DEEPSEC

valencia

Ready for anything.

Tales from the TTX

Running an Effective Simulation

About Us.

[firstname]@valenciarisk.com

Session Redirect:

DeepSec is Over-Simulated

We will instead share our best tips, learned from
our TTXs in CI, Government and Commercial sectors

Agenda

1. Simulation Speed Run
2. How to Scope, Plan, Cost
3. Participant & Facilitator Failures
4. Report, Repeat, Template

Introducing a TTX

Goal:

Understand key business, IT tasks, and rules that need to be followed after a cyber attack.

Make sure your organization is prepared to handle a security breach and its consequences.

Activity:

Engage participants in an intensive simulation of a cyberattack, where their responsibility is to make decisions and resolve issues.

Details and additional information are provided throughout the exercise.

Outcome:

Gain a better understanding of the responsibilities, actions, and tough choices involved in managing an actual security incident.

This will test how well your organization is prepared for such events.

Roles in the TTX

- CEO
- CFO
- CIO/CISO
- COO

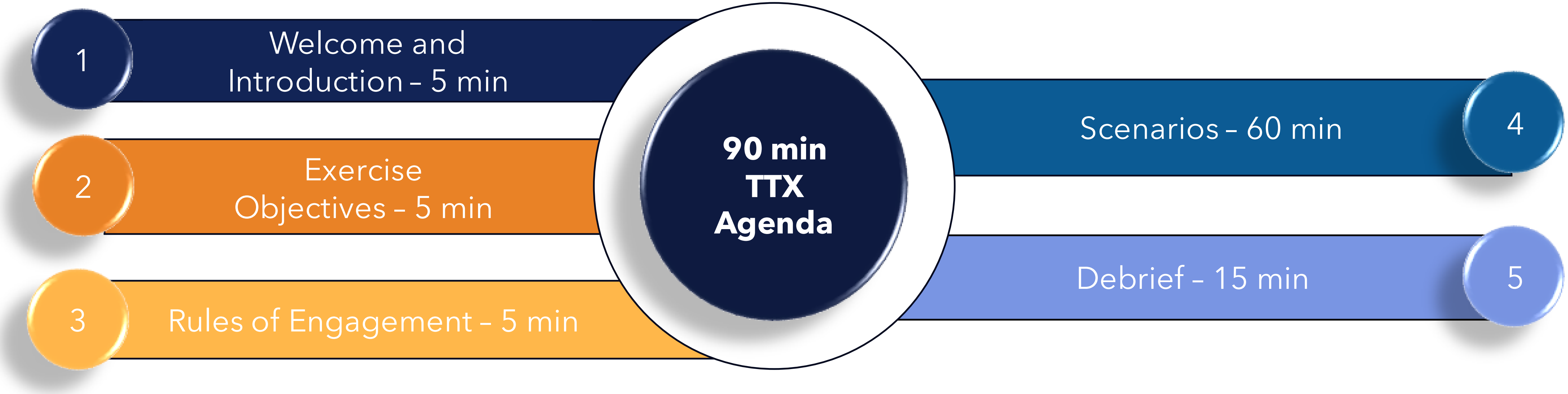
- Communications Director
- HR Director
- Legal Counsel

Simulation Speed Run

WIN CREDZ AND PRIZES BY DISABLING OPERATIONS

JOIN THE VIENNA AIRPORT CYBER SIMULATION

A TTX on Speed. It's Extendable.



90 min TTX Agenda

1 Welcome and Introduction – 5 min

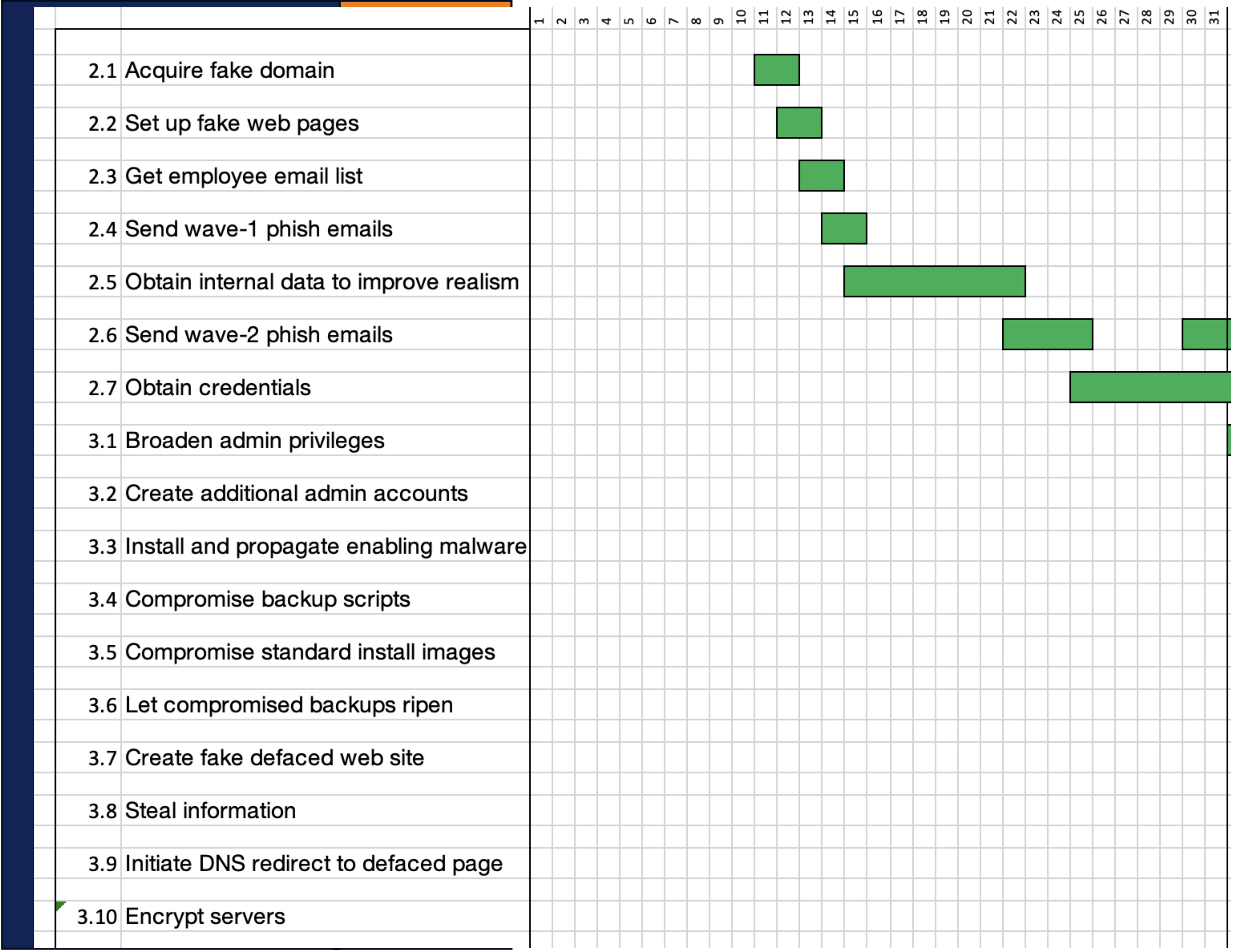
2 Exercise Objectives – 5 min

3 Rules of Engagement – 5 min

4 Scenarios – 60 min

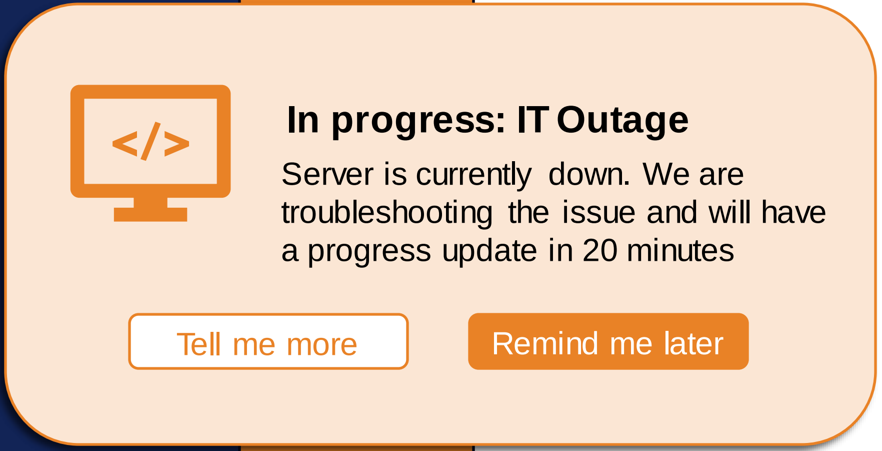
5 Debrief – 15 min

Prior to Simulation



		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
2.1	Acquire fake domain											🟩	🟩																			
2.2	Set up fake web pages												🟩	🟩																		
2.3	Get employee email list													🟩	🟩																	
2.4	Send wave-1 phish emails														🟩	🟩																
2.5	Obtain internal data to improve realism															🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩									
2.6	Send wave-2 phish emails																						🟩	🟩	🟩	🟩					🟩	🟩
2.7	Obtain credentials																									🟩	🟩	🟩	🟩	🟩	🟩	🟩
3.1	Broaden admin privileges																															
3.2	Create additional admin accounts																															
3.3	Install and propagate enabling malware																															
3.4	Compromise backup scripts																															
3.5	Compromise standard install images																															
3.6	Let compromised backups ripen																															
3.7	Create fake defaced web site																															
3.8	Steal information																															
3.9	Initiate DNS redirect to defaced page																															
3.10	Encrypt servers																															

Inject 1



In progress: IT Outage

Server is currently down. We are troubleshooting the issue and will have a progress update in 20 minutes

Received earlier today:

- Standard IT service interruption notice.
- Several systems are offline including critical systems for HR, business, and finances.
- Investigating.

Discussion

- Initial reaction?
- What would you do first?
- What information do you need?
- Are the right people in the room?

Steps to Take

Caution, don't jump to conclusions about its severity.

Work with IT to:

- Assess initial incident indicators.
- Try to manage and isolate the issue.
- Verify if security updates are current.
- Review security logs.

Ensure customer support remains secure.

Refrain from unneeded comms.

Inject 1 (b)

- **You have been called together in board room**
  - CEO has received an email.
- **Hacker group "Muse"**
  - Claims they are cause of outage.
  - Systems are locked, only Muse can restore.
  - They have also stolen info from databases.
- **Demanding 10 Bitcoin to restore systems**
  - 3 days to pay, then price goes up.
  - Will publish stolen information if not paid.

Discussion

- Initial reaction?
- What would you do first?
- What information do you need?
- Are the right people in the room?

Steps to Take

Dust off the Incident Response Plan.

Read your Business Continuity Plan.

Notify the cyber incident response team.

Move board and IR team to cyber 'bunker' site.

Talk to Legal and Insurance.

Make sure you know your Crown Jewels.

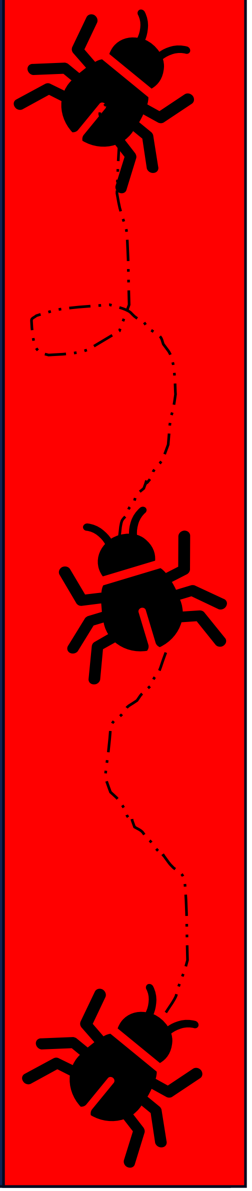
Ensure that IT has resources and plan to:

- Identify affected applications,
- Assess which business areas are impacted,
- Check if data backups are compromised,
- Restrict and isolate devices.

Inject 2

Initial Assessment from IT Department:

- Servers are inaccessible and unresponsive.
- Email seems to be working okay.



Cyber Security Threat

Inject 2 (b)

Security has been investigating since early this morning:

- **Theory:** Malware has spread through the network, propagating through USB drives initially. Someone may have brought in an infected drive.
- They seem to have admin credentials – that is why no "break-in" alarms.

Discussion

1. Confirm incident with Chief Information Security Officer (CISO).
2. Contact a specialized cyber incident team.
3. Find your company contacts list.
4. Dust off your BCP.
5. Look into the breach timeline to establish data backup integrity.
6. Have legal check the cyber-insurance details.
7. Alert the cyber-insurance company.
8. Implement your business recovery plans.
9. Plan for additional staff if prolonged disruption.
10. Make sure you know what/where Crown Jewels are.
11. Assess the financial impact.
12. Figure out what operations can continue manually.
13. Organize how to communicate with staff, clients, and partners without email.
14. Begin cleaning and restoring IT systems, like reimaging devices.
15. Keep the crisis management team updated.
16. Use emergency notification systems to advise staff on next steps.
17. Communicate with customers and partners about the situation.
18. No need to contact state or industry regulators yet.

⚠ UNAUTHORIZED ACCESS

Inject 3 (a)

Note from Security:

- Logs show a computer from operations connected to the jump box.
- Unsure of extent of compromise.
- The OT environment may have been accessed.

Inject 3 (b)

Sales call from a tech salesman:

- Have you heard of ransomware?
- You need our products.
- Urgent you let me come and make a pitch to you.

Cyber Security Threat

Inject 3 (c)

Note from Security:

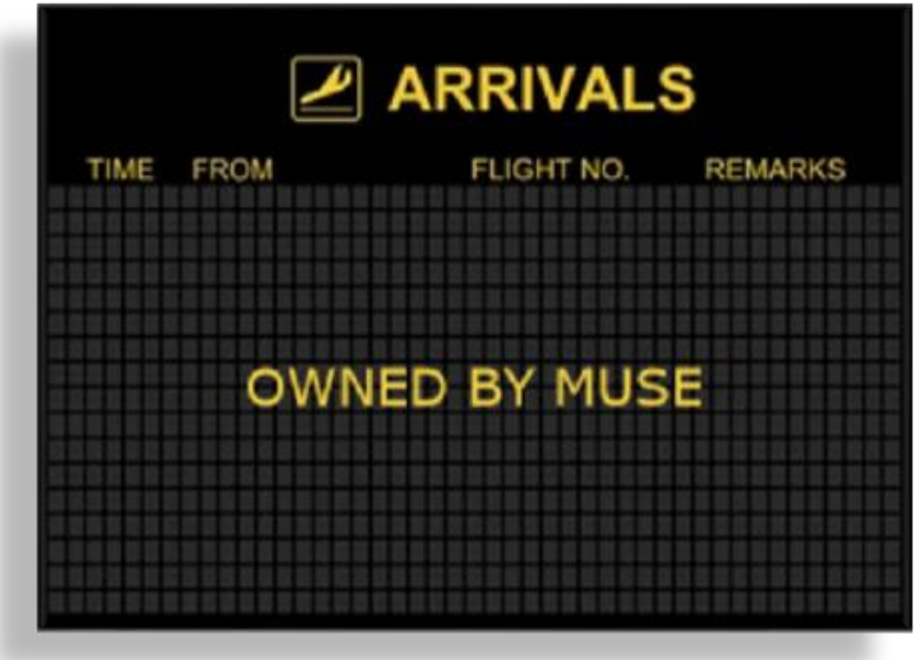
- They have admin credentials.
- They probably have other access we have not seen yet.
- Don’t assume email or Teams is secure.
  - Maybe they can see it.
  - Maybe they can send it.

Cyber Security Threat

Inject 3 (d)

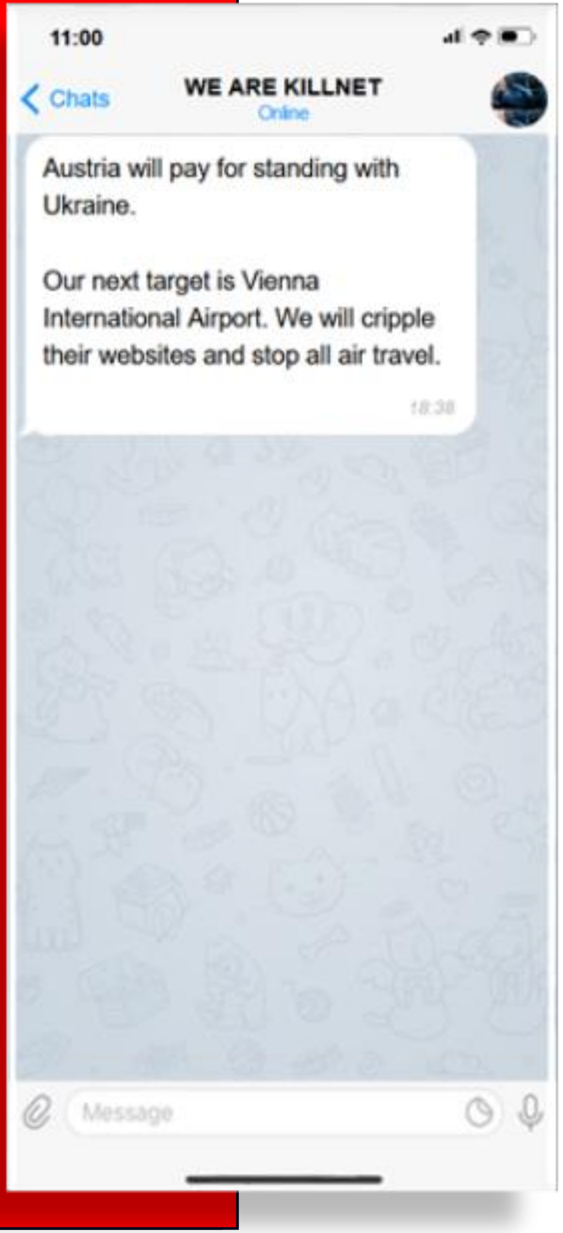
Note from Security:

- Arrival board has been compromised.
- Displaying the following image:



Discussion

1. Is anyone checking OT Systems?
2. Who is focusing on Comms?
3. Is the executive directing extra staff or consulting to IT and Cyber?
4. Consider consultation with legal counsel to navigate potential liabilities.
5. Initiate collaboration with additional forensic analysis teams to deepen investigative efforts.
6. Report the incident to law enforcement agencies as per regulatory requirements.
7. Contract with a public relations firm to oversee external communication strategies.
8. Manually compile operational data from respective departments to maintain business continuity.
9. Make sure Payroll and other core system can run
10. Look for Physical compromise
11. Assess the need for temporary suspension of affected business processes.
12. Maintain a detailed ledger of all incident-related expenditures for accountability.
13. Give Comms the bona fides of the team to project confidence in capabilities
14. Facilitate ongoing updates to the crisis management team to ensure cohesive response efforts.
15. Defer mandatory reporting to regulatory entities until comprehensive incident assessment is complete.


11:00

WE ARE KILLNET
Online

Austria will pay for standing with Ukraine.

Our next target is Vienna International Airport. We will cripple their websites and stop all air travel.

18:38

Cyber Security Threat

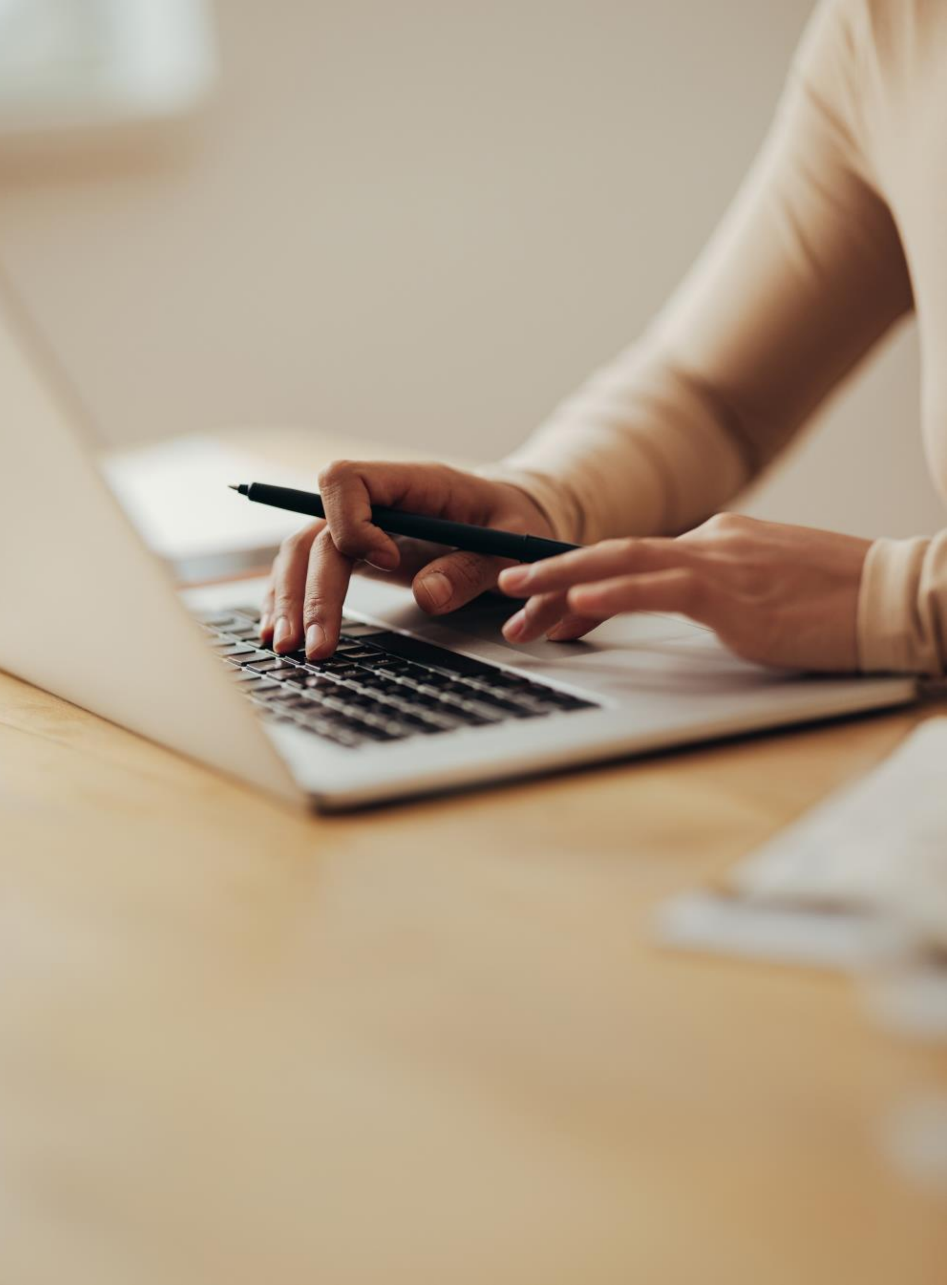
Inject 4 (a)

SOC has been made aware of a post on Telegram:

- Hacktivist group Killnet has announced they will be DDoSing the VIE airport.
- No system outages have been reported yet.

Inject 4 (b)

- **Note from IT:**
  - IT has noted the Vienna airport website seems to be receiving a large amount of traffic.
  - Possibly a DDoS attack, website is slow to respond and unresponsive for some.



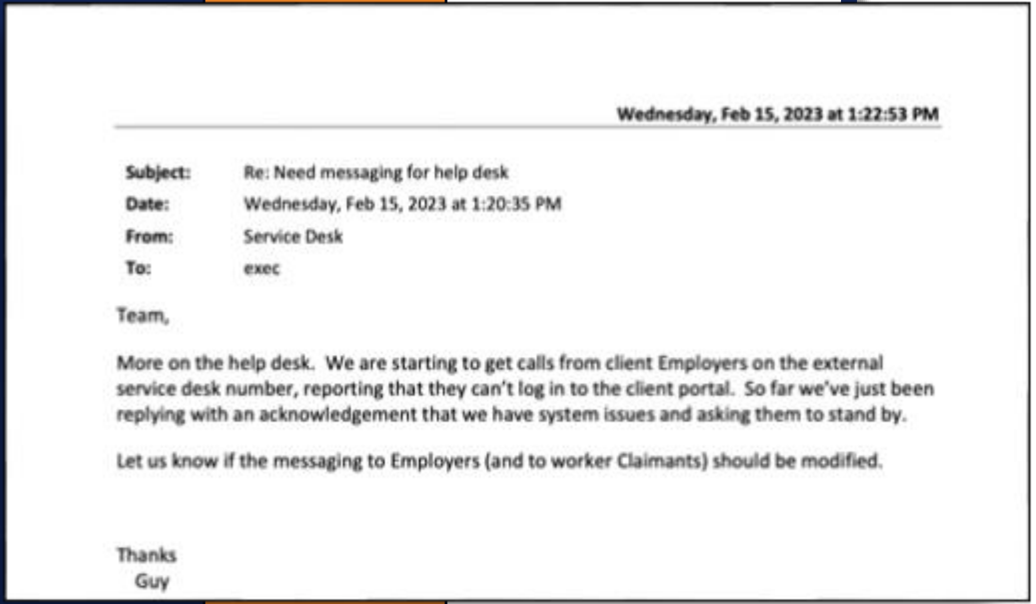
Inject 4 (c)

A journalist from the Wienner Zeitung has reached out with a request for comment regarding the attack launched by Killnet:

- Will this delay air travel?
- How long until the systems are restored?

valencia
Ready for anything.
DEEPSEC

Inject 4 (d)



Wednesday, Feb 15, 2023 at 1:22:53 PM

Subject: Re: Need messaging for help desk
Date: Wednesday, Feb 15, 2023 at 1:20:35 PM
From: Service Desk
To: exec

Team,

More on the help desk. We are starting to get calls from client Employers on the external service desk number, reporting that they can't log in to the client portal. So far we've just been replying with an acknowledgement that we have system issues and asking them to stand by.

Let us know if the messaging to Employers (and to worker Claimants) should be modified.

Thanks
Guy

- **Helpdesk is getting calls from employees:**
  - What should I do?
  - Where should I be?
- **They have no instructions on how to handle this.**

Discussion

- Initial reaction?
- What would you do first?
- What information do you need?
- Are the right people in the room?

Steps to Take

Acknowledge and share the status of the incident.

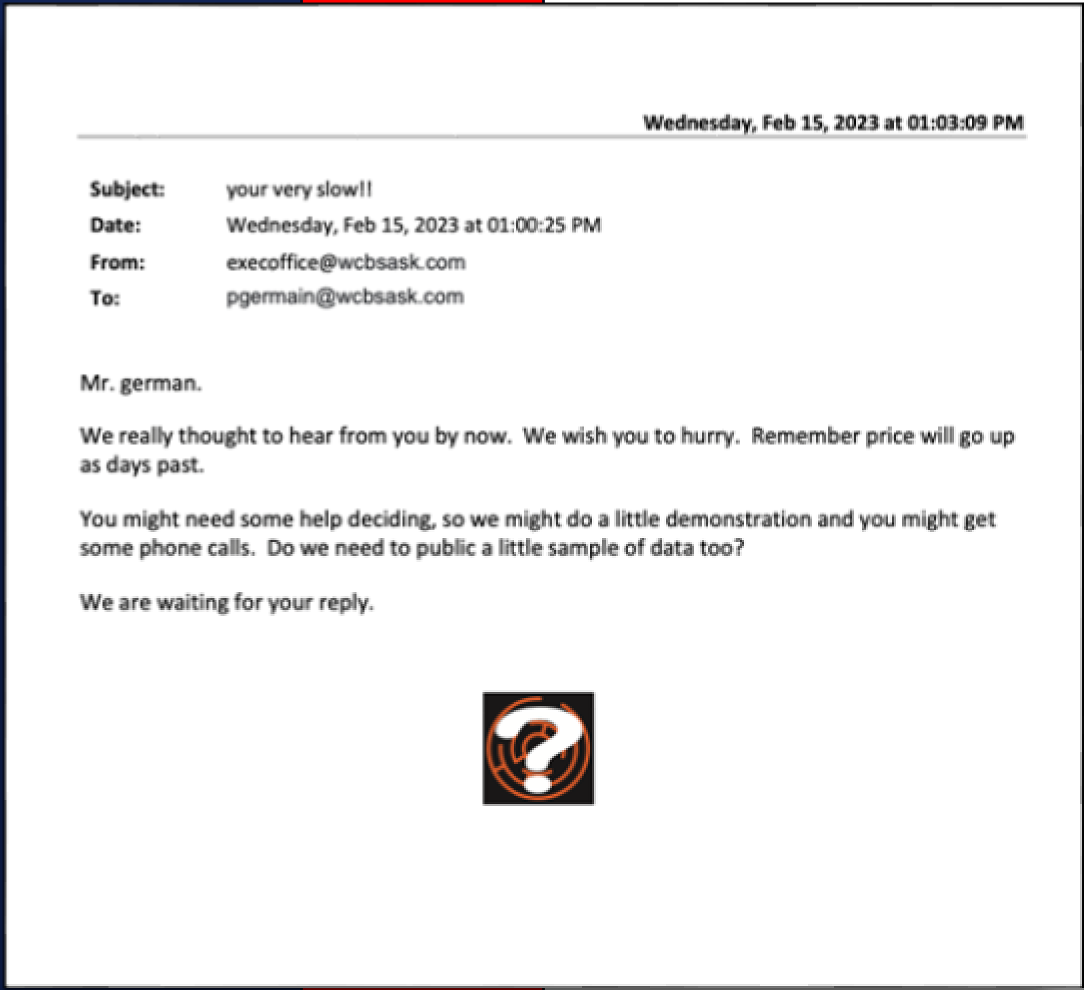
Synchronize communication efforts with external public relations firm and consult with legal advisors.

Direct employees to refrain from discussing the crisis publicly, and on social.

Engage with media outlets to schedule regular updates regarding the crisis.

Ensure IT and Cybersecurity teams and contractors are engaged and have resources needed.

Postpone formal communications with governmental and industry regulatory bodies until more is known.



Wednesday, Feb 15, 2023 at 01:03:09 PM

Subject: your very slow!!
Date: Wednesday, Feb 15, 2023 at 01:00:25 PM
From: execoffice@wcbsask.com
To: pgermain@wcbsask.com

Mr. german.

We really thought to hear from you by now. We wish you to hurry. Remember price will go up as days past.

You might need some help deciding, so we might do a little demonstration and you might get some phone calls. Do we need to public a little sample of data too?

We are waiting for your reply.

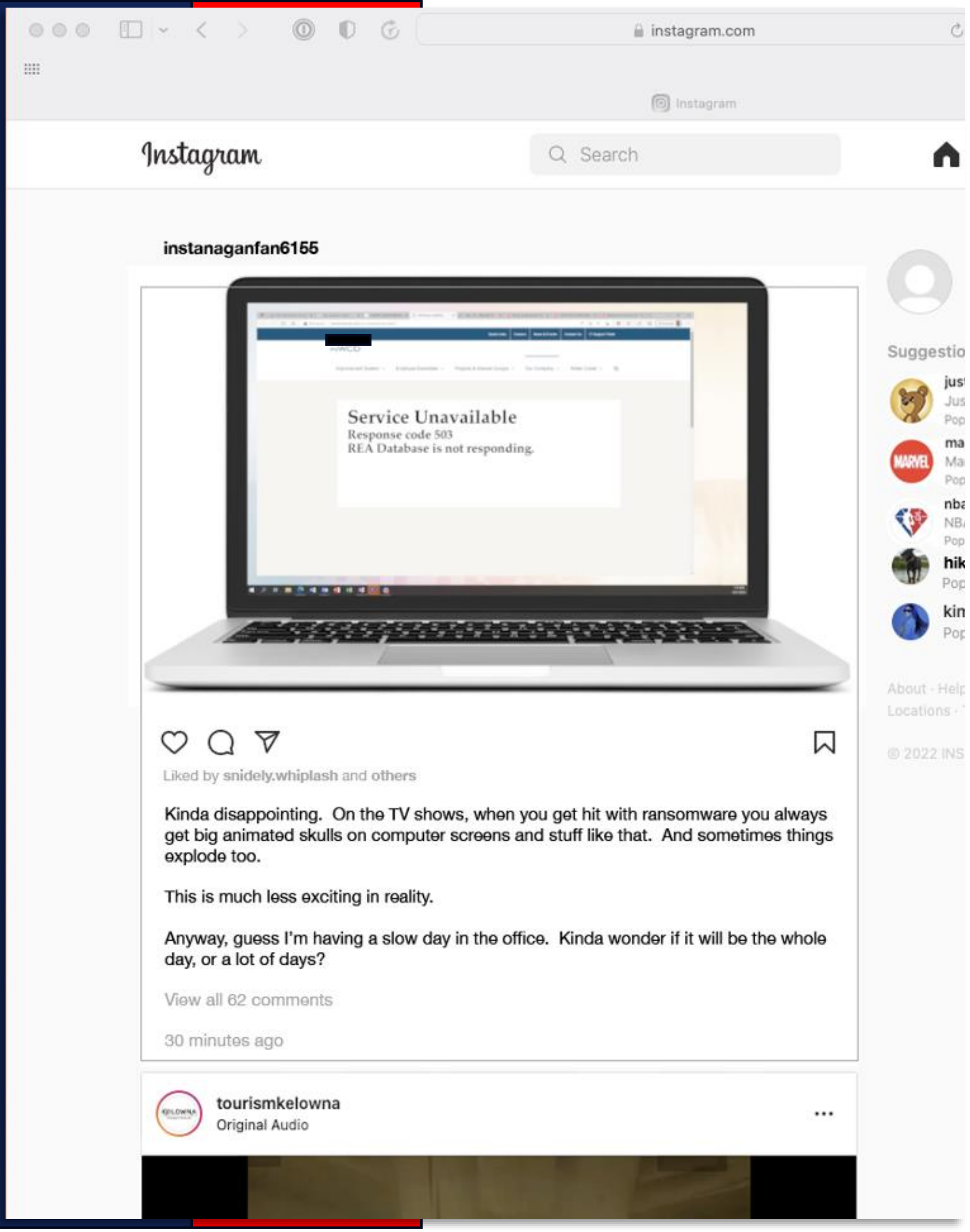
Inject 5 (a)

Hackers have written again:

- They seem impatient.
- Imply they may do something to turn up the heat.

Inject 5 (b)

- IT confirms Hackers *have* connected to the "jump box".
- Conveyor belts moving luggage have halted.
- Travelers have noticed the arrivals sign and are angry that their luggage has not arrived.



instanaganfan6155

[redacted]

Service Unavailable
Response code 503
REA Database is not responding.

Liked by snidely.whiplash and others

Kinda disappointing. On the TV shows, when you get hit with ransomware you always get big animated skulls on computer screens and stuff like that. And sometimes things explode too.

This is much less exciting in reality.

Anyway, guess I'm having a slow day in the office. Kinda wonder if it will be the whole day, or a lot of days?

View all 62 comments

30 minutes ago

tourismkelowna
Original Audio

Inject 6

- **Note from Communications:**
  - Someone couldn't resist posting an Instagram selfie.
  - Says "ransomware"
  - Looking closely, it's the VIE intranet.

Inject 7

4:05 PM:

- Journalist is back:
  - No doubt of an attack.
  - Article coming out soon, our chance to comment.
  - Somewhat aggressive information demands.

Discussion

$! $?

Do you pay?

$! $?

Wrap-Up Discussion

- How did you feel as this crisis evolved?
- Did you feel you knew enough to lead?
- How might we be better prepared?
- Anything we can do in advance?
- Lessons learned about communications, strategy, tools, procedures?
- Should the Simulation Continue?

Facilitator Hotwash Tasks

1. Review the effectiveness of the response.
2. Reflect on alternative actions for potential real-world scenarios.
3. Confirm adherence to the security incident response protocol.
4. Evaluate the use and effectiveness of business continuity and manual workaround plans.
5. Assess the implementation of the crisis management plan.
6. Examine the execution of the crisis communications strategy.
7. Identify successful aspects of the response.
8. Analyze the comprehensive impact, including customer and brand considerations.
9. Clarify decision-making and action-taking responsibilities.
10. Discuss whether all anticipated issues were addressed.
11. Investigate any systemic organizational issues highlighted by the incident.
12. Determine if there are indicators to predict such events in the future.
13. Evaluate the need for contractual revisions with security and disaster recovery vendors.
14. Assess the adequacy of current tools to prevent similar cyberattacks.
15. Consider how to make the response more effective or efficient.
16. Assess if key roles and personnel were effectively involved.
17. Identify areas for improvement in knowledge, tools, or processes.
18. Contemplate the real-world consequences had the incident occurred.

Common Activities for Participants

After-Action Report Checklist for Cybersecurity Breach Simulation:

1. Develop a RACI matrix for all parties, including third-party and partners.
2. Conduct joint CSIRT and Business Continuity Management (BCM) drills at least once a year.
3. Update your Playbooks
4. Improve SOPs for when IT systems are down, ensuring continuity and resilience.
5. Maintain updated contact lists and set up a ‘cyber bunker’ for secure comms
6. Get a really engaging, battle-scarred breach firm to do the simulations.
7. Review communication efficacy both internally and externally during the simulation.
8. Evaluate the time taken to detect and respond to the simulated breach.
9. Assess data backup and recovery processes.
10. Examine the impact on customer trust and service delivery.
11. Identify any gaps in staff training and awareness regarding cybersecurity practices.
12. Ask if legal and regulatory compliance was done right?
13. Calculate the injury and cost.

How to Scope, Plan and Cost

How to Scope

When scoping a cybersecurity incident tabletop simulation for executives, consider the following key points:

1. Objectives: Define clear goals for the simulation to ensure it aligns with the executive team's expectations and the organization's risk profile.

2. Scope: Determine the breadth and depth of the simulation, including which systems, processes, and scenarios will be tested.

3. Participants: Identify which members of the executive team will participate and whether to include leaders from specific departments such as IT, HR, legal, and communications.

4. Scenario Realism: Choose scenarios that are relevant and challenging for the organization, possibly based on recent threat intelligence or known vulnerabilities.

5. Executive Engagement: Ensure the simulation requires strategic decision-making, not just technical responses, to keep executives engaged.

How to Scope

6. Legal and Compliance Considerations: Address potential legal and regulatory impacts of the incident, involving the legal team in the planning phase.

7. Communication Channels: Plan how information will be shared among participants during the simulation, including the use of secure communications if necessary.

8. Incident Response Plan Review: Ensure that the simulation tests the organization's incident response plan and identifies any gaps or areas for improvement.

9. Recovery and Business Continuity: Include elements that test organization's ability to maintain or quickly resume critical operations during and after an incident.

10. Metrics and Success Criteria: Define how success will be measured and what metrics will be used to evaluate the effectiveness of the response.

11. Debriefing and Lessons Learned: Plan for a thorough debriefing session to discuss the outcomes, identify lessons learned, and develop an action plan for improvements.

12. Third-Party Involvement: Decide if and how to include third-party vendors or partners who would be involved in a real incident response.

13. Confidentiality: Ensure the scenario and discussions remain confidential to protect sensitive company information.

14. Resource Allocation: Assess the resources needed for the simulation, including time, budget, and personnel.

15. Follow-Up: Establish a follow-up process to address the findings and integrate them into the existing cybersecurity strategy and training programs.

How to Sell and Cost

1. Risk Management: Emphasize how simulations identify and help mitigate potential security risks, protecting against future breaches.

2. Regulatory Compliance: Highlight the importance of demonstrating due diligence and compliance with industry regulations like GDPR, HIPAA, or NIST frameworks.

3. Financial Impact: Discuss the potential cost savings by preventing breaches, which often far outweigh the investment in simulations.

4. Reputation Protection: Stress the value of protecting the organization's reputation by being prepared for cyber incidents

5. Executive Leadership: Underline the role of executive leadership in incident response and the importance of their engagement in cybersecurity culture.

6. Operational Resilience: Point out how simulations test and improve the organization's resilience to disruptions caused by cyber threats.

7. Training and Awareness: Showcase how simulations act as training tools for the executive team, increasing their understanding of cyber threats.

8. Real-World Scenarios: Ensure executives understand that the simulation will use tailored scenarios that reflect real-world threats.

9. Actionable Insights: Explain that simulations provide actionable insights for strengthening current security posture and response strategies.

10. Cross-Departmental Coordination: Highlight the benefit of improving coordination between departments, such as IT, legal, and public relations.

11. Incident Response Validation: Stress that simulations validate and refine the existing incident response plan, ensuring it is effective and current.

12. Leadership Example: Discuss how executive participation sets a proactive example for the rest of the organization regarding cybersecurity.

13. Competitive Advantage: Mention how strong cybersecurity preparedness can serve as a competitive advantage in the industry.

14. Customization: Assure that the simulation can be customized to the specific needs and concerns of the organization and its executives.

15. ROI Demonstration: Offer to provide a return on investment (ROI) analysis post-simulation, showing the value of the exercise.

16. Post-Simulation Support: Outline the follow-up support and improvements to the cybersecurity framework that will come after the simulation.

Participant and Facilitator Failures

Facilitator Failures

1. **Unprepared:** Not learning enough about the company's systems and risks before the simulation.
2. **Unclear Goals:** Not setting or explaining the aims of the exercise to everyone involved.
3. **Complex Scenarios:** Making the fake breach too complicated, causing confusion.
4. **Poor Instructions:** Giving too much or too little information before starting.
5. **Bad Timing:** Letting sessions drag on too long or rushing through important parts.
6. **Tech-Only Focus:** Ignoring how the breach affects non-technical business aspects, like laws and public relations.
7. **One Plan for All:** Using the same standard plan for every company without tailoring it.
8. **Executive Disconnect:** Not involving company leaders in the right way or considering their decision-making role.
9. **No Interaction:** Relying just on talks without hands-on activities or discussions.
10. **No Follow-Up**: Not providing steps to take after the simulation to improve security.

Tips for Technical Participants

1) **Understand the Objectives:** Know the goals of the simulation and specific aspects you're expected to address.

2) **Review Incident Plans:** Familiarize yourself with the incident response and recovery plans before the simulation begins.

3) **Stay Role-Focused:** Stick to your designated role and responsibilities during the simulation to ensure a realistic response.

4) **Active Participation:** Engage actively in the simulation, contributing your technical expertise and asking clarifying questions.

5) **Effective Communication:** Clearly communicate technical information so that non-technical participants can understand.

6) **Realism in Actions:** Make decisions and act as in a real breach scenario, considering the limitations and pressures.

7) **Collaboration:** Work collaboratively with team members, understanding that cybersecurity is a cross-functional effort.

8) **Document Actions:** Track actions and decisions for review during debrief for learning points and improvement.

9) **Stress Management:** Practice maintaining composure under pressure, a crucial skill during actual incident management.

10) **Learn and Adapt:** Be open to feedback and be adaptable based on simulation's outcomes for continuous improvement.

Report, Repeat, Template

How to Report

1. Start with a Summary: Begin the report with a brief summary of the simulation's scope, the scenario played out, and the main outcomes.

2. Be Clear and Concise: Use plain language that's easy to understand and avoid technical jargon unless it's explained.

3. Highlight Key Findings: Emphasize the most crucial aspects of the simulation, such as successful strategies and areas needing improvement.

4. Detail the Scenario: Describe the breach scenario in a way that's easy to follow, explaining why it was chosen and how it unfolded.

5. Outline Participant Roles: List who was involved and what roles they played, linking their actions to the outcomes of the simulation.

6. Recommend Actions: Clearly state recommendations for addressing weaknesses and reinforcing strengths revealed during the simulation.

7. Use Real Data: Support your findings and recommendations with real data and observations from the simulation.

8. Visual Aids: Include charts, graphs, or tables to make data more digestible and to visually highlight important points.

9. Follow-Up Steps: Provide a clear list of next steps, assigning responsibility and deadlines for each action item.

10. Encourage Feedback: Invite feedback on the report itself and the simulation to foster continuous improvement and engagement.

DEEPSEC

valencia

Ready for anything.

Thank you for participating.

hello@valenciarisk.com