DEEPSEC

valencia
Cyber Optimists.

From Simulations to Strategy

Advanced Simulations and Optimized Incident Preparation

About Us

Pavle Bozalo

pbozalo@valenciarisk.com

Aron Feuer

aron@valenciarisk.com

Matias Ulloa

mulloa@valenciarisk.com

Incident Response Services

Slice is your Incident Response Accelerator. It extends and enhances your capabilities.

We offer Slice as an annuity service. It includes simulations, a hosted virtual 'war room', and a retainer.

With Valencia's support, you are ready for anything.

valencia
Cyber Optimists.

Agenda

1. Why do we do them?
2. What do they look like?
3. How do we make them better?

Breach Simulations

Why do we do them?

What is a TTX Supposed to Do?

Goal

Improve Confidence.

Achieve the status of Cybersecurity Simulations as Fire Drills: Perfectly Normal.

Activity

Experience FUD

Experience Pressure.

Test the “Go Bags”.

Outcomes

Responders are trained.
Team is cohesive.
Long pauses are reduced.
Gaps are identified.

valencia Cyber Optimists. DEEPSEC

Selling Points: Why Do This?

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.

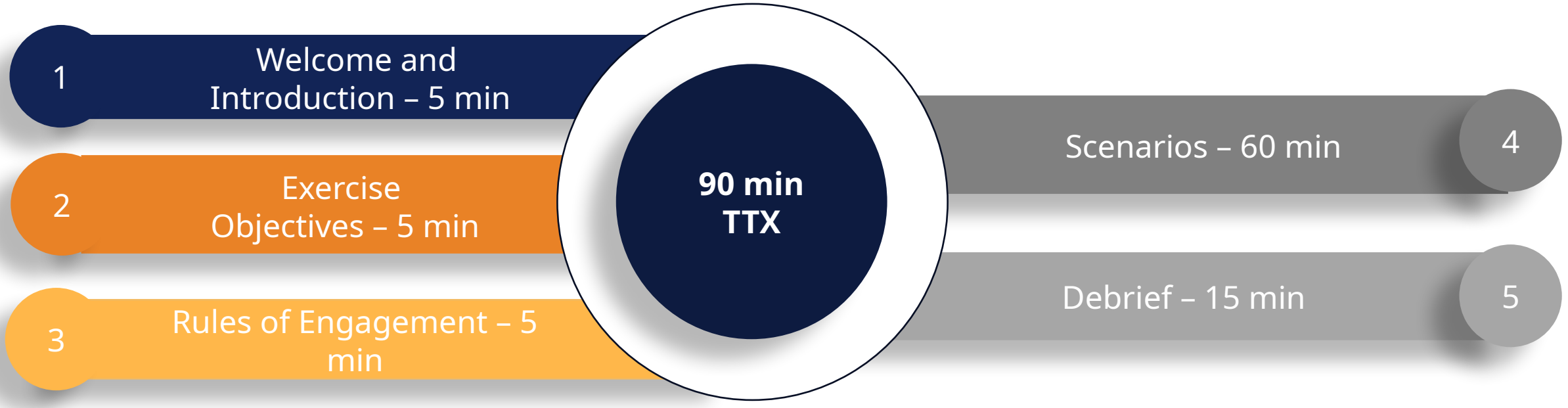
13. Competitive Advantage: Mention how strong cybersecurity preparedness can serve as a competitive advantage in the industry.

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.

How is a TTX Structured?



valencia Cyber Optimists. DEEPSEC

Who Sits in a TTX, and Why?

Role	TTX Responsibilities Overview
CEO	Provides overall leadership, ensures alignment with business objectives, and makes high-level decisions during the crisis.
CFO	Manages financial implications, evaluates the cost of the incident, and oversees budgeting for incident response efforts.
CIO	Leads IT response, ensures critical systems are protected, and supports the technical response to mitigate cybersecurity threats.
CISO	Directs the cybersecurity strategy, manages risk, leads the response to the breach, and ensures data protection during the incident.
Communications	Manages internal and external communications, ensuring accurate messaging and protecting the organization's reputation.
Legal Reps.	Advises on legal risks, compliance requirements, and manages any regulatory or litigation concerns arising from the incident.
HR Reps.	Coordinates personnel-related actions, including managing employee communication, handling insider threats, and ensuring workforce support.
Domain Experts	Provide specialized technical expertise to assess, contain, and resolve the cybersecurity incident based on their area of knowledge.

Breach Simulations

What do they look like?

Simulation Speed Run

WIN CREDZ AND PRIZES

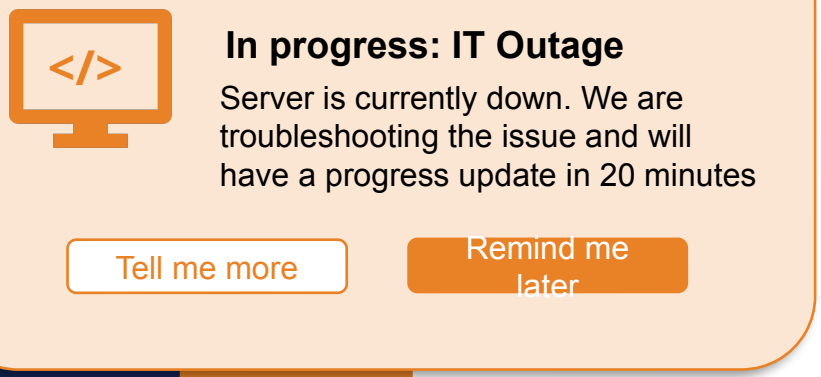
BY DISABLING

OPERATIONS

JOIN THE VIENNA AIRPORT CYBER SIMULATION

Inject 1

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



Inject 2

- **Initial Assessment from IT Department:**
  - Servers are inaccessible and unresponsive.
  - Email seems to be working okay.

Cyber Security Threat

Inject 2 (a)

- **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.

Inject 2 (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.

Inject 2 (c)

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.

Toolkit Slide – Breach Validation

- 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.

Toolkit Slide – Response Begins

- 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.

Cyber Security Threat

Inject 3

- **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.

Inject 3 (a)

Cyber Security Threat

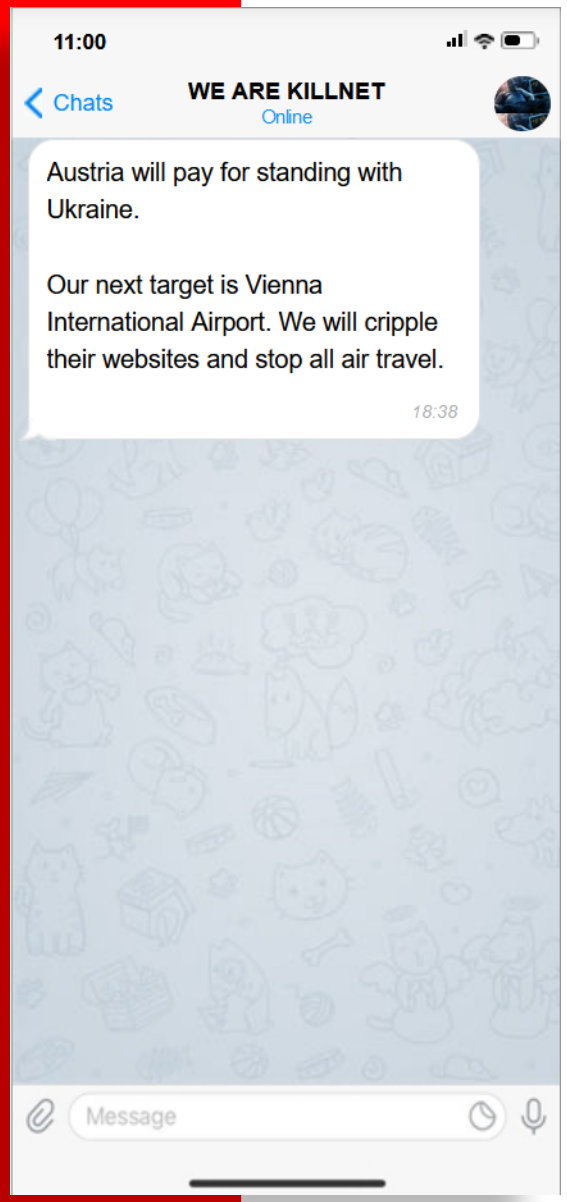
- **Note from Security:**
  - Arrival board has been compromised.
  - Displaying the following image:

Inject 3 (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.

Toolkit Slides: Pressurization Injects

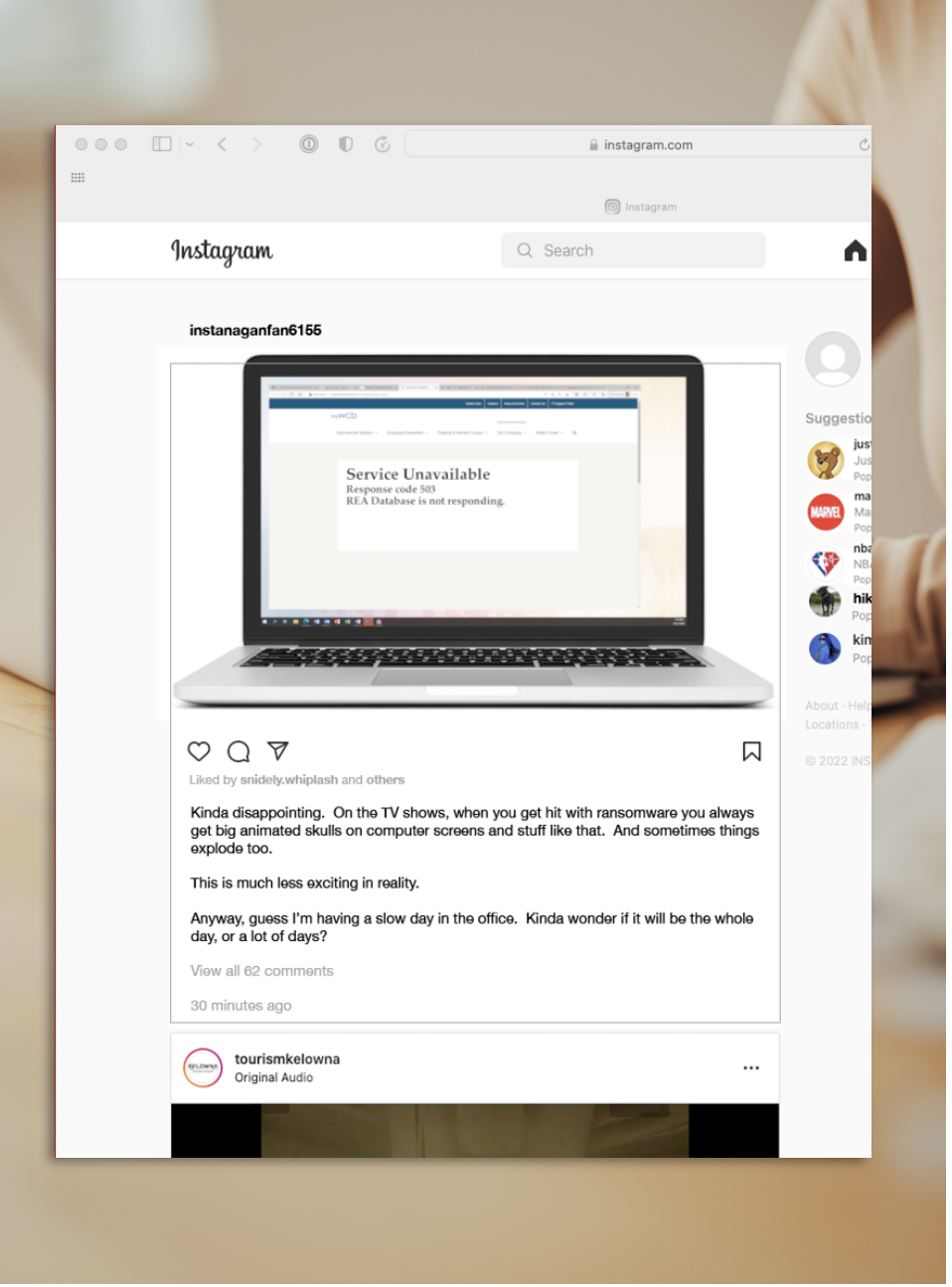
1. **Check Dependencies:** Even if seemingly unaffected, you should check the stability and security of key systems like OT, Payroll, and so on.
2. **Communicate Proactively:** Who is focusing on Comms? Know when and how to talk to law enforcement per regulatory and legal requirements. Hire a PR firm to handle outwards-facing communications as needed.
3. **Forge the Chain of Command.** Is the executive directing extra staff or consulting to IT and Cyber? Facilitate ongoing updates to the crisis management team to ensure cohesive response efforts.
4. **Forge the Chain of Custody.** Look for physical compromise and maintain a detailed account of all steps taken incident management steps; maintain a ledger of costs. Initiate collaboration with additional forensic analysis teams to deepen investigative efforts. Manually compile operational data from respective departments to maintain business continuity.
5. **Think outside yourself.** Consider consultation with legal counsel to navigate potential liabilities. Assess the need for temporary suspension of affected business processes.



Cyber Security Threat

Inject 4

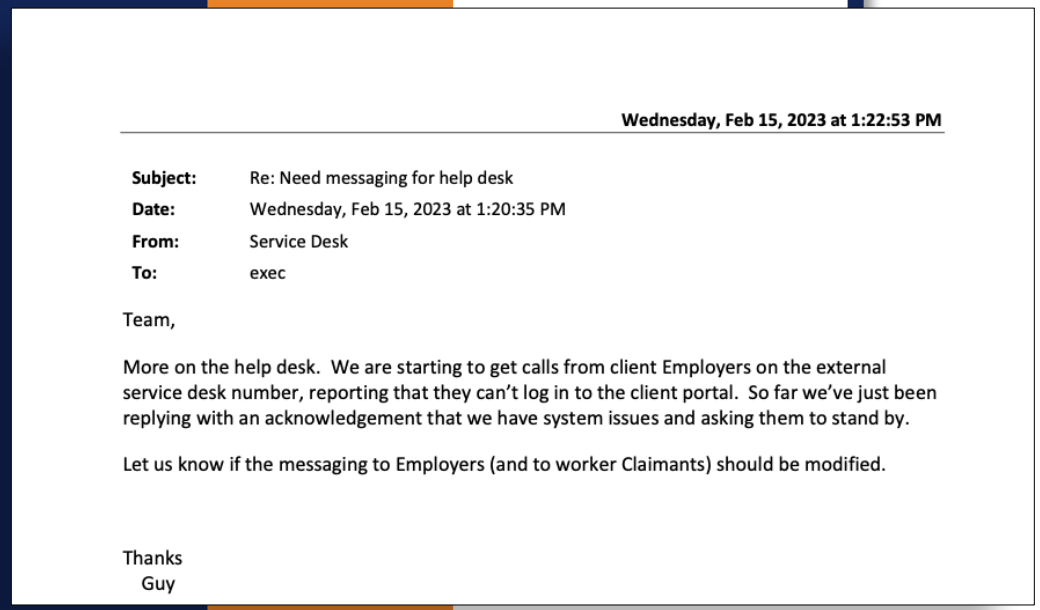
- **SOC has been made aware of a post on Telegram:**
  - Hacktivist group Killnet has announced they will be DDoSing the VIE airport.
  - No system outages have been reported yet.



Inject 4 (a)

- **A journalist from the Wienner Zeitung has reached out with a request for comment regarding the attack launched by Killnet:**
  - Noticed apparent employee post on Instagram alluding to ransomware attack.
  - Will this delay air travel?
  - How long until the systems are restored?

Inject 4 (b)



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.**

Toolkit Slide – Crunch Time

- 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@[redacted]
To: pgermain@[redacted]

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

- **Hackers have written again:**
  - They seem impatient.
  - Imply they may do something to turn up the heat.

Toolkit Slide - Hotwash

- 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.

Breach Simulations

How do we improve them?

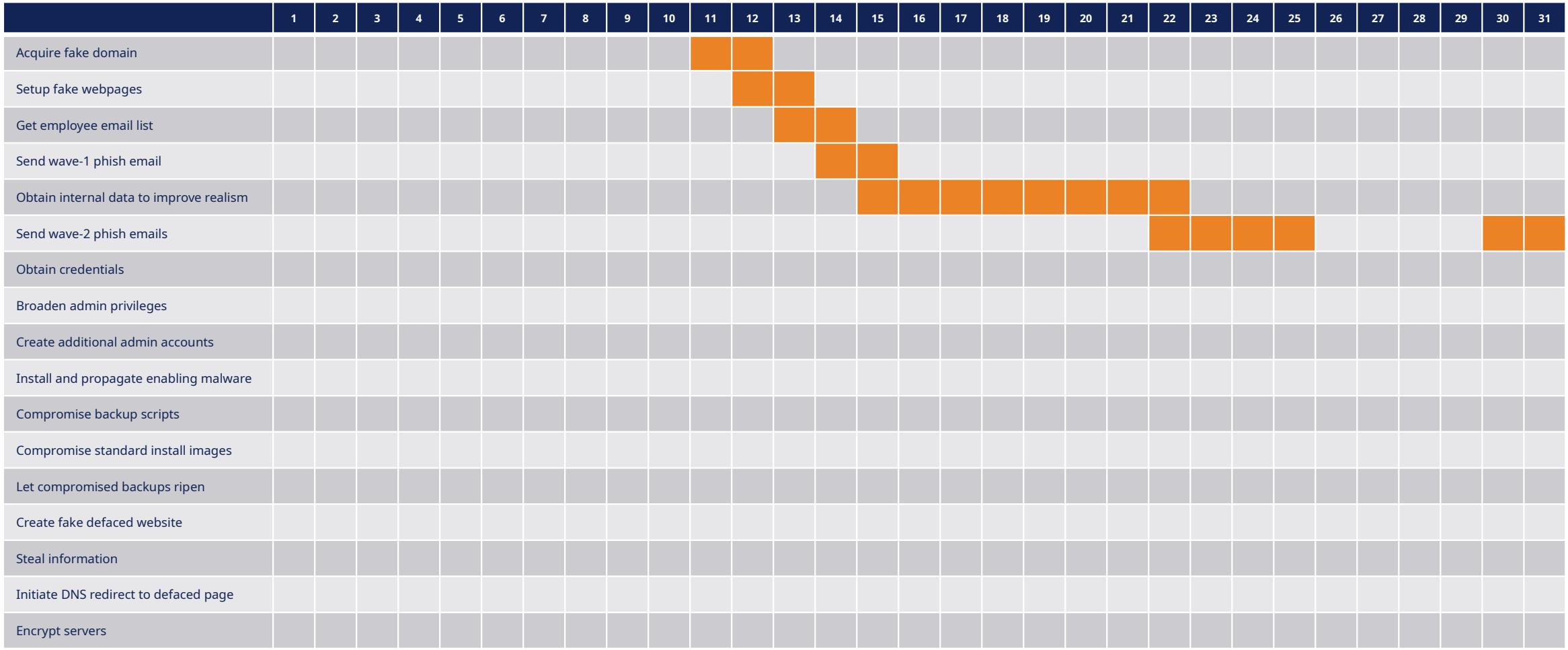
Building a Simulation

- [x] **Objectives:** Define clear goals for the simulation to ensure it aligns with the executive team's expectations and the organization's risk profile.
- [ ] **Scope:** Determine the breadth and depth of the simulation, including which systems, processes, and scenarios will be tested.
- [ ] **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.
- [ ] **Scenario Realism:** Choose scenarios that are relevant and challenging for the organization, possibly based on recent threat intelligence or known vulnerabilities.
- [ ] **Executive Engagement:** Ensure the simulation requires strategic decision-making, not just technical responses, to keep executives engaged.

A Good Simulation will Address

- [x] **Legal and Compliance Considerations:** Address potential legal and regulatory impacts of the incident, involving the legal team in the planning phase.
- [ ] **Communication Channels:** Plan how information will be shared among participants during the simulation, including the use of secure communications if necessary.
- [ ] **Incident Response Plan Review:** Ensure that the simulation tests the organization's incident response plan and identifies any gaps or areas for improvement.
- [ ] **Recovery and Business Continuity:** Include elements that test organization's ability to maintain or quickly resume critical operations during and after an incident.
- [ ] **Metrics and Success Criteria:** Define how success will be measured and what metrics will be used to evaluate the effectiveness of the response.
- [ ] **Debriefing and Lessons Learned:** Plan for a thorough debriefing session to discuss the outcomes, identify lessons learned, and develop an action plan for improvements.
- [ ] **Third-Party Involvement:** Decide if and how to include third-party vendors or partners who would be involved in a real incident response.
- [ ] **Confidentiality:** Ensure the scenario and discussions remain confidential to protect sensitive company information.
- [ ] **Resource Allocation:** Assess the resources needed for the simulation, including time, budget, and personnel.
- [ ] **Follow-Up:** Establish a follow-up process to address the findings and integrate them into the existing cybersecurity strategy and training programs.

Plan Well. The Technical Plan



valencia Cyber Optimists. DEEPSEC

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. **Unbelievable or 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 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. **Suspend Disbelief:** Do not expect every inject or scenario is ‘real-world’ for you. Your facilitator or planner may suck.
4. **Stay Role-Focused:** Stick to your designated role and responsibilities during the simulation to ensure a realistic response.
5. **Active Participation:** Engage actively in the simulation, contributing your technical expertise and asking clarifying questions.
6. **Effective Communication:** Clearly communicate technical information so that non-technical participants can understand.
7. **Realism in Actions:** Make decisions and act as in a real breach scenario, considering the limitations and pressures.
8. **Collaboration:** Work collaboratively with team members, understanding that cybersecurity is a cross-functional effort.
9. **Document Actions:** Track actions and decisions for review during debrief for learning points and improvement.
10. **Stress Management:** Practice maintaining composure under pressure, a crucial skill during actual incident management.
11. **Learn and Adapt:** Be open to feedback and be adaptable based on simulation's outcomes for continuous improvement.

Effective Behaviour and Practices

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

ToC from Word After Action Report

Table of Contents

valencia Cyber Optimists. DEEPSEC

Pavle's Perspective

- **Centrality of Preparation:** Tabletop exercises are essential for preparing teams to handle cybersecurity incidents effectively via a controlled environment.
- **Cross-Department Collaboration:** They are an excellent opportunity for different departments (IT, legal, PR, etc.) to work together. Tabletop exercises reveal gaps in coordination and help streamline communication processes.
- **Continuous Improvement:** Conduct a thorough debrief and identify areas for improvement. Regular exercises and updates based on lessons learned ensure that the incident response plan evolves with emerging threats.
- **Adaptation to Changing Threats:** The threat landscape is constantly evolving, so tabletop exercises should be regularly updated to reflect new tactics, techniques, and procedures used by cybercriminals.
- **Real-World Application:** The skills learned during these exercises should be regularly reproducible in actual security incidents to reinforce the training and ensure effectiveness.

Matias’ Musings.

- **Preparation Beats Panic:** Confidence comes from practice. TTX ensures readiness for real-world challenges
- **Real-World Relevance Matters:** Resources like The DFIR Report ground scenarios in actionable insights.
- **Collaboration is Key:** Cybersecurity specialists must unify teams under a shared goal during a breach.
- **Learn, Adapt, Repeat:** Every exercise is a stepping stone to stronger defenses and refined processes.
- **Leadership as a Cybersecurity Specialist:** Guide decisions with clarity and confidence, Build trust and foster collaboration across technical and non-technical teams.

Some Screws for your Toolkit

1. ecoDa Cybersecurity Risk Handbook
Website: ecoDa Cybersecurity Risk Handbook

- **Governance-Centric Guidance:** Bridges the gap between governance and cybersecurity practices.
- **Ransomware Readiness:** Strategies for assessing and preparing for ransomware incidents.
- **Cyber Risk Oversight Effectiveness:** Frameworks to enhance the board's role in managing cyber risks.
- **Incident Response Planning:** Guidance on developing effective recovery strategies..
- **Practical Guidance:** Provides metrics, M&A integration tips, and ways to foster CISO collaboration.

2. The DFIR Report
Website: The DFIR Report

- **Real-World Case Studies:** Provides in-depth, step-by-step reports on real cybersecurity incidents.
- **Actionable Intelligence:** Insights into attacker tactics, techniques, and procedures (TTPs).
- **Timely Updates:** Tracks emerging threats and trends to help stay ahead of adversaries.
- **Practical Learning:** Great for scenario building and enriching TTX exercises with real-world relevance.

3. Center for Internet Security (CIS) Tabletop Exercises
Website: CIS MS-ISAC Tabletop Exercises

- **Focus on Resilience:** Exercises aimed at building robust incident response capabilities.
- **Scalable Scenarios:** Designed for both small organizations and large enterprises.
- **Free Resources:** No-cost tools for governments, private sector, and academic institutions.
- **Alignment with Best Practices:** Based on CIS's well-established benchmarks and controls.

Some Screws for your Toolkit

4. NCSC Tabletop Exercise in a Box
Website: NCSC Exercise in a Box
•**Accessible Tools:** A free online tool for practicing responses to cyberattacks.
•**Variety of Scenarios:** Covers common cyber threats like phishing, ransomware, and insider threats.
•**Self-Paced Learning:** Allows organizations to practice exercises at their own convenience.
•**Comprehensive Support:** Includes all materials needed for planning, execution, and post-exercise review.

5. HackBack Gaming
Website: HackBack Gaming
•**Engaging Training:** Uses gamified cybersecurity challenges to train teams in an interactive way.
•**Scenario-Based Learning:** Builds both technical and soft skills in realistic, engaging simulations.
•**Team Collaboration:** Encourages teamwork and quick problem-solving during cyber scenarios.
•**Memorable Experience:** Makes cybersecurity training enjoyable and impactful.

6. CISA Tabletop Exercise Templates
Website: CISA Tabletop Exercise Packages
Comprehensive Guidance: Pre-built templates for various scenarios, from ransomware to supply chain attacks .
•**Customizable:** Tailored exercises for different industries and organizational sizes.
•**Credibility:** Developed by the Cybersecurity and Infrastructure Security Agency (CISA), a trusted authority.
•**Utility:** Includes discussion prompts, injects, and facilitation materials to make planning and execution seamless.

DEEPSEC

valencia

Cyber Optimists.

Thank you for participating.

cyberoptimist@valenciarisk.com