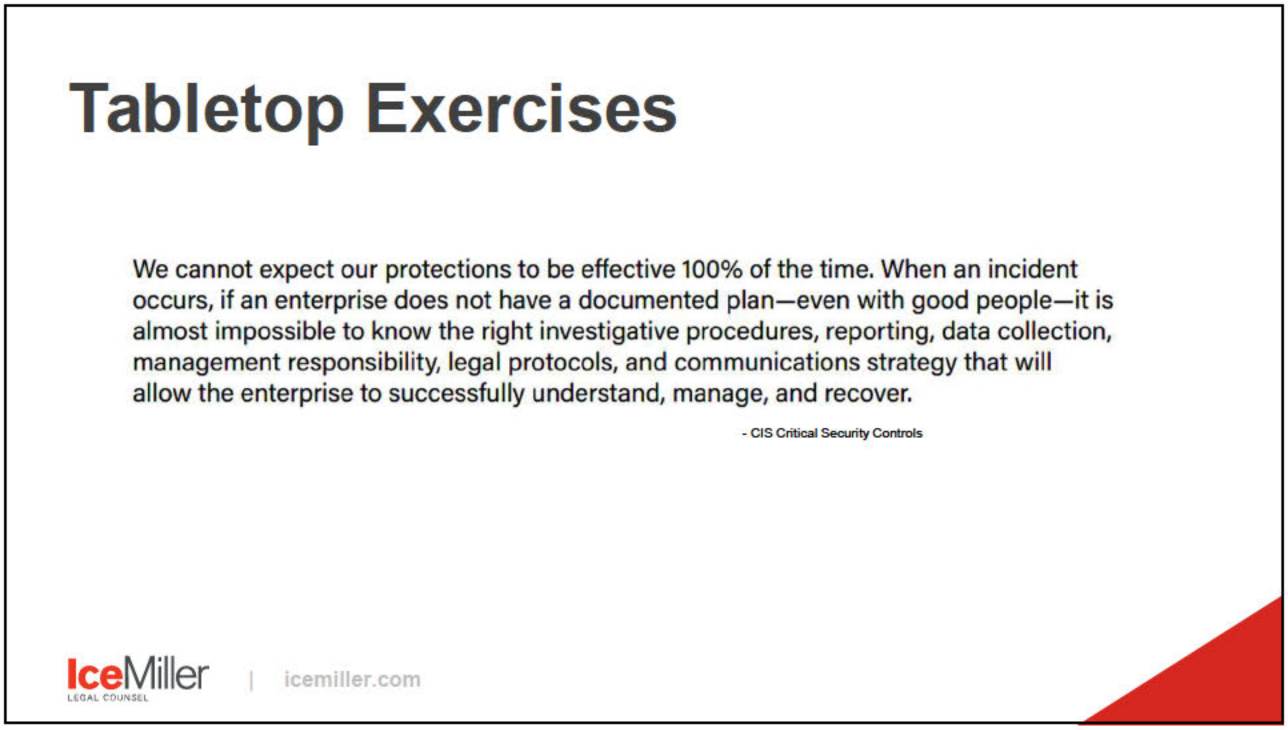
Tabletop Exercise! Cyber Security Fire Drill

April 9, 2024

NAHEFFA Spring 2024 Conference

IceMiller
LEGAL COUNSEL

1



Tabletop Exercises

> We cannot expect our protections to be effective 100% of the time. When an incident occurs, if an enterprise does not have a documented plan—even with good people—it is almost impossible to know the right investigative procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy that will allow the enterprise to successfully understand, manage, and recover.
>
> - CIS Critical Security Controls

IceMiller
LEGAL COUNSEL | icemiller.com

2

Goals Today

Photo credit: ePublicist / Foter / CC BY-ND

3

Inject #1 – Day 0

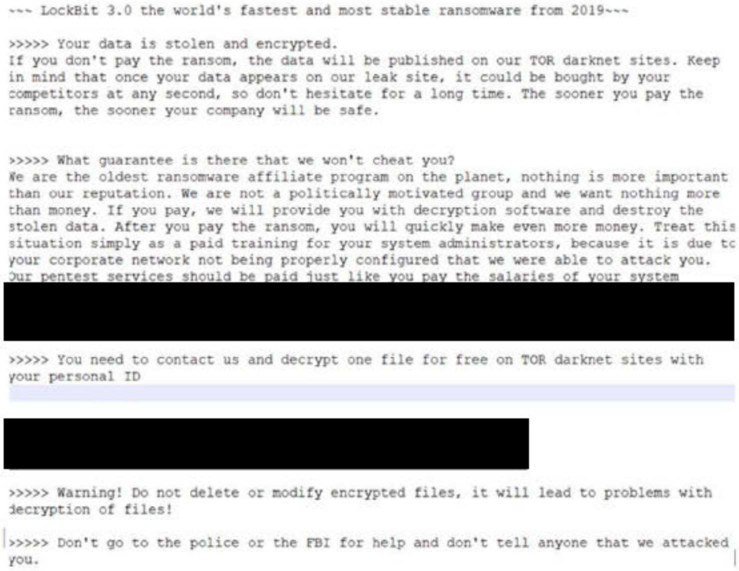
You get a call from your [CIO/IT Manager/Helpdesk] stating that we need to shut down all IT systems and computers because we’re having IT issues.

4

Prompt

- What would you do at this time?

Inject #1 cont’d: IT Discovers . . .



```
~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~

>>>>> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep
in mind that once your data appears on our leak site, it could be bought by your
competitors at any second, so don't hesitate for a long time. The sooner you pay the
ransom, the sooner your company will be safe.


>>>>> What guarantee is there that we won't cheat you?
We are the oldest ransomware affiliate program on the planet, nothing is more important
than our reputation. We are not a politically motivated group and we want nothing more
than money. If you pay, we will provide you with decryption software and destroy the
stolen data. After you pay the ransom, you will quickly make even more money. Treat this
situation simply as a paid training for your system administrators, because it is due to
your corporate network not being properly configured that we were able to attack you.
Our pentest services should be paid just like you pay the salaries of your system
[redacted]

>>>>> You need to contact us and decrypt one file for free on TOR darknet sites with
your personal ID

[redacted]

>>>>> Warning! Do not delete or modify encrypted files, it will lead to problems with
decryption of files!

>>>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked
you.
```

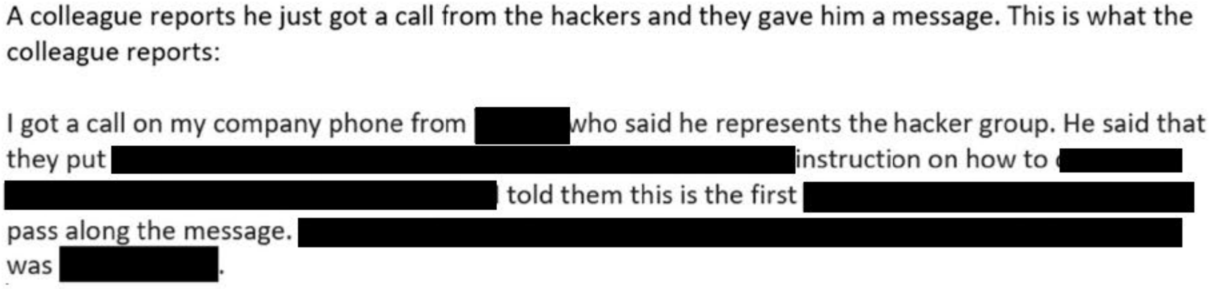
Prompt

- What do you do at this time?
- Who do you contact?
- How does this impact you?

7

Inject #2 – Day 1

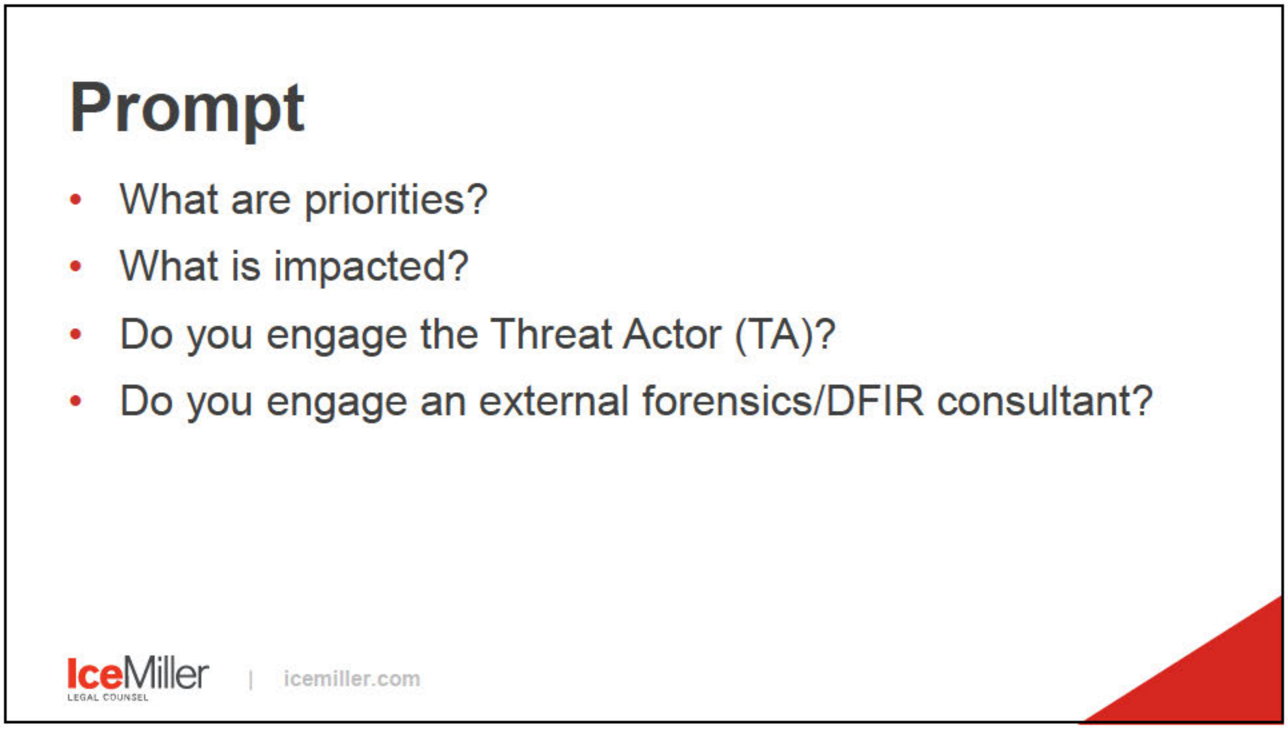
Incident response team discovers prolific IT issues throughout the environment.



A colleague reports he just got a call from the hackers and they gave him a message. This is what the colleague reports:

I got a call on my company phone from [redacted] who said he represents the hacker group. He said that they put [redacted] instruction on how to [redacted] [redacted] told them this is the first [redacted] pass along the message. [redacted] was [redacted].

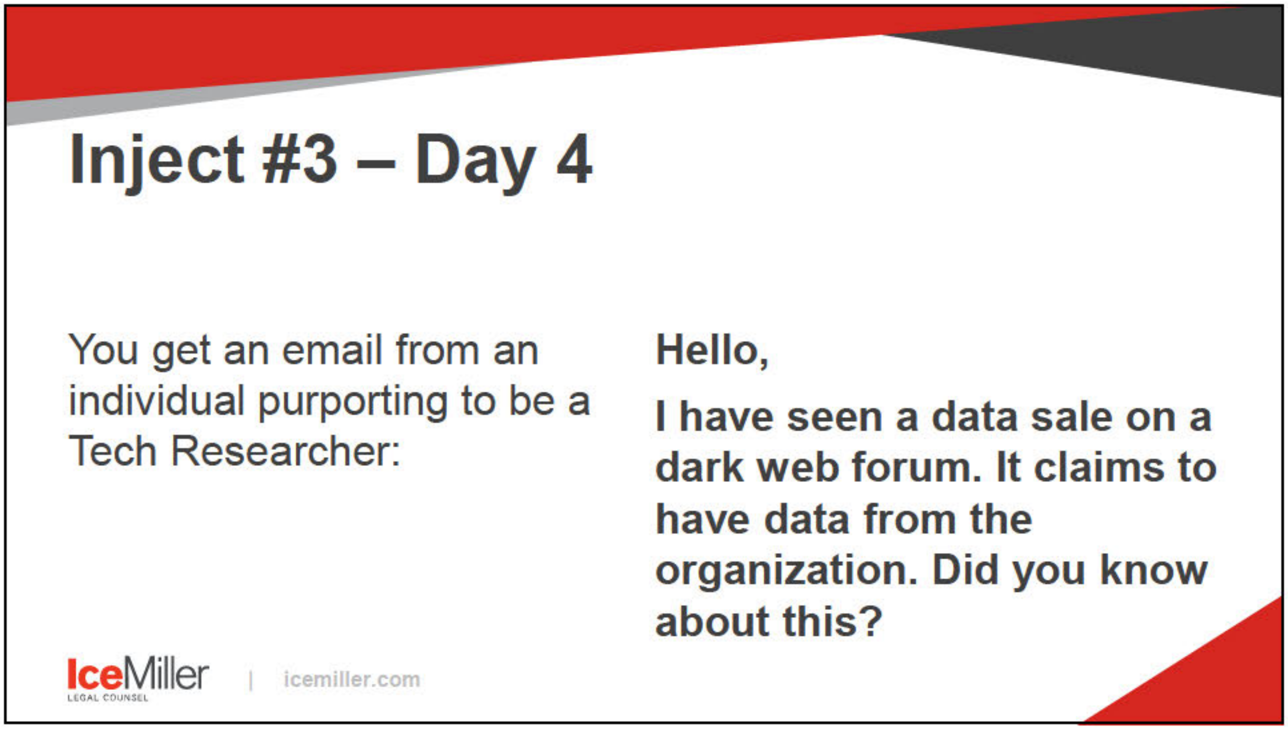
8



Prompt

- What are priorities?
- What is impacted?
- Do you engage the Threat Actor (TA)?
- Do you engage an external forensics/DFIR consultant?

9



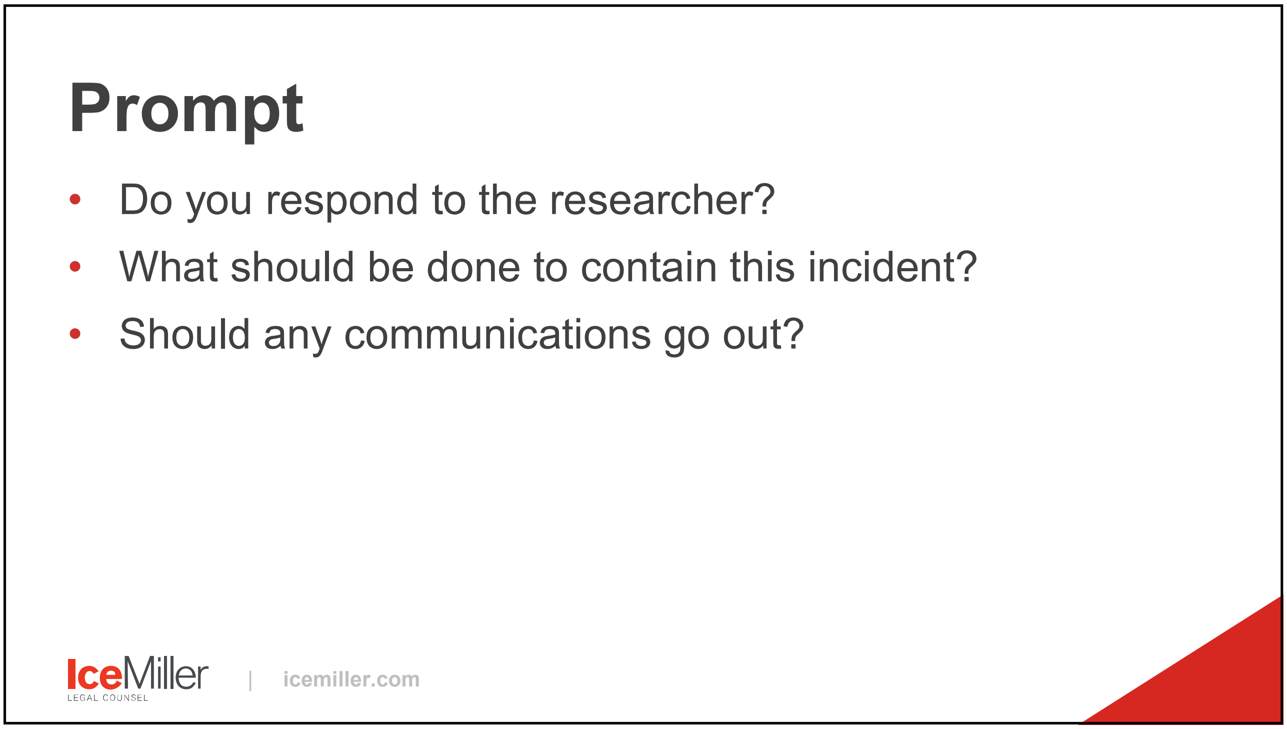
Inject #3 – Day 4

You get an email from an individual purporting to be a Tech Researcher:

Hello,

I have seen a data sale on a dark web forum. It claims to have data from the organization. Did you know about this?

10

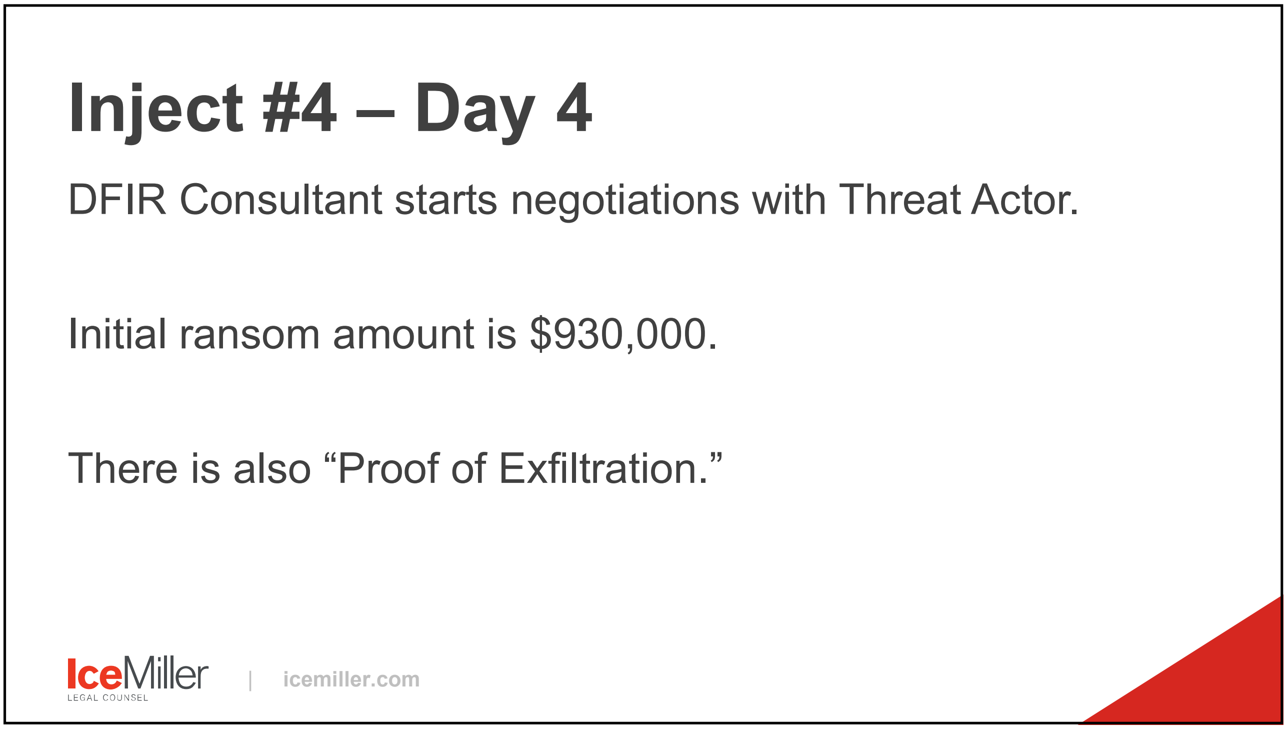


Prompt

- Do you respond to the researcher?
- What should be done to contain this incident?
- Should any communications go out?

IceMiller LEGAL COUNSEL | icemiller.com

11



Inject #4 – Day 4

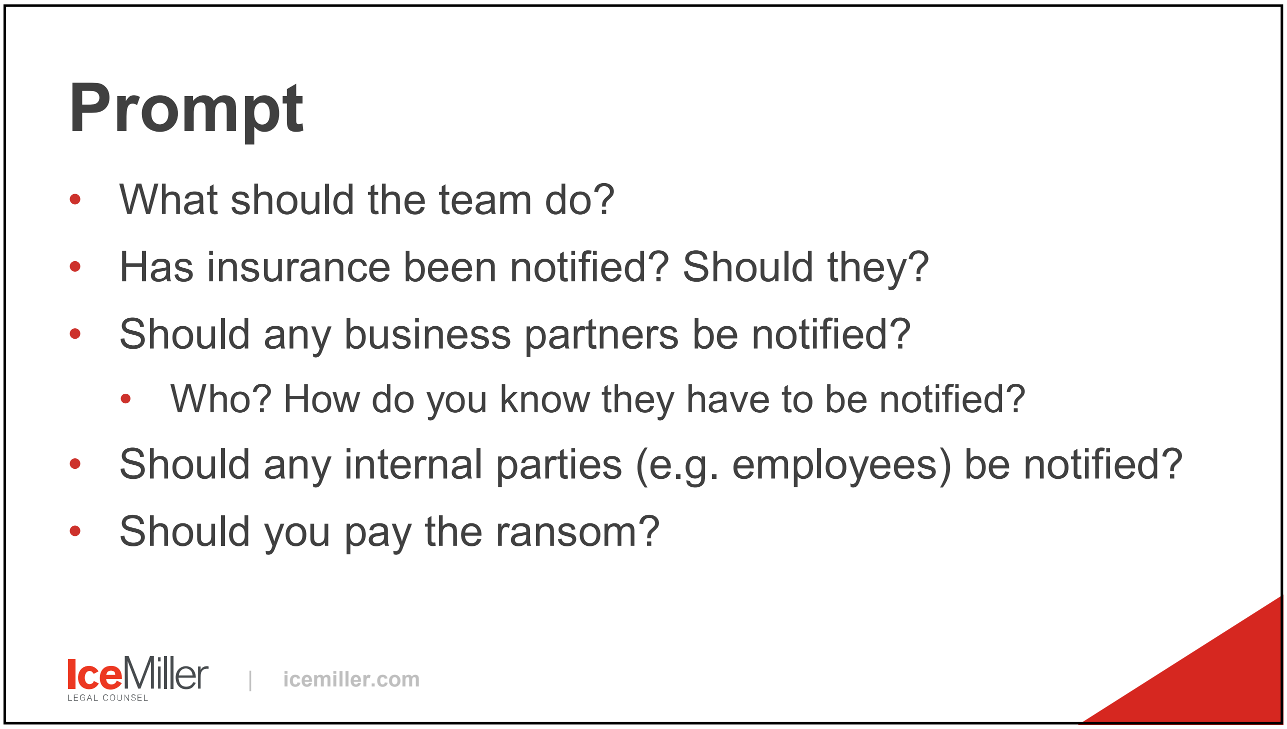
DFIR Consultant starts negotiations with Threat Actor.

Initial ransom amount is $930,000.

There is also “Proof of Exfiltration.”

IceMiller LEGAL COUNSEL | icemiller.com

12

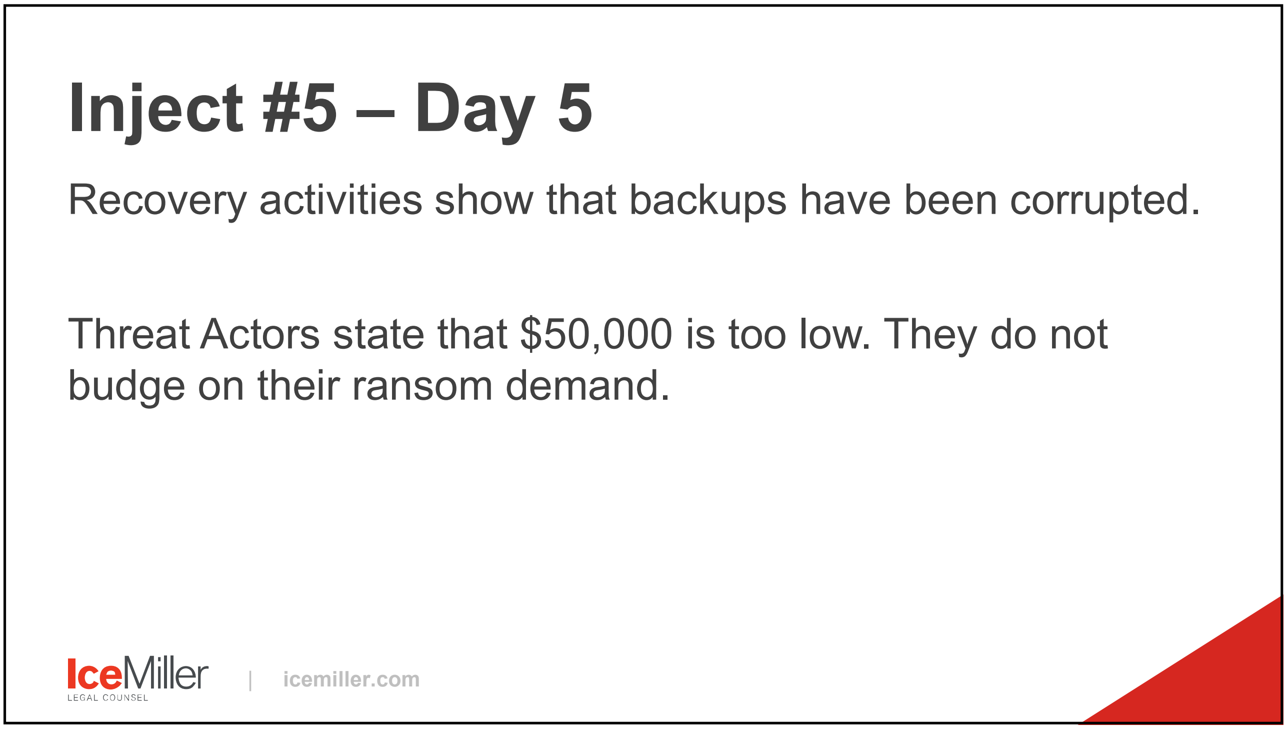


Prompt

- What should the team do?
- Has insurance been notified? Should they?
- Should any business partners be notified?
  - Who? How do you know they have to be notified?
- Should any internal parties (e.g. employees) be notified?
- Should you pay the ransom?

IceMiller LEGAL COUNSEL | icemiller.com

13



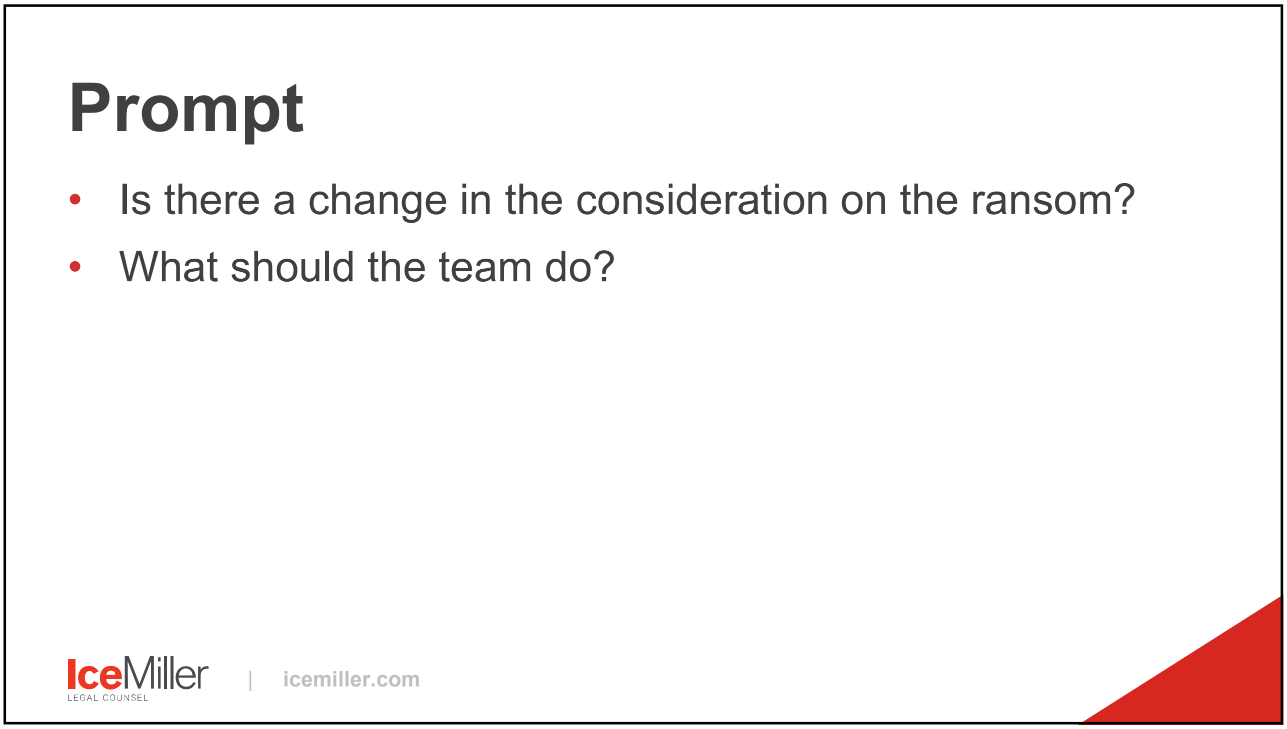
Inject #5 – Day 5

Recovery activities show that backups have been corrupted.

Threat Actors state that $50,000 is too low. They do not budge on their ransom demand.

IceMiller LEGAL COUNSEL | icemiller.com

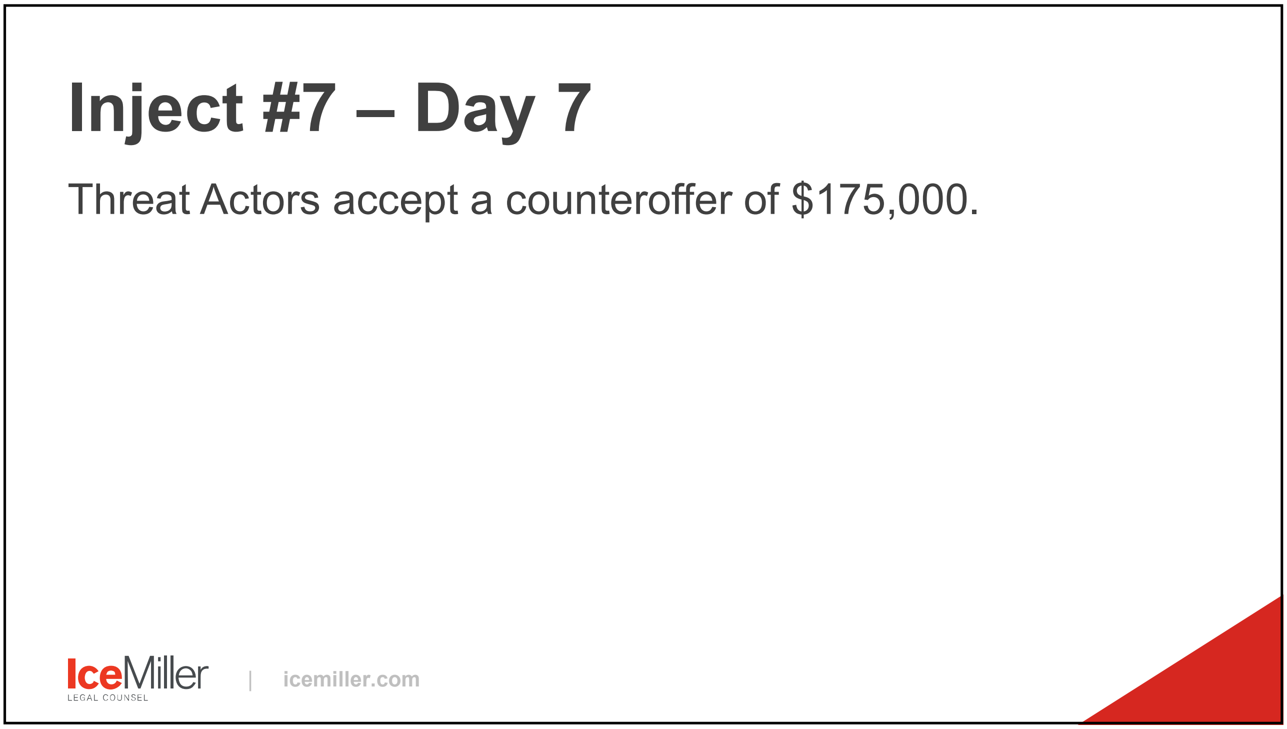
14



Prompt

- Is there a change in the consideration on the ransom?
- What should the team do?

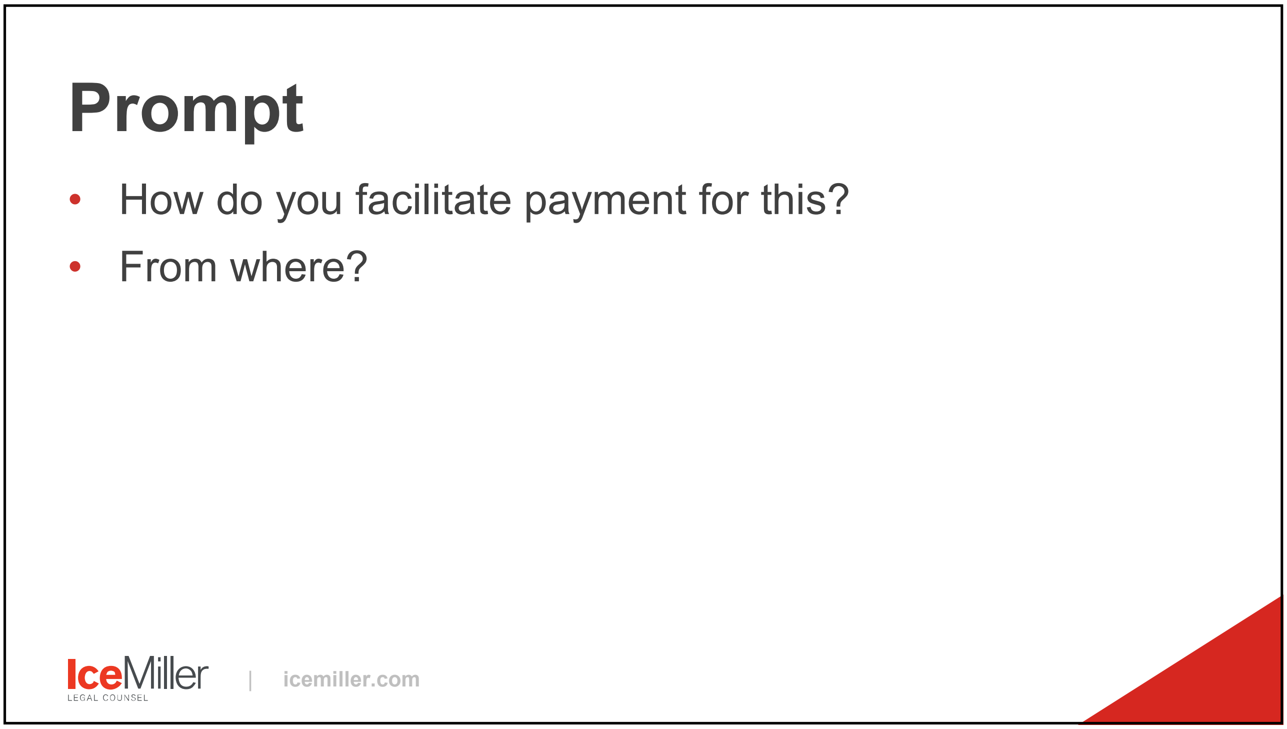
15



Inject #7 – Day 7

Threat Actors accept a counteroffer of $175,000.

16

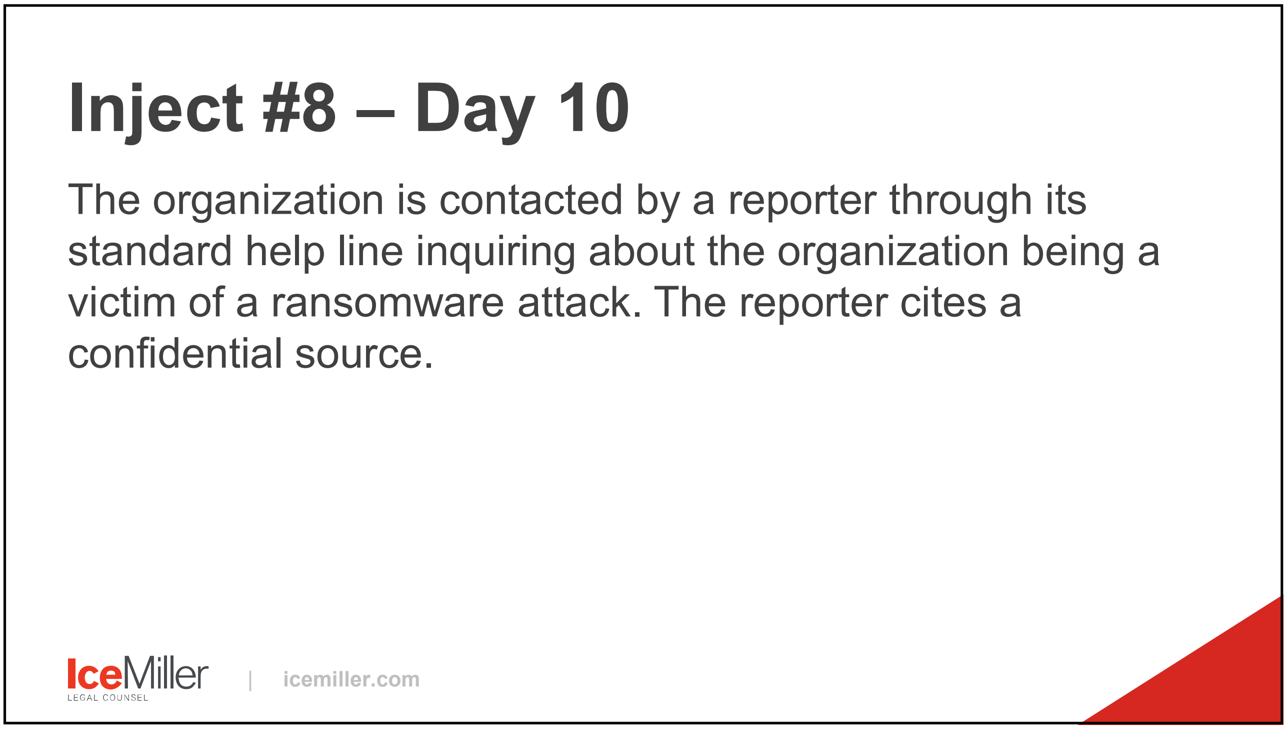


Prompt

- How do you facilitate payment for this?
- From where?

IceMiller LEGAL COUNSEL | icemiller.com

17



Inject #8 – Day 10

The organization is contacted by a reporter through its standard help line inquiring about the organization being a victim of a ransomware attack. The reporter cites a confidential source.

IceMiller LEGAL COUNSEL | icemiller.com

18

Prompt

- Should the organization engage the reporter?
- Are there any concerns about the researcher's report?
- What are public affairs concerns?
- Who is responsible for coordinating the public message? Is this process a part of any established plan?
- What information should be shared with the public? Employees?

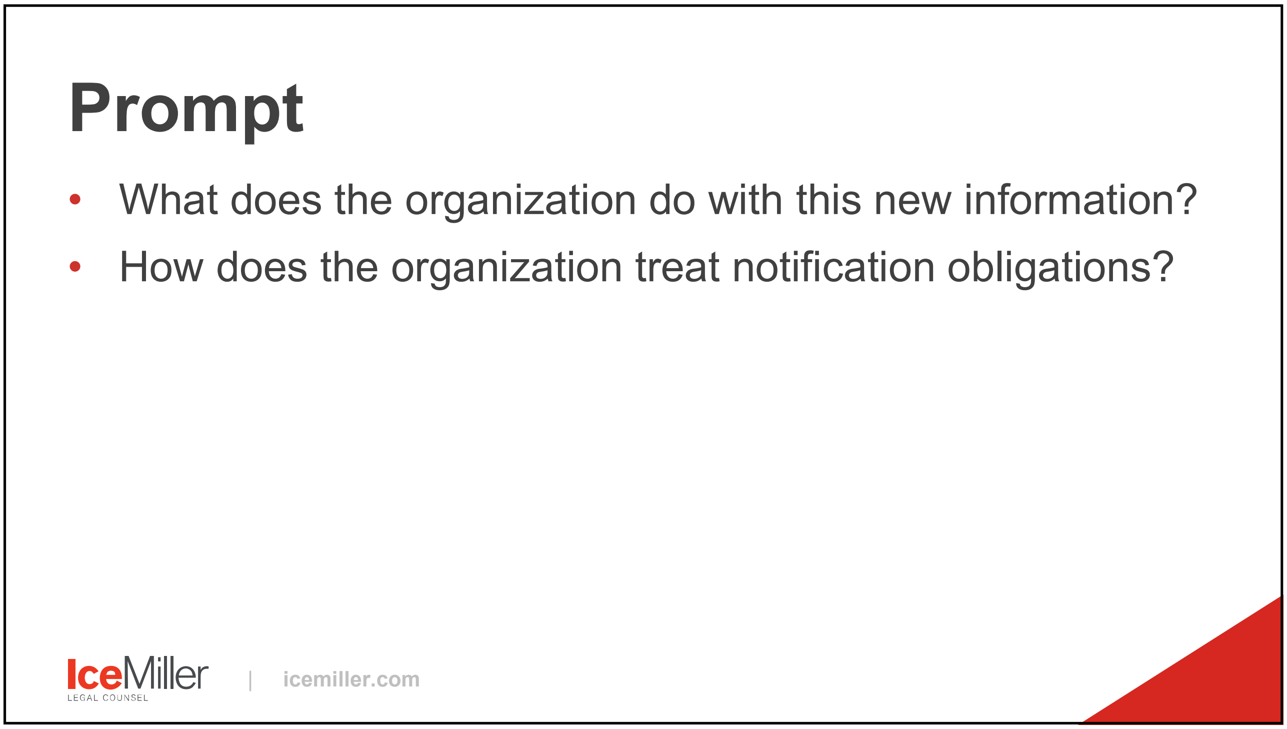
19

Inject #10

Recovery is mostly complete.

Analysis shows that all file shares were impacted.

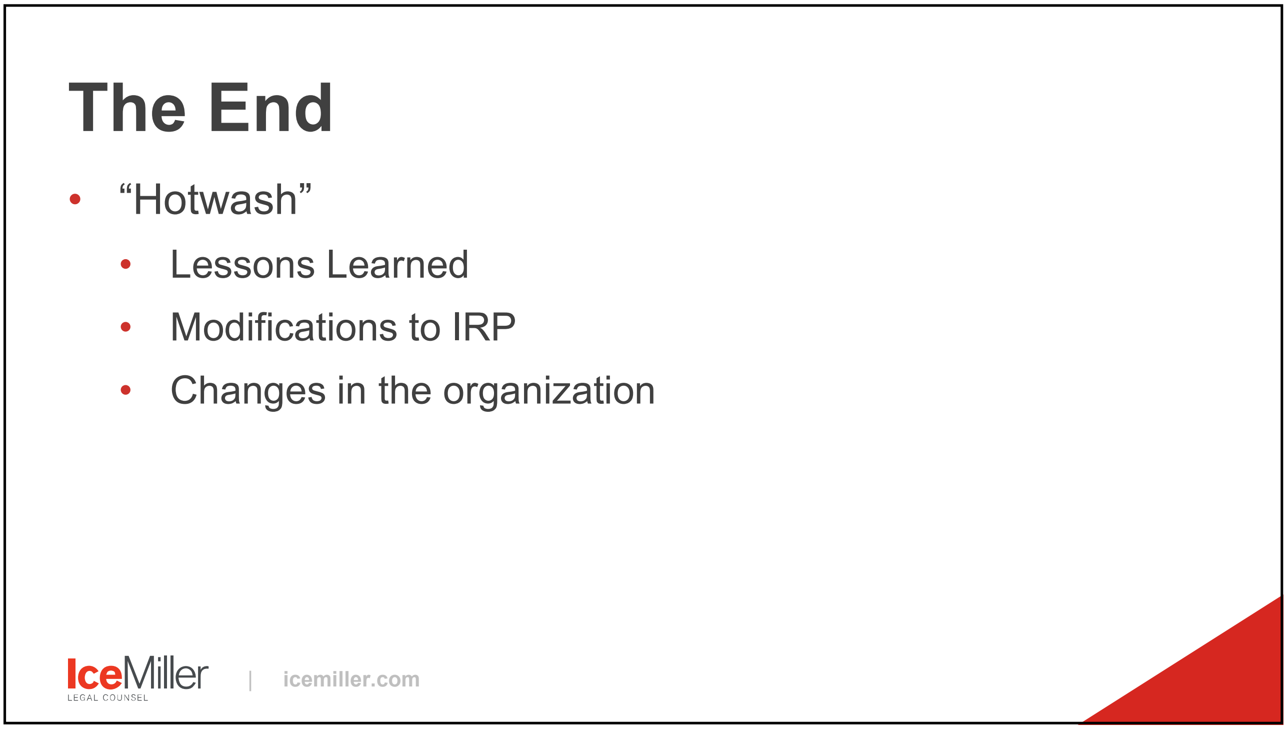
20



Prompt

- What does the organization do with this new information?
- How does the organization treat notification obligations?

21



The End

- “Hotwash”
  - Lessons Learned
  - Modifications to IRP
  - Changes in the organization

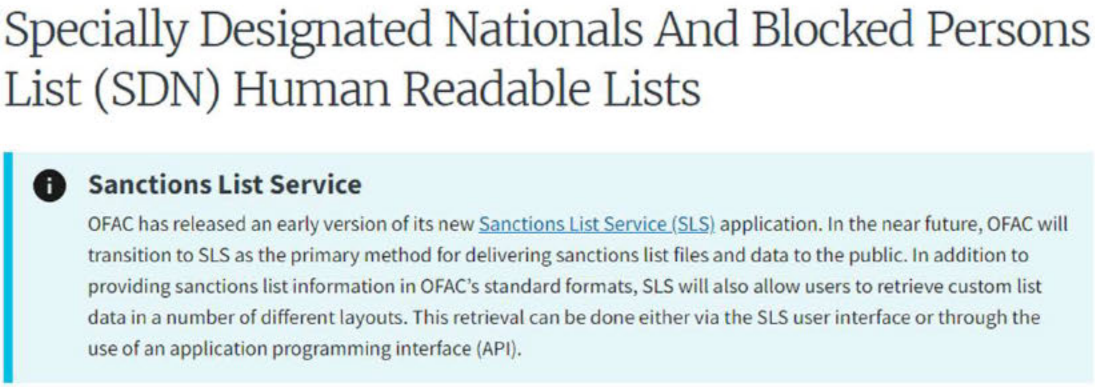
22

SEC Guidance

- In the Closing Remarks of a Compliance Conference on Dec. 7, the Director of the Office of Municipal Securities of the U.S. Securities and Exchange Commission noted the SEC recently finalized its cybersecurity rule for public companies.
- The Director then suggested that "**everyone take a minute to review the Adopting Release for the rule because there are some good points on how corporations can handle cybersecurity disclosures that may be useful for municipal market participants**."

IceMiller LEGAL COUNSEL | icemiller.com

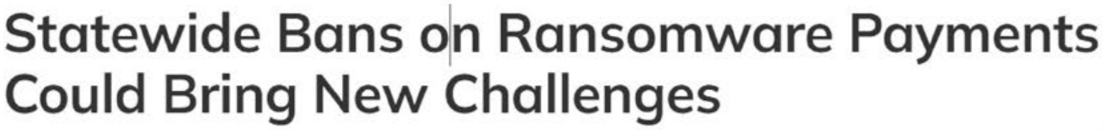
23



Specially Designated Nationals And Blocked Persons List (SDN) Human Readable Lists

Sanctions List Service

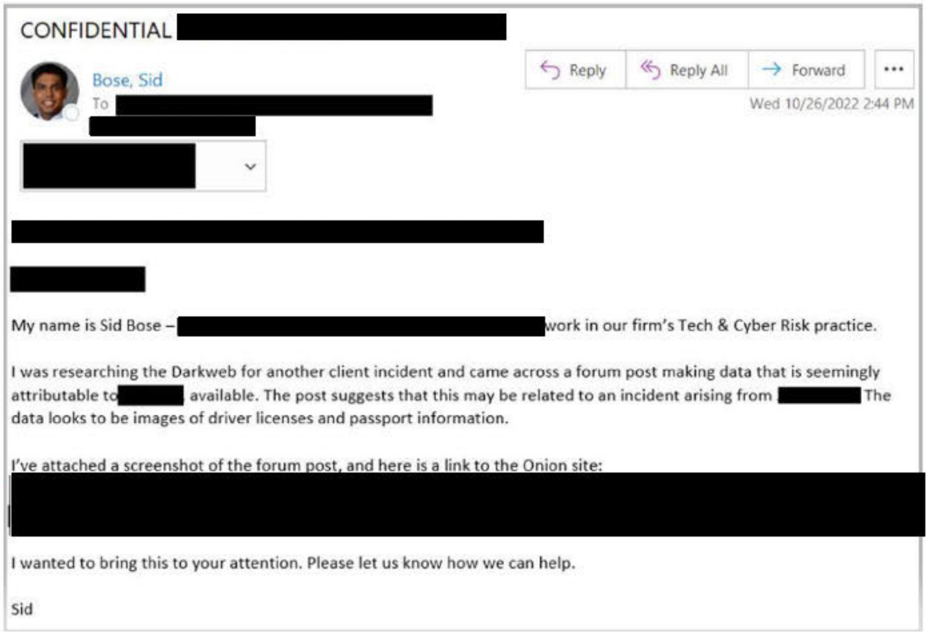
OFAC has released an early version of its new Sanctions List Service (SLS) application. In the near future, OFAC will transition to SLS as the primary method for delivering sanctions list files and data to the public. In addition to providing sanctions list information in OFAC's standard formats, SLS will also allow users to retrieve custom list data in a number of different layouts. This retrieval can be done either via the SLS user interface or through the use of an application programming interface (API).



Statewide Bans on Ransomware Payments Could Bring New Challenges

IceMiller LEGAL COUNSEL | icemiller.com

24



CONFIDENTIAL [redacted]

Bose, Sid

To [redacted]

[redacted]

Wed 10/26/2022 2:44 PM

[redacted]

[redacted]

[redacted]

My name is Sid Bose – [redacted] work in our firm's Tech & Cyber Risk practice.

I was researching the Darkweb for another client incident and came across a forum post making data that is seemingly attributable to [redacted] available. The post suggests that this may be related to an incident arising from [redacted] The data looks to be images of driver licenses and passport information.

I've attached a screenshot of the forum post, and here is a link to the Onion site:

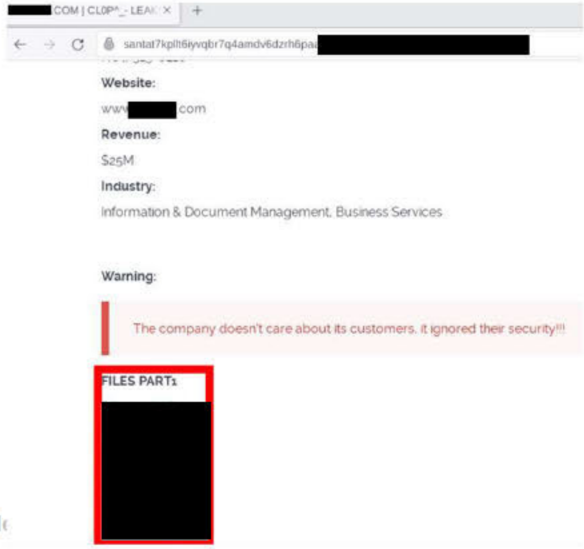
[redacted]

I wanted to bring this to your attention. Please let us know how we can help.

Sid

25

Threat Actor Data Leak Sites (DLS)


[redacted] COM | CL0P^_- LEAK
santat7kpllt6iyvqbr7q4amdv6dzrh6paa[redacted]

Website:

www[redacted]com

Revenue:

$25M

Industry:

Information & Document Management, Business Services

Warning:

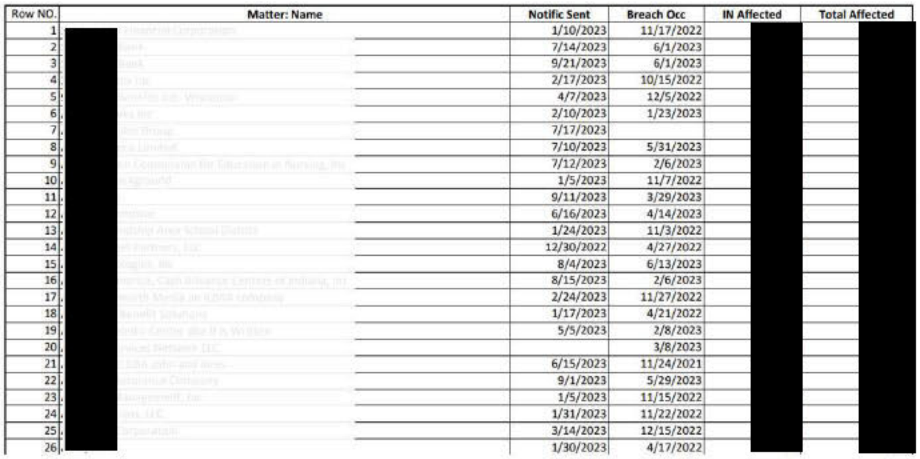
The company doesn't care about its customers, it ignored their security!!!

FILES PART1

[redacted]

26

Indiana AG Website



Row NO.	Matter: Name	Notific Sent	Breach Occ	IN Affected	Total Affected
1	[redacted]	1/10/2023	11/17/2022	[redacted]	[redacted]
2	[redacted]	7/14/2023	6/1/2023	[redacted]	[redacted]
3	[redacted]	9/21/2023	6/1/2023	[redacted]	[redacted]
4	[redacted]	2/17/2023	10/15/2022	[redacted]	[redacted]
5	[redacted]	4/7/2023	12/5/2022	[redacted]	[redacted]
6	[redacted]	2/10/2023	1/23/2023	[redacted]	[redacted]
7	[redacted]	7/17/2023		[redacted]	[redacted]
8	[redacted]	7/10/2023	5/31/2023	[redacted]	[redacted]
9	[redacted]	7/12/2023	2/6/2023	[redacted]	[redacted]
10	[redacted]	1/5/2023	11/7/2022	[redacted]	[redacted]
11	[redacted]	9/11/2023	3/29/2023	[redacted]	[redacted]
12	[redacted]	6/16/2023	4/14/2023	[redacted]	[redacted]
13	[redacted]	1/24/2023	11/3/2022	[redacted]	[redacted]
14	[redacted]	12/30/2022	4/27/2022	[redacted]	[redacted]
15	[redacted]	8/4/2023	6/13/2023	[redacted]	[redacted]
16	[redacted]	8/15/2023	2/6/2023	[redacted]	[redacted]
17	[redacted]	2/24/2023	11/27/2022	[redacted]	[redacted]
18	[redacted]	1/17/2023	4/21/2022	[redacted]	[redacted]
19	[redacted]	5/5/2023	2/8/2023	[redacted]	[redacted]
20	[redacted]		3/8/2023	[redacted]	[redacted]
21	[redacted]	6/15/2023	11/24/2021	[redacted]	[redacted]
22	[redacted]	9/1/2023	5/29/2023	[redacted]	[redacted]
23	[redacted]	1/5/2023	11/15/2022	[redacted]	[redacted]
24	[redacted]	1/31/2023	11/22/2022	[redacted]	[redacted]
25	[redacted]	3/14/2023	12/15/2022	[redacted]	[redacted]
26	[redacted]	1/30/2023	4/17/2022	[redacted]	[redacted]