NORTON ROSE FULBRIGHT

Life After Breach

Alexis Wilpon

April 6, 2023

Norton Rose Fulbright US LLP

Cybersecurity Background – Why it Matters

Is Cybersecurity a Risk that General Counsels Have a Role in Managing?

- Survey says…..
  - A 2022 ACC survey revealed that on a scale of 1-10, CLO's ranked Cybersecurity, on average, as the issue with highest level of importance to their business

Cybersecurity and Data Protection

Cyber Incident

Examples:
- Ransomware
- Phishing
- Malware and Viruses
- Employee Errors
- Insider Threats
- Business Email Compromises

Global 2021 Statistics

The average cyber attack cost **$8.6 million.**
Cost of a Data Breach Report 2021 | IBM

Most **common initial attack vector** was compromised credentials, resulting in **20%** of all breaches.
Cost of a Data Breach Report 2021 | IBM

Over **4,000 ransomware attacks per day**.
26 Cyber Security Statistics, Facts & Trends in 2022 (cloudwards.net)

32% of victims paid a ransom demand but only got **65% of their data back**.
Ransomware Statistics, Trends and Facts for 2022 and Beyond (cloudwards.net)

Likely Consequences of a Cyber Attack

Business Impact
- Disruption of business operations
- Remediation costs
- Legal costs and penalties
- Management shakeup
- Reputational harm (employees, insureds, brokers)
- Loss of business

Legal Implications
- Notification laws and disclosure obligations
- Government investigations/enforcement actions
- Law enforcement
- Private litigation and class actions
- Legal action against perpetrators and related parties
- Contractual obligations

NRF

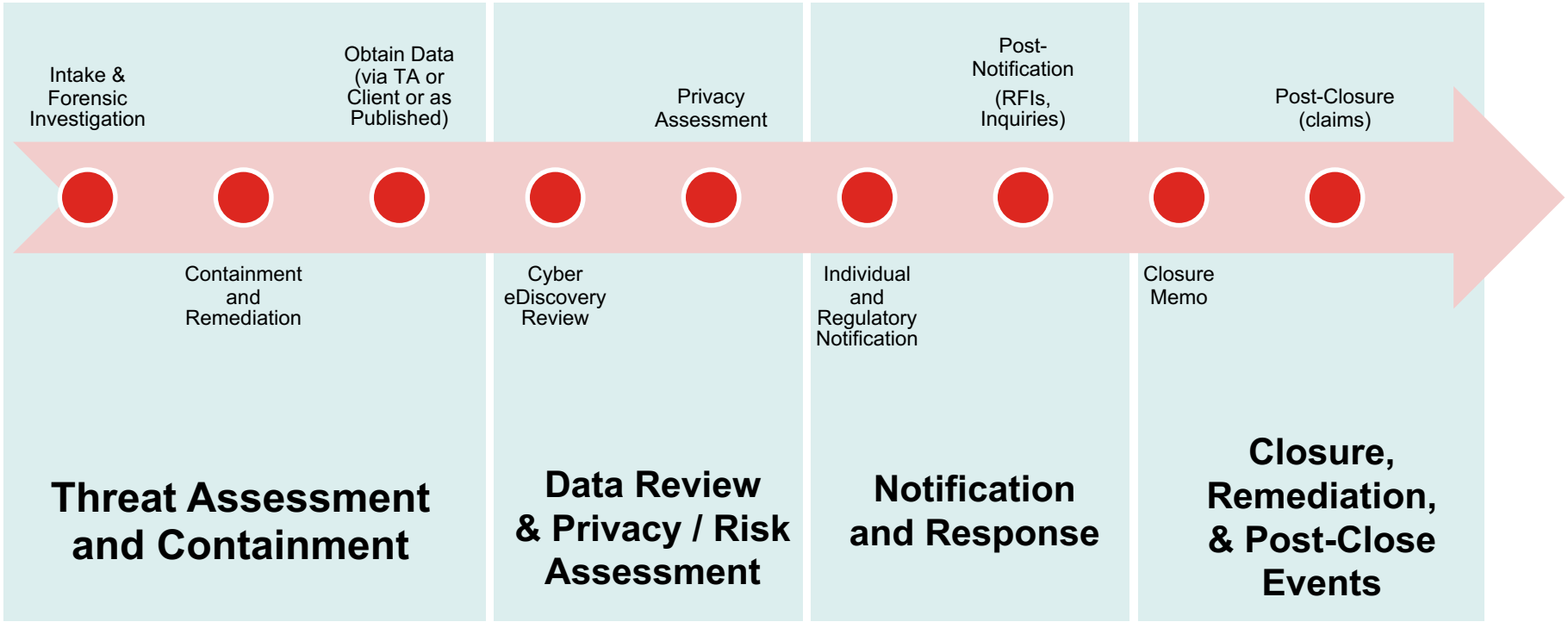
Common Types of Incidents

Ransomware	Extortion without Ransomware	Business Email Compromise	Software Compromise	ge,	Supply Chain Compromise	[illegible]
• Malicious software designed to block access to a computer system until a ransom is paid • Data is encrypted and inaccessible until decryption key is received • Data theft may also occur	• Large amount of data is stolen, but not encrypted • TA promises not to publish the data if ransom is paid	• TA gains access from compromised credentials (e.g., after a user clicks on a phishing email) • Credential harvesters may be hidden inside a phishing email that appears to come from an employee, client, vendor, or other third party • BECs are extremely common and often difficult to prevent, but luckily do not usually have significant operational impacts. • Significant data may be implicated if company does not have an email disposition program	• Cli ent ’s thir d- par ty sof tw	• Internal bad actor or nation state actor steals critical data	• Su ppl y ch ain co mp ro mi	• Adversarial third-party detecting, exploiting, and making-public a hardware vulnerability on a company product

Most common incidents

NRF

Timeline of a Cyber Incident Response



How has the Threat Landscape Evolved

- Ransomware and disruptive malware attacks
  - Ransomware combined with exfiltration and publication of data; strains and modules evolving
  - Growing in prevalence, with the malware attacks often aimed at causing operational disruption in key industry sectors – including an increase in attacks on critical infrastructure
  - Malware-as-a-service – in addition to RaaS, threat actors employed independent services to negotiate payments, assist victims with making payments and arbitrate payment disputes between themselves and other criminals
  - Increased pressure tactics from Threat Actor to force victim payments (e.g., DDoS attacks, shame sites, direct calls to employees) and increase in re-extortion after payment
  - **Ransomware as Service** – In October 2021, Conti ransomware began selling access to victims' networks, enabling follow on attacks by other cyber threat actors – In April 2022, Black Basta (which some believe is related to Conti), emerged as a new ransomware gang that is one of the most active RaaS groups currently
  - Increased focus on targeting cloud infrastructure, managed services providers, industrial processes and software supply chain
- Nation-state intrusions: growing frequency and severity, often with the aim of carrying out monitoring/ profile building / IP theft / financial gain. Key threat Actor Groups include APT 19, 30, 31, 40, 41 (China) – espionage/monitoring/tracking; APT 39, 35, 34 (Iran) – monitoring/tracking/surveillance; APT 37, 38 (N. Korea) – espionage / destructive / financial gain
- Vendor Incidents: Significant surge in vendor-caused incidents over the past two years, including Accellion, Kronos, and SolarWinds. As organizations utilize more vendors for SaaS, HaaS, IaaS, and entrust sensitive date to them, threat actors are targeting these vendors to maximize impact across a broad swatch of vendor clients.

NRF

Legal and Regulatory Environment

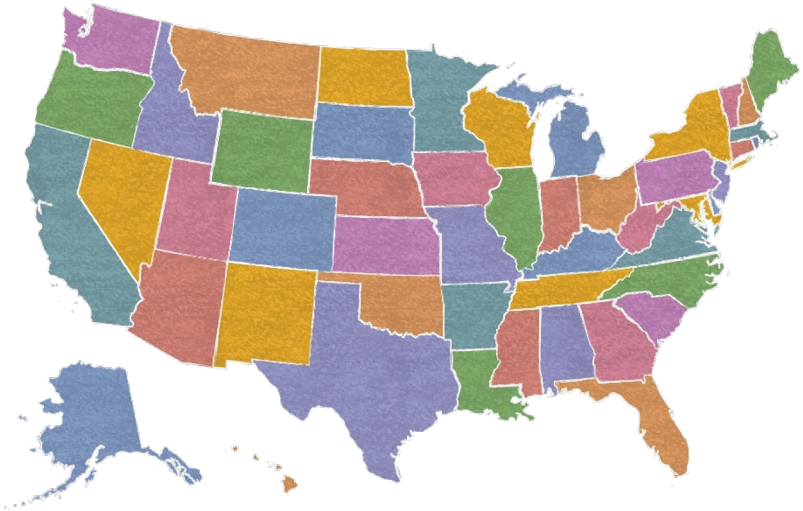
How has the Legal Landscape Evolved

- State Breach Notification Laws and "Reasonable Security" Requirements
  - Frequent amendment to state breach notification laws to expand the scope of “personal information” and impose timing requirements for notification
  - States are moving from general requirement of “reasonable security” to more prescriptive cybersecurity requirements
  - Sector-specific comprehensive privacy laws (e.g., NYDFS Part 500)
- Adoption of Comprehensive Privacy Regulations - GDPR/CCPA
- FTC - Section 5 of the FTC Act: Unfair and Deceptive Trade Practices
  - The FTC has brought enforcement actions for failure to employ “reasonable security measures” to protect consumers’ personal information as unfair business practice.
- FTC Health Breach Notification Rule
  - Broad definition of breach
- Federal Cybersecurity Requirements - HIPAA/GLBA
  - HIPAA/HITECH – establishes administrative, technical, and physical security standards for protection of PHI
  - GLBA - Safeguards Rule: Requires development, implementation and maintenance of written comprehensive information security program.

NRF

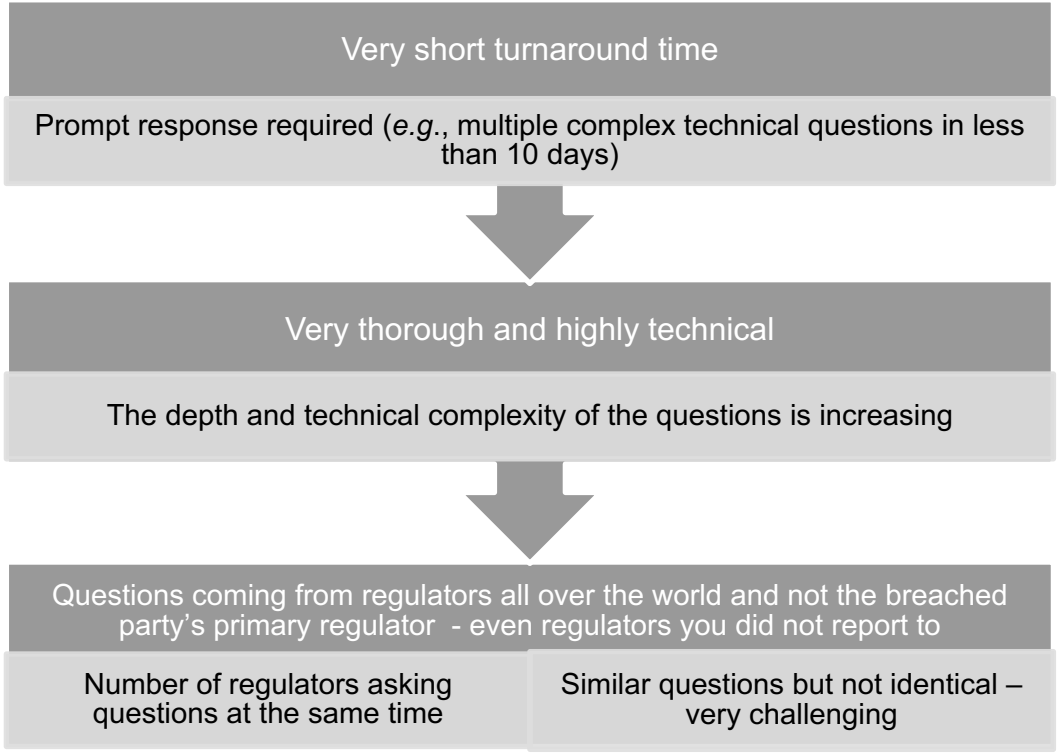
State Breach Notification Laws

- 50 States, D.C., and U.S. territories
- Apply based on residency of individuals whose information may be involved
- Definitions of “Personal Information” vary
  - Social Security number
  - Driver’s license number
  - Financial account number + password
  - Various other data elements may be included
- Exceptions for:
  - Encrypted or redacted data
  - No reasonable risk of harm
- Various requirements for reporting to regulators (Attorneys General)



After you report

Regulator activity – recent trends



Common Questions from Regulators

- Attack Method
- Malware and Evidence
- Timeline/Demographics
- Organizational Structure and Board Decisions
- Specific Systems Targeted
- Remediation
- Impacted Business Operations
- Documents Requested
- Security Controls like VPN or MFA
- Data Retention and Over-retention
- Issues related to Single Factor Authentication
- Credential Evidence and Theft
- Securing and Encrypting Data
- Database, applications, and server access
- Vulnerabilities and Conducted Exercises
- EDR/Firewall/Anti-Virus/Anti-Malware Tools
- Privacy and Security Programs
- Logging Capabilities
- Third-Party Vendors
- Public Concerns

NRF

Current regulator priorities

- Timeliness of notification
- Customer complaints/harm
- Remediation
- Third party vendor management
- Privacy governance – retention, storage/encryption, mapping
- Incident response planning and preparation
- Implementation of “Recognized Security Practices” or Reasonable Security

- Appropriate technical and organisational measures (TOMs)
  - Monitoring and detection
  - Endpoint monitoring and Anti-Virus/Anti-Malware
  - Identity management
  - MFA/SFA
  - Patch and vulnerability management
  - Remote access
  - Asset management

Private Rights of Action

- **California Privacy Rights Act ("CPRA")**
  - Effective January 1, 2023 (amending "CCPA")
  - Private right of action to consumers whose "personal information . . . Is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures . . ." § 1798.150(a)(1)
  - Consumers may seek damages between $100 - $750 *per consumer per incident* or actual damages, whichever is greater
  - Consumers may also seek injunctive or declaratory relief and any other relief the court deems proper
- **Biometric Information Privacy Act ("BIPA")**
  - Illinois statute governing processing of biometrics
  - Provides private right of action for any BIPA violation, with damages of the greater of $1,000 or actual damages (for negligent violations) or $5,000 or actual damages (for intentional or reckless violations)
  - BIPA litigation has seen the largest damages for all privacy-related lawsuits, including a recent award of approximately **$228 million**

NRF

Privilege Best Practices in Incident Response

Do

- Establish a governance structure across workstreams
- Engage outside counsel to retain third-party vendors.
- Mark documents relating to the Incident "Privileged and Confidential" and do not create free access to them.
- Specify which persons may receive privileged information and where work product will be stored (it should be somewhere separate from routinely created documents).

Don't

- Don't speculate in written communications, convey personal opinions, write or communicate in haste or anger or make unwarranted confessions / promises
- Don't assume that all communications with lawyers or other professional advisers will be privileged.
- Don't refer to privileged documents or legal advice in unprivileged documents
- Don't circulate communications widely without first referring to Legal
- Don't produce your own account of sensitive issues or your own notes or summaries of privileged documents

NRF

Takeaways

- Regulators serve an ***auditor function*** (i.e., key is to ensure business has implemented an appropriate information security program)
- Regulators are increasingly active in the cybersecurity space and use breach investigations as an opportunity to review your ENTIRE privacy program
- Priorities for enforcement are:
  - Timeliness of notifications
  - Effective remediation
  - Compliance with notification laws

Ransomware Payment Considerations

Criteria to Consider

Operational Impact
- Scope and criticality of systems involved in outage, if any
- Ability to contain proliferation of ransomware
- # of impacted stores, employees, and customers

Restoration
- Availability of backups
- Cost and time to restore/decrypt/rebuild systems
- Confidence in restoration with decryption key
- Costs of data loss if unable to restore

Scope of Data Impact
- Amount/sensitivity of impacted data
- Risk of misuse of data
- Ability to retrieve data from Threat Actor Repository

Reputational harm
- Media coverage
- Threat actor history of going public or posting sensitive information
- Impact to customer / business partner relationships/goodwill

Payment/Financial
- Amount of ransom
- Ability to pay ransom in cryptocurrency
- Ability of Academy's bank to process and release payment
- Threat actor reputation
- Business losses based on length of outage/loss of data
- Insurance coverage (Business Interruption/Extortion)
- Establishing precedent as payor

Legal Considerations
- Legality of payment (OFAC)
  - Specialty Designated Nationals and Blocked Persons List (SDN List)
  - Affiliation of threat actor with blocked countries
  - FinCEN/SAR requirements
- Breach notification requirements (Individual and Regulatory)
- Public company disclosure obligations (SEC)
- Regulatory risk (e.g., if data is exposed)
- Risk of third-party litigation/claims by impacted population

Counsel's Role in a Cyber Incident

Evolution of Lawyer's Role

- Cybersecurity and Privacy Compliance
- Inform Board of Cybersecurity Risks; ESG
- Public and regulatory communications
- Integrating Cybersecurity into Enterprise Risk Management
- Information Governance
- Third-Party Risk Management / Customer Questionnaires

Board and Executive Oversight of Cybersecurity Risks

- Assessing and Monitoring the Cybersecurity Program
  - Common theme of Boards receiving updates on cybersecurity is the information received isn't insufficient for Boards to truly understand the company's cybersecurity risk posture
  - Need to establish clear expectations on format, frequency and level of detail of cybersecurity-related information
- ESG
- Insurance/Cyberinsurance
- Reviewing budget and headcount decisions
- Board Expertise and Access to Expertise
  - Input from CISO, CIO, General Counsel, Chief Risk Officer
  - Leverage external advisors for perspective on cyber-risk trends and best practices
  - Education opportunities for the Board

NRF

Cyber Readiness

- Establish and update Enterprise and Info Sec Incident Response Plans
- Develop Ransomware Incident Response Playbook / Decision Tree
- Conduct tabletop exercises to build muscle memory and enhance the IRP
- Legal integrated into SOC alerting processes/immediate engagement of counsel
- Mapping the regulatory landscape applicable to the organization
- Oversee Cybersecurity Risk Assessment and Penetration Tests
- Conduct regulatory readiness assessment to better position the organization to quickly and comprehensively respond to requests by regulators in the first few days or weeks of an incident
- Prepare for future regulatory rules imposing short reporting requirements (e.g., proposed SEC Cyber rules for RIAs and Public Companies) and board/executive oversight of cybersecurity program

Law around the world

nortonrosefulbright.com