CYBERCRIME: HOW COUNSEL CAN MAINTAIN PRIVILEGE DURING INCIDENT RESPONSE

June 21, 2023

Kathleen McGee

Partner, The Tech Group, White Collar Criminal Defense

Heather Weaver

Counsel, Insurance Recovery Group

Courtney Edmonds

SVP, Chief Ethics & Compliance Officer, and Deputy General Counsel at Leidos

INTRODUCTION

- Courtney Edmonds
- Kathleen McGee
- Heather Weaver

OVERVIEW OF PRESENTATION

- Overview of Ethical Rules
- Before a CyberSecurity Event
  - Hypothetical and Audience Polling
  - Incident Response Planning
  - General Counsel Roles, Responsibilities & Ethical Considerations
- After a CyberSecurity Event
  - Hypothetical and Audience Polling
  - Legal Team Roles, Responsibilities & Ethical Considerations
- Facing lawsuits following a CyberSecurity Event
  - Hypothetical and Audience Discussion
  - General Counsel Roles, Responsibilities & Ethical Consideration
- Concluding Thoughts and Questions

SETTING THE TABLE: ETHICS CONSIDERATIONS

- Virginia Rules of Ethics
  - Va. R. of Prof'l Conduct 1.1 - Requires competent representation to a client, including understanding benefits and risks of technology used
  - Va. R. of Prof'l Conduct 1.6(d) - Requires reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to confidential work product and other documents protected by the attorney client privilege
  - Va. R. of Prof'l Conduct 1.4 - Requires a lawyer thoroughly inform client in a manner sufficient for client to make informed decision
- ABA Ethics Guidelines
  - Model Rules of Prof'l Conduct R. 1.1 – Duty to provide competent representation and understand benefits and risks of technology used
  - Model Rules of Prof'l Conduct R. 1.6(c) – Duty to make reasonable efforts to prevent inadvertent and unauthorized disclosure
  - Model Rules of Prof'l Conduct R.1.4(b)- Duty to explain things in a manner that allows client to make informed decision regarding representation, including cybersecurity risks

RULE COMMENTARY AND RELEVANT ETHICS OPINIONS

- Competence in understanding the technology
- Communicating securely with clients
- Using cloud computing services to maintain client documents
- Counsel's responsibilities to clients after a data breach

ROLE OF THE GENERAL COUNSEL IN CYBER PREPAREDNESS

- Know Your Operational Landscape
  - Types of Data Collected?
  - IT & Privacy – In-house or Outsourced?
  - Threat Monitoring
  - Incident Response Team Composition & Capability
- Know Your Organization's Obligations & Coverage
  - Contractual & Regulatory
  - CyberInsurance
- Know Your Executives / Board
  - BoD and Executive Support
  - Risk and Audit Committees
- Set Boundaries for Communications Relating to Legal Advice and Non-Legal Guidance

HYPOTHETICAL #1

- You are the general counsel of a private mid-size company that sells app-controlled home devices for retail customers' use in their homes. The home device has a voice and video recording function. The app collects geo-location information and must be open for the device to be operational. The devices collect user data including first and last name, residential address, email and password for the app, mobile device number, voice and video recordings, and geolocation information.
- The company has an internal IT team but no CISO. The company has a growing internal software development team and a few consultants. Data is stored in the cloud, with payroll outsourced. The company has B2C contracts with users. The company has a culture of communicating via Slack for regular software development team meetings.
- At the most recent board meeting, the board, who is looking at a substantial fundraising opportunity, raised the question of whether the company is "covered" for cybersecurity. They have asked you to pull together an initial assessment of preparedness and risk. As the amazing GC you are, you know maintaining privilege is an important element of this assessment.

QUESTION #1

- What do you do first?
  - A: Coordinate with your IT team.
  - B: Review your company's contracts.
  - C: Review regulatory landscape.
  - D: Review cyberinsurance policy.
  - E: Evaluate third-party cyber risks.

ANSWER TO QUESTION #1

- Answer: There is no right way to start here, but each of these need to be addressed in short order. If you have an outside counsel, ask them to assist in evaluating the regulatory coverage.

QUESTION #2

- Are all your communications here privileged?
  - A: Of course, I'm the general counsel.
  - B: Only with the company staff.
  - C: Only with the company staff and board.
  - D: Only with the company staff, board, and outside counsel.
  - E: None of the above.

ANSWER TO QUESTION #2

- Answer: E. Not all board communications with general counsel are privileged communications. There are some exceptions you should be aware of. Communications with company staff and outside counsel are generally considered privileged, but the communications do need to be related to legal advice. Ensure all your communications are clearly marked in some way as a legal risk assessment and at least initially, keep the meetings in-person or over video-conference until you can make an initial assessment about the state of the company's security program.

QUESTION #3

- Your outside coverage counsel identified some changes to your cyber insurance program to assure cybersecurity coverage, and has provided an opinion letter regarding the proposed changes. In requesting the changes, you share the opinion letter with your insurance broker.

- Does sharing the opinion letter with an insurance broker waive the privilege?
  - A. Yes.
  - B. No.
  - C. It depends.

ANSWER TO QUESTION #3

- Answer: C. It depends. In some states, sharing privileged communications with an insurance broker waives the privilege.

POST-EVENT CONSIDERATIONS

- Cyberinsurance
  - What to say and when
- Outside Counsel
  - Who to call and when
- IT Forensics
  - Do you need them?
- Board Reports
  - When and what do you tell them?
- Communications
  - Internal and external communications: what to say and when?
- Law enforcement
  - Do you need to get them involved?

GROWING BODY OF CASELAW PIERCES PRIVILEGE CLAIMS IN CYBERSECURITY EVENTS

- ***In re Marriott Customer Data Sec. Breach Litig.*** **(D. Md. 2021)**
- ***In re Rutters Data Sec. Breach Litig.*** **(M. D. Pa. 2021)**
- ***Wengui v. Clark Hill, PLC*****, (D.D.C. 2021)**
- ***In re Capital One Consumer Data Sec. Breach Litig.,*** **(E.D. Va. 2020)**
- ***In re Premera Blue Cross Customer Data Sec. Breach Litig.*****, 296 F. Supp. 3d 1230 (D. Or. 2017)**
- ***In re Target Corp. Customer Data Sec. Breach Litig.*** **(D. Minn. 2015)**
- **Key Takeaways**

HYPOTHETICAL #2

- You are still general counsel of the company described in Hypothetical #1. Before you can complete your full assessment to the Board, but after you've completed a draft report of your findings, your IT department calls you – it is the Friday before the July 4th holiday weekend. They have told you that at noon today, the systems went dark and were replaced with a ransomware note demanding $5M in ETH payment. Your users cannot use their systems until the company gets things back online, and much of your company planned to leave early for the holiday.

QUESTION #4

- What is most important as a first response?
  - A: Totally freak out
  - B: Send a company-wide email about the ransomware event
  - C: Call your insurer
  - D: Call outside counsel
  - E: Order IT to unplug the computers

ANSWER TO QUESTION #4

- Answer: If you had to choose from the above, D is the best answer. Why? Because no general counsel can handle this alone. Ideally, you would have had time to work on an incident response plan. But, since you haven't gotten here yet in this hypothetical, we will walk you through some of the issues you'll face in the first 48-72 hours after a ransomware event that you need to be aware of, particularly as they related to maintaining privilege.

QUESTION #5

- Which communications between general counsel and the following are privileged when addressing a ransomware attack?
  - A: Outside counsel
  - B: Internal IT
  - C: Insurer
  - D: Company board
  - E: All of the above

ANSWER TO QUESTION #5

- Answer: It depends. Answer A is the safe choice here. What about B, C, and D?

HYPOTHETICAL #3

- You are still general counsel of the company described in the previous hypotheticals. You learn that, as part of the cyber attack, customer data has been exposed. Months later, a class action is filed against your company alleging violations of various privacy statutes. You communicate with your trusted insurance coverage counsel regarding whether there is any coverage available for that suit. You share your counsel's analysis with your insurance broker and the broker reports the claim to your company's insurance company.

QUESTION #6

- After receiving notice, your insurer requests that you provide all of defense counsel's analysis regarding the merits of the class action lawsuit. Must you share the requested information?
  - A: Yes
  - B: No

ANSWER TO QUESTION #6

- Probably not.
  - Insurance policies contain a cooperation obligation, but such provisions typically do not require disclosure of, or permit insurers unfettered access to, all defense files.
  - Further, until your interests with your insurer are aligned, there is a risk of waiving privilege by sharing
  - A bizarre exception is found in *Waste Management Inc. v. Int'l Surplus Lines Ins. Co*, 144 Ill. 2d. 178, 579 N.E.2d 322 (Ill. 1991), which holds that the insured and insurer share a common-interest mandating that the policyholder share defense files with the insurer. Even that decision, however, has its limits.

QUESTION #7

- In the underlying class action, the plaintiffs request that your company produce all documents it shared with its insurance company, including defense counsel's analysis of the suit. Can the plaintiffs obtain the requested discovery?
  - A: Yes
  - B: No

ANSWER TO QUESTION #7

- Probably not, but it depends so be very careful.
  - Insureds and insurers often share a common legal interest, such that sharing may not result in a waiver
    - Tip: consider having an agreement before sharing any privileged materials with the insurer
  - Further, under Fed. R. Civ. P. 26(b)(3)(A), attorney-work product protection extends to "documents and tangible things that are prepared in anticipation of litigation or for trial by or for another party or its representative (**including the other party's** attorney, consultant, surety, indemnitor, **insurer**, or agent)"
  - However, there is a risk of waiver depending on the reason the document was created/shared and on the insurer's coverage position
    - If the insurer has accepted the defense without a reservation of rights, the risk of waiver is low
    - If the insurer is defending under a reservation of rights, it will depend on applicable state law
    - If the insurer has denied coverage, the argument for finding waiver is much stronger

QUESTION #8

- Your insurer reserves the right to deny coverage based on an exclusion, but agrees to reimburse for defense counsel at partner rates of $200/hour and associate rates of $100/hour, provided that defense counsel agree to the insurer's stringent litigation guidelines. How should you respond? What ethical rules are implicated by the insurer's position?

ANSWER TO QUESTION #8

- Strategic considerations
  - Are you entitled to independent counsel? If so, who gets to choose?
    - Tip: consider specifying defense counsel in the policy during underwriting
  - Is it a duty to defend or duty to reimburse defense costs policy?
  - Which state law applies?
  - What is a reasonable hourly rate?
  - Does the policy incorporate any litigation guidelines?
- Ethical considerations
  - The ABA Standing Committee on Ethics and Professional Responsibility and state ethics committees have developed guidelines governing panel counsel's obligation to withdraw from representation of an insured, panel counsel's obligations to abide by "panel counsel guidelines," and panel counsel's submission of work description and legal bills to insurers and third party auditors
  - Who does defense counsel represent – the policyholder or the insurance company?

QUESTION #9

- Your Chief Legal Officer recommends obtaining litigation funding in connection with counterclaims asserted against the insurance company. You provide counsel's extensive analysis and other privileged materials to the litigation finance firm so that the firm can evaluate funding for the suit. Has privilege been waived?
  - A: Yes
  - B: No

ANSWER TO QUESTION #9

- Possibly yes. The law is developing on this issue so care is critical.
  - New York Bar Formal Opinion 2011-2:
    - This opinion does not address whether such communications between the client or lawyer and a financing company result in a waiver of the attorney-client privilege or other applicable protection. We note, however, that the argument has been made that the common interest privilege does not apply to such communications because the financing company's interest in the outcome of a litigation is commercial, rather than legal.
    - With the foregoing in mind, a lawyer may not disclose privileged information to a financing company unless the lawyer first obtains the client's informed consent, including by explaining to the client the potential for waiver of privilege and the consequences that could have in discovery or other aspects of the case. In making disclosures to the financing company, a lawyer should take care not to disclose any more information than is necessary in his or her judgment.

CLOSING CONSIDERATIONS

- Ethical obligations to serve client, maintain privilege where possible, and protect user privacy
- Cannot do this alone
- Having a plan is essential to preparedness and response

KATHLEEN A. MCGEE

Partner, The Tech Group, White Collar Criminal Defense

New York
T: 1.646.414.6831
E: kmcgee@lowenstein.com

Education

Boston University (J.D. 2001)

University of Chicago (M.A. 1996)

Sarah Lawrence College (B.A. 1994)

Admissions

New York

U.S. District Court for the Eastern District of New York

U.S. District Court for the Southern District of New York

Kathleen's unique public sector experience gives her an edge in counseling emerging and mature companies on a broad spectrum of regulatory issues concerning technology, data security, and privacy. In addition, Kathleen's experience in municipal government and her understanding of how the administrative code affects business have given her a unique perspective on the intersection of commerce and the law. Clients appreciate her insights into how to identify unanticipated problems and develop creative, business-focused solutions.

As Bureau Chief of the Bureau of Internet & Technology for the New York State Attorney General's Office, Kathleen was at the forefront of regulation, enforcement initiatives, and public policy involving privacy, data security, and consumer protection, among other issues. She led the NYAG's successful litigation against illegal daily fantasy sports operations (New York v. Draft Kings, Fan Duel), as well as investigations of New York State's internet service providers and successful litigation against the state's largest internet service provider (New York v. Charter Communications).

Earlier in her career, she served as Director of the Office of Special Enforcement in the New York City Mayor's Office where, as lead counsel, she directed litigation on a number of intellectual property and civil nuisance matters, including the Counterfeit Triangle litigation encompassing an entire city block in Chinatown. She was also a policy leader on issues ranging from data analytics to human trafficking. While with the mayor's office, Kathleen also developed the New Business Acceleration Team to streamline regulations and fast-track new business development. Kathleen started her legal career as an Assistant District Attorney for the Bronx County District Attorney's Office in New York, where she prosecuted domestic violence, child abuse, and sex crimes.

KATHLEEN A. MCGEE

With close to two decades of experience as a prosecutor and leading regulator, including as Bureau Chief of the New York Attorney General's Bureau of Internet and Technology, Kathleen is a highly accomplished attorney with a unique and valuable skill set. Kathleen regularly leverages her extensive experience in the public sector by representing clients before federal, state, and local law enforcement and regulators on issues ranging from white collar criminal defense matters and criminal and civil investigations before the DOJ, SEC, FTC, and state attorneys general, to commercial disputes and advisory matters involving technology, data commodification, cybersecurity and privacy, consumer protection issues, tech M&A, data governance, and corporate governance. Clients benefit from both her sophisticated grasp of technology-related criminal matters and her on-the-ground experience as a lead prosecutor in both jury and bench trials.

Kathleen's practice includes representing established global businesses, scale-ups, and startups (including fintechs, investment groups, and governments) in multiple sectors, including ad tech, financial services, insurance tech, biotech, IoT, and retail. Her experience encompasses data, M&A, technology procurement, privacy, data breaches and cybersecurity, consumer protection, and product launches. Kathleen's practice covers all aspects of technology, data, privacy, and intellectual property, with a focus on emerging technologies, data services, and cybersecurity. With the advent of the CARES Act, Kathleen has established herself as a go-to resource for PPP loan applicants navigating the process.

An author of several state and local bills and laws, including New York State's SHIELD Act on data security, Kathleen brings a strong sense of regulatory policy and advises clients on the legal landscape affecting their business models. She is a regular speaker, author, and interviewee for events and publications ranging from government investigations to data security and privacy and tech regulation.

HEATHER WEAVER

Counsel, Insurance Recovery

New Jersey
T: 1.862.926.2134
E: hweaver@lowenstein.com

Education

Brooklyn Law School (J.D. 2011), cum laude; Carswell Merit Scholarship; notes and comments editor, Brooklyn Law Review

Pennsylvania State University (B.S. 2008), cum laude; Dean's List; Distinction Honor, Smeal College of Business

Admissions

New York

New Jersey

U.S. District Court for the Eastern District of New York

U.S. District Court for the Southern District of New York

Heather has more than a decade of experience litigating and pursuing alternative dispute resolution for a wide range of complex insurance coverage and commercial disputes in state and federal courts. She regularly represents policyholders in high-stakes insurance litigation arising out of commercial property policies, commercial general liability policies, professional liability policies, and product liability policies. To date, she has secured hundreds of millions of dollars in recoveries on behalf of her clients.

Heather also regularly counsels policyholders on the availability of coverage for various types of claims, including business interruption and other first-party property claims, mass torts, environmental damage, cybersecurity, and bodily injury. She has deep experience with a broad range of coverage issues, including allocation, additional insured disputes, late notice disclaimers, bad faith disputes, and bankruptcy issues.

In addition, Heather has extensive experience counseling with respect to insurance issues in the transactional context. Working closely with deal teams across the firm, she leads litigation and insurance diligence efforts for companies across a range of industries, including manufacturers, banks, private equity firms, and asset managers. She analyzes target companies' pending and potential claims and liability on behalf of buyers and assesses the adequacy of available insurance coverage and potential risk.

Heather also assists clients with the placement and renewal of their insurance programs, focusing on enhancing coverage tailored to their specific business needs. Her knowledge in this area enables her to minimize risk and ensure adequate protection for her clients.

Prior to joining Lowenstein Sandler, Heather was counsel at an Am Law 100 law firm.

Chief Ethics & Compliance Officer

COURTNEY EDMONDS

Courtney Edmonds is Leidos' Chief Ethics & Compliance Officer. In this role he is responsible for designing, developing, and administering the company's Ethics and Compliance Program in accordance with the Federal Acquisition Regulations and other relevant laws, regulations, and guidance. The program includes administering the Code of Conduct, ethics and compliance training, the ethics case management and investigative process, and corporate compliance policies and procedures. Prior to joining the Ethics and Compliance Office, Courtney was the Assistant General Counsel for Leidos' Intel Group and the Lead Attorney for the Leidos Innovations Center. His responsibilities included all aspects of procurement law, including bid protests, identifying and mitigating organizational conflicts of interest, dispute avoidance and resolution, internal investigations, ethics and compliance, and drafting and negotiating contract terms and conditions. Before joining Leidos, he was in private practice for seven years in the government contract practice groups of two national law firms.

Courtney graduated from Averett College with a B.B.A and holds an M.A. in Management and M.B.A. from Webster University. He completed his J.D. in 2002 and LL.M (National Security Law) in 2015 at Georgetown Law. He began his career in federal procurement as a Contract Specialist for the U.S. Navy's Fleet Industrial Supply Command Norfolk, Det. Washington. Prior to that role, he proudly served on active duty for ten years in the U.S. Air Force as a Law Enforcement Specialist. Courtney holds a Leadership Professional in Ethics & Compliance certification from the Ethics & Compliance Initiative.