LINKSQUARES BREACHRX

# Q4 Legal Landscape

October 2023

## Andy Lunsford

CEO, BreachRx

## Robb McCune

VP, IT & Security,
LinkSquares

# Agenda

**01.**

Threats your organization may be facing

**02.**

How legal should work with other teams in the organization for peak security

**03.**

The new rules and regulations you should be aware of

**04.**

How to use technology to improve your cybersecurity posture

**05.**

Q&A

# Cybersecurity risks you're facing and why incident readiness is critical

- Phishing
- Misdirected Emails
- Corporate Account Takeover (CATO)
- Hybrid work environment/ cloud security
- Malware
- Ransomware
- Third-Party Risks
  Supply Chain

# Your role as an in-house legal team - cybersecurity and beyond

- Orchestrating the terms of security within your agreements
- Handling breach incidents effectively
- Overseeing risk management
- Understanding and adhering to regulatory guidelines
- Keeping abreast with the latest rules, regulations, and laws
- Assembling a responsive and capable team
- Doing more with less

# Working with your IT and security team

- Conduct regular audits and reviews
- Implement legal risk policies
- Legal teams should embrace digital transformation to better manage risk
- Don’t create a punitive environment - create a culture where people feel comfortable and empowered to reach out to security or legal team if something happens – (*ex. clicking on a phishing link*)

# Staying up to date on new rules and regulations is crucial

- Legal teams must have a thorough understanding of data privacy laws
  - GDPR in Europe
  - CCPA in California
  - Other relevant regional and international laws

- This allows legal teams to guide their organizations towards ethical and legal data practices, protecting both the organization and client data

- IAPP Tracker

# New SEC Cyber Rules - how it may affect you and your company

- SEC will require public companies to disclose within four days all cybersecurity breaches that are material
- Rules went into effect in September, new notifications required starting December 18, 2023
- Even non-public companies will see impacts from these rules

# Data privacy & client data

- **Securing Client Data:** Legal teams should work with the IT department to ensure all client data is securely stored and protected
- **Data Minimization:** Legal teams should advocate for data minimization, meaning the company only collects and stores the client data that is necessary for its operations
- **Be Proactive:** A proactive approach towards cybersecurity can prevent data breaches and protect client data can help prevent issues in the future

# Quick Tips for Protection

- Regular Software Updates- *critical to managing risk related to exploited vulnerabilities*
- Employee training and awareness programs - *establish a healthy phishing defense and reporting culture*
- Multi-factor Authentication - *critical in defending against credential harvesting attacks*
- Backup critical data regularly and store backups securely and separately- *critical to ransomware attack recovery*
- Data Loss Prevention (DLP) - *prevents sensitive information from leaving the perimeter*

# How to use your legal team's technology to improve your cybersecurity posture

- Identifies specific sections, clauses, and data points in your legal agreements
- Helps measure and report on the types and frequency of incidents and on response efficiency
- Exposes what is and isn't guaranteed in your vendor agreements
- Empowers you to put contractual force behind your security preferences
- The use of technology (contract and incident management) can help you stay on top of all of your data

# Additional Resources

- Webinar: How to Survive a Data Breach (and Avoid Litigation)
- Guide: 4 Things to Get Right When Operationalizing Your Data Privacy Plan
- eBook: 6 Game-Changing Trends Impacting Incident Reporting and How to Keep Up
- BreachRx: CISOs are Overlooking this Critical Aspect of the SEC's New Cybersecurity Guidance

  Track Breach Regulations: free access to BreachRx Cyber Regscout

  Guided Tabletop Exercises: BreachRx Cyber Exercise Overview (will be sent in a follow up email to audience)
- NIST Cybersecurity Framework: The Five Functions
- 2023 Data Breach Investigations Report
- 2023 Cost of a Data Breach Report

LINKSQUARES BREACHRX

# Thank You!

Questions?

# AI - Why your company needs and AI Policy

- **Risk Mitigation:** In-house legal teams can supervise the responsible and ethical use of AI in business, thereby mitigating potential risks
- **Data Management**: Assist teams in digitization and data cleansing processes - ensuring data integrity and reducing the risk of data breaches
- **Legal Compliance**: In-house legal teams can ensure that the use of AI is compliant with existing laws and regulations through the development and implementation of an AI policy
- **Cost Effectiveness**: Ensures its appropriate use, maximizing benefits while minimizing potential risks
- **Future Preparedness:** Equips in-house legal teams to adapt and respond to future changes and challenges, minimizing potential risks

1.