The Legal Side of Cyber
An Overview

www.eckertseamans.com

Matthew H. Meade, Esq. | March 9, 2021

ECKERT SEAMANS
ATTORNEYS AT LAW

Cybersecurity Focus: U.S. Legal Landscape

Work Product Cyber Investigation

- *In re: Capital One Customer Data Security Breach Litigation*, E.D. Va., No. 1:19-md-02915
- **Nature of Mandiant's services**. Services would have been performed in substantially similar form even in the absence of litigation.
- **Timing of Mandiant's engagement**. Focus on prior, ongoing engagement between Capital One and Mandiant, which dated back to 2015. Also focused on statement of work underlying Mandiant's forensic services which was signed in January 2019, before incident.

Work Product Cyber Investigation

- **Payment**. Capital One had designated Mandiant's work as a "Business Critical" expense, not a "Legal" expense.
- **Use of Mandiant's report**. Court viewed the disclosure of Mandiant's incident report to an external accountant as "not necessarily" rising to the level of "waiver" but as evidence that purpose of report was not driven by litigation and legal needs.

Work Product Cyber Investigation

- **Wengui v. Clark Hill PLC**, No. 19-3195 (D.D.C. Jan. 12, 2021)
- Report would further business as it set forth investigation findings and remediation recommendations, and thus in the court's view "would have been prepared in any event as part of the ordinary course of defendant's business.“
- Rejected 2 track because firm that issued report was hired to replace prior firm
- True objective was gleaning" the cybersecurity firm's "expertise in cybersecurity, not in obtaining legal advice from its lawyer."

Work Product Cyber Investigation

- Shared the report with members of Clark Hill's leadership and information technology teams, as well as the FBI to assist the FBI's investigation.
- Court further observed that the declaration submitted by Clark Hill's general counsel stated that the report was used to assist the firm "in connection with managing any issues, including potential litigation, related to the cyber incident," and did not say that litigation was the only use.

Work Product Cyber Investigation-Factors

- Who hired the investigator;
- Timing of the investigator's retention;
- Statement of purpose in the engagement agreement with the investigator;
- Declarations submitted by the company about the nature of and reason for the work;
- Whether there was a separate business-focused investigation, which can reinforce the argument that the investigation under review was for distinct legal reasons;
- Who received the forensic report and how they used it;
- What company said publicly about the investigation;
- Whether company designated the work as a legal expense; and
- Content of the actual forensic report and related documents.

Mini Scenario

Misdirected Email

Scenario	Questions
▪ An employee mistakenly emails six other employees a spreadsheet containing the Social Security numbers and checking account numbers for 20 new hires. ▪ One of the recipients contacts the sender and alerts him of the error. ▪ Each recipient opened the attachment.	• What should you do once you learn of the incident? • Is this incident a data breach? • What questions would you ask recipients? • How would you counsel the employee?

Misdirected Email

KEY TAKEAWAY	
▪ 73 P.S. § 2302 Good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity is not a breach of the security of the system **if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure**	As long as no further unauthorized use then no breach Still need to look at state residency of impacted individuals to make sure that similar language is in state breach notification law

Ransomware

The Ransom Note

All of your files are currently encrypted by CONTI ransomware.
If you try to use any additional recovery software - the files might be damaged or lost.

To make sure that we **REALLY CAN** recover data - we offer you to decrypt samples.
You can contact us for further instructions through:
Our website
TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://contirecj4hbzmyzuydyzrvm2c65blmvhoj2cvf25zqj2dwrrqcq5oad.onion/

HTTPS VERSION:
https://contirecovery.best

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded your data and are ready to publish it on out news website if you do not respond. So it will be better for both sides if you contact us ASAP

The threat actor is asking for 50 bitcoin for the encryption key

- The Company decides not to pay because it can recover the information from backups. Who makes this decision?
- The threat actor is frustrated by your unwillingness to pay the ransom and sends 25 sample files to show that they have been in the network and mean business.
- The files include sensitive information related to customers and employee PII.

Action Steps

- Should the Company use the IT firm it has an ongoing support relationship with to conduct the forensic investigation?
- Why or why not?
- What is the amount that the Company is willing to pay to get its data back and prevent the release? Who decides?
- What is the amount of ransom payment covered by insurance?

Negotiating with the Threat Actor

- In order to avoid reputational damage, you instruct the negotiator to offers the threat actor 5 bitcoin

FIREEYE: We have seen what you have . . . 5 BITCOIN? Yes or no?

SUPPORT: That is not enough. We think that you are not completely aware of the seriousness of the situation. In the event of a further delay, we will be able to use information resource https://continews.best and will start to sell you private data on the black markets.

We will publish the full dump of your data on our news website with 1,000 visitors per day, 50% of them are mass media reporters and regulators, the other part is blackhat hackers. We are not interested in this, and we gain nothing from data publication, that is why we are offer you a deal.

1) your customers data will be used by criminals

2) your ciustomers will fill lawsuit against you

3) government regulators will fine you for data breach, if you have in clients at least one EU resident then you will be also fined by EU government by GDPR law with millions of dollars of fine or permit ban for working with EU citizents. US has the similar laws, but they are not so costly, however the total cost will exceed the asked amount from you, so our offer is the best deal for you to resolve this issue.

FIREYE: We have no EU concerns. We are very aware of what you have. Most of the info, if not all, is available to the public. $5 Bitcoin?

If You Decide to Pay Ransom (Mechanics)

- Third Party negotiator typically handles all negotiations with threat actor
- Proof of Life-Third Party negotiator provides threat actor with sample of encrypted files to prove that threat actor can decrypt
  - Encrypted files need to be generic. (Do not send file with PII in it)
- Payment in bitcoin is made by third party after receipt of funds from the Company
- Third party verifies that payment is not going to a country or group on US restricted list as required by recent OFAC advisory
- Third party makes bitcoin payment (there is typically an additional charge associated with facilitating the payment)

Investigation Continues

- What steps should IT take with respect to the 25 files?
- If you are able to identify the source of the files, what are the next steps?
- Would the source of the files impact the willingness to pay more to the threat actor? Why or why not?
- Is there a data breach as to any of the 25 files?

Data Released

- The threat actor ultimately rejects the offer and publishes 20 GB of data on the Dark Web
- The files on the Dark Web include:
  - data subject to non disclosure pursuant to vendor agreements
  - information provided in litigation subject to a confidentiality order
  - PII

Notifications

- What notification obligations with respect to vendor agreements, PII, and litigation?
- How would you determine this?
- Who would review records?

Questions?
Thank You.

Matthew H. Meade, Esq.
(412) 566.6983 | mmeade@eckertseamans.com

ECKERT SEAMANS
ATTORNEYS AT LAW