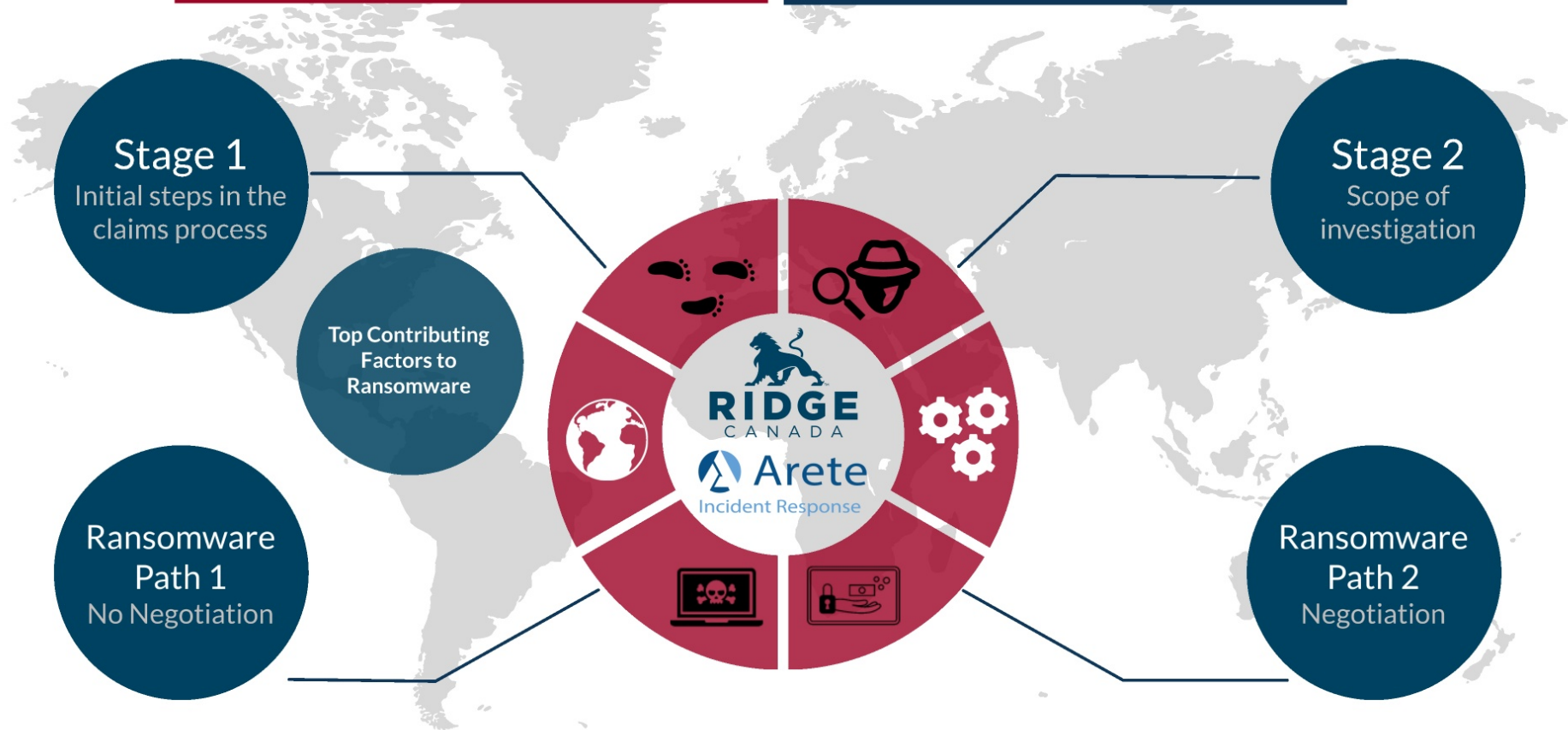


The Broker/Client Claims Journey

What to expect and do when dealing with
Business Email Compromise or Ransomware



Presented February 18, 2021 by:
Ryan Durrell - Axxima
Greg Markell - Ridge Canada Cyber Solutions Inc.
Jaycee Roth - Arete Incident Response
Sophia Kudlyk - Arete Incident Response

Stage 1

Step 1: Making Contact



Call the 24/7/365 line to engage the breach coach

- Advise you are a Ridge Canada client & have your policy number ready



Breach coach does a conflict check to ensure they can represent the client

- The conflict check typically takes less than an hour at which point the client will get a call back



Alert Ridge Canada of the potential claim

- Can be done by the broker

Consent
Checkpoint 1

Step 2

Stage 1

Consent Checkpoint 1: Approval of the Breach Coach

The **insurer** is party who approves and authorizes the appointment of the breach coach. Therefore the *insured* must obtain the **insurers** consent prior to making any formal arrangements with a breach coach



Ridge Canada approves appointment of the breach coach and the claim continues to move forward

Stage 1

Step 2: Assessment



Consent
Checkpoint 2



Breach coach speaks with the client to gather details about the incident and assess next steps



The breach coach provides guidance to the client and advises if forensics are required



Arete
Incident Response



If required, Statements of Work (SOWs) are created

Stage 1

Consent Checkpoint 2: SOW review & approval

The SOW outlines the scope of tasks and services the forensic firm plans to perform during their initial investigation. The **insurer** reviews the SOW to: 1) verify the scope of work is appropriate and in line with the policy; 2) costs are reasonable in the current market



Breach coach and client provide the SOWs to Ridge Canada for review

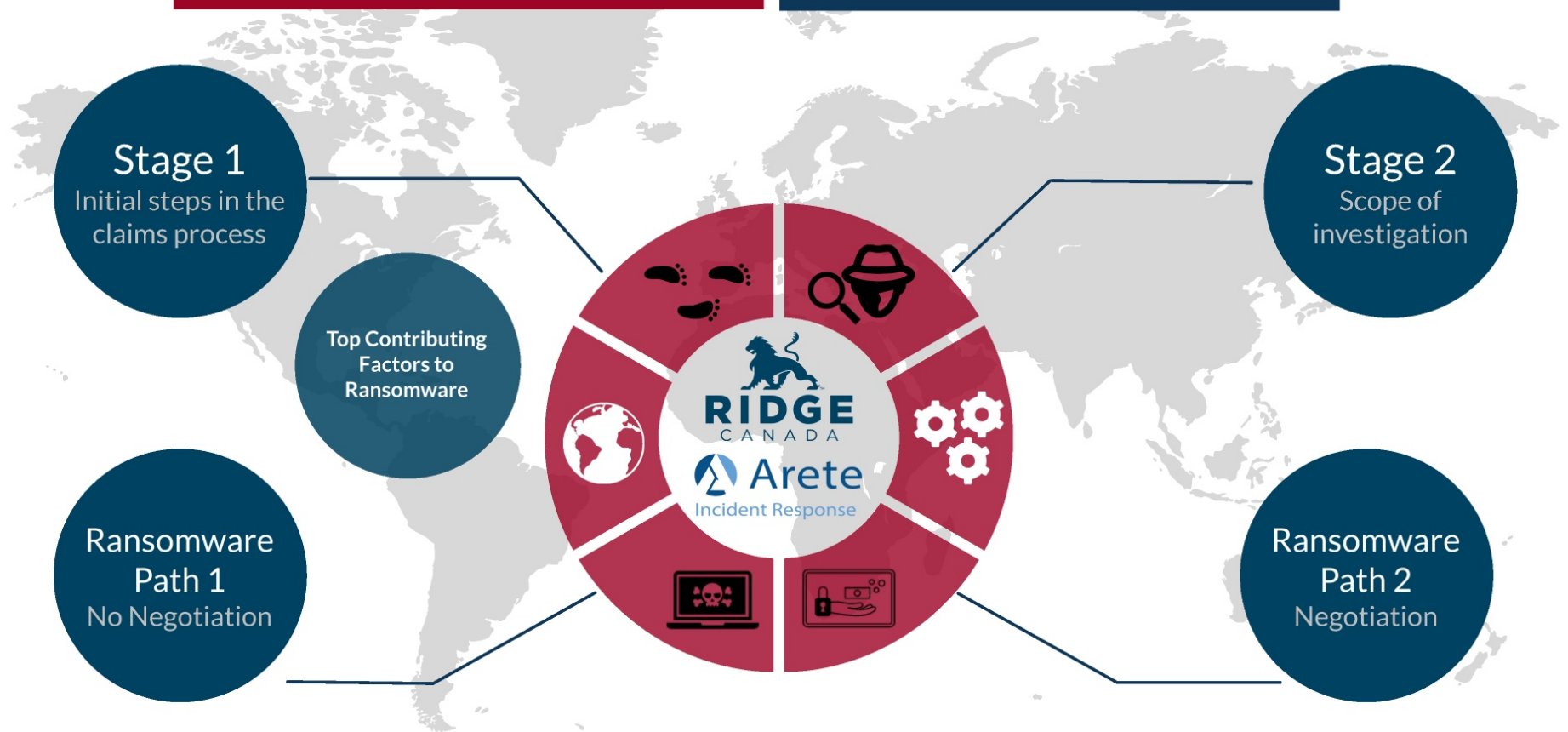
- SOWs can also be given to coverage counsel if they are involved



Once reviewed and approved, direction is provided to engage the forensic firm and initiate the investigation

The Broker/Client Claims Journey

What to expect and do when dealing with
Business Email Compromise or Ransomware



Stage 2

Initial Forensics



Consent
Checkpoint 3



Forensics tools are deployed and a forensic level initial assessment is provided. The assessment answers questions like:

- What are we dealing with?
- What needs remediation?
- Can we stop the bleeding?
- What sort of timing are we dealing with?



An initial report from the assessment is ascertained, the breach coach and forensics firm work with the insured to review what's in front of them and determine next steps

Stage 2

Consent Checkpoint 3: Review & approval for additional forensics

Similar to SOWs, approval for further forensic analysis/engagement should be requested from insurer. The **insurer** reviews the request for additional forensics to: 1) verify the additional scope of work is appropriate and in line with the policy; 2) costs are reasonable in the current market



Business Email Compromise

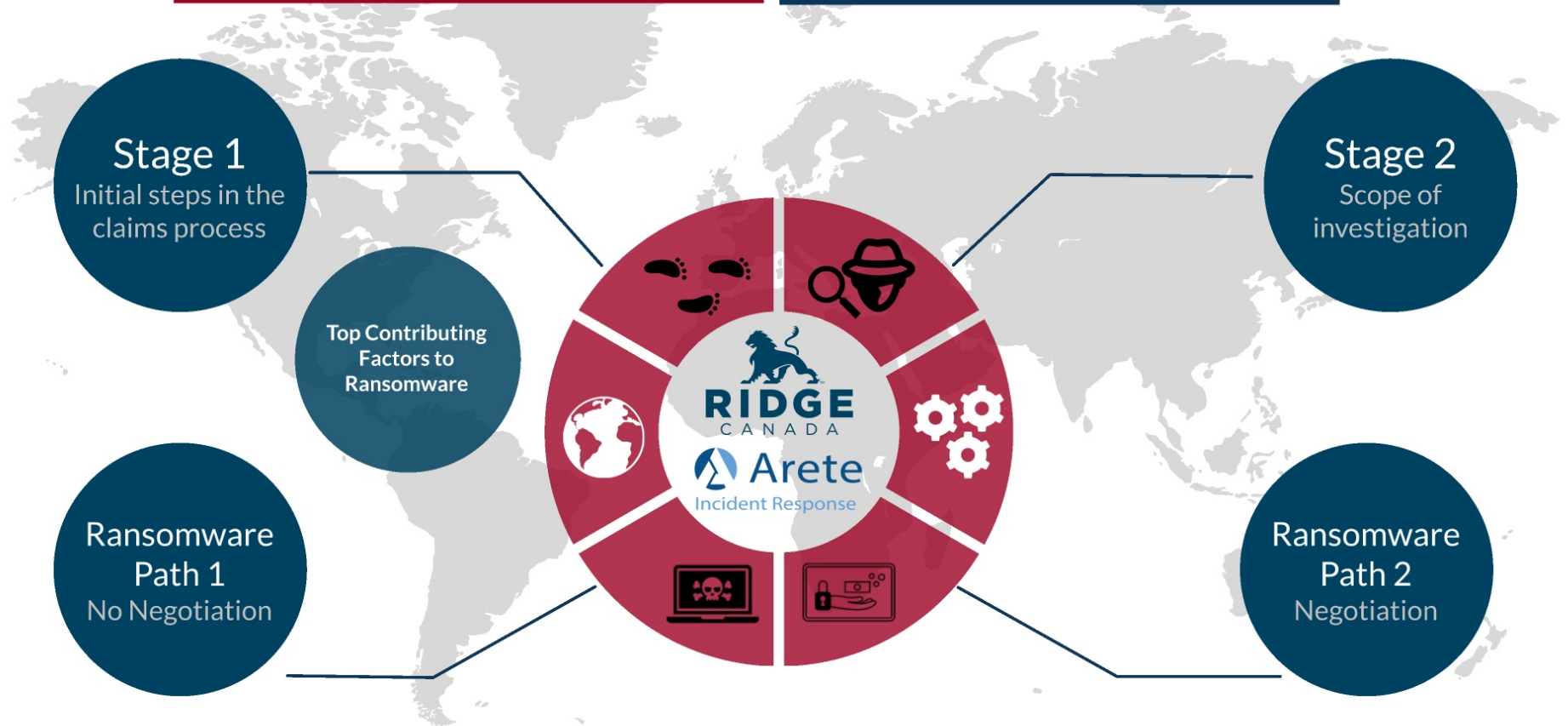


Ransomware

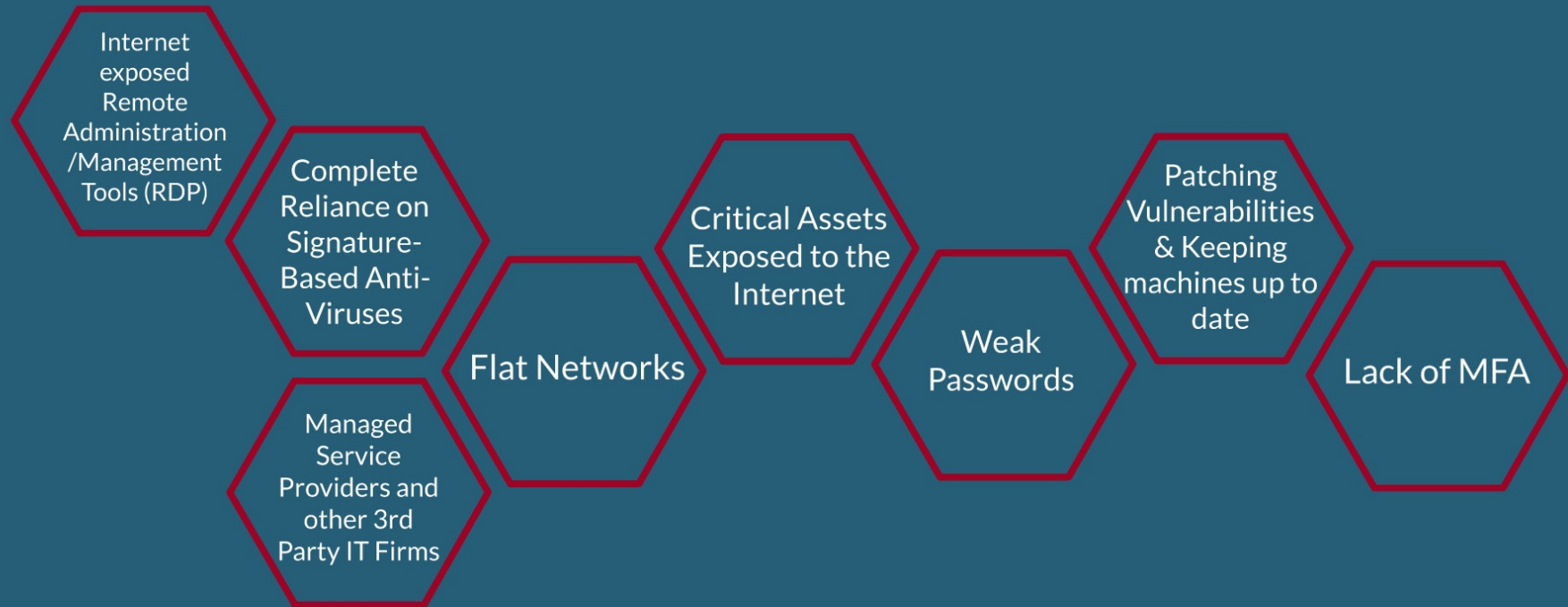
- Consent for additional forensic analysis has likely already been sent to the insurer
- First major juncture for potential friction between client and insurer

The Broker/Client Claims Journey

What to expect and do when dealing with
Business Email Compromise or Ransomware



Top Contributing Factors Leading to Ransomware



So you've been hit, now what?

Do's and Don'ts of Ransomware



- Remove infected systems from the network/take them offline
- Follow the instructions in the ransom note related to powering off systems
- Preserve all data, including systems - as well as Firewall, VPN, and Proxy logs for the forensic analysis that will need to take place
- Deploy advanced endpoint protection to all systems
- Plan on up to 2 weeks to be fully operational again based on org size



Shut down, power cycle, or reboot any infected systems

Contact the threat actor yourself or try to negotiate, leave this to the experts

Wipe or reimage any systems as these are needed for the forensic investigation

Rely on your anti-virus that failed to stop the ransomware

Assume that once a decryptor is purchased its all down hill

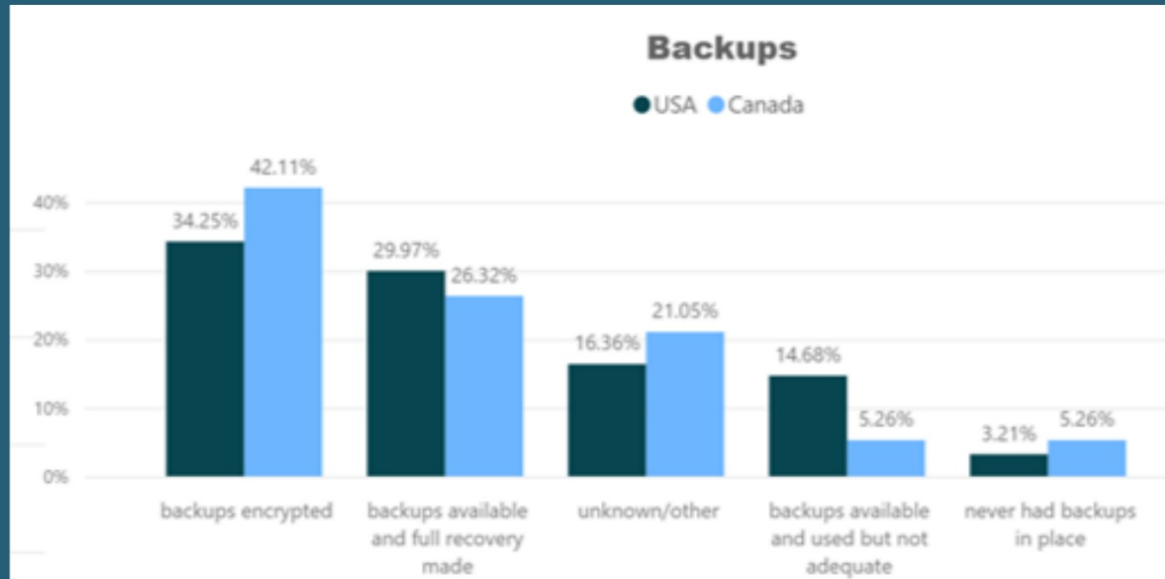
Things to consider

Identify critical stakeholders or parties to be involved in the decision making process

Communication with external partners, employees and clients?

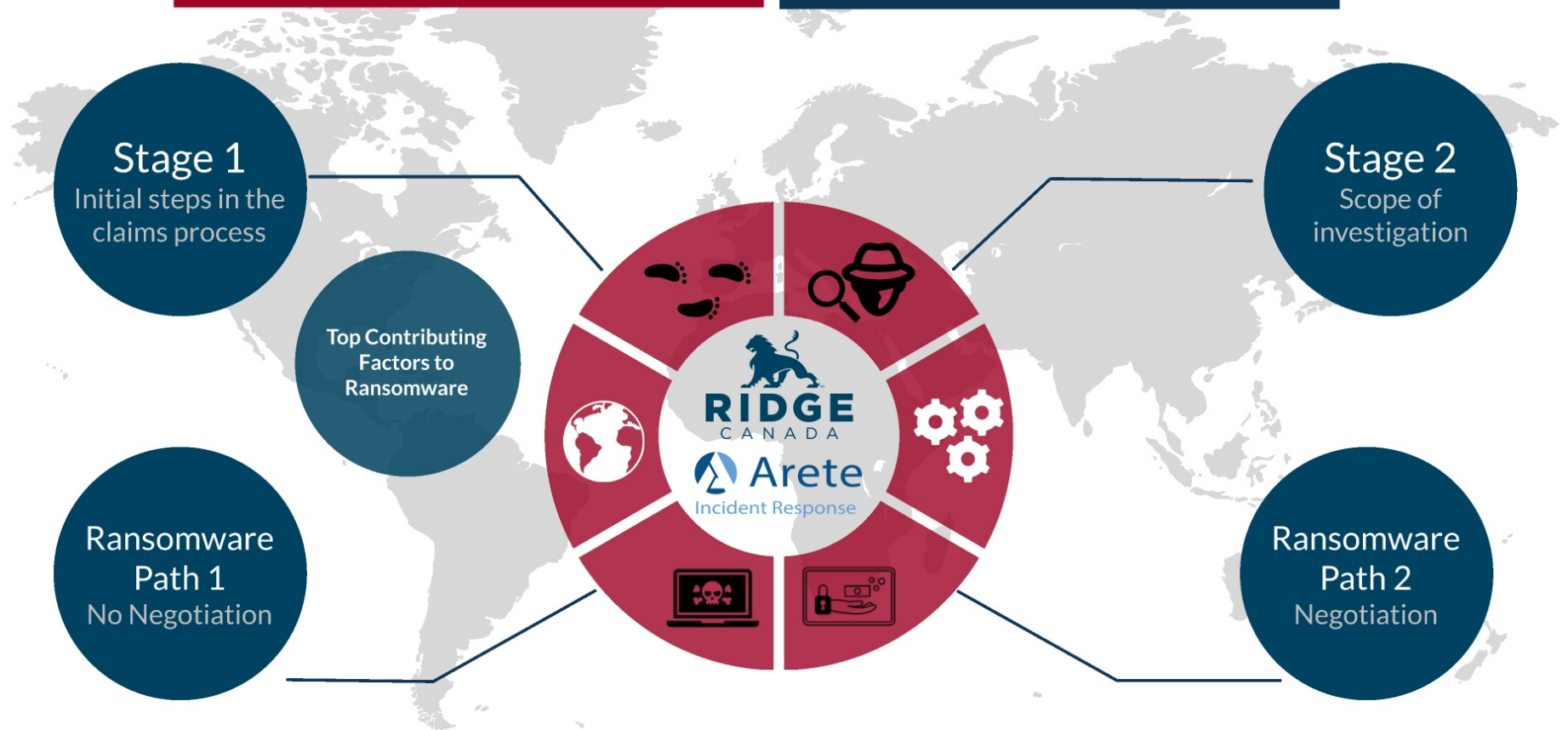
Prepare for outside assistance

Evaluating your Backups



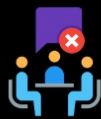
The Broker/Client Claims Journey

What to expect and do when dealing with
Business Email Compromise or Ransomware



Ransomware

Path 1: No Negotiation



Backups are available, and recoverable



Assess what information has been encrypted and/or exfiltrated



If exfiltrated:

- Does it pose a “real risk of significant harm” to affected individuals
- Work with breach coach to determine risk exposure to regulatory loss

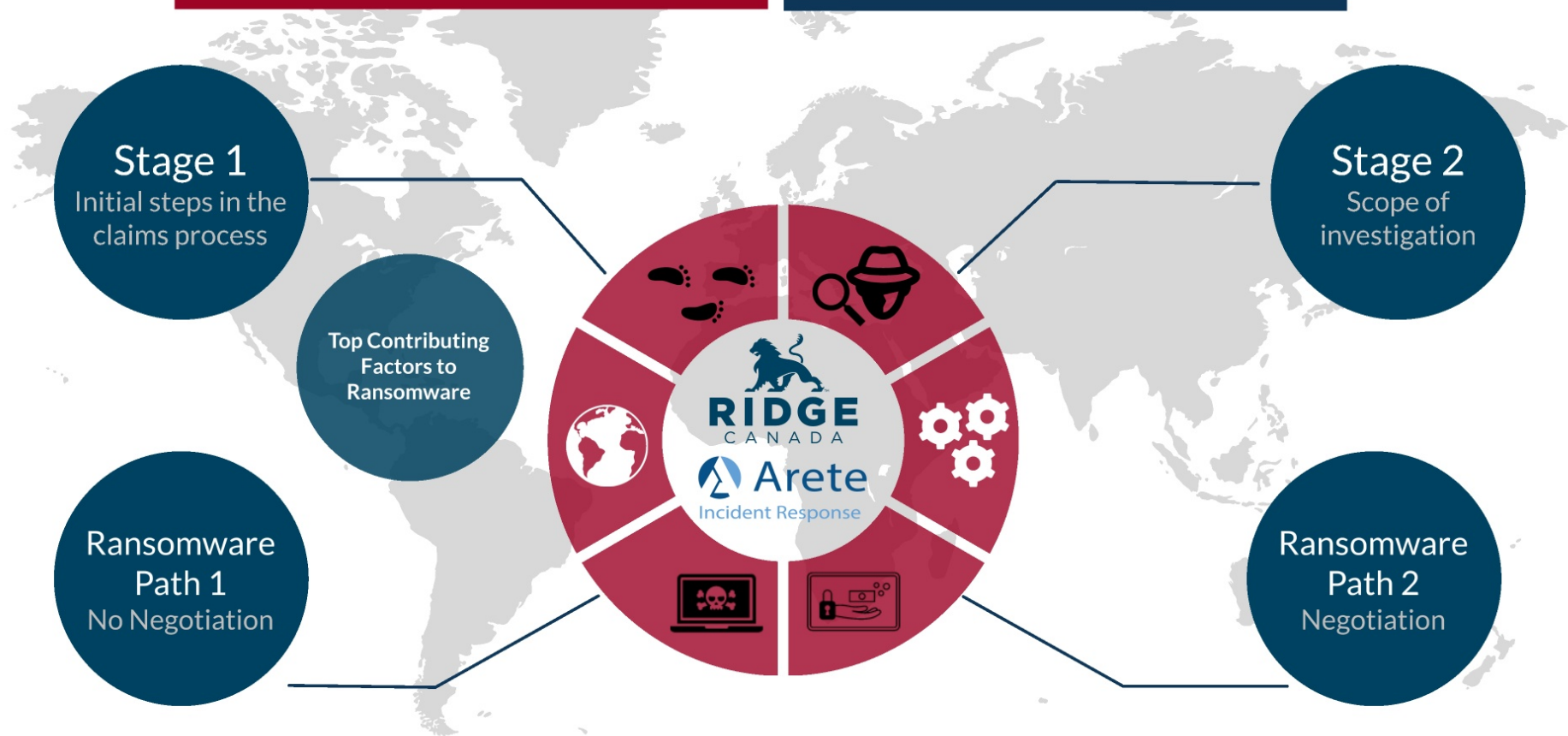


If not:

- Nearing the end of the pain of ransomware!

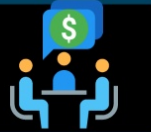
The Broker/Client Claims Journey

What to expect and do when dealing with
Business Email Compromise or Ransomware

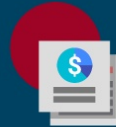


Ransomware

Path 2: Negotiation



If consent checkpoint #3 provides authorization to negotiate with the threat actor, the forensics firm will already be involved at this stage



Work with forensics firm and breach coach to deliver a best outcome

Consent
Checkpoint 4

Negotiation
Objectives

Negotiation
Deliverables

Negotiation
Styles

Ransomware

Consent Checkpoint 4: Review prior to paying the ransom

OFAC



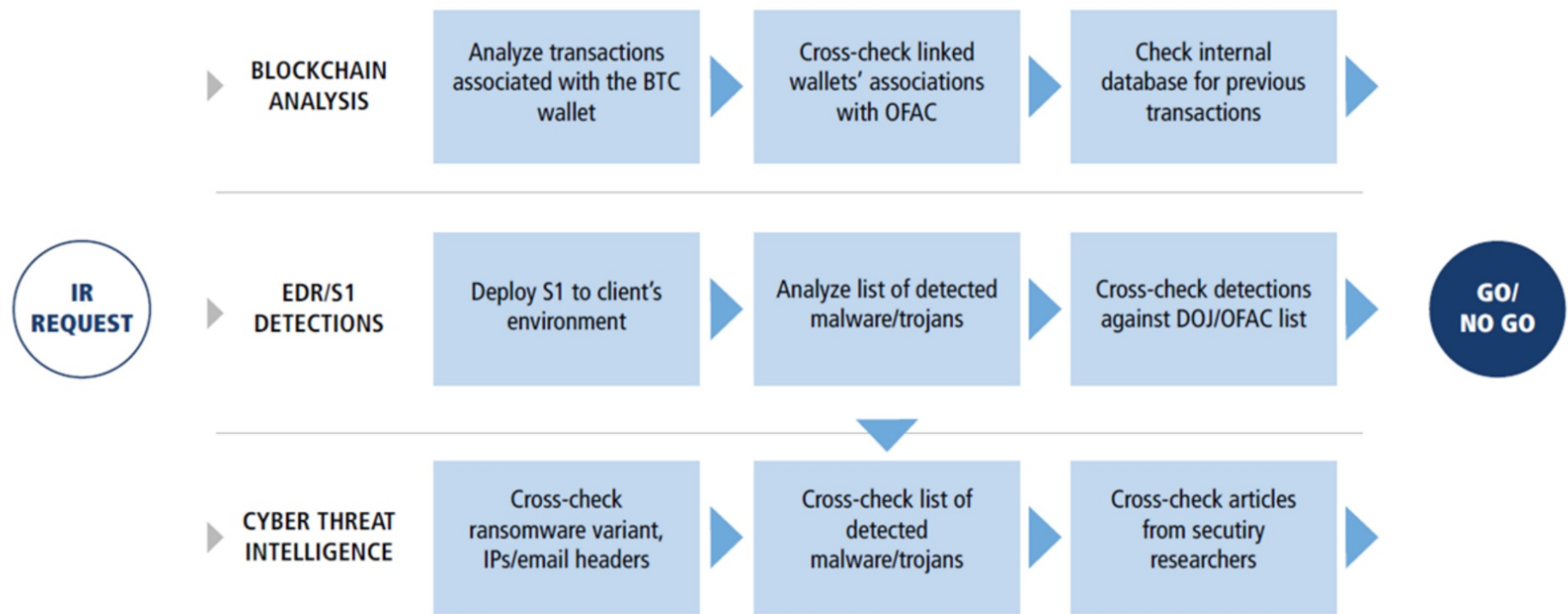
Paying the ransom? If payment is the only option, there are several items that need to be satisfied before consent can be provided:

- Sanctions check against the wallet in question
 - Would payment be against OFAC sanctions guidelines?
 - Does law enforcement need to be involved, and would consent from OFAC be required?



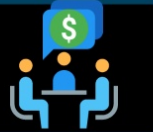
Forensics will provide a snapshot of the threat group

- Are they trustworthy?
- What have success factors been in other situations

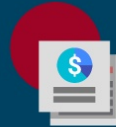


Ransomware

Path 2: Negotiation



If consent checkpoint #3 provides authorization to negotiate with the threat actor, the forensics firm will already be involved at this stage



Work with forensics firm and breach coach to deliver a best outcome

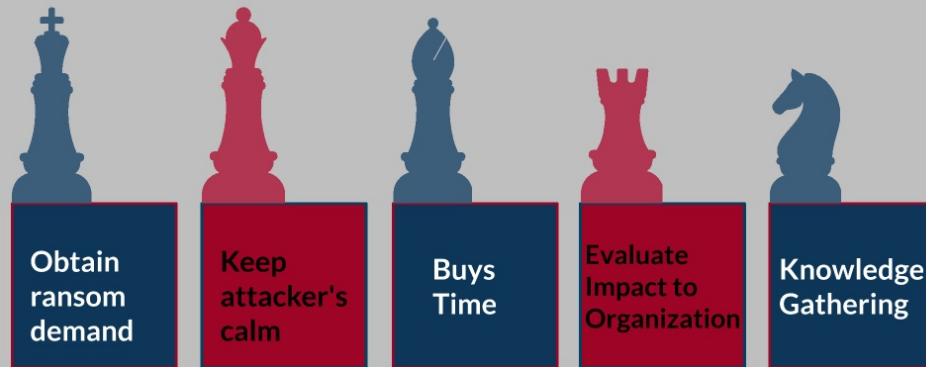
Consent
Checkpoint 4

Negotiation
Objectives

Negotiation
Deliverables

Negotiation
Styles

Main Objectives with Negotiations



Negotiation Deliverables

Decryption tools

Data deletion

Data exposure

Security Report

Passwords

Negotiation Styles

Slow and Steady- Ideal Negotiation Pace

- Less desperation
- Some money is better than no money to the attackers
- If time permits downplay importance of the data and go silent
- With the passing time it is costing attackers money (data storage & employee time)

Vs.

Quick Pay - only used in specific situations

- Client is very eager to get decryption tool.
- Demand is low enough that it is not too giant of a counteroffer.
- There has been back and forth, and client wants to reach a resolution quicker
- It is not the typical route since once money is on the table you can't take it off
- Not always successful and a certain degree of confidence and experience is needed with the attacking party.

Slow and Steady

Support: Overall price is \$2,500,000. For this price you will get everything mentioned above. Please pass this information on to your management. In the future, we are ready to communicate only with the representative who can make such decisions. We are ready to provide you with a small set of files from different servers of your company.

🕒 11/15/2020, 6:22:46 AM

Drago Rus: Hello again, sorry for the delay. We managed to convince the bank to give us a loan so we got \$250,000 together that we can turn into BTC and send to you for the decryption tool, file tree, and some sort of log showing that our data has been deleted?

🕒 11/22/2020, 7:44:57 PM

Support: Considering the steps you are taking, we are ready to make you a very good offer only if you quickly enter the deal. New price for you \$ 1,250,000

🕒 11/23/2020, 11:01:05 AM

Drago Rus: Thank you for the offer, we know that is probably much larger than you usually offer. Unfortunately we are just not in the position to pay an amount like that. We are based in Canada and are currently going through another full lockdown so there is zero travel income. We can call the bank we went to before to see if they can adjust their loan to add on a bit more but it won't be near what you are asking for. We want to make a deal with you but we really are in a bad situation financially.

🕒 11/23/2020, 7:53:43 PM

Support: Give us your final proposal. And we will decide what to do with you.

🕒 11/23/2020, 8:46:55 PM

Drago Rus: Hello again, we went back to the bank after your proposal to see if we could get anything else to offer you. They were very hesitant to give us additional funds but we were able to convince them to give us one last loan. We have a total amount of \$325,000 USD that can be converted into btc and transferred to you, unfortunately we are not going to be able to get you more than this.

🕒 11/24/2020, 6:23:02 PM

Support: We got your offer. We will contact you back tomorrow.

🕒 11/24/2020, 6:48:56 PM

Support: Good morning. We appreciate your honesty. If you are ready to close the deal today, then our management has decided to further reduce the price to \$ 350,000. This is the final price. Waiting for your decision.

🕒 11/25/2020, 10:23:02 AM

Bet Against Themselves



Quick Pay

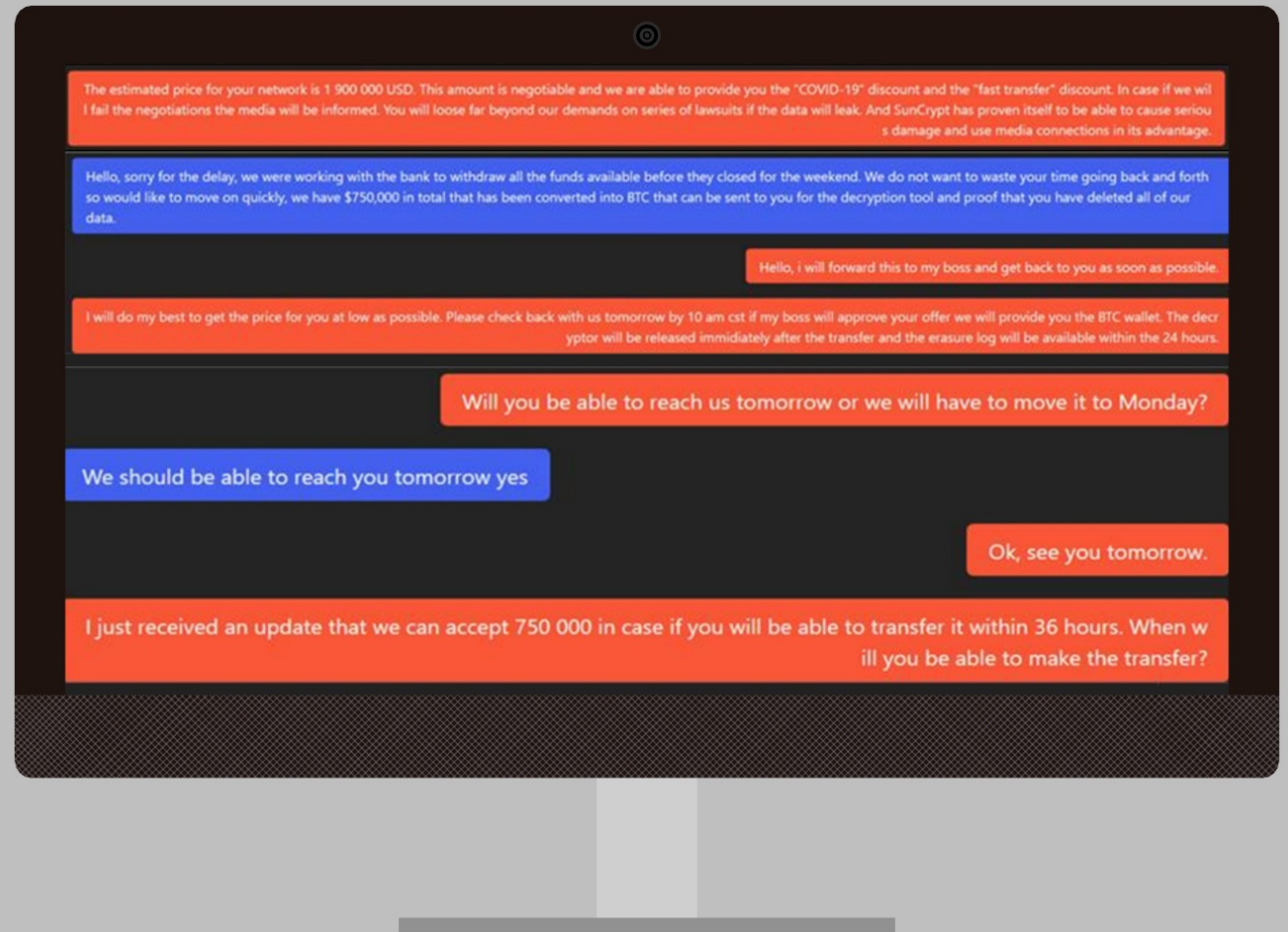
Starting demand of 1.9M

Attacker mentioned “Fast Transfer” discount

Client could not afford to waste time with the decryption and was willing to offer a large counteroffer from the start.

Our experience with this attacker gave us high confidence the offer would be accepted.

Final price 750K



The Broker/Client Claims Journey

What to expect and do when dealing with
Business Email Compromise or Ransomware

