This Webcast Will Begin Shortly

Thank you. We hope you enjoy the webinar.

2019 Cybersecurity and Data Privacy Year in Review

John Rondini
Co-Chair Cybersecurity
jrondini@brookskushman.com

Matt Jakubowski
Co-Chair Cybersecurity
mjakubowski@brookskushman.com

Todd Dishman
Shareholder
tdishman@brookskushman.com

Ben Harel
CIO
bharel@brookskushman.com

Overview

2019 breaches and technology update

- 2019 significant breaches
- Ransomware and beyond
- Emerging security tools & services

FTC update

- Changes to FTC orders
- Review of significant FTC actions

Cyber/Privacy regulatory and framework update

- CCPA Update
- Additional State Privacy Law Update
- IoT law update
- NIST privacy framework and SAE vehicle framework
- Federal legislation update

Cyber Insurance

- Update on changes to cyber insurance coverage
- Recent legal decisions pertaining to insurance coverage

BREACHES AND TECHNOLOGY CHANGES

2019 Major Breaches

Online Betting Sites via Elasticsearch (JAN 2019) – 108 Million Records
Three online betting sites copied data to Elasticsearch cloud storage without securing it. No password or authentication of any kind was needed to access or download unsecured data including names, addresses, phone numbers, email addresses, birth dates, usernames, account balances, IP addresses, browser and OS details, games played, and win and loss information.

Facebook (APR 2019) – 540 Million Records
Two different third-party apps holding Facebook datasets were left exposed to the public online via unprotected servers. Account names, Facebook ID, passwords, and user activity and more were exposed.

Orvibo (JUL 2019) – 2 Billion Records
Database of smart home IoT devices, exposed personal information of private individuals and businesses with Orvibo smart devices. The data breach affected users worldwide, including users in China, Japan, Thailand, US, UK, Mexico, France, Australia and Brazil.

2019 Major Breaches

Zynga (SEPT 2019) - 218 Million Records
Hackers claimed to access a database that included data from Android and iOS players, including names, email addresses, login IDs, hashed passwords, phone numbers, Facebook IDs and Zynga account IDs. Players of the popular games Draw Something, Words With Friends, and Farmville were exposed.

Disney+ (**NOV 2019) - TBD Users**
Users of Disney+ streaming services were locked out of accounts. Disney+ members' login credentials, including usernames and passwords, were found for sale on the Dark Web starting at $3 per record.

TrueDialog (DEC 2019) – 1 Billion Records
Hosted by Microsoft Azure and run on the Oracle Marketing Cloud in the USA, included 604 GB of data. This included nearly 1 billion entries of highly sensitive data.

Ransomware and Beyond

Over 948 government agencies, educational establishments and health-care providers where subjected to some form of ransomware attack in 2019

- Some surveys show losses for businesses can average $2,500 per incident, with some approaching $1 million
- *Ryuk* demands $288,000 per incident, compared to around $10,000 demanded by other ransomware
- Nearly 40 percent of victims paid the ransom

City of Baltimore (MAY 2019) – Ransomware infected city computer system affecting the city government for over a month. Estimates put recovery cost over $18 million, although malware attacker only demanded $76,000 worth of Bitcoin

City of New Orleans (JAN 2020) - Ransomware attack cost the city over $7 million. Cybersecurity insurance policy provided $3 million—which may indicate the city was still underinsured.

**Often attacked parties find their files remain encrypted after payment of the ransom!!*

Ransomware and Beyond

Cloud Misconfiguration Attacks

- Successful cloud attack vectors occurred due to misconfiguration, where a human error created a vulnerability.
- Rapid introduction of new tools within cloud platforms has led to a lack of maturity in security vetting and procedures

Rise of Deepfakes (*Top item from McAfee Labs 2020 Threat Predictions Report*)

- Social engineering's role in cyberattacks will continue to rise
- Broader availability of deepfake tools will enable less-skilled threat actors to generate campaigns

Voicemail Phishing ("Vishing") Voice impersonation schemes to increase

- Attacks lure email recipients into opening an attachment purporting to be a voicemail message to play the message but instead links to phishing URLs
- (Sept 2019) Attackers used commercially available AI software to create a voice impersonating UK energy company senior executive. Recipient was instructed to transfer $243,000 to a Hungarian supplier

Emerging Security Tools & Services

Cyber Deception Tools Go Mainstream

- Creates attack decoys and honeypots within your environment
- Lure attackers with fake breadcrumbs to catch threats
- Completely automated solutions removing the burden of scale and configuration
- Deception is no longer limited to network assets but now extends to identity access management solutions

Managed Security Service Providers (MSSPs) Are Now Platforms

- A new “breed” of MSSPs are emerging. Building their own security platform for collaboration and detection.
- The hybrid security operations approach is now a valid use-case
- Keep your in-house security teams and ship out the low-value activity’s

User Behavior Analytics (UBA) Build Behavioral Patterns Of Users

- Collects various types of user data such as permissions, data access, patterns of work, location, sessions, and expertise to build a profile of usage
- Reports anomalies defined as risky based on the potential impact
- UBA can integrate directly with identity management systems to challenge users

Emerging Security Tools & Services

Zero-Trust Networks Are Production Ready

- Provides network access to users only to the systems they need to complete their tasks.
- Dynamically provisions access to network systems based on logical operators and conditions
- Microsegments all endpoints including IOT devices
- Move away from the traditional castle-and-moat approach to network security, assume no trust for devices and end-users

Breach & Attack Simulations (BAS) Software Emerges

- Continuously simulate attack vectors based on MITRE ATT&CK™ matrix that dynamically updates over-time
- Provide insight into the effectiveness of existing's tools or hidden attack vectors without a full attack exercise
- Run APT style attacks simulations safely without a Red Team or danger to your environment
- Lets Red Teams focus on high-value activities within an engagement

CHANGES WITH FTC OVERSIGHT IN 2019

FTC's "New and Improved" Orders

LabMD, Inc. v. FTC

891 F.3d 1286 (11th Cir. 2018) (2018)

- FTC alleged LabMD failed to implement "basic" data security practices
- FTC held that this failure resulted in the personal information of LabMD clients being disclosed
- LabMD challenged the FTC's authority to regulate the data security practices of private companies
- The 11th Circuit held that the FTC's order mandating a complete overhaul of the LabMD's data-security program was unenforceable

Changes to FTC 2019 Orders

- **More specificity** – require implementation of comprehensive, process-based data security program and require implementation of specific safeguards
- **Increased third-party assessor accountability** - orders clearly and specifically require assessors to identify evidence to support their conclusions, including independent sampling, employee interviews, and document review
- **Elevation of data security considerations to the C-Suite and Board level** - companies must now present their Board or similar governing body with their written information security program

ClixSense

FTC Allegations

- ClixSense deceived consumers by falsely claiming it "utilized the latest security and encryption techniques to ensure the security" of customer information
- ClixSense stored personal information in clear text with no encryption
- ClixSense did not implement readily available measures to limit access between computers on ClixSense's network
- ClixSense failed to change default login and password credentials for third-party company network resources

2019 Order

- ClixSense must implement a comprehensive information security program and **obtain independent biennial assessments** of this program
- ClixSense is prohibited from making misrepresentations to the third party performing the biennial assessments of any information security program
- ClixSense must provide an **annual certification of compliance** to the Commission

DealerBuilt

FTC Allegations

- DealerBuilt's dealer-management system software and data processing services collects personal information about dealership consumers
- A DealerBuilt employee connected a storage device to the company's backup network without ensuring that it was securely configured
- Failed to perform vulnerability scanning, penetration testing, or other measures that would have detected the improperly connected storage device
- Failed to develop and implement a written security policy and training for employees

2019 Order

- DealerBuilt prohibited from transferring, selling, sharing, collecting, maintaining, or storing personal information unless it implements and maintains a comprehensive information security program
- Requires the company to obtain **biennial third-party assessments** of its information security program
- **Senior corporate manager** must take responsibility for overseeing DealerBuilt's information security program to certify compliance with FTC order

Facebook

FTC Allegations

- Facebook repeatedly used deceptive disclosures and settings to undermine users' privacy preferences in violation of its 2012 FTC order
- Facebook did not take adequate steps to deal with apps that it knew were violating its platform policies
- Cambridge Analytica obtained information for millions of Facebook users. Data was purchased and user was able to collect information about users that had not consented to allowing their data to be provided

2019 Settlement

- Facebook fined **$5 Billion** for violating 2012 FTC order
- Facebook must conduct privacy review of every new product or service it develops
- Privacy reviews must be submitted to the CEO **and** a third party assessor every quarter

REGULATORY AND FRAMEWORK UPDATES

CCPA Key Dates

	Description	Date
Operative	Date that the law became "operative." CCPA, § 1798.198(a)	January 1, 2020
Private Right of Action	Date that individuals can bring suit for an alleged violation of the data security provisions. CCPA, § 1798.150(a)(1)	January 1, 2020
A.G. Discretionary Regulations	Date by which the Attorney General can adopt additional regulations on other topics that may "further the purposes" of the CCPA	No deadline
A.G. Mandatory Regulations	Attorney General must "adopt" regulations on mandatory topics. CCPA, § 1798.185(a)(1)-(7)	On or before July 1, 2020
A.G. Enforcement Actions	Date by which the Attorney General can bring an enforcement action under the CCPA. CCPA, § 1798.185(c)	July 1, 2020 (unless final regulations are published

Attorney General CCPA Regulations

1st draft released October 2019

2nd draft released February 2020

Interesting points included in revised regulations:

- Opt-out provisions need to be easy for consumers to execute with minimal number of steps
- Opt-out notices and privacy policies must be reasonably accessible by consumers with disabilities
- Businesses cannot require consumer to pay fee for verification when consumer requests to opt-out or have information deleted
- Privacy policy must be presented in format that is easily readable and understandable by consumer. Cannot include “technical” or “legal jargon”

Barnes v. Hanna Andersson

Class Action Filed Feb 3, 2020; ***1st Private Action Suit Based on CCPA***

Complaint alleges that the Defendants violated California's Unfair Competition Law (Cal. Bus. and Prof. Code §17200) based on unlawful actions that **were in violation of the CCPA**

Complaint alleges Plaintiffs engaged in unlawful business practices by:

- Failing to establish reasonable security practices and procedures to adequately protect and store California resident's personally identifiable information ("PII") in violation of the CCPA
- Failing to disclose the data breach to the affected California residents in a timely and accurate manner also in violation of the CCPA

Damage award could range between $1,000,000 and $7,500,000

Additional States Enacting Stricter Data Privacy Laws

	Consumer Rights									Controller Obligations						
	Access to collected data	Access to be shared data	Correction of data obtained	Deletion of data on request	Right to restrict sale of data	Portability of personal info	Opt-Out or Opt-In	Right against automated decision making	Private Right of Action	Age-Based Opt-in	Notice/Transparency Requirement	Data Breach Notification	Risk Assessment	Non-discrimination	Processing Limitation	Fiduciary Responsibility
California (January 1, 2020)	X	X		X		X	X		X	16	X			X		
Maine (July 1, 2020)					X		X				X			X		
Nevada (October 1, 2019)							X				X	X				
Hawaii	X	X		X		X	X			16	X	X		X		
Massachusetts	X	X		X		X	X		X	18	X			X		
New York	X	X	X	X	X	X	X	X	X		X	X			X	X
Rhode Island	X	X		X		X	X		X	16	X			X		
Washington	X	X	X	X	X	X	X	X			X	X	X			

IoT Regulatory Updates

California: SB-327 (In effect Jan 1, 2020)

- IoT device manufactures must equip devices ***with "reasonable security" features*** to prevent unauthorized access, modification, or data exposure
- Passwords must either be unique to IoT device or force new user password during initial setup. (***prevents guessing of default PW***)

Oregon: Bill 2395 (In effect Jan 1, 2020)

- Mimics Cal. "reasonable security" requirement
- Narrower → Only for devices "used primarily for ***personal, family, or household purposes***"
- Adds ***private right of action***

*Illinois, Kentucky, Massachusetts, Maryland, New York, Rhode Island, Vermont and Virginia all considered IoT legislation in 2019

GDPR Fines Ramped Up In 2019

2018: 1 fine; €400,000 **2019**: 27 fines; € 428,545,407 Total

Date	Offender	Fine Amount	Occurrence
Jan 2020	TIM Group (Italy)	**€ 27,800,000**	Promotional phone calls to opted-out users
Dec 2019	1&1 Telecom (Germany)	**€ 9,550,000**	PII made publicly available to anyone who provided name and data of birth of a customer
Oct 2019	Deutsche Wohnen (Germany)	**€ 14,500,000**	Unlawful storage of PII in archive without option to delete old data
Oct 2019	Austrian Post (Austria)	**€ 18,000,000**	Sold detailed personal profiles of ~3 million users to various companies and political parties
Jul 2019	Marriott (UK)	**€ 123,000,000**	Reservation database hacked impacting 30 million EU residents - Ongoing hack 2014-2018
Jul 2019	British Airways (UK)	**€ 204,600,000**	Website attack compromised ~500k customer records
Jan 2019	Google Inc. (France)	**€ 50,000,000**	Auto-creation of Google account during configuration of mobile phone

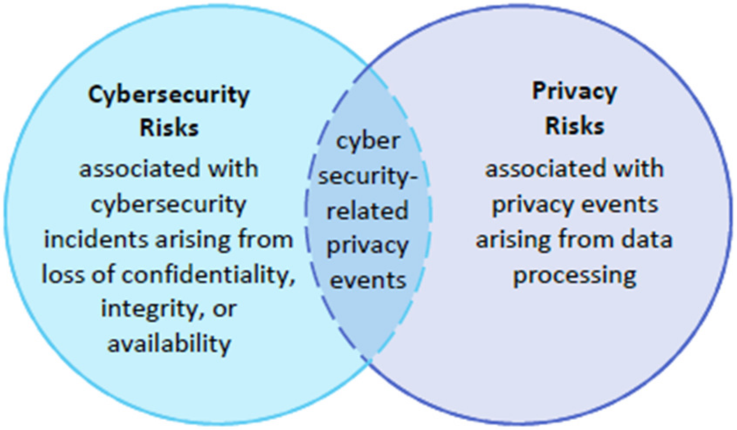
Sources: https://alpin.io/blog/gdpr-fines-list/ https://www.enforcementtracker.com/

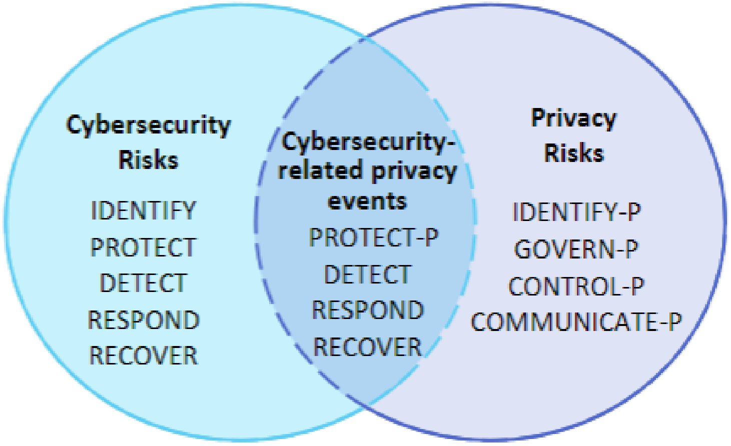
NIST Introduced New Privacy Framework

- Framework is intended to manage privacy since risks can arise by incidents unrelated to cybersecurity

- Privacy framework is meant to be flexible to:
  1. the size and complexity of the organization
  2. scope and nature of data processing activities
  3. volume and sensitivity of the consumer data

- FTC and FBI provided comments about the importance of NIST’s work to create a new U.S. privacy framework

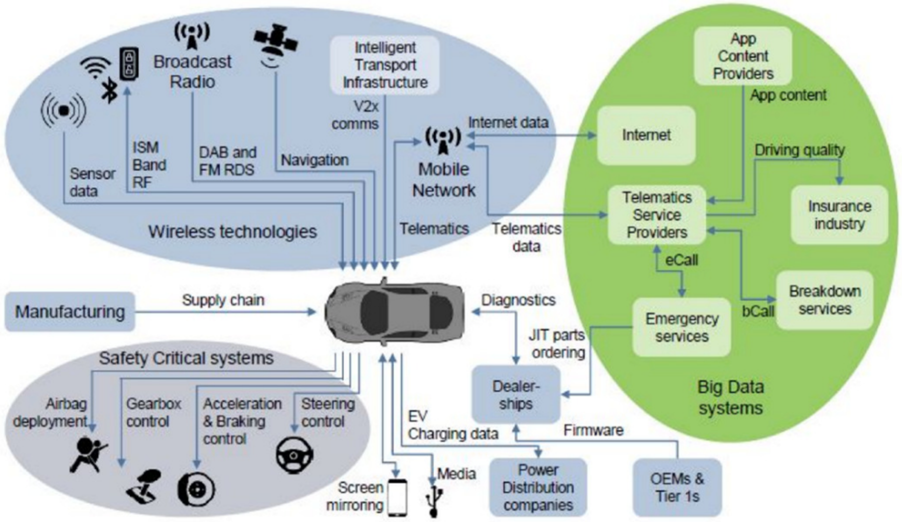

Cybersecurity Risks
associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability
cyber security-related privacy events
Privacy Risks
associated with privacy events arising from data processing



NIST Privacy Framework V 1.0, January 16, 2020

Automotive Cybersecurity Frameworks

- **SAE J3061 (2016)** – **Cybersecurity Guidebook** for Vehicle Systems
  - Corollary of NIST standard
  - Applies to Safety Systems
  - Addresses PII



Scott J. McCormick1, Elaina Farnsworth, *Secure Connected Vehicle Architecture for Software and Telecommunications, Aug 2019*

- **SAE J3101 (2020)** – **Hardware-Protected Security**: 4 Main Focus Areas
  - **Secure Boot** - validate HW and SW components (root trust)
  - **HW Security** – detect tampering w/ boot loaders & critical OS files
  - **Network Security** – OTA message authentication; verify approved sources
  - **Cloud Security** – secures authenticated channels to the cloud

- **ISO/SAE 21434 (FEB 2020)** – Road Vehicle Cybersecurity
  - Draft joint international standard

Federal Privacy Law Update

- **Republican Bill** – "United States Consumer Data Privacy Act"
  - ➢ Covers "information [or device] that identifies or is linked or reasonably linkable to an individual"
  - ➢ Includes rights for access, correction, deletion and portability of consumer data
  - ➢ Grant's enforcement authority to FTC
  - ➢ FTC to approve certification programs

- **Democratic Bill** – "Consumer Online Privacy Rights Act"
  - ➢ Covers "information that identifies, or is linked or reasonably linkable to an individual or a consumer device, including derived data"
  - ➢ Includes rights for access, deletion and correction, and the right to data security
  - ➢ Bill requires the FTC **AND** NIST publish guidance for covered entities on how to provide effective data security and privacy training

- Key issues being debated:
  1. Private Right of action – Democratic bill includes and Republican bill omits
  2. Preemption of State Law - Democratic bill would allow state laws to prevail, but the Republican bill would preempt them
  3. Enforcement – Discussing how to strengthen FTC authority to enforce. Discussing whether state attorney generals should also have authority to enforce.

CYBER-INSURANCE

Cyber Insurance Policies Changing Rapidly

- Cyber insurance premiums rising 5% to 25% annually
  - ➢ Increases have been driven by ransomware losses
  - ➢ Experts blame insurance companies for paying the ransom

- Coverages evolving and expanding to cover regulatory risk, reputational damage, forensic accounting and gap exposures
  - ➢ Carriers are adjusting ransomware coverage to limit or exclude coverage for ransomware attacks
  - ➢ Insurance carriers are vetting customers and charging customers with lax cybersecurity practices and processes higher premiums
  - ➢ Carriers adjusting policies to reflect new laws (e.g., GDPR, CCPA)

“Silent” Cyber Coverage

- Non-affirmative, or Non-Cyberspecific coverage may not cover claims for Cyber Events
  - **War exclusions** in traditional policies may preclude losses from individual foreign national hacker attacks – Insurance provider consider them to be acting on “behalf” of their foreign state
  - Failure to comply with "industry standards" on security
- New and emerging Cyberrisks remain in a gray area for Traditional Policies
  - **Traditional Policy Underwriters** may not accurately assess risk (and price) – leading to later claim disputes
  - **Cyber Policy Underwriters**
- Companies switching from endorsement to standalone policies
  - Avoid gaps
  - Create more comprehensive coverage

“Silent” Cyber Coverage Disputes

- *Landry v. Insurance Co. of the Penns.,* 18-cv-02679 (S.D. Tex. May 2019)
  - Landry owns Bubba Gump Shrimp, Rainforest Café and Joe's Crab Shack
  - Hackers spent two years in Landry's system looking at credit card information
  - Paymentech (JP Morgan's payment processing arm) sued Landry for the bank's post-breach assessments conducted by Visa and Mastercard
  - Landry sued its insurance company for reimbursement under CGL policy
  - Claim denied because express language of policy does not cover losses
  - *Court*: (1) **No “oral or written publication”** of customer material (i.e., data was just hacked); and (2) **no “privacy” damages** because Landry was being sued for breach of contract by Paymentech – not by consumers whose data was hacked

---

- *National Ink & Stitch, LLC v. State Auto Property & Casualty Insurance Co*., No. 18-cv-2138 (D. Md. Jan 2020)
  - State Auto denied NIS claim the on ground that ransomware cyber-attack and computer systems damage was not a “**direct *physical loss* of or damage to**” covered property
  - Policy expressly defined “covered property” to include “electronic media and records (including software)”
  - *Court*: Claims recoverable under the Policy based on either (1) loss of data and software, **OR** (2) loss of functionality of computer system itself