LINKSQUARES BREACHRX

Cybersecurity and Data Privacy 101 for Legal Teams

September 2023

Andy Lunsford

CEO, BreachRx

Mollie MacDougall

Product and Cyber Expert

Jonathan Greenblatt

VP of Legal, LinkSquares

Cody Wamsley

Partner, Sterlington PLLC
Cybersecurity,
Data Privacy and Intellectual Property

Agenda

01.

Statistics

02.

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

03.

How to prep your legal team & what your role as an in-house counsel is

04.

Why contract & incident management tech is your best defense against the dark arts & how to use your contracts (+ technology) to improve your cybersecurity posture

05.

Q&A

*From Verizon 2023 Data Breach Investigations Report

2023*

Data Breach Stats

83% of breaches involved external actors—with the majority being financially motivated.

74% of breaches involved the human element, which includes social engineering attacks, errors or misuse.

50% of all social engineering attacks are pretexting incidents—nearly double last year's total.

Statistics

- 83% of companies have experienced more than one data breach in 2022*
- The cost per breach averaged $4.45 million for those involving just 2,000 to 102,000 records
- Legal leaders name cybersecurity and data protection, regulations including privacy laws, and compliance, as their top priorities for 2023.
- Only 30% of data breach costs are security-related–more than 70% of data breach costs are legal and other related long-tail activities
- The three primary ways in which attackers access an organization are stolen credentials, phishing and exploitation of vulnerabilities.

*IBM Report

What is cybersecurity? What are you actually needing to protect?

- **Cybersecurity**:
  - The practice of protecting computer systems, networks, and data from theft, damage, disruption, and any unauthorized access.

- **Key Components of Cybersecurity:**
  - Information Security
  - Network Security
  - Application Security
  - Endpoint Security
  - Cloud Security
  - Physical Security
  - Identity Management
  - Disaster Recovery & Business Continuity
  - Educational Awareness

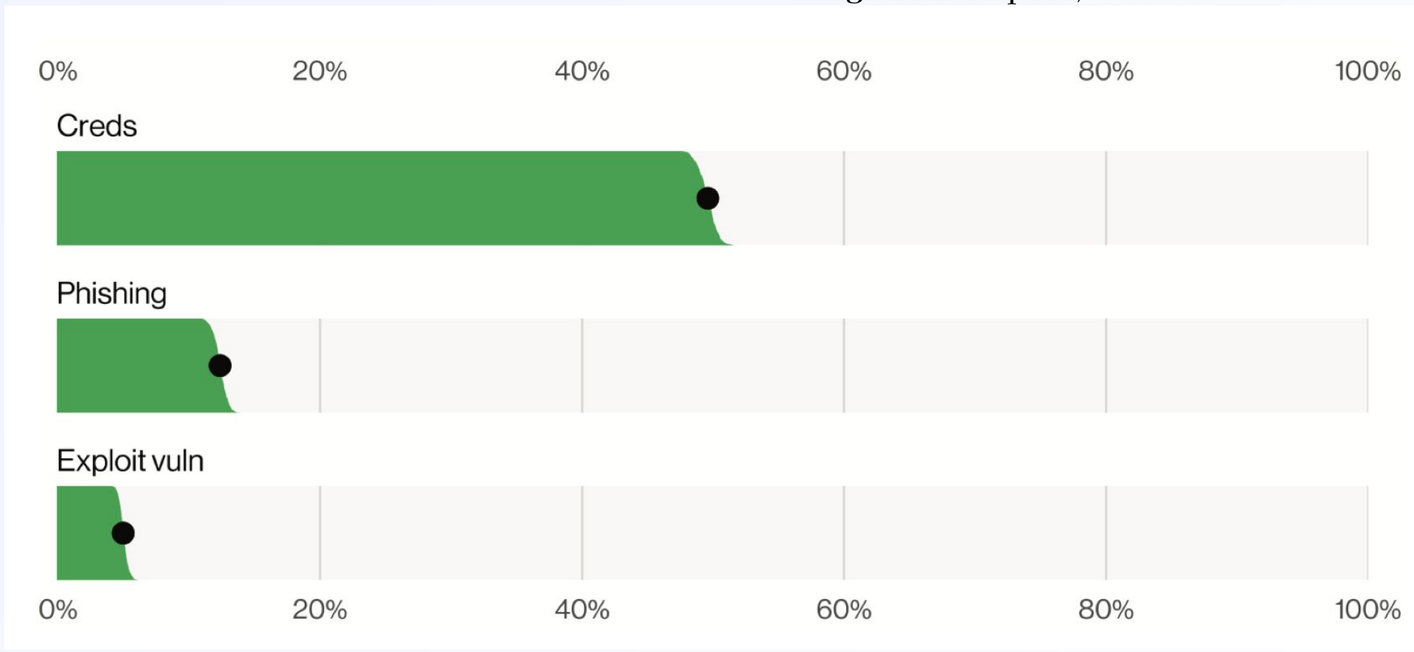
Cybersecurity risks you're facing and why incident readiness is critical

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

Common Attack Vectors

- Phishing (Email, Vishing, Smishing, Social Media)
  - Business Email Compromise (BEC)
  - Credential Harvesting
  - Gain Network Access
- Malware/Ransomware
- Exploit Kits
- Man-in-the-middle Attacks
- DDoS Attacks
- Insider Threat Attacks
- Supply Chain Attacks

Source: 2023 Data Breach Investigations Report, Verizon



Three primary ways attackers access an organization: credentials, phishing, exploited vulnerability

Cybersecurity adversaries you may be facing:

- Nation State Actors/Advanced Persistent Threats (APTs)
  - Typically motivated by espionage, sabotage, or geopolitical leverage
  - Some believed to be financially motivated as well (DPRK, Iran)
- Cybercriminals (ranging from sophisticated to script kiddies)
  - Typically seeking financial gain, via fraud or theft.
  - May steal money directly, or seek sensitive information they can sell.
- Hacktivists
  - Typically pushing a political or social agenda; generally engage in acts of protest, publicity, or damage.
- Insider Threats
  - Employees or others with inside information - often bribed or disgruntled
- Terrorists
  - Seeking to cause fear, physical harm, or disrupt critical infrastructure

Supply Chain Attacks an Increasing Concern

- **NotPetya (2017)**
  - Attack that targeted Ukraine, but spread far beyond Ukrainian organizations
  - Designed to look like Petya ransomware, but could not be decrypted. Wiper disguised as Petya- hence “NotPetya” nomer.
  - Ukrainian Tax Accounting Software (M.E.Doc.) used to deploy malware to thousands of targets
  - Impacted tens of thousands of systems across several sectors (Maersk, FedEx severely impacted)

- **Kaseya Supply Chain Attack (2021)**
  - REvil ransomware gang exploited two vulnerabilities in software from Kaseya to break into 50 managed service providers that used Kaseya products.
  - From there, infected several MSP customers with ransomware
  - Attack paralyzed as many as 1,500 organizations, according to Reuters.

AI & Phishing

WSJ The Wall Street Journal

Generative AI Could Revolutionize Email—for Hackers

Phishing attempts can already be made indistinguishable from legitimate emails, with all red flags eliminated. But some security experts are...

The Guardian

AI chatbots making it harder to spot phishing emails, say experts

Poor spelling and grammar that can help identify fraudulent attacks being rectified by artificial intelligence.

SC Magazine

AI abuse grows beyond phishing to multistage cyberattacks

Abuse of artificial intelligence (AI) by criminals is going beyond polished phishing emails and is on the cusp of driving a wave of...

CNBC

A.I. is helping hackers make better phishing emails

Cyber criminals can do things faster and easier with artificial intelligence, making it more difficult for cybersecurity experts to protect...

Forbes

Almost Human: The Threat Of AI-Powered Phishing Attacks

Artificial Intelligence (AI) is undoubtedly a hot topic, and has been hailed as a game-changer in many fields including cybersecurity.

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*

Questions to Ask Yourself: Cybersecurity Readiness

- What are you protecting? (IP, client data, etc.)
- What is my risk profile?
- How do I compare to others in my industry?
- Which countries do we operate in?
- What processes do we currently have in place in the case of an attack?
- Who is my team of cybersecurity & privacy champions?
- Do you know where to find your cybersecurity obligations?
- What are my cyber insurance & incident reporting requirements?

The Five Functions - Cybersecurity Framework*

What does that mean for legal teams?

When does a legal person come in?

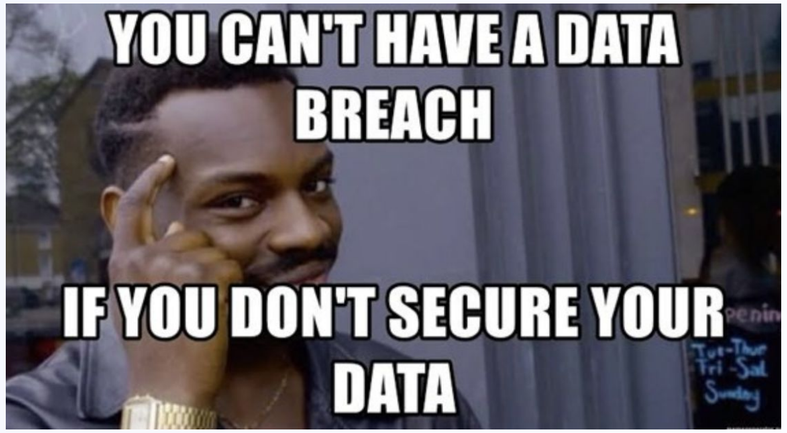
*Info and graphic from NIST

Incident Response Program Maturity Model

Program Maturity	0 - Denial **No incident response plan**	1 - Reactive **Generic incident response template**	2 - Managed **Detailed incident response plans**	3 - Systematic **Routine updating and implementation of IR plans**	4 - Proactive **Dynamically updated IR Program**
Org. Maturity	No full-time privacy or security team	Dedicated team responsibilities	Detailed incident response team + duties	Detailed workflows + annual tabletop	IR team integrated + Regular exercises
Regulation & Contract Maturity	Little to no in-house knowledge of applicable privacy and cybersecurity regulations	Some tracking of regulations + obligations	Active tracking of regulations + obligations	Centralized management of global regulations + contracts	Proactive integration of regulations + contracts into incident response workflows
Tech. Maturity	No system in place	Manual processes + spreadsheets	Spreadsheets + basic ticketing system	Basic system + manual exercises	Automated processes + exercises

Your role as an in-house legal team

- KNOW YOUR BUSINESS
- Negotiating security terms in your contracts
- Responding to breaches
- Managing risk
- Knowing and complying with regulations
- Staying up to date on new rules, laws and regulations
- Creating a team of responders



Managing Risk

- 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*)

Knowing, complying and staying up to date on new rules, laws, and regulations

- 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

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 last week, new notifications required starting December 18, 2023
- Even non-public companies will see impacts from these rules

Data privacy & client data

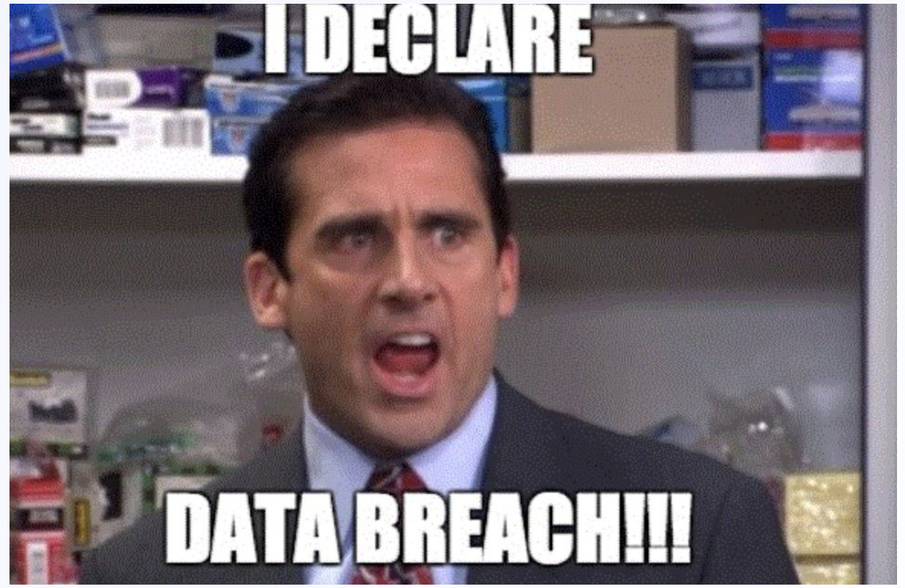
- **Securing Client Data:** Legal teams should work with the IT department to ensure all client data is securely stored and protected

- **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

Responding to breaches

- **Data Breach Response Plan:** Legal teams should help develop a data breach response plan so the company is prepared to respond quickly and effectively if a breach does occur.
- Building a team of responders
- **Technology:** Can help identify specific sections, clauses, and data points in your legal agreements
- Practice exercises



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

Best Practices for Improving Your Cybersecurity

Tips & Tricks

- Raise cybersecurity awareness within your organization
- Protect access to critical information and data
- Build a robust cybersecurity policy and actionable response plan
- Protect access with efficient contract management and incident management tools
- 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*)

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.