Florida Bar Consumer Protection Law Committee Cyberside Chat

CYBER ATTACKS
Hope for the Best, Prepare for the Worst

October 5, 2021

Presented by:

Alicia Dietzen, General Counsel, KnowBe4, Inc. – CIPP/E
Aaron Tantleff, Partner, Foley & Lardner LLP – CIPP/E
Lecio DePaula Jr., Director of Data Protection, KnowBe4, Inc. - CISSP, FIP, CIPM, CIPP/US, CIPP/C, CIPP/E
Colin Murphy, Security Liaison and CIO, KnowBe4, Inc. - CISSP, CEH

Alicia Dietzen,

General Counsel
KnowBe4, Inc.

- General Counsel of KnowBe4, Inc., a publicly traded security awareness training and simulated phishing company
- Experience with privacy, security and technology transactions
- Member of Association of Corporate Counsel's Women's Committee
- 2019 Tampa Bay Business Journal Top Corporate Counsel Award Honoree and a 2018 finalist
- Association of Corporate Counsel 2021 Top 30-Somethings
- Business Observer's 2021 40 Under 40
- IAPP, CIPP-E

Aaron Tantleff,

Partner
Foley & Lardner, LLP

- Privacy, Security & Information Management & Technology Transactions & Outsourcing
- Represents companies in technology, AI, IoT, data analytics, privacy, security, cyberattacks, incident response, and intellectual property related matters, both domestically and in the EU
- Served as both in-house and outside counsel, including as the global director of IP for a global software company and as acting AGC for a global information technology and management consulting company.

Colin Murphy,

CIO
KnowBe4, Inc.

- Chief Information Officer for KnowBe4
- Over 13 years of executive experience in security and software development
- Experience working in heavily regulated industries (Private Equity/Financial, Energy deregulation)
- Actively involved in penetration testing
- Expertise in OSINT methodologies, web applications Testing, cloud security, enterprise networking
- CISSP and CEH certified
- Cybersecurity evangelist for KnowBe4

Lecio De Paula,

VP of Data Protection
KnowBe4, Inc.

- VP of Data Protection for KnowBe4
- Experience with practical privacy compliance with GDPR, PDPA, CCPA, etc,
- CISSP and FIP certified
- 5+ years if information security and privacy experience
- Privacy Evangelist for KnowBe4

***Disclaimer**: The opinions expressed are solely the opinions of each presenter and do not express the views or opinions of their respective employers. This presentation is intended for educational purposes only and do not replace independent professional judgement nor should it be relied upon as legal or professional advice.*

Key Takeaways

- An understanding of the evolving nature of cyber-attacks and latest trends
- An updated framework for responding to and mitigating damages caused by attacks
- An understanding of how to establish a “reasonable efforts” worthy compliance program
- An overview of recent legislation

Presentation Overview

- Recent high profile attacks
- Simulated phishing attack
- Mitigation of risks and liability
- Security awareness best practices
- Current legal landscape
- Q&A

Recent High Profile Attacks

Types of Attacks

- Ransomware and extortion
  - Zero-Day/Failure to patch
  - Social engineering
- Phishing
  - SMS/Vishing
  - Spearphishing
- Credential attacks
  - “Stuffing” & “Spraying”
- Supply Chain Attacks
- Mobile
- IoT (Internet of Things)

Solarwinds Supply Chain Attack

Attack Summary

- Nation-state APT-initiated
- Active by March 2020
- Publicly revealed Dec. 13, 2020
  - Earlier related attack revealed on Dec. 8th by FireEye
- Compromised Solarwinds ORION software, which allowed a Remote Access Tool (RAT) to be placed in the software build process

Lessons Learned

- When customers downloaded Solarwinds update and ran it, it installed RAT in their environment
- Impacted at least 30K environments, including many security companies, government agencies, etc.

Microsoft Exchange Zero Day Attack

Attack Summary

- Discovered/reported to MS on Jan. 5th
- Publicly announced and patch delivered March 2nd
- 7 new MS-Exchange zero-days (4 actively exploited)
- Affected MS-Exchange 2010 and later
- Allowed complete control over server and could be used as a base of attack for rest of environment
- 100,000’s companies impacted
- Nation-state attack at first, followed by dozens of new APT groups

Lessons Learned

- Nation-State/APT attacks not scared to do brazen, widespread 0-day attacks
- Monitoring for new files and executables for detection was key
- Patch took 2 months to deliver publicly (ready on Feb. 12th)
- Once patch was released, other hackers took advantage of it

Verkada

Attack Summary

- Super admin credentials posted online with no MFA
- Customers allegedly impacted – Schools, gyms, prisons, hospitals, homes, banks (TSLA, Cloudflare)
- Hacktivist group APT-69420
- God Mode - lack of in-house security controls
- Cameras with root access, could execute code
- Some cameras had facial recognition – privacy concerns

Lessons Learned

- MFA should be enabled
- Password hygiene
- Closer monitoring of published leaks
- Audit/technical controls only work if enforced
- SaaS managed IOT devices create unique attack surface
- Isolate IOT devices on the network
- Controversial services attract Hacktivists
- Simple hack – complex repercussions

Third Party Risk and Attack Surface

Why is this important?

- Organizations are more vulnerable than ever due to sheer amount of applications managed by the organization
- The average mid-size organization leverages 1k+ third parties
- Presents an almost infinite number of third, fourth, fifth party risk

How are third parties vulnerable?

- Poor security + privacy programs
- Misconfigurations
- Lack of audit
- Poor management of apps across the organization
- Lack of resources amongst IT and information security teams to adequately managed third party apps
- Third parties generally face the same issues that your organization does across IT and information security.

Examples

- Marriott 2020 Breach - Employee Credentials exposed and leveraged to siphon 5MM+ records
- Quest Diagnostics 2019 - 11.9MM patients - due to billings collection vendor
- FBI 2019 - 3TB records relating to investigations exposed by third party

Risk Reduction Considerations

- Protecting against risks as the vendor
  - Importance of assessing ability to comply with customer terms
  - Ensuring customer has sufficient obligations in the contract
  - When not to budge on risk allocation
  - How to get ahead of the vendor questionnaires
    - Build out security on website
    - CAIQ
    - FAQs
- Protecting against vendor risk as the customer(the contract and beyond)
  - Dealing with historical contracts and the importance of reviewing and refreshing terms routinely
  - Great contract, insufficient vetting/auditing of vendor
    - Utilizing third parties for vetting and threat intelligence
    - What to ask for?
      - SOC 2
      - ISO 27001 certifications
      - Security questionnaires/CAIQ
  - Common contractual considerations
- Reporting requirements/notification obligations
- Supply chain risks
- How to think about forensics during the aftermath of a breach

Walkthrough of a Phishing Attack

1. Step by step on how one is crafted, from finding the target, recon, choosing the attack surface,and the aftermath.
2. Review how the evolution of attacks impact incident response programs and updated approaches for responding to and investigating phishing attacks, including, investigating the Dark Web databases, marketplace, and information trade.

Selecting the target and reconnaissance

- Identify users/staff at the organization
  - CV's, LinkedIn, Leaked information, company website
  - Examples 1, 2
- Evaluate attack surface through public resources
  - OSINT - Public data brokers, breach searches, DNS
    - Data discovered - plaintext passwords, DOB, name, phone, address, other domains, additional staff
    - Continuous refinement by running discovered data through OSINT
    - Technical research of target firm: email provider, dns records, security services
  - Examples 3, 4, 5, 6, 7

Crafting the attack/delivery

- Weaponize discovered data
  - Technical services (Outlook)
  - Personalized (use known technical details or contacts)
  - Credential spray
- Preparing the attack
  - Almost indistinguishable from realsite
  - MITM attack bypasses multifactor
  - Example 1, 2, 3, 4
- Payload types
  - Theft of credentials/session
  - Access to VPN or other resources

Hacker Supply Chain

- Understanding the Motive
  - Exfiltrate data to sell (breaches)
  - Ransomware, cryptomining, botnet
  - RDP, Business email compromise
  - Examples 1, 2, 3, 4
- Improving our visibility and culture
  - Services for external monitoring: DARKINT, OSINT, Breach management
    - Easier to manage known attack surfaces
  - Access monitoring, AI/anomaly detection
    - Push to cloud has made it harder to detect attacks
    - Centralize point of entry for resources (VPN)
  - Security Awareness Training

Checking the Right Boxes

How to mitigate your risks and decrease damage potential

“Reasonable Efforts?”

What is a reasonable effort?

- Using “reasonable measures” to assess and mitigate risks; and
  - Organizations are required to create and maintain their own “reasonable measures” and “fact-based analysis” to assess and mitigate risks
- Making “reasonable efforts” to manage vendors.
  - Obligation for “reasonable efforts” to manage vendors
  - Vendor management
  - Due diligence on the vendor’s cybersecurity systems and policies
  - Review vendor agreement, policies
  - Allocation of Liability
  - Dispute resolution

Key Aspects of a “Reasonable” Compliance Program

- Policies/Programs
  - Incident Response Plans
  - Information Security Policy
  - Privacy Policies/Notices (and the importance of action behind the paper)
  - Acceptable Use Policies
- Testing and Training
  - Security Awareness
- Data protection
- Frequent testing/auditing
- Vendor management program (quantitative approach, active monitoring, active vulnerabilities etc)
- FAIR model (Factor Analysis of Information Risks)

Common Subpoena Requests

- Security program
- Policies/training
- audits/investigations conducted
- Messages (emails, chats, texts, etc)
- Prior incidents
- Privilege and confidentiality issues

Common Subpoena Requests Sent to Security Vendors:

- Any and all communications and documentation with client regarding services to be provided related to preventing unauthorized exfiltration of PII/PHI
- The actual usage of the products and services as well as pricing and documentation to share participation including activity logs
- Documentation showing any other security protections in place
- Any and all communications related to termination of use of the vendor services
- All written reports related to security of client
- Any documents related to audits, assessments, or investigations
- Any knowledge of unauthorized access of clients systems or discussions around data breaches

The Dangers of a Lackluster Privacy and Security Program

- Data Leaks
- Loss of customer confidence (especially apparent in B2B companies where there will be compliance department scrutiny from customers)
- Regulatory Fines
- Poor user behavior
- Lack of visibility into your environment

U.S. Consumer Privacy Legislation – 2021 Trends

– – –

- 29 comprehensive consumer data privacy bills were introduced
- 2 bills passed (Virginia's and Colorado's)
- 2 bills stalled after introduction (one being Ohio's, which could still move).
- 22 bills got stuck in committee
- 3 bills died in cross-committee

Legislation that Passed in 2021

- Colorado
  - Colorado Privacy Act (CPA) (effective 7/1/2023). Provides comprehensive privacy protections for consumers including access, correction, deletion, and opt-out rights. Requires companies to provide clear and meaningful privacy notices, specify purpose(s) of processing, minimize data collection, obtain consent for processing of sensitive data, and conduct risk assessments in certain situations (among other things). Regulates dark patterns, targeted advertising, and profiling. Enforced by the AG and district attorneys. Includes no private right of action. Regulated businesses will have an opportunity to cure violations for 60 days, but only until 2025.
- Virginia
  - Virginia Consumer Data Protection Act (VCDPA) (effective 1/1/2023). Provides comprehensive privacy protections for consumers including access, correction, deletion, and opt-out rights. Requires companies to provide clear and meaningful privacy notices, specify purpose(s) of processing, minimize data collection, obtain consent for processing of sensitive data, and conduct risk assessments in certain situations (among other things). Regulates targeted advertising and profiling. Exempts non-profits from the law's purview. Enforced by the AG. Includes no private right of action. Regulated businesses will have an opportunity to cure violations for 30 days.

Legislation that's Active in 2021

- Illinois
  - HB2404, the Right to Know Act. Requires companies to disclose information sharing practices and have data protection safety plans. Includes a private right of action. *Re-referred to Rules 3/27/21.*
  - HB3910, Consumer Privacy Act, a modified version of the CCPA. Consumer right to request what info has been collected, request deletion of personal info collected, and right to opt-out of the sale of their personal information. Permits business to provide financial incentives to consumers authorizing sale of info. Includes a private right of action. *Re-referred to Rules 3/27/21.*
- North Carolina
  - SB 569, the Consumer Privacy Act of North Carolina. Provides comprehensive privacy protections for consumers including information, access, correction, deletion, and opt-out rights. Requires companies to implement administrative, technical, and physical data security practices; conduct annual risk assessments; and provide clear and meaningful privacy notices. Enforced by the AG, but also includes a private right of action. *Referred to Senate Rules and Operations Committee after first reading 4/7/21*.
- Massachusetts
  - S. 46 (SD 1726), Massachusetts Information Privacy Act. Establishes general data protection principles and duties for companies, including a duty of care, duty of loyalty, and duty of confidentiality. Short form privacy notice must have a 600-word limit, be tailored to an 8th grade reading level, and include data retention limits, the names of third parties that received the personal information, as well as a log showing when such disclosures happened. Companies must read the notice out loud (if it is communicated verbally to consumers). Requires handwritten consent for processing biometric information. Includes a full private right of action and minimum and maximum fines. *Referred to the Joint Committee on Advanced Information, the Internet, and Cybersecurity with House concurrence 3/29/21*.

Legislation that's Active in 2021 (continued)

- Ohio
  - HB 376, Ohio Personal Privacy Act. Most closely resembles the VCDPA. Requires companies to conspicuously post an accessible privacy policy including specified information. Provides companies with 30 days to cure noticed violations and an affirmative defense against certain alleged violations if it complies with the National Institute of Standards and Technology (NIST) Privacy Framework. Does not include a private right of action. *Referred to the House Committee on Government Oversight 9/16/21*.
- Pennsylvania
  - HB 1126, the Consumer Data Privacy Act, modified version of the CCPA. Applies to professional and employment-related information. Grants consumers information, access, deletion, and opt-out rights. Requires companies to notify consumers of any sale of personal information to a third party and provide an opportunity to opt out. Prohibits the sale of personal information of minors younger than 16 without consent. Includes a private right of action similar to that provided under the CCPA.

Legislation scheduled for review in 2022

- Oklahoma
  - HB 2969, Oklahoma Computer Data Privacy Act of 2022. Requires businesses to “apprise” consumers of their right to opt out of personalized advertising. Provides consumers the right to deletion, right to know/access, right to data portability, right to correct inaccurate information, and right not to be discriminated against for exercising their rights. Businesses that disclose personal information to service providers must enter into contracts that require service providers to adhere to the bill’s restrictions. Mandates specific content requirements for privacy notices similar to those required by the CCPA and CPRA. Enforceable by the AG only. No private right of action included. *Pre-filed for 2022 Legislative Session (opens Feb. 7, 2022)*

Legislation the Died in 2021

- Alabama
  - HB216, Alabama Consumer Privacy Act, similar to CCPA with broader application. Limited private right of action. *Session ended 5/17/21 without action*.
- Alaska
  - SB 116 and HB 159, similar to CCPA with notable differences. *Session ended 5/19/21 without action*.
- Arizona
  - HB 2865, similar to CCPA but enforced by AG only. Sale requires monetary consideration. *Session ended 4/24/21 without action.*
- Connecticut
  - Raised SB 893, similar to VCDPA. AG has exclusive authority to enforce. Includes no private right of action. *Session ended 6/9/21 without action*.
- Florida
  - SB1734, the Florida Privacy Protection Act, is a modified version of the CCPA. *Session ended 4/30/21 without action.*
  - HB969, the Florida Information Privacy Act, is a modified version of the CCPA. *Session ended 4/30/21 without action.*
- Kentucky
  - HB408, similar to CCPA but enforced by AG only. No right to delete data. *Session ended 3/30 without action*
- Maryland
  - SB 930, Maryland Online Consumer Protection Act, modified CCPA. AG enforcement. *Session ended 4/12/21 without action*.
- Minnesota
  - HF 36 and HF 1492 / SF 1408, Minnesota Consumer Data Privacy Act. *Died following failure to pass the Minnesota House Commerce Finance and Policy Committee 6/14/21*.
- Mississippi
  - SB 2612, Mississippi Consumer Data Privacy Act, effectively the CCPA. *Died in Committee on 2/2/21.*

Legislation that Died in 2021 (continued)

- North Dakota
  - HB1330, obtain opt-in consent before selling personal information and authorized class action lawsuits. *House voted against the bill 75-19.*
- New York
  - S.6701/A.680A, New York Privacy Act. Provided comprehensive consumer privacy rights. Required companies to, among other things, (i) obtain express opt-in consent before personal data is processed; (ii) develop, implement, and maintain reasonable safeguards to protect personal data; and (iii) conduct annual risk assessments. Included a private right of action. *Session ended 6/10 without action*.
- Oklahoma
  - HB1602, the Oklahoma Consumer Data Privacy Act, was a modified version of the CCPA. Included a right to opt-in for data sales instead of opt-out like CCPA. Consumer right to request what info has been collected, request deletion of personal info collected. Original bill included private right of action but amended to be enforced just by the AG. *Session ended 5/28/21 without action*.
  - HB1125, amended the Oklahoma Consumer Protection Act, to prohibit false or misleading statements regarding the use of personal information. *Session ended 5/28/21 without action*.
- Rhode Island
  - HB 5959, the Rhode Island Transparency and Privacy Protection Act seeks to help the consumer identify information collected by online service providers and commercial websites and which is then shared or sold to third parties and to properly protect their privacy, personal safety, and financial security, by outlining information sharing practices, requiring for transparency in the way consumer data is collected, among other things. Enforceable by the AG. *Session ended 6/30/21 without action*.

Legislation that Died in 2021 (continued)

- Texas
  - HB 3741, the Data Privacy Omnibus, shared similarities with the CCPA and CPRA. Enforced by AG. No private right of action. *Session ended 5/31/21 without action*.
- Utah
  - SB 200, the Utah Consumer Privacy Act, was similar to the VCDPA. *Failed 3rd reading in the Senate*
- Washington
  - SB 5062, the Washington Privacy Act, proposed to give consumers the right to access, correct, delete, and opt-out of data for targeted advertising and sales. Required companies to issue a privacy notice and maintain reasonable security. Included no private right of action and AG had enforcement authority. Amended to include a limited private right of action that would provide consumers injunctive relief. *The House failed to advance a bill before the Washington legislative session ended 4/25/21*.
  - HB 1433, the Peoples Privacy Act, was a competing data privacy bill supported by the ACLU and included a private right of action. *Session ended 4/25/21 without action*.
- West Virginia
  - HB 3159, similar to CCPA (less business friendly) would have protected consumer data by providing a right to opt-out of the sale or sharing of personal information, the right to request a copy of the personal data collected twice a year, and the ability to request deletion or correction of certain personal information. Enforceable by the AG. Limited private right of action. *Session ended 4/10/21 without action*.
- Vermont
  - H 160 (one-paragraph bill) proposed to adopt consumer privacy protections and give Vermont residents control over their personal information, and "to adopt other protections as provided in the California Consumer Privacy Act." *The bill failed to advance prior to the end of the Vermont legislative session on May 28*.

Questions