. Attendees requesting CLE credit must attend the entire program. CLE credit is not available for on-demand webinar recordings.

Additional Resources



Speakers

Benjamin Powell
Partner; Co-Chair,
Cybersecurity and Privacy
Practice
WilmerHale

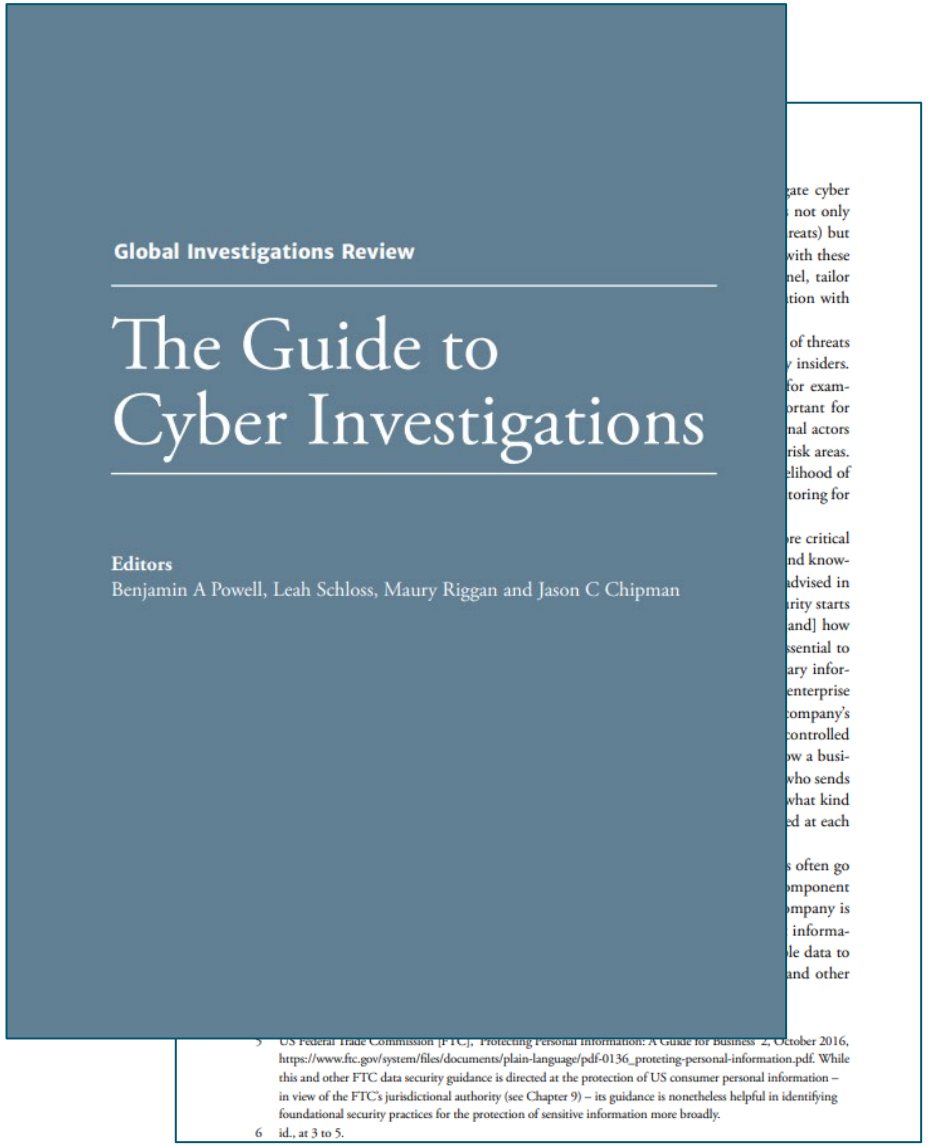
Jason Chipman
Partner
WilmerHale

Dr. Martin Braun
Partner; Co-Chair, Big Data
Practice
WilmerHale

Arianna Evers
Counsel
WilmerHale

Overview

- **Prepare**
  - Current threat landscape, including a discussion of SolarWinds and recent ransomware developments
  - Important considerations for incident preparedness
- **Respond**
  - Regulatory enforcement in the United States
  - Developments in data breach litigation
  - Regulatory developments in the European Union
- **Anticipate**
  - Key expected developments in cybersecurity, including what to expect from a Biden/Harris administration and from regulators in 2021




The Current Threat Landscape

Cybersecurity Threats Continue to Proliferate

- Cybersecurity threats and attacks show no sign of slowing down
  - COVID-19
  - Increased threat actor coordination and sophistication
  - Continued interest and investment by nation states in intelligence/espionage
- In November, German insurer Allianz reported a 950% increase in cyber insurance claims over the last three years:
  - Average cost to a business of a cyberattack is now $13 million
  - Data breaches involving one million personal records or more cost businesses an average of $50 million
  - Approximately 60% of financial losses linked to interrupted business as corporate systems are taken offline

SolarWinds – Background

- **Timeline**:
  - Tuesday, December 8, 2020: Cybersecurity firm FireEye/Mandiant ("FireEye"), discovers its systems are compromised, and that a number of tools they use to identify cybersecurity compromises have been accessed
  - Friday, December 11, 2020: FireEye discovers that corrupted updates to SolarWinds' Orion software had been the source of the compromise
  - Monday, December 14, 2020: SolarWinds releases a statement announcing that "fewer than 18,000 customers" downloaded the compromised software
  - Tuesday, January 5, 2021: The FBI, CISA, ODNI, and NSA joint statement explaining that an "Advanced Persistent Threat (APT) actor, likely Russian in origin, is responsible for most or all of the recently discovered, ongoing cyber compromises of both government and non-governmental networks"

SolarWinds – Background

- Information continues to surface on a daily basis as investigations develop
- So far, cyber forensics have shown:
  - Attackers executed what is known as a **supply chain attack** by injecting malware into an update of SolarWinds' Orion software
  - Malware may have been **present and undetected** between March and June 2020
  - **Two versions of malware** have been identified and some analysts are addressing them as separate attacks: SUNBURST (or Solorigate) and SUPERNOVA

SolarWinds – Takeaways

- **Scope of Actual Exploitation Still Unknown**
  - The actual exploitation of an organization's networks would have required hands-on-keyboard involvement by individual hackers. As such, several the avenues for malicious actors may have been left unused.
- **Forensics and Incident Response**
  - Many companies may be able to determine, after careful examination of forensic evidence, that the vulnerabilities have not been exploited.
  - For organizations that were manually targeted by the attackers for exploitation of the vulnerability, the remediation process may be much more difficult.
- **Communications**
  - Careful communications and consideration of all stakeholders—including customers, employees, vendors, shareholders, board members and others—are essential.
  - Public communications will need to be carefully reviewed for accuracy and compliance with securities laws.

SolarWinds – Takeaways

- Pay attention to your supply chain. Initial and ongoing diligence of all vendors is critical
- Review your response to this attack and understand your ability to respond to a cyber incident requiring: (i) rapid action across multiple parts of the organization, and (ii) an understanding of potential exposure
- Especially in situations where a vulnerability has not been exploited, this is a good opportunity to stress-test incident response plans, processes, and resources
- Key questions include:
  - Does your company have access to adequate forensic resources?
  - Does your company have the ability to conduct cyber forensics quickly in response to a fast-moving incident?
  - Does your company's incident response plan need to be updated based on any lessons learned from this incident?
- Keep the potential for future enforcement actions and/or litigation in mind as you respond and communicate findings to any third-parties
- **WilmerHale Resource**: "Quick Takeaways: SolarWinds Cybersecurity Incident"

Ransomware Attacks

- Threat of ransomware attacks continues to increase and shows no signs of slowing down
- New variants and methods
  - "Doxxing" and extortion threats
  - "Ransomware as a service"
- Increased coordination between threat actor groups and resource sharing
- Sanctions risks associated with facilitating ransomware payments
  - Two recent advisories: (1) U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC), and (2) Financial Crimes Enforcement Network (FinCEN)
  - Potential for violation of OFAC sanctions regulations, which are strict liability and carry civil penalties
  - Suspicious Activity Reports (SARs) may be required or appropriate

Ransomware Attacks

- Expectation that entities will inform or otherwise support law enforcement as part of their response to an attack
- **WilmerHale Resource**: "Ransomware Attacks—Financial Crimes Compliance Requirements"

Incident Preparedness

- Develop an incident response plan and regularly test it
- Regularly discuss cybersecurity with your Board and Senior Leadership
- Build relationships and establish lines of communication before the incident (both internal and external)
- Identify workstreams and responsible individuals
  - E.g., communications, contract obligations law enforcement, statutory and contractual notice obligations, SEC disclosure considerations, risk management, regulators.
- Vet outside experts pre-incident and be thoughtful about agreements
- Initial and ongoing due diligence of third-party agreements
  - Service providers
  - Customer and other relationships whether there might be notice obligations
- **WilmerHale Resource**: The Guide to Cyber Investigations


US Regulatory Enforcement
& Litigation Developments

Recent State Attorneys General Settlements

- ***Zoom Video Communications, Inc.***
  - Separate settlements with the NY AG, NY DOE, and FTC
  - Settlement with the NY AG in five weeks
  - Settlement with the FTC in November 2020, with Commissioners Chopra and Slaughter dissenting
- ***Anthem, Inc.***
  - 2014 data breach compromising personal information of 78.8 million customers
  - $39.5 million 43-state settlement, with Connecticut leading (Executive Committee of Illinois, Indiana, Kentucky, Massachusetts, Missouri, and New York assisting), separate settlements with California and HHS OCR

Recent State Attorneys General Settlements

- ***The Home Depot, Inc.***
  - 2014 data breach compromising payment card information of 40 million customers.
  - $17.5 million settlement with 46 states and the District of Columbia
- ***Dunkin' Brands, Inc.***
  - 2015 compromise of online accounts resulting from credential stuffing
  - $650,000 settlement with New York

State Attorneys General – Key Takeaways

- States continue to be the primary enforcers of data security in the absence of federal legislation
- Certain attorneys general continue to be more active players, either playing a leadership role in a multistate or "going it alone"
- Others have developed a particular expertise in certain areas
- Settlements continue to take years of negotiations, but many impose similar requirements related to information security programs, technical security requirements, information security assessments, and ongoing state AG oversight

New York Department of Financial Services

- Oversight of banks, insurance companies, and financial advisors, but increasingly exerting jurisdiction over a wide variety of companies doing business in New York, including at least two social media companies
- Active in enforcing its Cybersecurity Regulation (23 CRR-NY Ch I, Pt. 500)
- First cybersecurity enforcement action taken this year against First American Title Insurance Company
  - Nebraska-based stock insurance company and licensee authorized to write title insurance in New York; no evidence that New York residents had their non-public personal information accessed
  - Nebraska Department of Insurance also investigated and did not take action
- Potential model for new agencies in other states

Litigation Developments

- Consumer, employee, and shareholder class actions continue to pose significant risks for entities that have experienced a data breach
- *In re Capital One Consumer Data Sec. Breach Litig.*, No. 1:19-MD02915 (E.D. Va.)
  - Third-party forensic report found not to be attorney work product
  - Key question: would the report have been created in essentially the same form absent litigation?
  - Carefully consider the effect and structure of any pre-existing relationships with forensics vendors

Litigation Developments

- Continued reliance on common law causes of action in addition to asserting new statutory claims
  - *In Re: Wawa Inc. Data Security Litigation, No. 2:19-cv-06019 (E.D. Pa.)*
- Courts continue to take conflicting approaches to Article III standing issues, though they are generally trending more permissive towards plaintiffs, with some notable exceptions
  - *Blahous v. Sarrell Regional Dental Center for Public Health, Inc., No. 2:19-cv-00798 (N.D. Ala.)*
  - *Hartigan v. Macy's, No. 1:20-cv-10551 (D. Mass.)*

European Union Regulatory Developments

EU Regulatory Developments – Breaches

- EU continues to see lots of data breaches, SolarWinds has also affected EU governments and companies
- Reminder: Under GDPR breach notification requirements, regulators have to be informed more often than affected individuals, multitude of breach notification obligations in addition to GDPR, including EECC/ePD, PSD2
- Many of the larger GDPR-related larger fines are based on non-compliance with Art. 32 GDPR (technical and organizational measures), e.g.
  - British Airways (2020): £20m (original proposal: £183m)
  - Marriott (2020): £18.4m (original proposal: almost £100m)
- First European Data Protection Board dispute resolution decision – in a Twitter data breach matter
  - EDPB statements regarding the amount of the fine
  - EDPB statements regarding notification obligations in the event of a data breach

Other Developments in the EU

- Regulation 2019/881 ("Cybersecurity Act") entered into full force in June 2020
  - Introduction, for the first time, of an EU-wide cybersecurity certification framework for ICT products, services and processes
  - New and permanent mandate for ENISA, the EU Agency for Cybersecurity
- Ongoing activities and discussions regarding security of 5G networks and 5G network providers
  - January 2020: European Commission communication regarding a "toolbox"
  - July 2020: Report of the European Commission regarding the implementation of the toolbox
- The EU has activated Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States
- ENISA Guidelines for Securing the Internet of Things (November 2020)


Anticipated Cybersecurity
Developments in 2021

Anticipated US Cybersecurity Developments in 2021

- Biden/Harris administration will be particularly attuned to cybersecurity
- More federal authority and resources for cybersecurity as a result of the National Defense Authorization Act, including the creation of a National Cyber Director and CISA administrative subpoena power
- Renewed focus by regulators on supply chain cybersecurity risks and vendor due diligence / ongoing oversight
- State legislative initiatives in the absence of federal legislation
- Attorneys general will continue to actively investigate data security incidents, frequently as part of large multistate coalitions. They are increasingly sophisticated about cybersecurity and information security-related issues:
  - Better at identifying information security shortcomings during investigations
  - Will require increasingly specific controls in any settlement agreements, as well as ongoing oversight of information security programs

Anticipated US Cybersecurity Developments in 2021

- Increased oversight by sector specific regulators and shorter notification times
  - NY DFS, California Privacy Protection Agency
  - Proposed Rule: Computer Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers (Treasury, Federal Reserve System, Federal Deposit Insurance Corporation)
  - US Financial Stability Oversight Council recommendations
- Baseline standards for IoT device cybersecurity due to the recent passage of the Internet of Things Cybersecurity Improvement Act

Anticipated EU Cybersecurity Developments in 2021

- Directive (EU) 2020/1828 on representative actions for the protection of the collective interests of consumers
  - "Qualified entities" will have standing to bring lawsuits based on alleged non-compliance with the GDPR
  - Must be implemented in national law by December 25, 2022
- Directive (EU) 2019/771 on certain aspects concerning contracts for the sale of goods
  - Must be implemented by mid-2021, national rules must be applicable from January 2022
  - National law will require that traders ensure that the consumer is informed of and supplied with updates, including security updates, necessary to keep the digital content or digital service in conformity
  - The directive also contains more detailed rules on the obligation to provide updates

Anticipated EU Cybersecurity Developments in 2021

- Updated Dual Use Regulation to be published in the Official Journal
  - Cyber-surveillance goods that allow for the “covert surveillance of natural persons by monitoring, extracting, collecting or analyzing data, including biometrics data” fall under new export restrictions
- Update of European cybersecurity framework
  - EU Cybersecurity Strategy for the Digital Decade
  - Proposal for an update of the 2016 NIS Directive ("NIS2")
  - Proposal for a Directive on the resilience of critical entities
- Ongoing discussions regarding encryption of electronic communications and lawful access

Contact

Benjamin Powell
Partner; Co-Chair, Cybersecurity and Privacy Practice
WilmerHale
benjamin.powell@wilmerhale.com

Jason Chipman
Partner
WilmerHale
jason.chipman@wilmerhale.com

Dr. Martin Braun
Partner; Co-Chair, Big Data Practice
WilmerHale
martin.braun@wilmerhale.com

Arianna Evers
Counsel
WilmerHale
arianna.evers@wilmerhale.com

WilmerHale Privacy and Cybersecurity Law Blog

Twitter: @WHCyberPrivacy

A Review of 2020 Privacy Law Developments and a Look Ahead

Webinar

JANUARY 26, 2021 | 12-1 PM ET

WILMERHALE

REGISTER NOW

Additional Resources