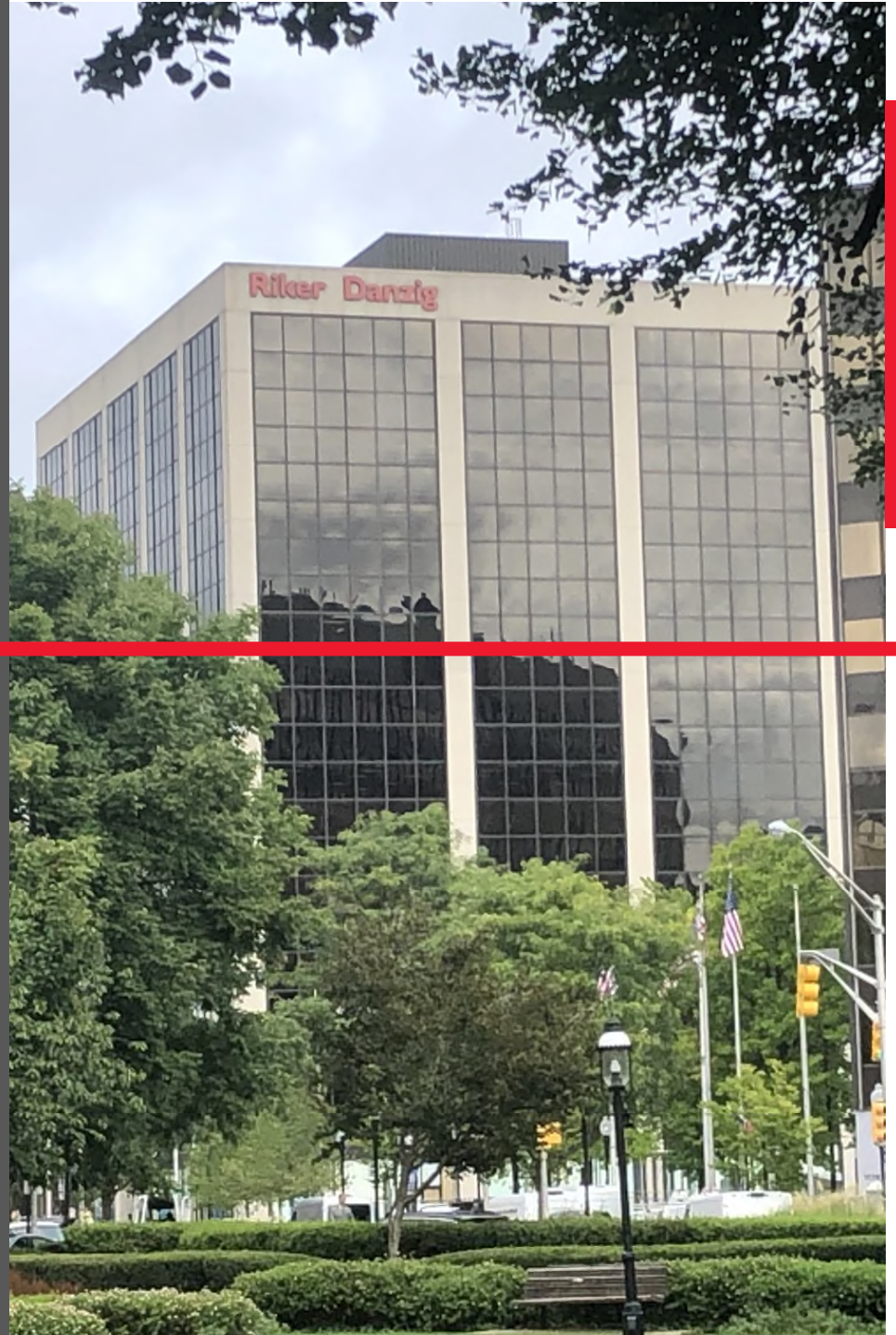
November 16, 2023



Riker Danzig LLP

Current Trends in Cybersecurity and Data Privacy

riker.com

Agenda

Current Trends in Cybersecurity and Data Privacy

1. Why Cybersecurity and Data Privacy Matter
2. Cybersecurity Landscape
3. Data Privacy Landscape
4. Preparing for an Attack/Breach
5. Cyber Insurance
6. Responding to an Attack/Breach
7. Final Thoughts and Questions

Why Cybersecurity and Data Privacy Matter

Why Cybersecurity and Data Privacy Matter

"The single biggest existential threat that's out there, I think, is cyber."

Michael Mullen, ADM, U.S. Navy (Ret.)
Chair of the Joint Chiefs of Staff 2007-2011

Why Cybersecurity and Data Privacy Matter

- **$4.45 million** – The global average cost of a data breach in 2023, a 15% increase over 3 years (Source: 2023 IBM Data Breach Report)
- **2,116 data compromises** – Through Q3, a 17% increase from the 1,802 total compromises tabulated in 2022. (source: Identity Theft Resource Center (ITRC))
- **43** – percent of cyber attacks targeting small businesses (source: Accenture)

Recent High-Profile Cyber Attacks and Data Breaches

- "*U.S. Homeland Security, thousands of businesses scramble after suspected Russian hack*"
  (2020 SolarWinds Attack)

- "*Emergency declaration issued in 17 states and D.C. over fuel pipeline cyberattack*"
  (2021 Colonial Pipeline Attack)

- "*Casino giant MGM expects $100 million hit from hack that led to data breach*"
  (2023 MGM/Caesars Attack)

- "*An entire state's population just had its data stolen by a ransomware group*"
  (2023 MOVEit Global Security Incident)

Riker Danzig

Cybersecurity Landscape

Threat Actors

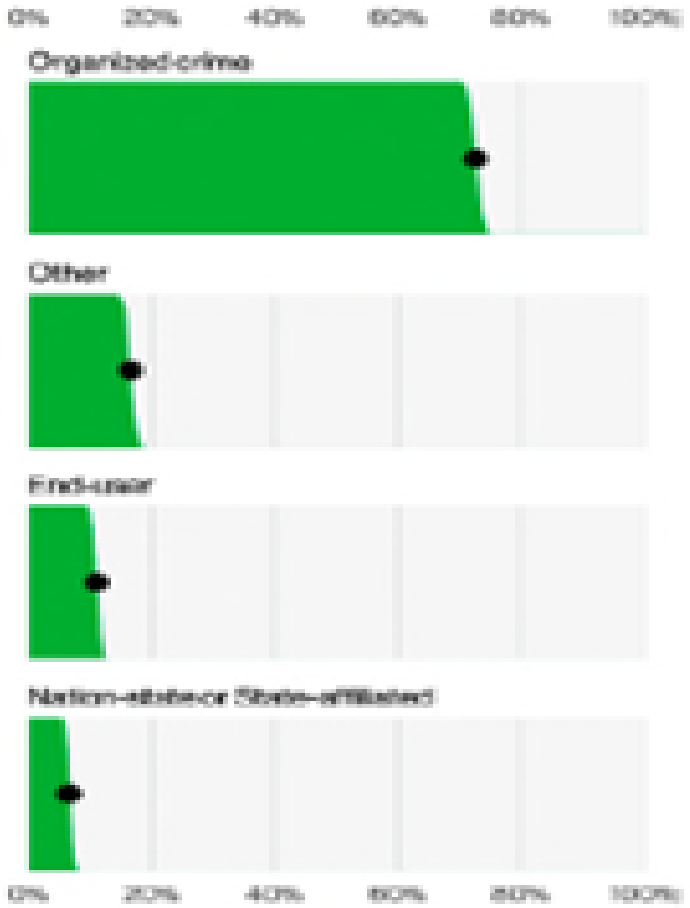


Figure 13. Threat actor Varieties in breaches (n=2,489)

- Advanced Persistent Threats (APT)
- Criminal Syndicates
- Hacktivists
- Insiders/Partners

Source: 2023 Verizon Data Breach Investigations Report

Types of Incidents

- Ransomware
- Social Engineering - Pretexting/Phishing
- Physical Loss
- Stolen Credentials
- Privilege Abuse
- Vulnerabilities Exploits
- DoS/DDoS
- Backdoor/C&C
- Misdelivery
- Misdirected Payments

Regulation of Data Security

- Regulations and Regulators
  - FTC
  - CISA (DHS)
  - SEC – Cyber Disclosure Rule
  - Sector Specific – e.g., HIPAA Security Rule
  - State Regulations
- Cybersecurity Standards
  - NIST Cybersecurity Framework
  - ISO Standards
  - SOC 2 (AICPA)
  - Reasonableness Standard

FTC Authority to Regulate Companies' Data Security

- FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015)

- LABMD, Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2018)

SEC Cyber Disclosure Rule (2023)

- Requires registered companies to provide disclosures concerning their risk management, strategy, and governance relating to cybersecurity risk in their annual reports.
- Also mandates disclosure of material cybersecurity incidents that must include information about the nature, scope, and timing of an incident and its impact or reasonably likely impact on the company.
- The disclosure must generally be made within four days of the time that the company determines an incident to be material unless a determination is made by the United States Attorney General that immediate disclosure would pose a substantial risk to national security or public safety.

23 NYCRR 500: The New York Cyber Regulation

- Applies to covered entities regulated by DFS - insurance companies, producers, agents and brokers, banks, investment companies, credit unions, mortgage brokers and lenders, and other financial institutions
- Requirements
  - Establish and maintain a cybersecurity program
  - Implement a cybersecurity policy
  - Designate a chief information security officer (CISO)
  - Conduct penetration testing, vulnerability assessments, and periodic risk assessments
  - And more
- November 1, 2023 Amendments to Cybersecurity Regulation

New Jersey

- New Jersey Consumer Fraud Act
- New Jersey Computer Related Offenses Act
- New Jersey Identity Theft Protection Act

Riker Danzig

Data Privacy Landscape

Privacy Concepts

- PII/PHI/SPI
- Privacy Policy
- Privacy Notice
- Data Controller
- Data Processor

Data Privacy Legal Landscape

- GDPR (EU)
- Federal Patchwork
  - FTC Act
  - SOX/SEC Regulations (public companies)
  - HIPAA (healthcare)
  - GLBA (financial)
  - FCRA (consumer report)
  - COPPA (children)
  - Others: ECPA (electronic communications), VPPA (video rental privacy*), Telecommunications Act of 1996 (CPNI), GINA (genetic information), FERPA (education), DPPA (MVC information), Cable Communications Policy Act of 1984 …
- State Laws
  - Comprehensive Data Privacy Laws (e.g., CCPA/CPRA)
  - State UDAP laws
  - Illinois BIPA
  - California Delete Act
- Common Law – Tort/Negligence
- American Data Privacy and Protection Act, H.R. 8152 (Introduced 2022)

Data Breach Notification Laws

- State Laws

- Federal Level
  - Personal Data Notification and Protection Act (PDNPA) (proposed 2015)
  - Patchwork
    - Sector specific – e.g., HIPAA
    - FTC Safeguards Breach Notification Rule (Adopted Oct. 2023)
    - Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)

CCPA/CPRA: A Case Study

- **Individuals Rights Under CCPA/CPRA**
  - Right to know
  - Right to access/disclosure
  - Right to opt-out of sale or sharing
  - Right to correct
  - Right to limit use and disclosure of sensitive personal information
  - Right to delete
  - Right to non-discrimination
- **California Privacy Protection Agency (CPPA)**

California Delete Act (2023)

- Under CCPA, California residents can request deletion of data but have to make individual requests to each business.
- The Delete Act provides for the establishment of an online deletion mechanism by January 1, 2026 to permit consumers to submit a single deletion request.
- Deletion requests apply to all "data brokers," defined as businesses that knowingly collect and sell to third parties the personal information of California residents with whom the consumer does not have a direct relationship (excepting certain regulated entities).

New Jersey Disclosure and Accountability Transparency Act (Pending)

- Would establish Office of Data Protection and Responsible Use in the New Jersey Division of Consumer Affairs
- Requires, among other things:
  - Data subject rights for consumers;
  - Affirmative consent for the processing of personal information; and
  - Transparency in the processing of personal information;
- Regulates automated decision-making processing; and
- Establishes rules regarding securing consumer personal data.

Riker Danzig

Preparing for an Attack/Breach

Steps to Prepare

- Comprehensive Written Information Security Program (WISP)
- Incident Response Plan
- Cyber Vendors and Professionals
- Insurance

Written Information Security Program

- **Assign Responsibility**
- **Identify information assets to be protected**
  - Both under company control and outsourced
- **Conduct periodic risk assessment**
  - Identify and evaluate threats, vulnerabilities, and damages
  - Considers available options
  - Include suppliers and trading partners
- **Select and implement appropriate security controls**
  - That are responsive to the risk assessment
  - That address the required categories of security measures
- **Regularly monitor and test the controls**
  - To ensure they actually work
  - To ensure they are effective
- **Continually review, reassess and adjust the program**
  - To address new threats, vulnerabilities and available options
- **Address third parties**
  - Outsource providers/cloud providers
  - Third parties with access.

Incident Response Plan

- Identify Roles and Responsibilities;
- Assemble IR Team;
- Develop authority to call an incident and when;
- Develop and document IR policies;
- Define Communication guidelines and procedures;
- Review and test the plan, train and retrain the team;
- Assess your threat detection capability; and
- Interaction with Law Enforcement

Cyber Vendors and Professionals

- Internal security resources
- External incident response professionals
- Forensics vendor
- Counsel
- Insurance
- Crisis Management/PR

Practice Tips

- Tips to address cybersecurity risks within your company:
  - **Utilize the expertise of your staff;**
  - **Understand the risks facing your company;**
  - **Consider what data you collect and really need;**
  - **Consider updating your Terms of Use/Privacy Policy;**
  - **Ask your vendors about their data practices/review contracts with them;**
  - **Evaluate the coverages identified today;**
  - **Review the language of your coverages;**
  - **Consider engaging a cyber broker; and**
  - **Enact a plan to handle cyber events.**

Riker Danzig

Cyber Insurance

Cyber Insurance

- Standalone cyber policies
- Traditional lines of coverage ("silent cyber") and exclusions
- Both first-party and third-party coverages

Standalone Cyber Policies: First-Party Coverage

- Cyber Extortion

  Provides coverage for ransomware damages. Usually requires the insurer's written consent before payment is covered.

- Business Interruption

  Provides coverage for business disruption due to cyber event with reimbursement for lost income and extra expenses.

- Data Asset Loss

  Provides coverage resulting from loss of data, including costs to recover data that might be maintained in a backup.

- Breach and Notification

  Provides coverage for investigating data breaches, issuing notifications, providing credit monitoring, and covering costs relating to regulatory response.

- Funds Transfer Fraud

  Provides coverage when a cyber criminal accesses a computer network and then uses such access to fraudulently transfer or otherwise obtain money.

Standalone Cyber Policies: Third-Party Coverage

Information Security Liability

- Provides coverage for claims against the insured based on security breaches.

Privacy Liability

- Provides coverage for claims against the insured based on compromised information or violations of federal and state law.

Content Liability

- Provides coverage for claims relating to the substance of data maintained or transmitted by the insured.

Riker Danzig

Responding to an Attack/Breach

Implementing the Incident Response Plan

- Have a fully developed, up-to-date incident response plan;
- Select internal incident response team;
- Alert external parties who may need to be involved;
- Conduct a forensic investigation with internal incident response team and external parties;
- Address any disclosure obligations; and
- Plan for problems.

Managing a Forensic Investigation

- Select and retain outside counsel ahead of time;
- Working with counsel, select and retain your forensic team ahead of time;
- Know what documentation you want developed;
- Consider requirements for handling, storing, transferring forensic data;
- Understand rules for preserving privilege and attorney work product;
- Manage communications; and
- Consider involvement of other third parties.

Working with Law Enforcement

- Weighing the risks and benefits
- May not have all of the information about the investigation
- Can help in obtaining information from providers/third parties
- Can result in delayed notification
- Identifying who to contact (local, state, federal)
- International cooperation
- Expected in some contexts

Breach Disclosure Timing Considerations

- Laws vary & can extend to international jurisdictions;
- Can involve required disclosures to consumers, employees, regulators, law enforcement, investors, media, and others;
- Communications capabilities need to be in place;
- Investigation may be ongoing/incomplete;
- Cyber coverage considerations;
- Disclosure can trigger lawsuits, regulatory investigations, legislative hearings; and
- Risks of notifying too soon or saying the wrong thing.

Preparing for Notification

- Consider notice issues before an incident happens;
  - Data inventory and data mapping;
  - Know what notice obligations the data you collect may trigger;
- Be prepared to comply with varying requirements for form, content, timing, etc.;
- Consider developing notice templates;
- Have roster of points of contact, including insurance; and
- Notify with an eye toward litigation.

Managing the Regulators and Lawsuits

- Regulatory investigations, demands for information;
- Consumer class-action litigation;
- Shareholder actions;
- Managing discovery and preserving privilege.

Conduct a Lessons Learned Review

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

NIST SP 800-61 Rev. 2

Other Post-Incident Activity

- Create a report
- Organize and utilize incident data
- Collect and retain evidence

Riker Danzig

The Future of Cybersecurity and Data Privacy

Final Thoughts and Questions

- Artificial Intelligence (AI) … the Next Frontier
- Questions?

For questions or more information, please contact:

Michael P. O'Mullan - momullan@riker.com

Robert P. Vacchiano - rvacchiano@riker.com

Attorney Biographies

Riker Danzig LLP

E: momullan@riker.com

PARTNER

Michael P. O'Mullan

Practice Areas

Commercial Litigation and Class Action Practices
Cyber Security & Data Privacy
Financial Services and Loan Workout
Insurance and Reinsurance Law
Products Liability, Toxic Tort and Mass Tort
Securities Litigation, Arbitration, Regulation and Investigations

Education:

Fordham University School of Law, J.D. cum laude, 1996
Rutgers University, B.S., magna cum laude, 1993

Michael P. O'Mullan is a partner in the Firm's Cyber Security & Data Privacy Group and Commercial Litigation Group, where he helps clients navigate a wide range of complex cybersecurity, data privacy, business and commercial disputes

Mike advises businesses, business owners, corporate officers and directors, and others in a wide variety of business disputes, including those involving data privacy and cyber breaches. Mike concentrates his litigation practice on business and commercial disputes, including data privacy and cyber security matters, financial services and securities litigation, products liability actions, insurance matters, and consumer claims. He often collaborates with attorneys in other practice areas within the Firm and acts as New Jersey counsel for out-of-state attorneys and their clients.

Mike also represents business, insurance companies, reinsurance companies and related parties in claims investigations, insurance coverage matters and litigation involving a wide range of matters, including claim investigations and coverage matters arising from cyber losses.

He is a frequent speaker on civil discovery matters and cybersecurity issues including before the NJ ACC and has also been quoted numerous times on cyber breaches and liability issues.

Mike has attained the Certified Information Privacy Professional/U.S. (CIPP/US) designation from the International Association of Privacy Professionals (IAPP).

E: rvacchiano@riker.com

Robert P. Vacchiano

Practice Areas

Cyber Security & Data Privacy
Insurance & Reinsurance
Professional Liability Defense

Education:

Fordham University School of Law, J.D., *magna cum laude*, 2011
George Washington University, B.A., *cum laude*, 2008

Robert P. Vacchiano is an attorney in the Firm's Cyber Security & Data Privacy Group and Insurance and Reinsurance Group.

As a member of the Firm's Cyber Security and Data Privacy Group, Robert provides advice and representation on legal issues presented by cyberattacks, ransomware, data breaches, errors in electronic fund transfers, and other privacy and security related matters.

Robert has attained the Certified Information Privacy Professional/U.S. (CIPP/US) designation from the International Association of Privacy Professionals (IAPP). IAPP certifications are considered the global industry standard in the field of data privacy and security, and the CIPP/US certification reflects a demonstrated understanding of the patchwork of federal, state, and local laws governing private-sector information privacy obligations in the United States.

Robert also serves as a member of the Firm's Insurance and Reinsurance Group representing insurers, reinsurers, retrocessionaires, and intermediaries in a broad range of complex insurance matters. Robert has more than a decade of experience litigating in this area and has authored articles on cyber liability and cyber insurance.

Robert also has significant experience handling a wide variety of commercial litigation and professional liability matters. In addition to his work as a litigator, Robert helps counsel businesses large and small on a range of matters, including contracts, technology licensing arrangements, employment issues, data privacy obligations, and intellectual property matters.

We Are Riker Danzig

Our proven track record is highlighted by our numerous awards and accolades, including 2022 "Powerhouse Law Firm" by *Law360* and 2022 "Litigation Department of the Year" by the *NJ Law Journal*. We are proud that *Best Lawyers*, *U.S. News - Best Lawyers* "Best Law Firms," *Chambers USA Guide*, and other highly-regarded legal sources consistently single out Riker Danzig's practice groups and attorneys with distinction. Our proud history with luminaries in the legal community serves as the foundation of our current experienced and vibrant partnership, poised to meet the most complex challenges faced by our clients.

Riker Danzig has a long history of commitment to diversity and inclusion in the workplace. We are proud of our heritage as a leader in promoting women and people of color, including some who broke traditional leadership barriers within law firms, and others who built on their foundation at Riker to break new ground in the courts and government, including most recently: our Firm Co-Chair who is the **First** female in a Top 20 New Jersey-based law firm in the senior role; Riker Of Counsel who is the **First** African-American appointed as a Judge to the New Jersey Superior Court, Middlesex County, and the **First** African-American Assignment Judge and Presiding Judge, General Equity, of that vicinage; and former Riker Partner who is the **First** Muslim American federal judge in U.S. history and the **First** Asian Pacific American to serve on the federal bench in New Jersey history.

IN ADDITION TO OUR MORRISTOWN AND TRENTON OFFICES IN NEW JERSEY, OUR MIDTOWN MANHATTAN OFFICE SERVES THE NEEDS OF OUR NEW YORK CLIENTS.

Riker Danzig LLP

MORRISTOWN

Headquarters Plaza
One Speedwell Avenue
Morristown, New Jersey 07962
Tel: (973) 538-0800
Fax: (973) 538-1984

NEW YORK CITY

489 Fifth Avenue
33rd Floor
New York, New York, 10017
Tel: (212) 302-6574
Fax: (212) 302-6628

TRENTON

50 West State Street
Suite 1010
Trenton, New Jersey 08608
Tel: (609) 396-2121
Fax: (609) 396-4578