



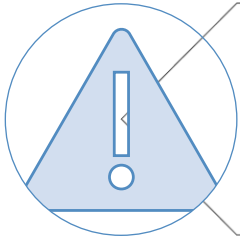
Alpine Privacy Days

MANAGING GLOBAL DATA BREACHES

Kate Brader, Partner

FTI Head of Crisis

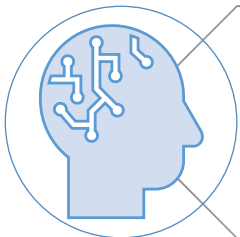
TODAY'S SESSION – 1 HOUR



Communicating Through a Cyber Crisis



Data Breach Simulation: Key Decision Points



Looking Ahead & Questions



THE CYBER LANDSCAPE

NEWS

[Home](#) | [InDepth](#) | [Israel-Gaza war](#) | [War in Ukraine](#) | [Climate](#) | [UK](#) | [World](#) | [Business](#) | [Politics](#) | [Culture](#)[Technology](#)

Don't blame us for people suffering - London hospital hackers



| The hackers' logo as it appears on their darknet website

Joe Tidy

Cyber correspondent, BBC World Service

[@joetidy](#) >



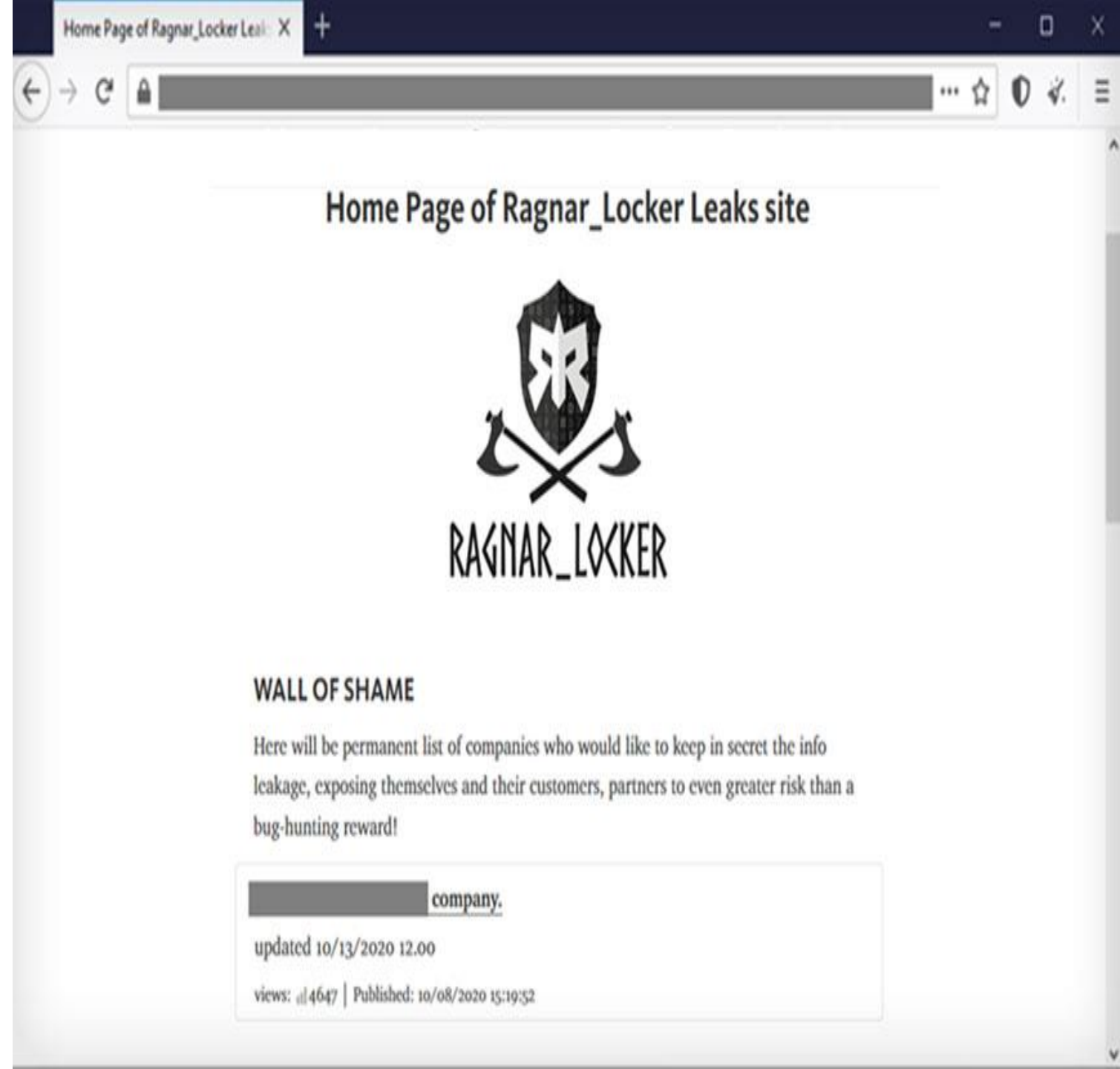
COMMUNICATING DURING CYBERSECURITY CRISES

‘GOING PUBLIC’ NO LONGER IN YOUR CONTROL

Used to be an element of control around if and when you confirmed publicly that you had been subject to a cyberattack.

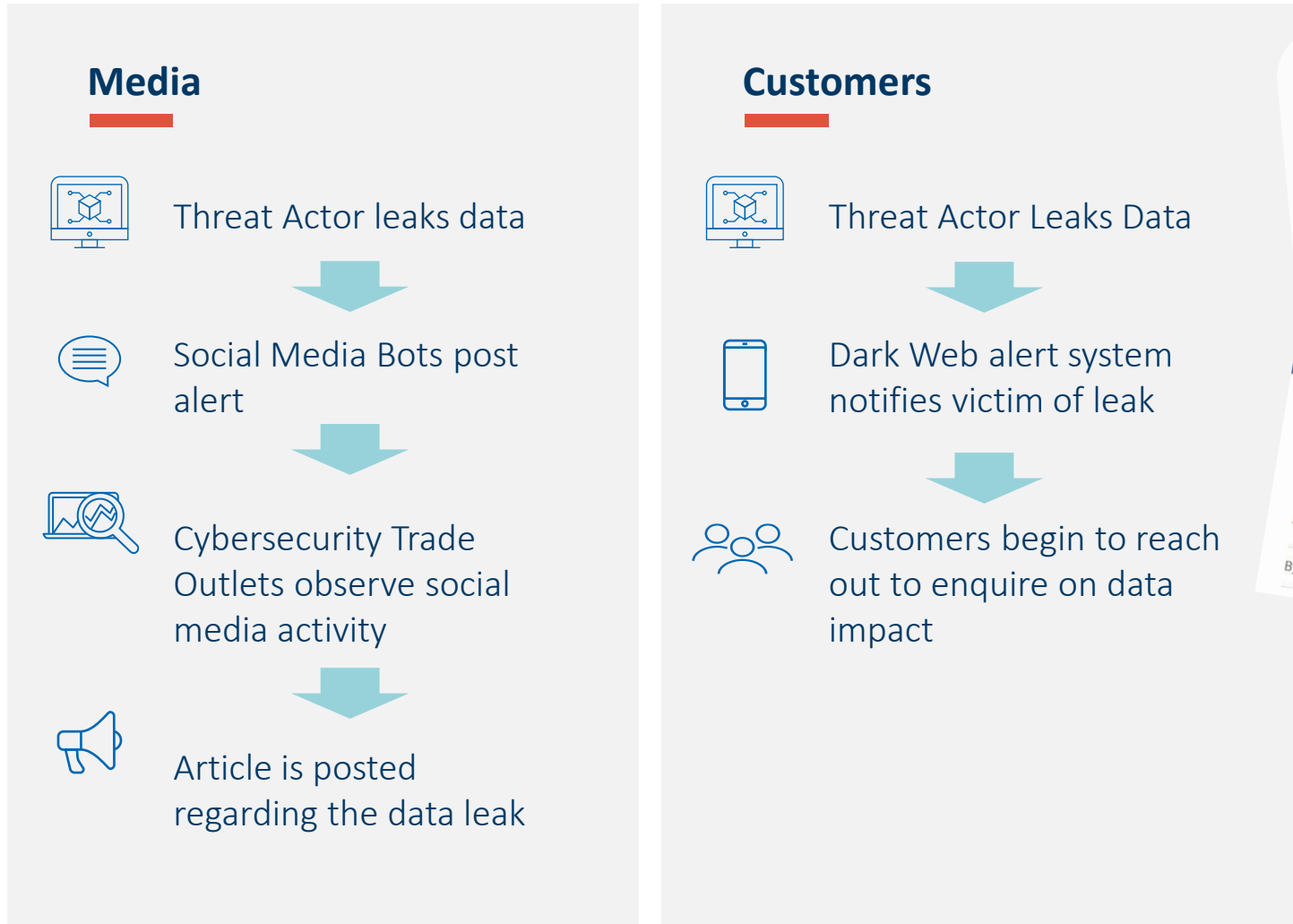
Increased used of “Shame Sites” and other more aggressive tactics becoming the norm.

Combined with greater regulatory compulsion to share the information – particularly for listed entities.



AGGRESSIVE EXTORTION TACTICS – A CLOSER LOOK

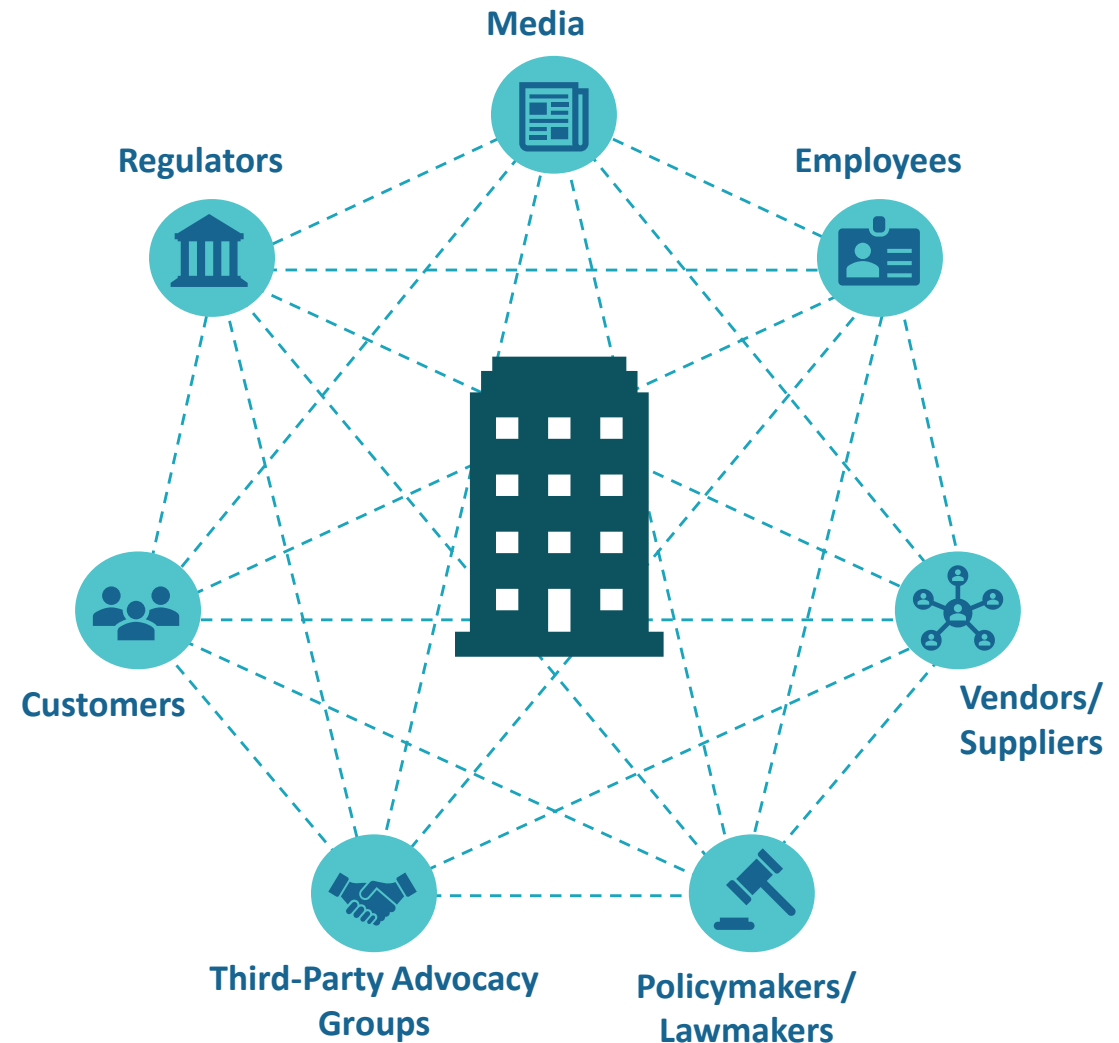
Once the Threat Actor leaks data to the dark web, it sets off a chain reaction of events that require stakeholder-specific communications materials to address enquiries and ensure there is no misinformation regarding the leak.



MULTI-STAKEHOLDER CONSIDERATIONS

It's imperative to know what to say, how and when to say it, and to whom.

- Likely influx of stakeholder enquiries related to the incident
- Customers, employees and/or vendors based in multiple countries or jurisdictions may be affected
- Rumours should be addressed rapidly and effectively
- Specific information is not always available – both immediately after and in the weeks following
- Potential for follow-on litigation and/or regulatory ramifications
- Negative impact to reputational branding and, ultimately, company bottom line



STAKEHOLDER PERCEPTIONS ARE EVOLVING

1 Timely information sharing expected – particularly in FS

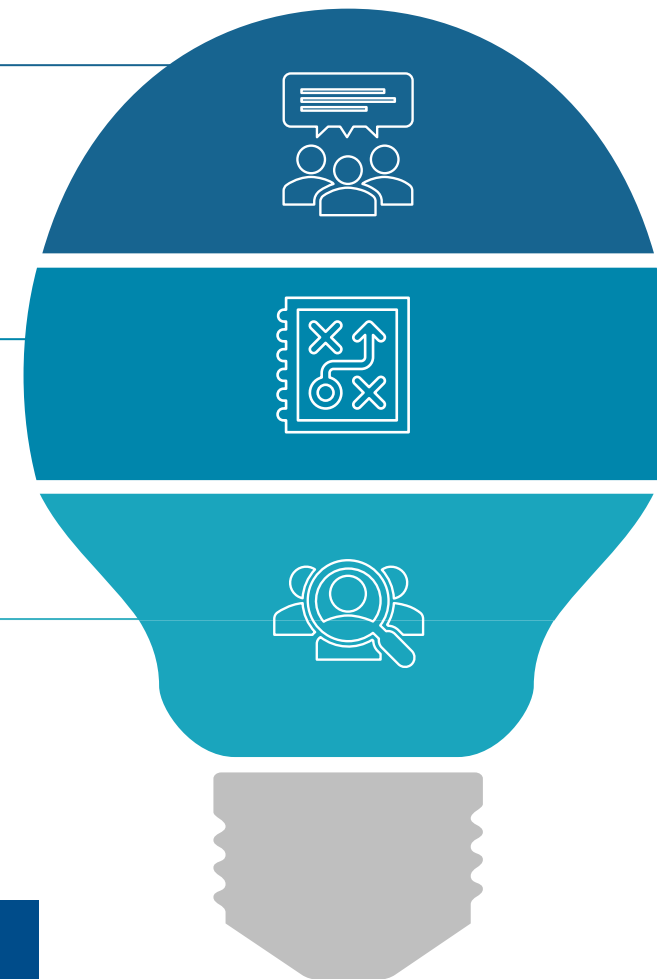
The expectations placed on an organisation that experienced a cyberattack have evolved over recent years. Stakeholders expect to be informed of an incident in a timely manner, with transparency about what information is known and frequent updates throughout the investigative process.

2 Threat Actors Manipulative – Social Engineering

Threat actors' evolving communications tactics have changed how we previously thought of cyber communications. The cybercriminal organisations responsible for many cyberattacks are nimble and creative about how they choose to add pressure on their targets.

3 Media less important as a stakeholder

At a time when cyberattacks seemingly pervasive, there has been a sense of “breach fatigue” among media, which has shifted communications priorities. Stakeholders, such as customers, expect to hear directly from impacted companies, which can no longer rely on the press to drive messages.

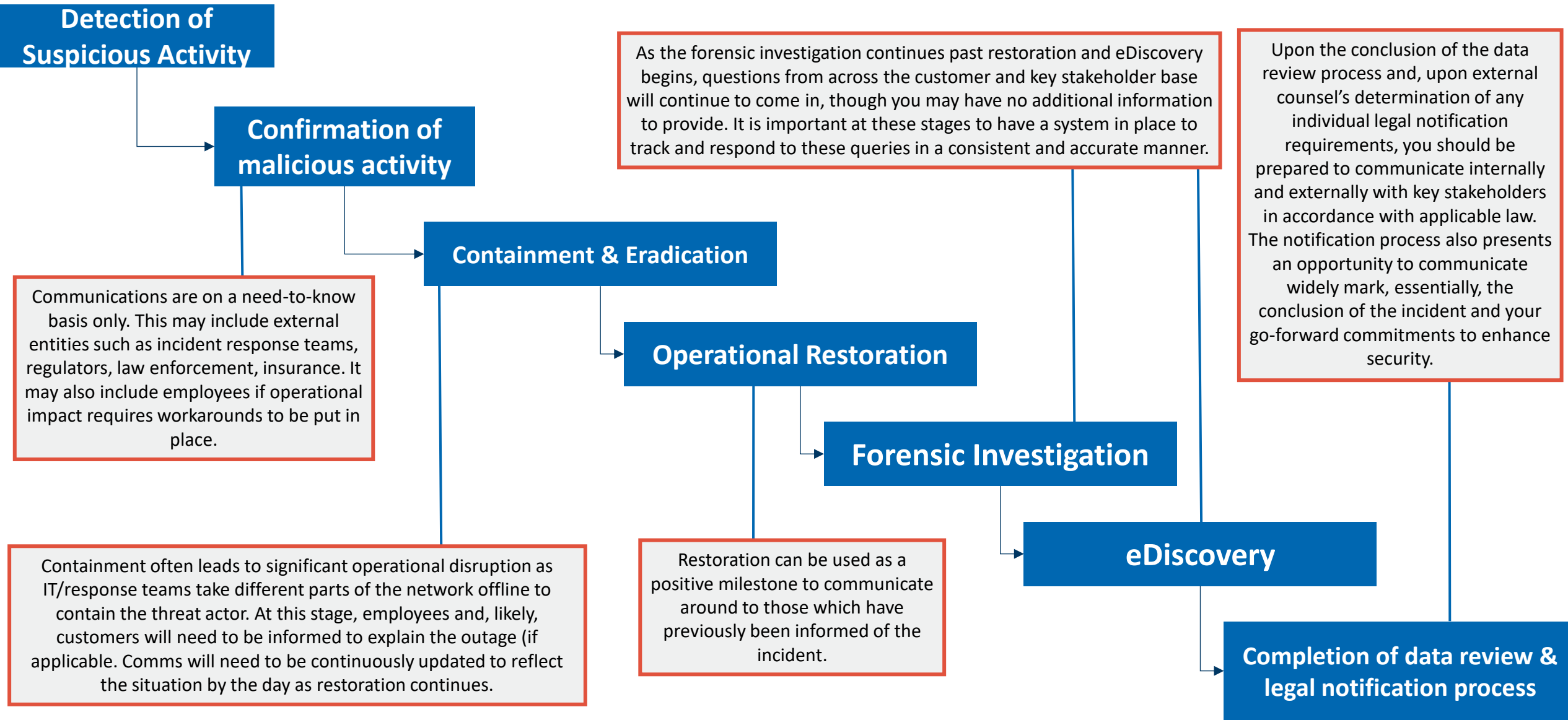


Key Takeaway:

Criminals have PR departments and stakeholders demand engagement. The cyber communications world has shifted irreversibly.

KEY POINTS OF A RANSOMWARE INCIDENT

One of the common high-profile ways of a data breach occurring is a ransomware incident in which the cybercriminal exfiltrates data in order to extort the victim by requesting payment in exchange for deletion of the data and/or by selling the data to the highest bidder on the dark web.

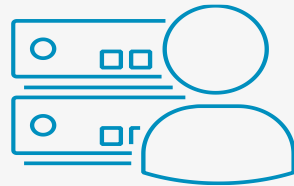


INCIDENT RESPONSE COMMUNICATIONS CORE PRINCIPLES



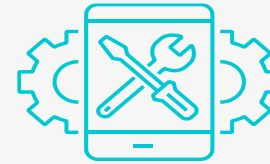
Security

Communicating externally prior to containment creates additional risk



Stakeholder Trust

Communicate actionable information to key stakeholders (business partners, team members, shareholders)



Accuracy

Our communications strategy is only as good as the facts on the ground



Transparency

Convey honesty, while balancing transparency and risk

WHAT DOES SUCCESS LOOK LIKE?

Success Metrics:

1. Preserve stakeholder trust and protect brand reputation
2. Limit legal risk, to the extent possible
3. Protect long-term impacts to stock price
4. Preserve “licence to operate”

The Realities...

- ***Bad news is a given*** – keep news cycles limited and don’t “break into jail”
- ***Lawsuits may be inevitable*** – minimize legal liability through accuracy and a “depersonalised” approach
- ***Financial impacts are likely*** – reduce risk by communicating the right information to the right stakeholders, projecting clarity and not panic, and demonstrating a competent approach to remediation and stakeholder engagement
- ***Criticism from stakeholder groups should be expected*** – maintain stakeholder trust through providing timely and accurate messaging, responsive actions and actionable information



DATA BREACH SIMULATION

INSTRUCTIONS AND CONSIDERATIONS

- 1. For the purpose of this exercise, we ask that you suspend disbelief under the circumstances presented.** The developments that we will present today would typically occur over a period of days or weeks, rather than just a couple of hours.
- 2. This exercise is limited to the participants present in the room.** For each inject, tables must act as a team to discuss how Brader International should respond.
- 3. We suggest taking notes around decision making, actions taken and messaging.** Artificial Intelligence is an emerging field with clear, formidable consequences. Being prepared for navigating a crisis like the one we are simulating today is critical.

Setting the Stage

Brader International is a large **international bank** headquartered in Zuoz. Like many other companies, BI integrated an **AI-powered identity verification and authentication system** (IVAS) for its mobile application within the last two years. In addition to users accessing their accounts through this system, it is also used for a number of automated decision-making processes including fraud detection and risk scoring.

For the following slides, the participants at your table must act as a team to determine how Brader International should respond to each trigger. Throughout this simulation, please consider your actions and responses as the Business Continuity Management team.

INJECT 1: THE RANSOM

- The Head of Information Security received a **critical alert** from the IVAS indicating a **spike in authentication failures** across multiple regions, including the UK, EU, and North America
 - Users are reporting being locked out of their accounts
 - Others are claiming their accounts have been accessed by an unauthorized party
- The Security Operations Center (SOC) submits a report that the IVAS database **shows evidence of being tampered with**
 - The IVAS contains the following sensitive data:
 - **Biometric Data**
 - Facial Recognition
 - Voice authentication
 - **Personally Identifiable Information**
 - Names
 - Emails
 - Dates of birth
 - In addition, access to credential through the IVAS could give a malicious actor access to **financial information**
 - The team cannot yet confirm any specifics around data impact

- A well-known cybersecurity researcher and journalist has posted the following on X:



- Employees in the IT and SOC have begun speculating that this story is about Brader International
- The following ransom note has been sent to Brader International directly

RANSOM NOTE SENT DIRECTLY TO BRADER INTERNATIONAL

We' ve had a good laugh. Your "advanced" AI authentication system? Pathetic. It took us a matter of minutes to break through your defenses. You were too busy patting yourselves on the back, thinking you were untouchable.

You can' t even protect the most basic of data, and now everyone knows it. Accounts, biometric info, customer data—all of it is ours. But don' t worry. We' re not here to make you disappear. We just want to remind you that your security isn' t worth the bits it' s built on.

Here' s the deal:

- Pay us what we ask, and you' ll never see this mess again.
- Fail to comply, and we' ll make sure the world knows just how weak your systems are. The press will eat this up. We' re sure your customers will love hearing how easily we walked in.

You' ve got 48 hours. No extensions. CHF2.5M.

Your move.
The Jackal



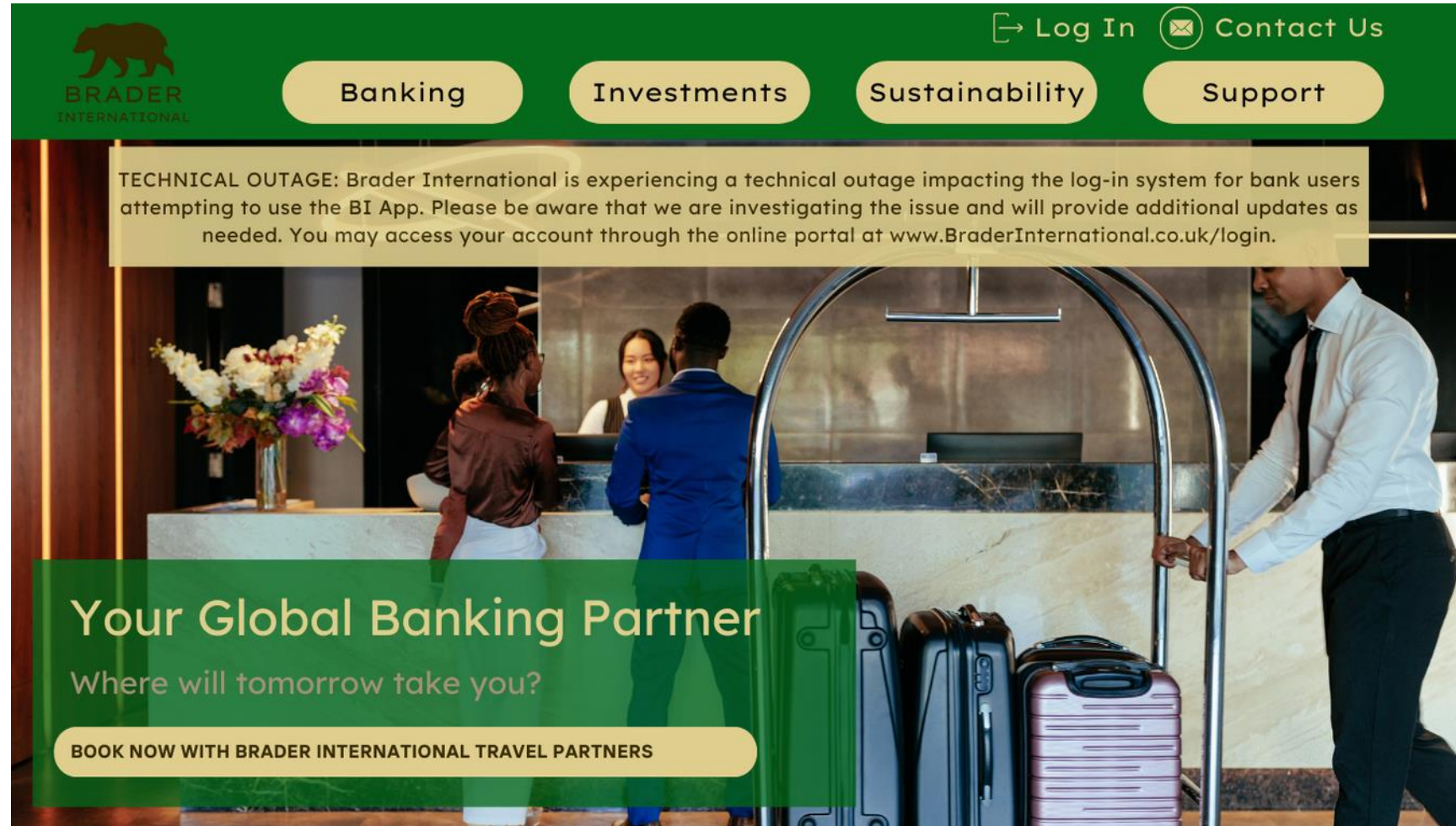
QUESTIONS FOR DISCUSSION

- Which internal and/or external teams should you be engaging with at this point?
- Do you have regulatory requirements at this stage?
- Would you like to take any steps to shut down the IVAS system? What are the risks of keeping it online versus shutting it down?
- Will you pay the ransom? What factors would influence this decision?
- Should you be communicating with any stakeholders proactively at this point?
- Are you going to contact the journalist?
- How are you handling the employee chatter and speculation, if at all?
- Are there contractual obligations you need to think about at this point?



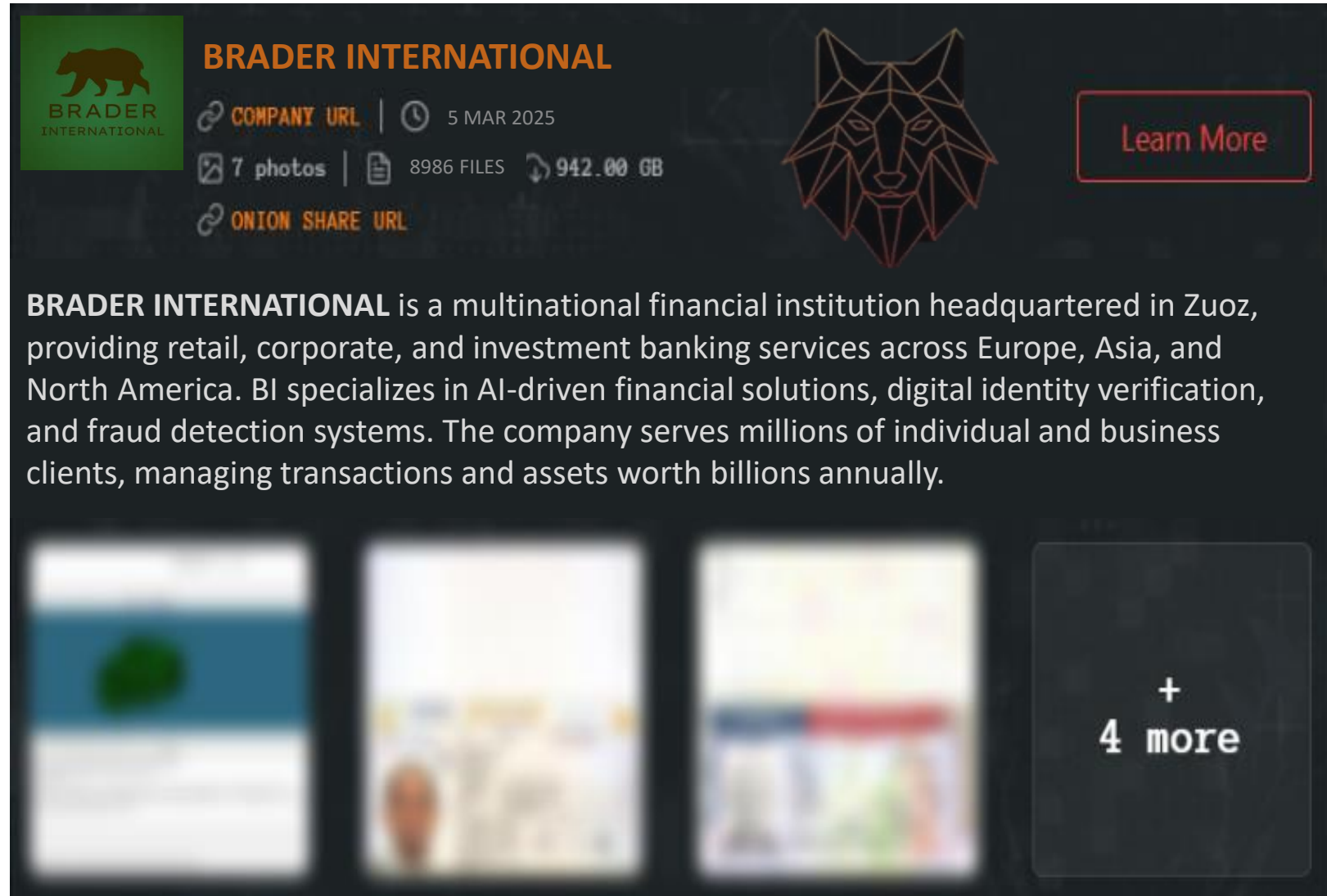
INJECT 1: KEY DECISIONS

- A leading third-party cybersecurity firm has been engaged to assist in the investigation – they are currently **working to contain and eradicate** the threat actor from your system
- The IVAS system has **not** been shut down pre-emptively
- You have **not engaged** with Julie Albright and you have decided **not to pay** the ransom.
- A **briefing** has been provided to the ELT, customer-facing employees have been given **talking points**, and the following **website statement** was posted:



INJECT 2: DATA PUBLISHED

- The Jackal has **acted on its threat** to publish the stolen data
 - Initial investigation of the published data indicates **user PII** and potentially **financial information** including account numbers from personal account users across the **UK and EU** were involved
- Within moments of the publication of the data, Julie Albright (from X) **published** her story she teased two days prior at the onset of the incident
- The Threat Actor infiltrated the IVAS's fraud algorithm, leading to over **CHF800M in fraudulent charges from accounts** going through over the 7 days of access
- Social and traditional **media interest** has picked up significantly and **questions** from key investors, customers (both businesses and individuals), and regulators have been pouring in.



BRADER INTERNATIONAL

COMPANY URL | 5 MAR 2025

7 photos | 8986 FILES | 942.00 GB

ONION SHARE URL

[Learn More](#)

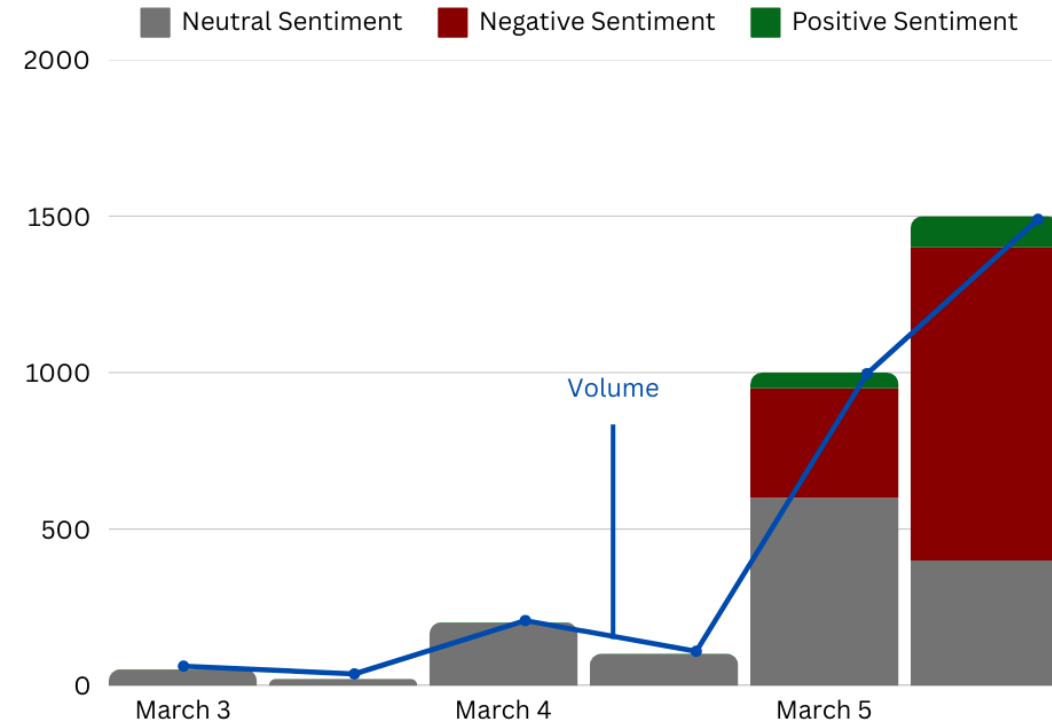
BRADER INTERNATIONAL is a multinational financial institution headquartered in Zuoz, providing retail, corporate, and investment banking services across Europe, Asia, and North America. BI specializes in AI-driven financial solutions, digital identity verification, and fraud detection systems. The company serves millions of individual and business clients, managing transactions and assets worth billions annually.

+ 4 more

QUESTIONS FOR DISCUSSION

- Has anything changed given this update:
 - Internal and external teams involved
 - Regulatory requirements
 - Stakeholders to communicate with proactively
 - Contractual obligations
- Are you going to pay individuals the CHF800M in fraudulent charges?
- How are you handling the increased public attention?
- How might your incident response strategy differ between the EU and UK markets?

MEDIA COVERAGE SINCE INCIDENT BEGAN





LOOKING AHEAD

LOOKING AHEAD, WHAT CAN WE EXPECT?



Cyber is a **business risk, not just an IT risk**. The response to evolving cyber threats requires **increased engagement** across the organisation and **synchronisation between business units** including IT, Risk, Governance and Communications



AI capabilities will continue to increase the **velocity** and **effectiveness** of attacks against institutions worldwide. Active Cyber Defence will require the incorporation of AI tools as standard to cohere and enable a robust response.



Consumers and data subjects are increasingly aware of the **key risks** and their **rights** during a data breach. Organisations will have to **think beyond standard responses** and consider alternate ways to reassure and protect



An **evolving regulatory landscape** will place a higher burden on organisations to **prepare, demonstrate** and **regularly audit** their preparation and response capabilities

WHAT YOU CAN DO NOW

➤ Establish relationships before the crisis

- Identify key external partners (insurance, legal, communications, forensics)

➤ Develop a plan

- Develop/enhance your incident response plan and related communications plan
- Establish appropriate governance structure

➤ Check for blind spots

- Refresh your data mapping to better understand what sensitive data is stored where

➤ Test and train to build muscle memory

- Practice operational downtime procedures
 - Continue to practice/test plans in customized tabletop exercises
-



Experts with Impact™