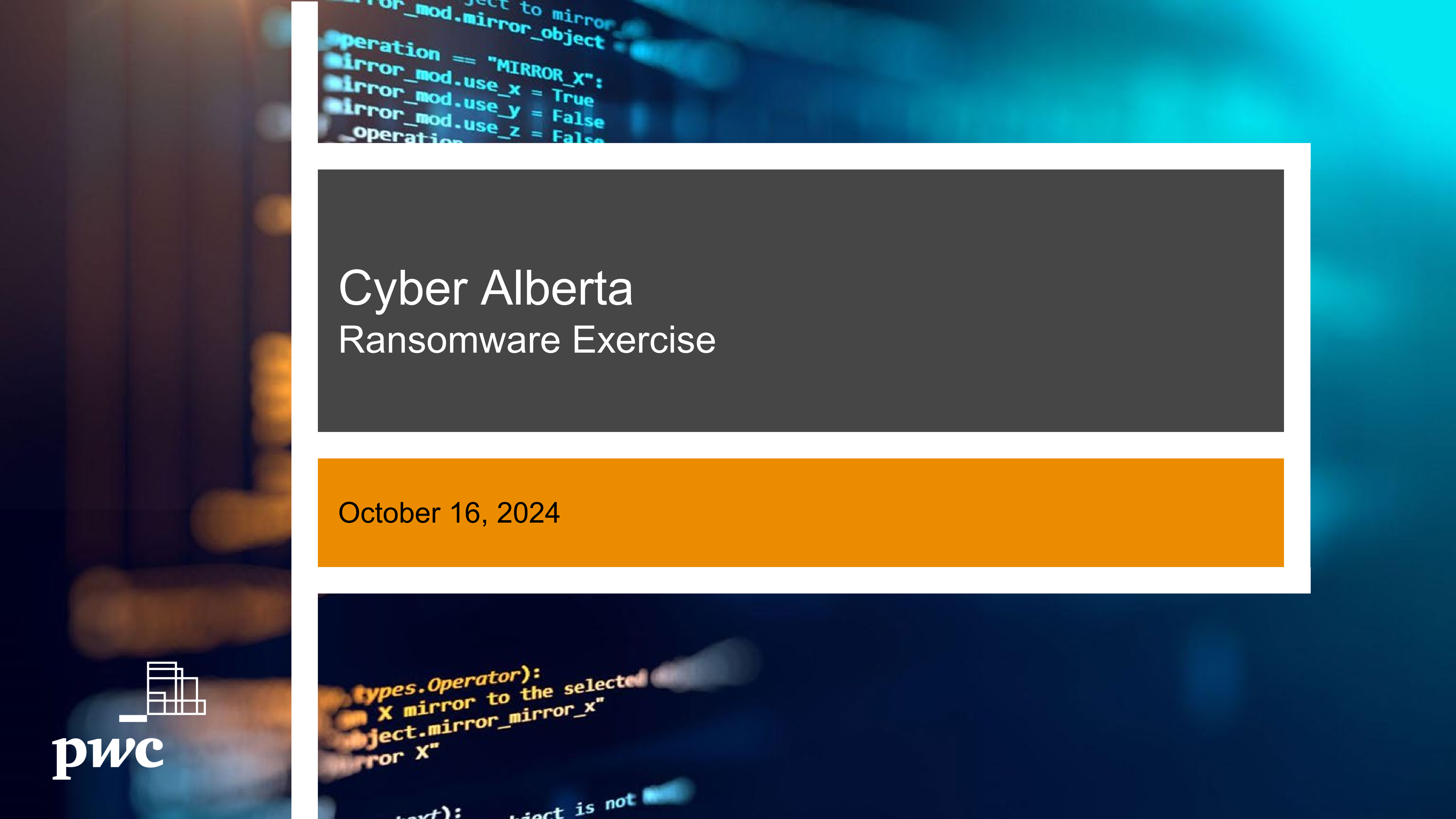


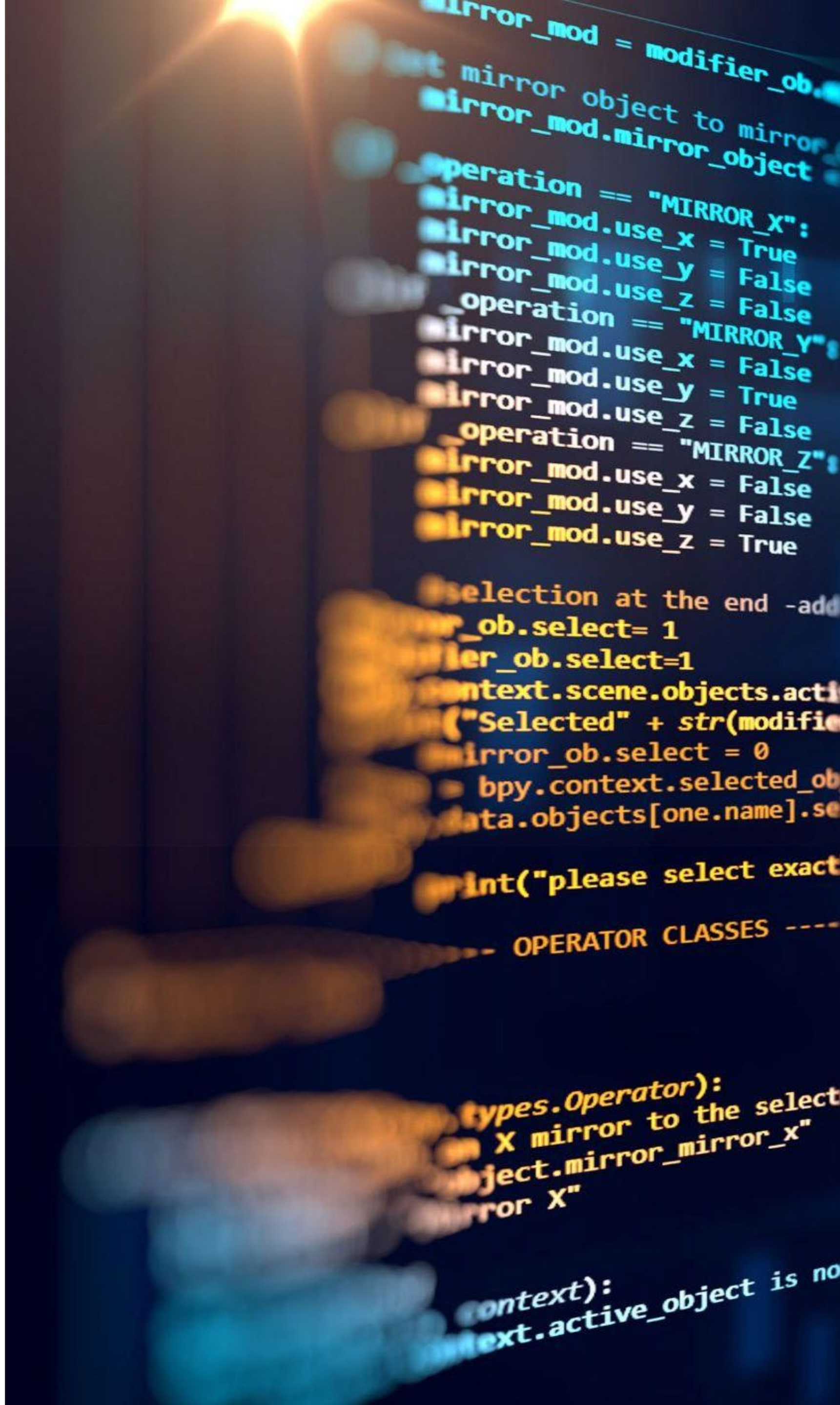
Cyber Alberta

Ransomware Exercise

October 16, 2024

Agenda

Time	Activities
5 minutes	Welcoming Remarks and Introductions
15 minutes	Exercise Briefing
85 minutes	Exercise
15 minutes	Exercise Debrief and Wrap-up



```
irror_mod = modifier_ob
mirror object to mirror
irror_mod.mirror_object
peration == "MIRROR_X":
irror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
 operation == "MIRROR_Y"
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
 operation == "MIRROR_Z"
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True

election at the end -add
_ob.select= 1
ier_ob.select=1
ntext.scene.objects.acti
("Selected" + str(modifie
irror_ob.select = 0
 bpy.context.selected_ob
ata.objects[one.name].se

int("please select exact

- OPERATOR CLASSES ----

types.Operator):
 X mirror to the select
ject.mirror_mirror_x"
rror X"

ontext):
xt.active_object is no
```

Ransomware Overview

Ransomware has evolved into a complex extortion scheme in which criminals not only use ransomware encryption to encrypt victims' data, but also use a range of other extortion measures to force victims to comply with demands.

1. Loss or destruction of crucial information

Ransomware can have a devastating effect on the company and most often results in enormous data loss even with proper backup procedures in place.

2. Business Downtime

Ransomware can severely impact a company, leaving it vulnerable, requiring some time to recover and implement safeguards to prevent the incident from happening again.

3. Loss of Productivity

With the company in the process of recovering from reputational and financial loss, they will find it hard to execute on value propositions resulting in a further loss in productivity.

4. Reputational Damage

Major incidents such as these risk damage to the reputation and brand of the organization resulting in loss of revenue and increased operating costs.

5. Data Exfiltration & Privacy

Sensitive data and personal information is commonly exfiltrated for the purposes of extortion. Data exposure could lead to regulatory concerns, reputational damage, and loss of public trust.

Goals & Objectives

Overall Goal

To engage in meaningful discussion that enables participants to increase awareness of response and recovery protocols, and identify learnings to minimize business disruption from a cyber incident involving ransomware.

Objectives of this Exercise

- Practice roles, responsibilities, key decisions, actions, and information needed to respond to a cyber incident
- Consider the impact to business operations and functions in the event of an incident
- Set and manage stakeholder expectations
- Practice quick and critical decision-making
- Validate the communications process and channels in a crisis
- Validate the usability of incident response activities and materials, and identify areas for improvement

Exercise

Move 1

Initial Situation

Move 1

Initial Situation Evaluation

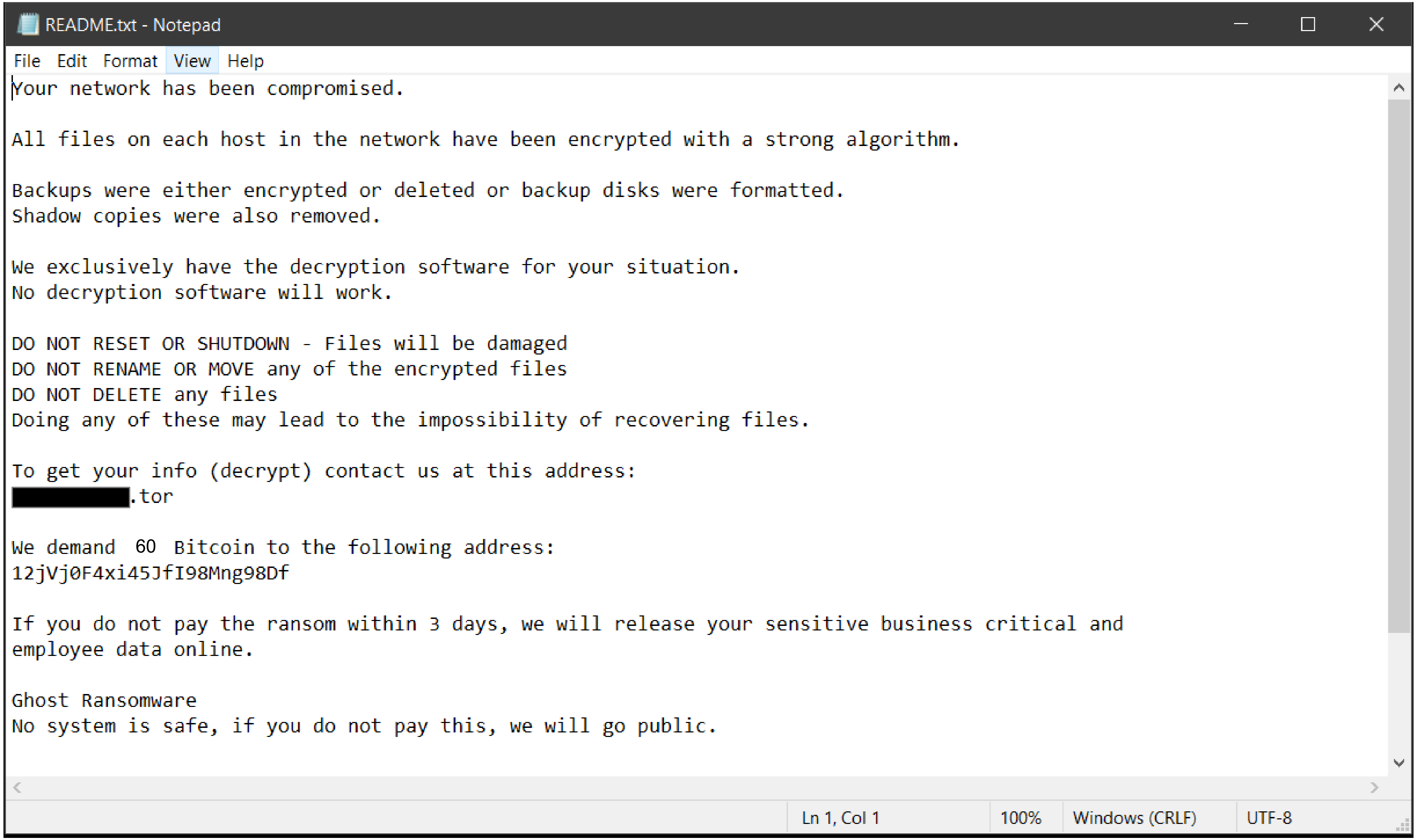
Date: Friday
Time: 12:30

Early today, there had been reports from staff stating that they had been experiencing a series of issues with it's IT infrastructure.

It began at 6 am this morning when staff lost access to a critical IT system. The functions that have been impacted are affecting our operational capability. Based on the current preliminary investigation, we uncovered that these servers are fully encrypted. Due to this encryption, we cannot use or access any information on them.

We have uncovered a ransom note with a payment demand of $5 million CAD, the ransom note is attached.

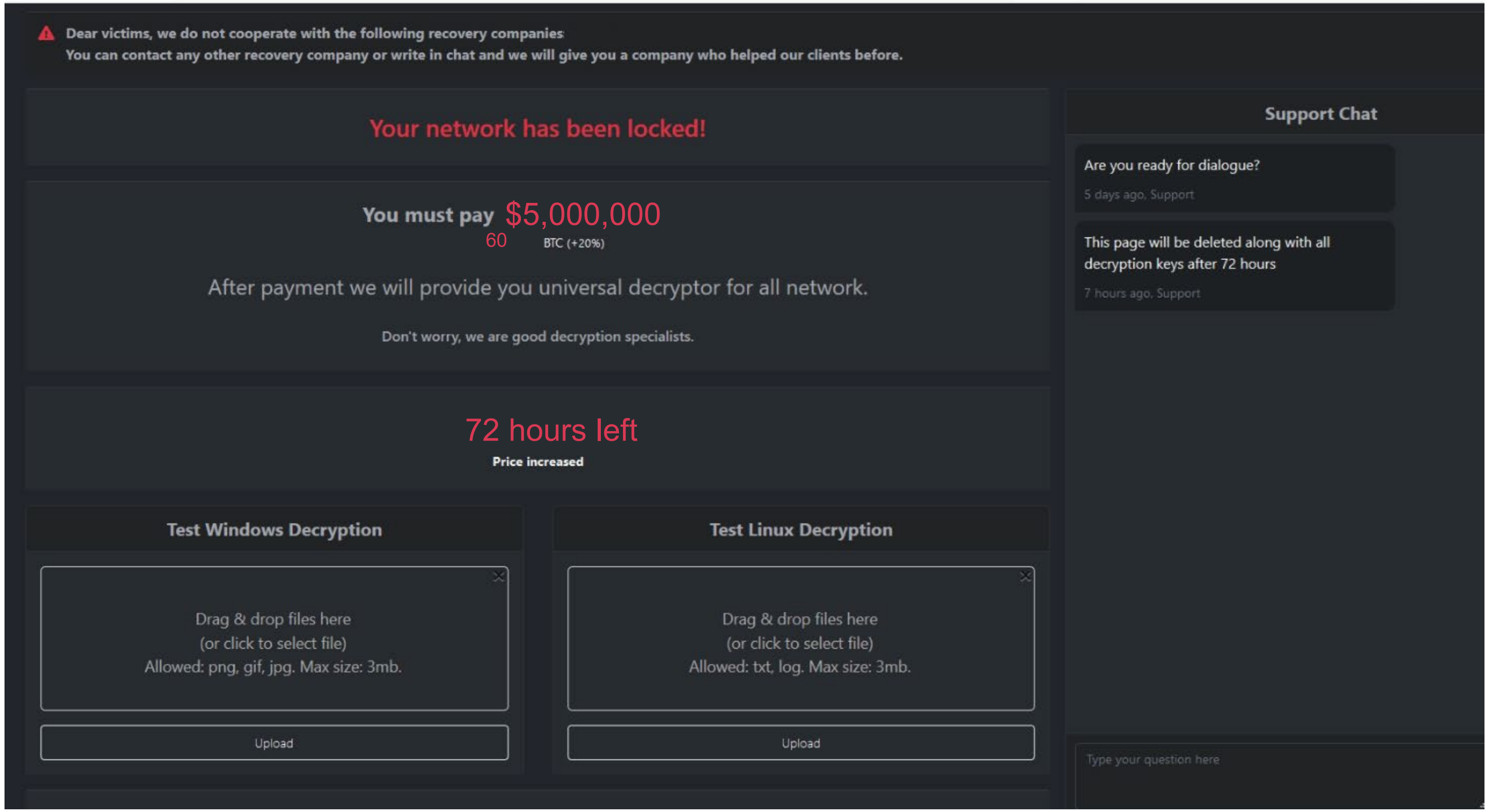
Ransom Note



```
Your network has been compromised.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies were also removed.

We exclusively have the decryption software for your situation.
No decryption software will work.

DO NOT RESET OR SHUTDOWN - Files will be damaged
DO NOT RENAME OR MOVE any of the encrypted files
DO NOT DELETE any files
Doing any of these may lead to the impossibility of recovering files.

To get your info (decrypt) contact us at this address:
[redacted].tor

We demand  60  Bitcoin to the following address:
12jVj0F4xi45JfI98Mng98Df

If you do not pay the ransom within 3 days, we will release your sensitive business critical and
employee data online.

Ghost Ransomware
No system is safe, if you do not pay this, we will go public.
```

This is a fictional scenario. To be used for educational purposes only.

Landing Page



Dear victims, we do not cooperate with the following recovery companies:
You can contact any other recovery company or write in chat and we will give you a company who helped our clients before.

Your network has been locked!

You must pay $5,000,000
60 BTC (+20%)

After payment we will provide you universal decryptor for all network.

Don't worry, we are good decryption specialists.

72 hours left
Price increased

Test Windows Decryption

Drag & drop files here
(or click to select file)
Allowed: png, gif, jpg. Max size: 3mb.

Test Linux Decryption

Drag & drop files here
(or click to select file)
Allowed: txt, log. Max size: 3mb.

Support Chat

Are you ready for dialogue?
5 days ago, Support

This page will be deleted along with all decryption keys after 72 hours
7 hours ago, Support

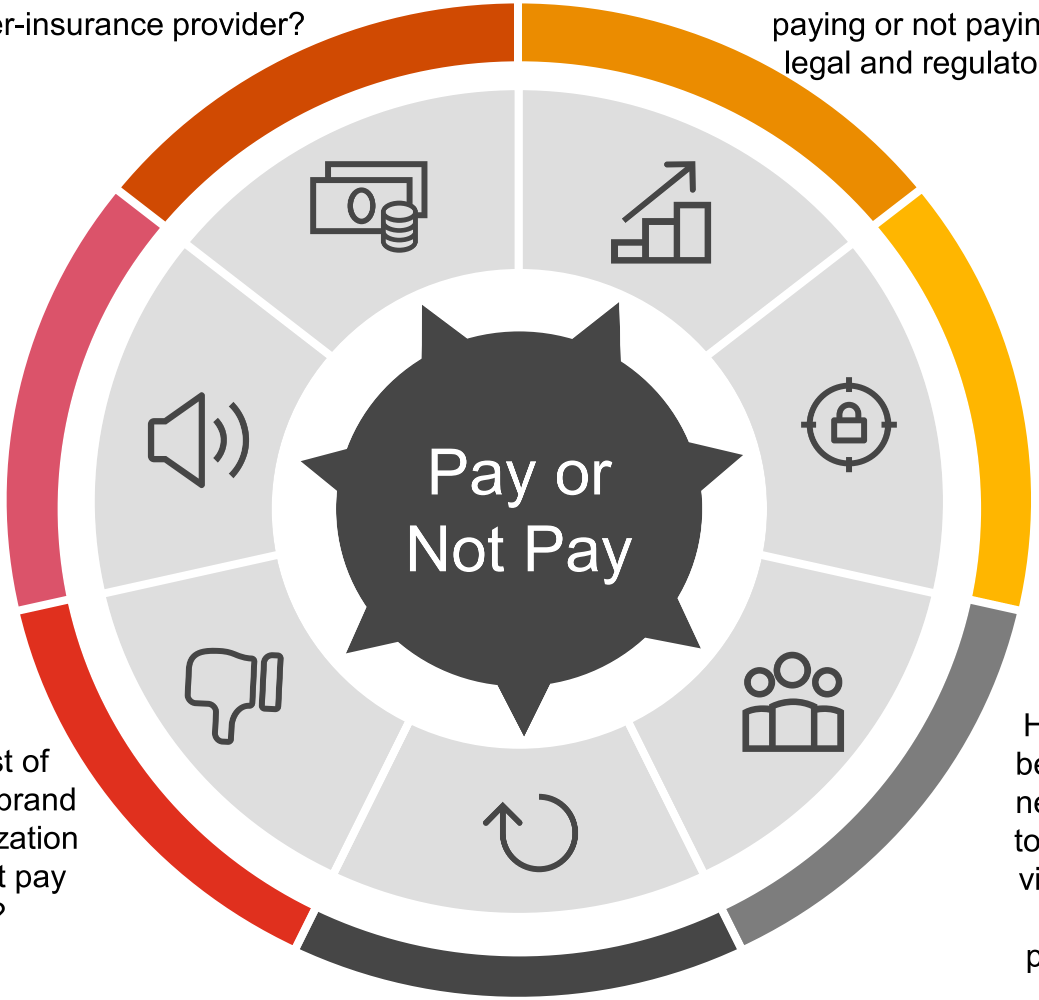
Key areas of focus

1. Do we preserve evidence, or should we focus on recovering?
2. Who would you contact?
3. Is there any notifications which must take place?
4. Are there any other stakeholders who would be included?
5. How will we establish and manage privilege and confidentiality?
6. What should be documented, when should we start documenting, and who would do the documentation?
7. Are there any urgent communications that are required (internal or external)? If so, to whom?

Ransom Payment

High level considerations for ransom payment

The decision to pay a ransomware demand must be taken carefully, with acknowledgement and acceptance of risks and in concert with various stakeholders – legal counsel, law enforcement, cyber insurance carrier, and security experts.



Will the organization pay out-of-pocket for this ransom payment or claim this amount with cyber-insurance provider?

Have you discussed payment with external legal counsel/breach coach to understand ramifications of paying or not paying including legal and regulatory issues?

If you make the payment, are you likely to receive the decryption key?

Has the organization been in contact with a negotiating third-party to cross-reference the viability of performing the ransomware payment transaction without being impacted by any regulatory fines?

Are system backups available and in good condition to recover?

What is the cost of reputational and brand damage if organization does or does not pay the ransom?

What is the cost and impact of downtime for business-critical services and crown jewels? Does this cost exceed the sum demanded by the ransomware?

Move 2

Data Exfiltration

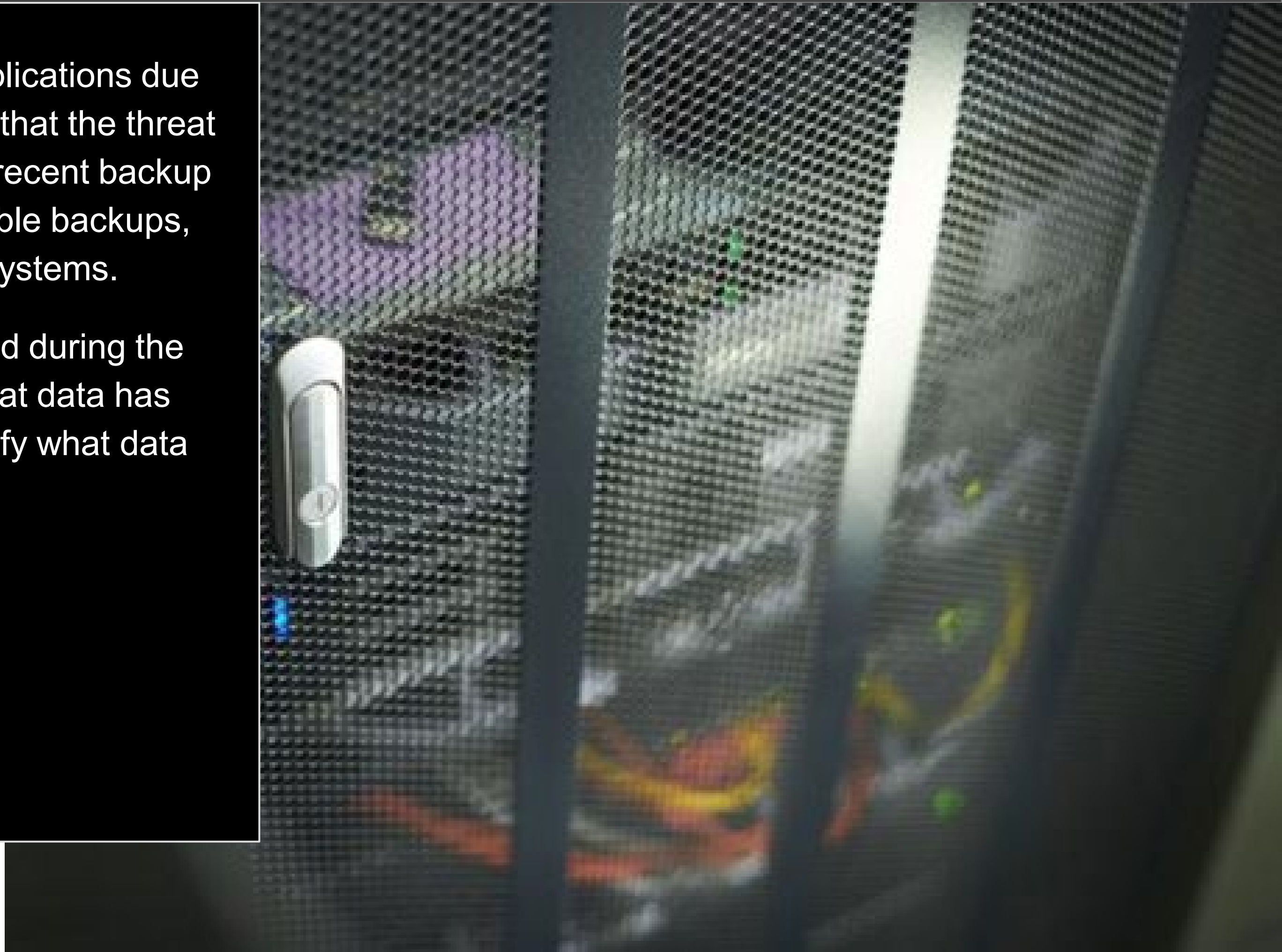
Move 2

Data Exfiltration

Date: Saturday
Time: 05:00

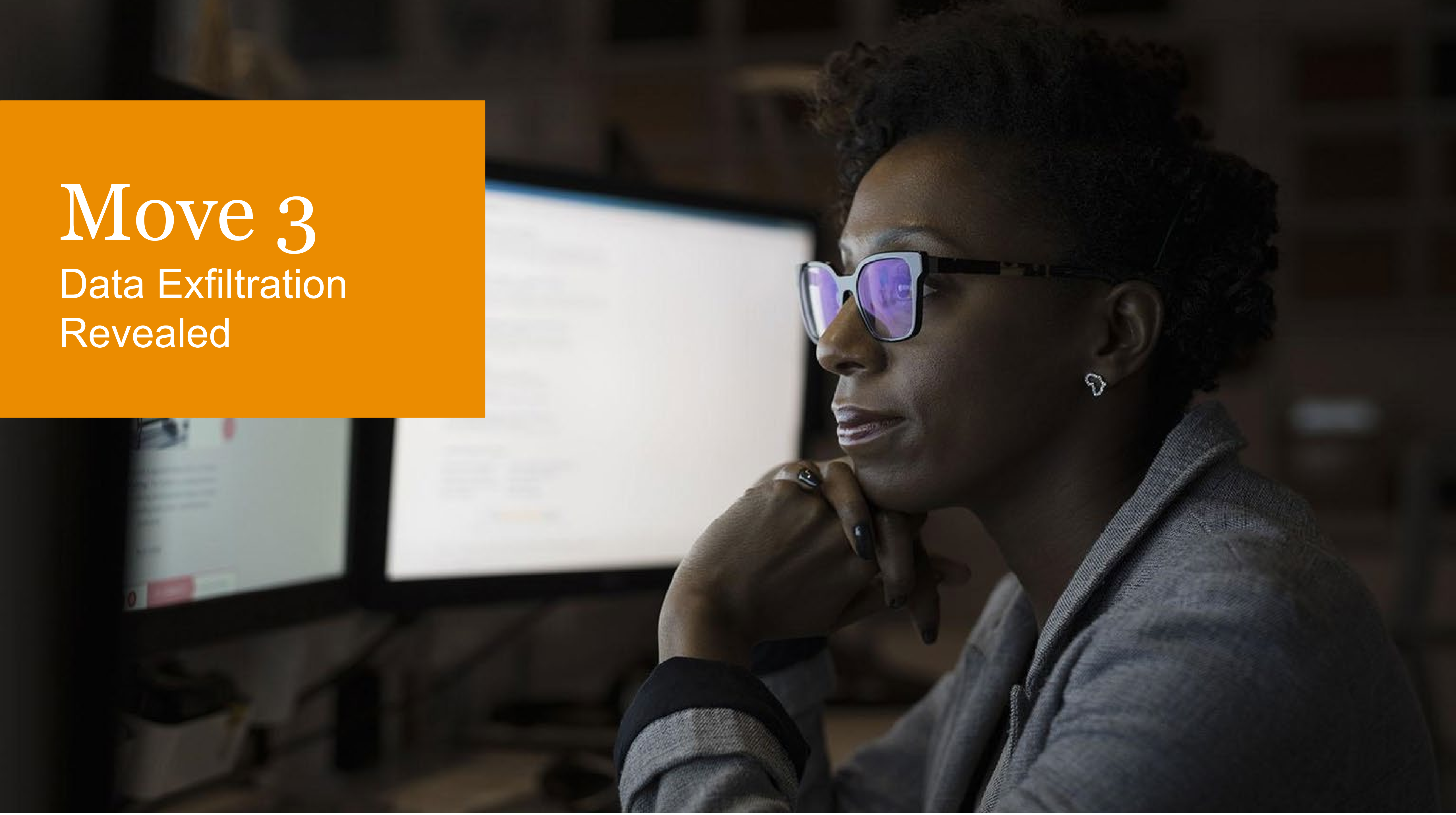
We have attempted to recover from backup, but there have been complications due to data in recent backups already having been encrypted. We suspect that the threat actor has been persisting in our network for up to a month resulting in recent backup corruption. Due to this, we may have to revert to historical and immutable backups, which could result in the loss of up to 30 days of data on the affected systems.

It was discovered that there was a large amount of data traffic outbound during the time of encryption. Due to the volume of data traffic, we also believe that data has been exfiltrated from our system. Currently, we are attempting to identify what data has been exfiltrated.



Key areas of focus

1. What are your primary concerns relating to data exfiltration?
2. What are the thoughts on a proactive vs reactive communications strategy?
3. Is the recovery timeline a concern? How much damage would 30 days worth of lost data cause?
4. Are there any solutions which can be implemented during the downtime?
   a. What is your current contingency strategy?
5. Do additional supporting roles need to be included in the response effort? Why would this addition be considered a requirement?
6. Are there any third parties that need to be advised due to the breach?



Move 3

Data Exfiltration Revealed

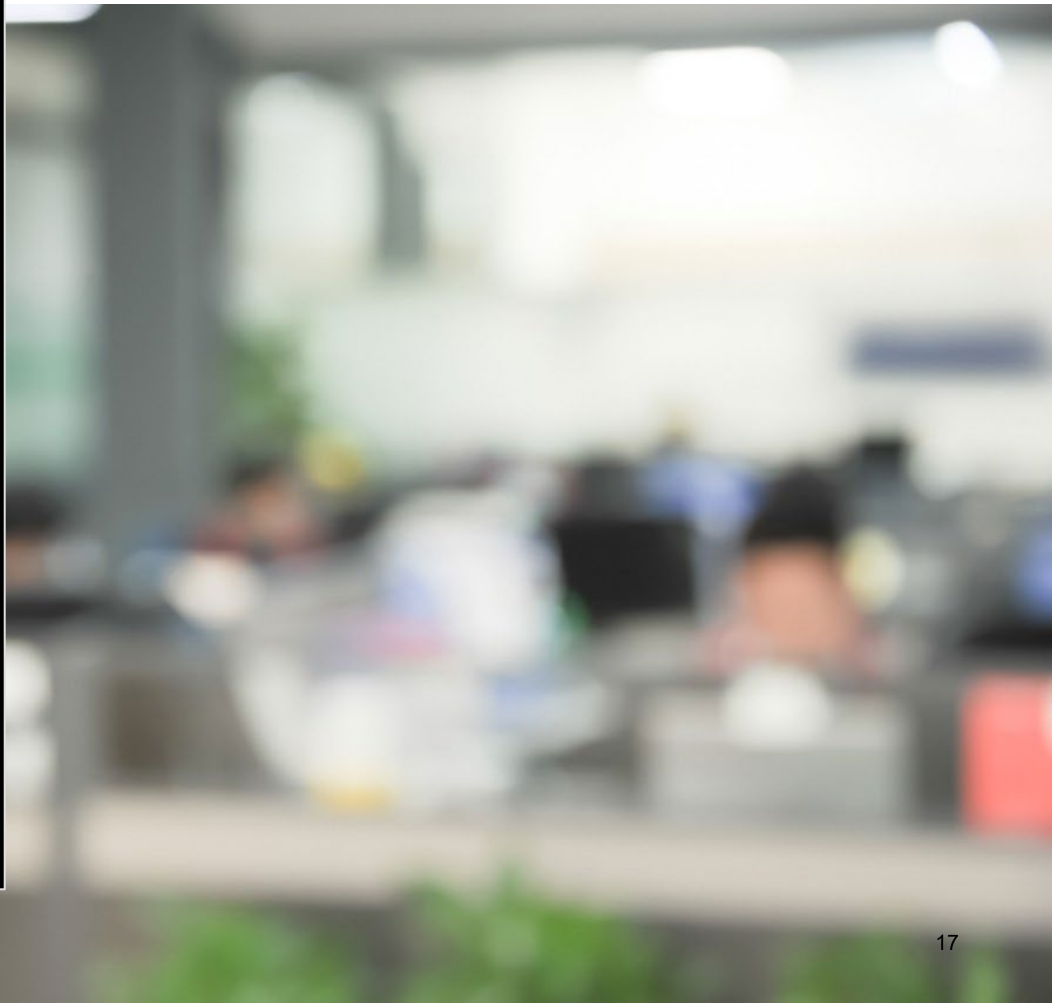
Move 3

Data Exfiltration Revealed

Date: Friday
Time: 20:45

Through our analysis, we have concluded that the attacker has extracted sensitive data that contains Personally Identifiable Information (PII).

We are not entirely sure how much data the threat actor has, but we have confirmed multiple types of PII were on the impacted systems.



Key areas of focus

- Have you revised your communications strategy with the new information?
  - What updates will you provide key internal/external stakeholders?
- What are the new risks associated with the exfiltration PII?
- Are you in breach of any of our contract or regulations as a result of the incident?
- What support is required for the affected stakeholders?
  - How will you communicate to stakeholders that their data is safe?
- Should you involve the media at this point?
- What are your information gaps?
  - What other items need to be addressed?

Move 4

Data Leaks

Move 4

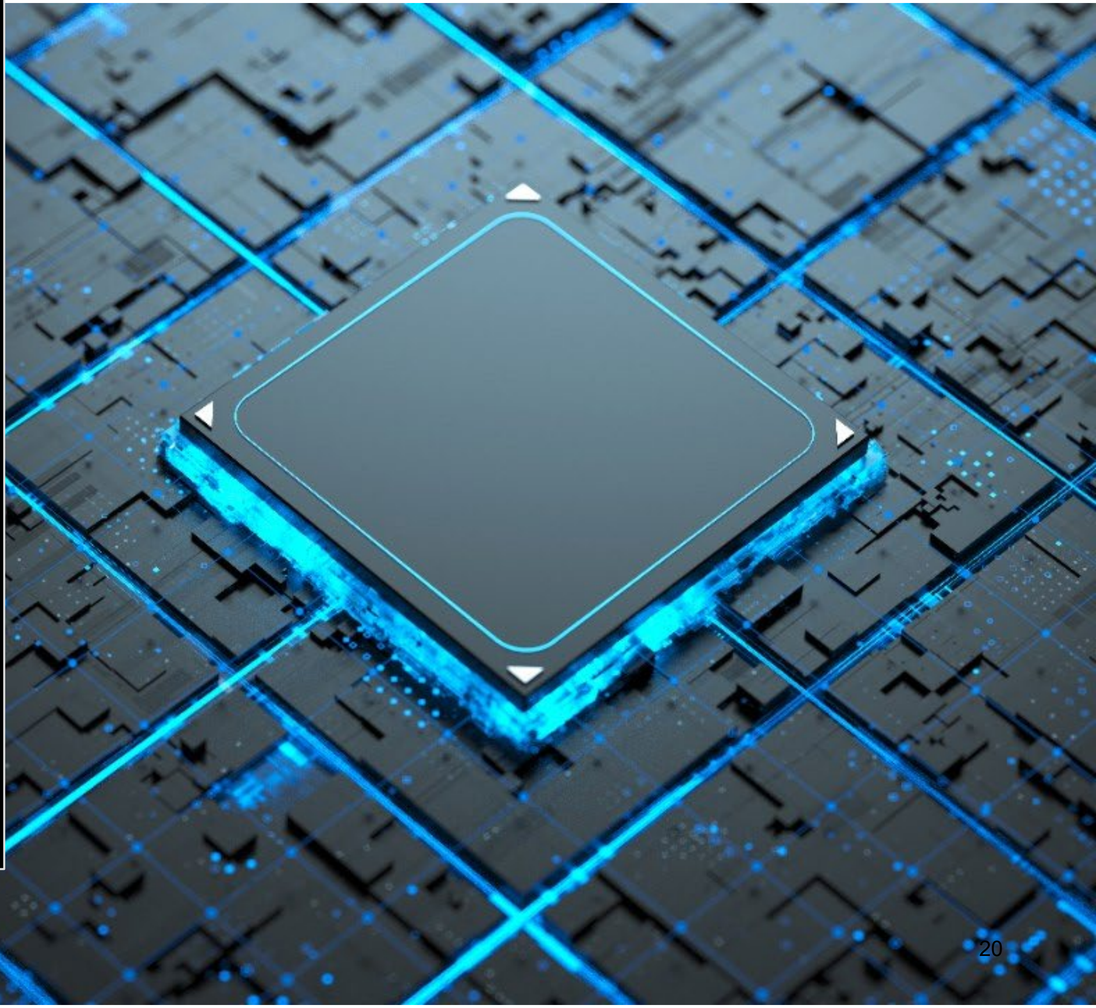
Data Leaks

Date: Saturday
Time: 20:00

The Executive team asked their incident response team to perform a search on the dark web relating to the data breech.

The investigators located a dark web data leak site. This site states that 10% of the exfiltrated information has been made available, and they will release the other 90% unless payment is made.

The information has been reviewed and it appears that is contains PII.



Key areas of focus

1. Are there regulatory concerns or notification requirements?
2. What new risks were introduced with the data exfiltration?
   a. How damaging would it be if all this information was leaked?
   b. What is the risk of the PII residing on the dark web?
3. Is there a reputational impact concern?
4. What support would you provide to the people affected?

Move 5

Media Engagement

Move 5

Media Engagement

Date: Sunday
Time: 11:00

The communications and marketing team have identified that **posts on social media** have started to increase relating to the breach. There is a possibility that an employee leaked the information online, either on purpose or by accident. **Media inquiries begin to pour in.**

LIVE
BREAKING NEWS
CYBER BREACH
13:51
RANSOM DEMANDED, CONFIDENTIAL DATA RELEASED, IF YOUR DATA AT RISK?

Canadian Exclusive

FOR TRAINING PURPOSES

Key areas of focus

1. How will the organization respond to the media reports? Who will be responsible to respond?
2. How will we address member/employee concerns?
3. What would be the impact to brand reputation?
4. Do we communicate that we are the victim of a cyber attack? What does the messaging look like?

Exercise Debrief

Exercise debrief

How did the exercise go?

What went well and what could have been done better?

What did you learn?

How can you improve your response next time?

Do you have any feedback for us?