



# AR-IN-A-BOX

## How to Build your Custom Awareness Program

By Alex Zacharis  
(ARET,TREX,CBU)

BE THE STRONGEST LINK  
BREAK THE KILLCHAIN



# AGENDA

1. Why AR-In-A-Box?
2. Designing A Cyber Awareness Programme
3. Design Your Cyber Awareness Campaign
4. Promotion Tools And Channels
5. Cyber Awareness – Measuring Impact
6. Cyber Crisis Communication Guide



# CYBER AWARENESS PROGRAMME

*“A plan encompassing multiple awareness raising activities over a long period of time following the organizational strategy for cybersecurity”*

**OR**

*“An (internal) marketing strategy designed to raise **cyber security awareness.**”*

- Teaches employees **how to mitigate the impact of cyber threats.**
- Incorporates activities, materials and training to promote a **culture of cyber security.**



# WHY HAVE ONE?

- New threats are emerging.
- Organizations can no longer just rely on their technological defenses to be safe.
- Cybercriminals use sophisticated social engineering techniques to by-pass defenses.
- All it takes is one employee to click on a malicious link and it's game over!
- Your employees are your first line of defense.

**A comprehensive Cyber Security Awareness program is the best way to educate staff and create a security-first culture.**




# STILL NOT SURE?

## ISO 27001/2 & Information Security Awareness Training

For ISO 27001 compliance, it is essential to comply with **clause 7.2.2**.

The ISO 27001/2 clause 7.2.2 states:

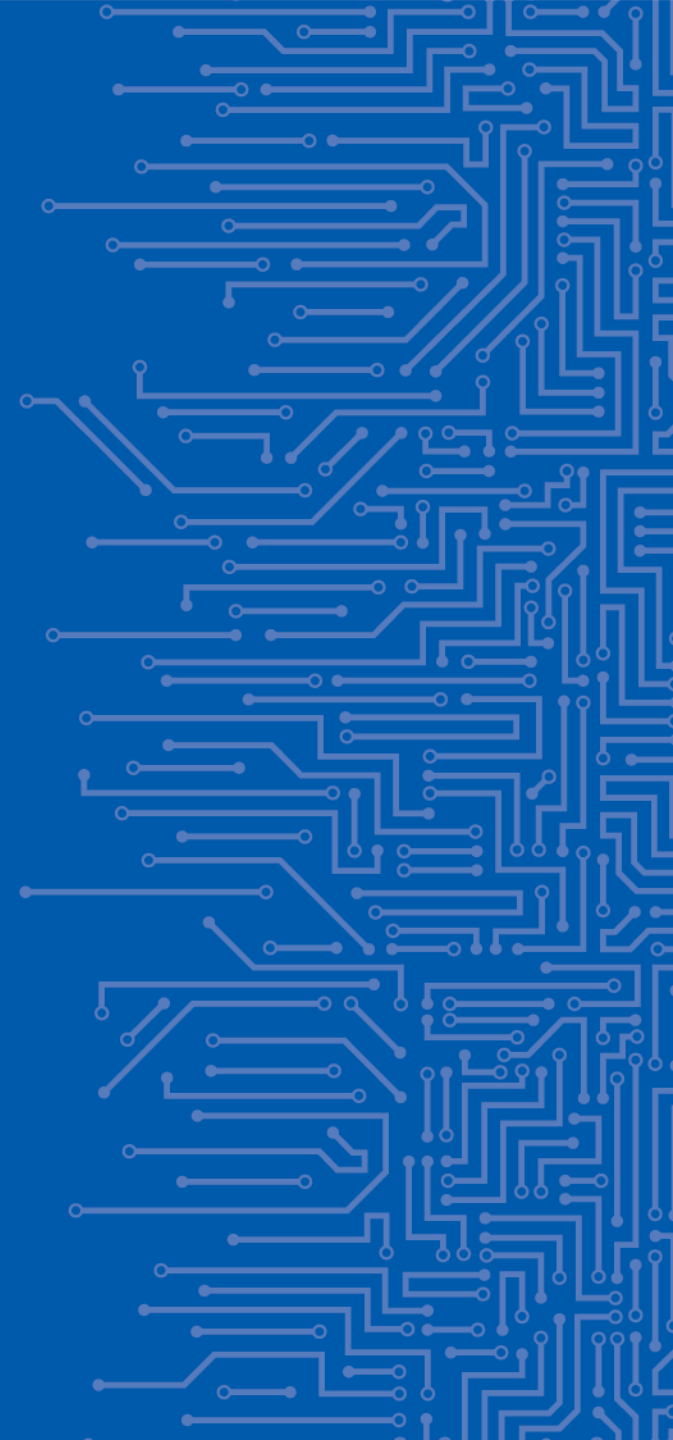


*'Information security awareness, education and training - All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function'.*

# AR IN-A-BOX



# DESIGNING A CYBER-AWARENESS PROGRAMM



# MAIN ACTIVITIES

In order to create an **internal** cyber-awareness programme, tailored to your employees' needs, you need to follow these 8 steps







# IDENTIFY OBJECTIVES

- The awareness-raising objectives stem from a risk assessment.
- Every organisation can set different objectives
- Some are always applicable
- Easy to convert to SMART objectives

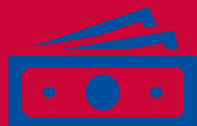
## Objectives:

1. **To raise cybersecurity awareness** by promoting cyber hygiene and providing guidance on good practices for individuals.
2. **To promote cybersecurity education and culture** within the organization by identifying communication channels and common language to be used.
3. **To be prepared for incidents** by identifying the right order of actions to be taken and to help key actors involved.

# SECURE FINANCIAL RESOURCES

## Management

- Plays critical role in the adoption and implementation of any awareness-raising activity.
- Catalyst role in the viability of an awareness-raising strategy
- Should be involved in the design and objectives-setting phase of the awareness programme from an early stage.
- Their vision can shift the scope of the strategy, based on their risk appetite.
- **Budget** allocation depends on their support.



## Securing the budget

1. Use real examples and statistics of the money to be saved or the risks to be avoided (based on the risk assessment)
2. Collect data on incidents and breaches from your organisation, or similar ones, to justify the need for an awareness-raising programme.



# ENSURE HUMAN RESOURCES (HR)



## Cybersecurity officer

- assist in the design of a programme



## Public relations and communications

- Disseminating the right message internally



## Information and communications technology (ICT)

- customise the content based on the operation reality



## Incident response teams

- feed the awareness programme with information



## Human resources

- promoting but also engaging the different target audiences



## Data protection office / legal department

- cover specialised security topics of the awareness-raising training agenda



## Instructors

- responsible for delivering the programme content to the target audience

# SETTING TARGET GROUPS

Target groups is paramount when developing a strategy for cyber awareness and cyber-culture development, as they improve the dissemination of key messages to the appropriate recipients.

Audience groups		Clustered audiences
1.	Generic employee	Generic employee
2.	Contractor	
3.	HR	
4.	Communications and marketing	
5.	Legal	
6.	Operations and research and development	C-level, decision-makers, handling budgets
7.	Finance and procurement	
8.	Managers, officers	
9.	Heads of unit, directors	
10.	Cybersecurity professionals	Professionals / horizontal implementors of cybersecurity measures and users of cybersecurity solutions, working for organisations and/or individuals
11.	Information technology (ICT) professionals	

# CHOOSE THE RIGHT TOOLS



## Infographics - Posters

Easy to deploy physically, e.g. in elevators, common spaces



## Ads - Videos

Able to hold and convey a lot of information



## TOOLS FOR AWARENESS RAISING



## Puzzles - Quizzes

Ensure and test understanding of concepts



## Live presentations

Direct interactions with participants



# CREATE A TIME PLAN

A time plan should be tailored to business activities, the workload and the topics of the campaign. Furthermore, do take into consideration that you need to devote time beforehand, in order to identify the current cybersecurity posture of the organisation

<b>January</b>  Baseline quiz	<b>February</b>  Training topic	<b>March</b>  Videos and dissemination material	<b>April</b>  Videos and dissemination material
<b>May</b>  Training topic 2	<b>June</b>  Simulation exercise	<b>July</b> HOLIDAYS	<b>August</b> HOLIDAYS
<b>September</b>  Back-to-school training	<b>October</b>  Games/test/quiz	<b>November</b>  Insights collections	<b>December</b>  Report to management



# IMPLEMENT THE PROGRAM

Three occasions are considered relevant for delivering cybersecurity-awareness training to your employees

## Onboarding

- When someone joins an organization, induction to its cybersecurity culture is important

## Post-incident

- If a security incident occurs in your organization, it can be a good time to offer a refresher course.

## Continuous

- The idea here is to set up a curriculum that covers the most common security threats (this will change over time as new ones come to the fore) and keeps cybersecurity top of mind through a regular cadence of education and awareness.

# EVALUATE THE PROGRAM

Upon implementation of the programme, you need to assess its effectiveness in order to identify the lessons learned and the changes that may need to be made in the future.





# GAMIFICATION EXAMPLES



# CYBER AWARENESS GAMES

## Gamification helps!

- ✓ Determine how your team will react to a theoretical cyber attack and how effective your plan is.
- ✓ Identify flaws or gaps in the organization's response and make adjustments
- ✓ Testing consequences in a safe environment
- ✓ Coordination between different departments
- ✓ Save money



# TABLE-TOP GAMES

**DOUBLE WAY DOOR**  
**SECURE DOOR WITH PIN**  
**EMERGENCY EXIT**

**CLUELESS Joe**  
 ICT  
 ID: IT23RL2

**CLICKALL Jack**  
 LEGAL  
 ID: AL3XZA4

**MILL Anna**  
 CFO  
 ID: FA23RN1

**DARC Marc**  
 ICT - Contractor  
 ID: IT21NO6

**MARLY Maria**  
 ICT  
 ID: IT11NI9

**MEGACORP  
 FLOOR PLAN  
 & ACCESS BADGES**

The floor plan shows a 'SERVER ROOM' with three servers, a 'SECURE AREA' with four desks (#1-#4), and various rooms with door types indicated by red and blue labels. Room numbers 731, 732, 733, 734, and 735 are also marked.

## SCENARIO - MEGACORP HACKED

MegaCorp, a leader in online retail has been hacked based on information leaked on the public internet.

Attackers appeared to have gained initial access via a successful **PHISHING ATTACK**.

To make matters worse **UNAUTHORISED ACCESS** has been detected in MegaCorp headquarters and a **RANSOMWARE** hit the company the same day.

You are the lead Cyber Security Investigator recruited to provide answers on who is behind the hack and try to stop him/her before its too late.

We generated as much evidence as possible. Analyze them quickly.

You have 30 minutes left before all our data are wiped out.

**(GOOD LUCK)**

## ANSWER SHEET

What is the name of the first known victim of the PHISHING ATTACK?  
 (Name Surname as seen in the Badge with space\*)

Which Badge ID was used to performed unauthorized access?

ENCIPHERMENT KEY

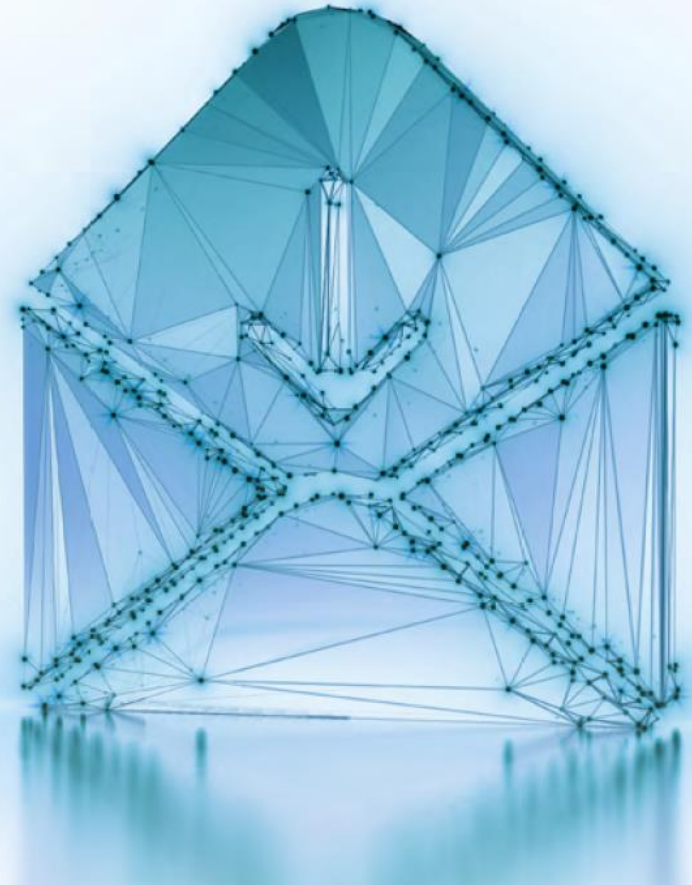
What is the filename of the decrypted file?

The answer sheet includes a grid for the name, a diagram for the badge ID, a grid for the encryption key, and a grid for the filename. A calendar icon with a checkmark is also present.

# WHICH TYPE OF CYBER-ATTACK IS COMMONLY PERFORMED THROUGH EMAIL?



- A Phishing**
- B Smishing**
- C Vishing**
- D Ransomware**



# ONLINE GAMES

## AR-in-a-Box Game

🕒 Less than an hour    📖 Intermediate

### Course details

AR-in-a-Box is a comprehensive solution for cybersecurity awareness activities designed to meet the needs of public bodies, operators of essential services, and both large and small private companies. It provides theoretical and practical knowledge on how to design and implement effective cybersecurity awareness programmes.

This course provides an example of an awareness raising game in order to self evaluate any audience on their awareness level against popular cyber threats.

### Target audience

Anyone can play this game after receiving a basic cyber awareness training.

### Learning objectives

Solve the riddle by answering to some questions and prove that you are cyber aware.

### Offered by

This content is offered by the European Union Agency for Cybersecurity (ENISA). ENISA is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe.



★★★★★ 5 (1)

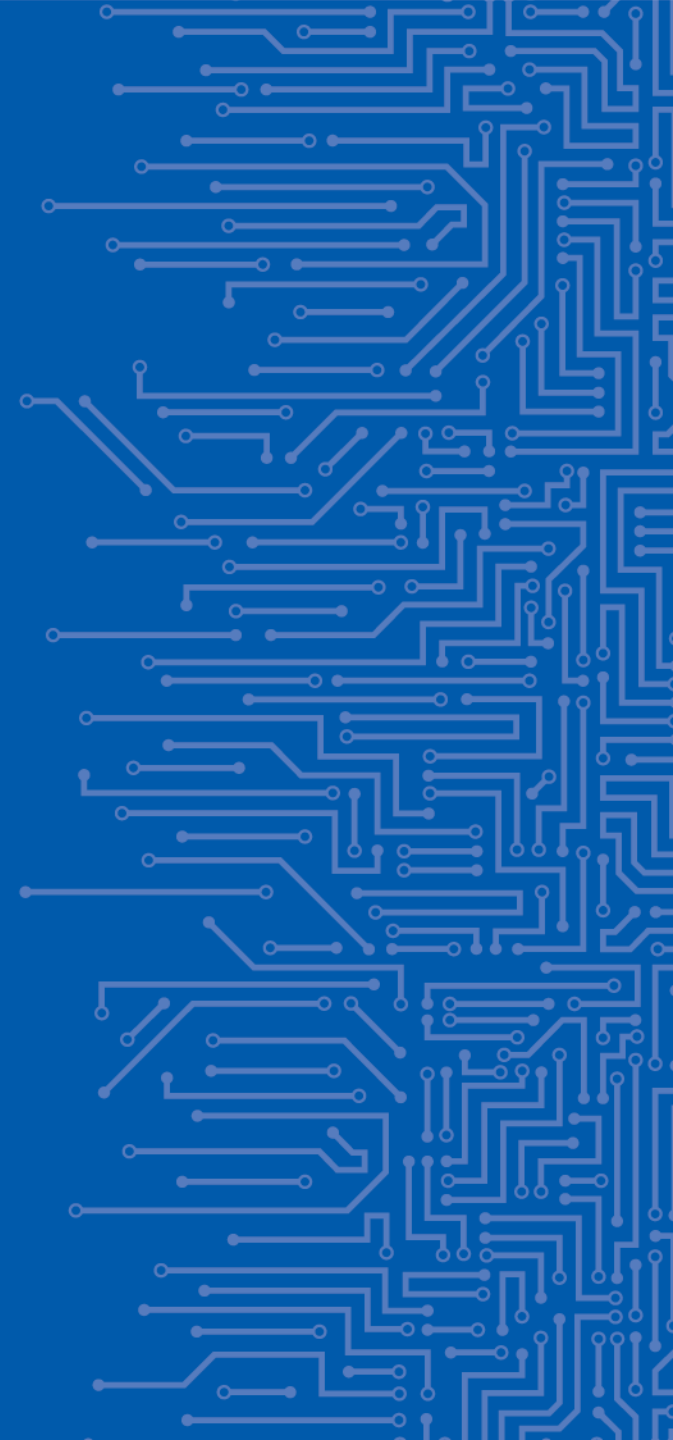
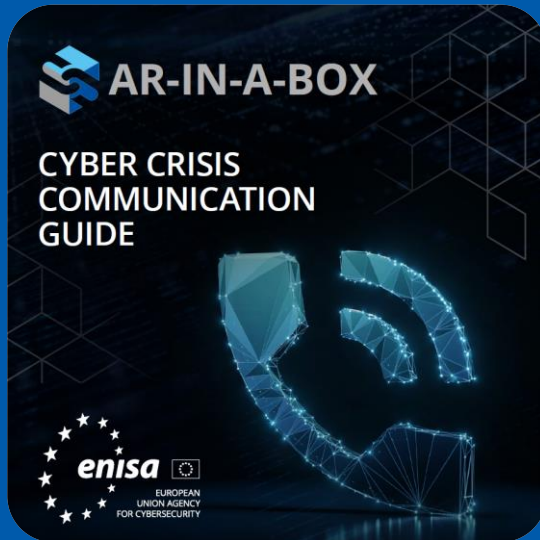
### Schedule

- Introduction
- The Game: Online Retail Hack Investigation
- Closure & Conclusions



[academy.europa.eu/courses/ar-in-a-box-game](https://academy.europa.eu/courses/ar-in-a-box-game)

# CYBER CRISIS COMMUNICATION GUIDE





IT'S NOT JUST  
THE CRISIS  
ITSELF  
THAT  
CAN  
SHAPE  
OPINION

## HOW AN ORGANIZATION **RESPONDS**

TO A CRISIS MAY HAVE A MORE  
SUBSTANTIAL IMPACT THAN  
THE CRISIS ITSELF.

85%

of people form opinions  
about organisations  
based on how they  
react in times of crisis

36%

of people have  
discussions with others or  
share information about  
organisations' scandals or  
wrongdoings



# WHY HAVE A COMM CRISIS GUIDE?

- ✓ Compliance
- ✓ Negative publicity mitigation
- ✓ Be effective in handling the incident
- ✓ Be on top of the narrative

When a disaster strikes, it is essential for an organisation be able to communicate internally and externally about the incident.

- If an organisation is unable to keep the outside world informed of its recovery status, the public is likely to fear the worst and assume that the organisation is unable to recover
- It is necessary that the organisation communicates about disaster internally so that employees know what steps they are expected to take in that situation





# PURPOSE OF THE GUIDE

## **Set of guidelines to:**

- 1. Ensure professional and coherent approach to dealing with a crisis situation.**
- 2. Towards a consistent use of public communication messages by all relevant stakeholders.**

## **What can be expected from the Guide?**

- Common language & framework for building a crisis communication management capability.**
- Practical guidance for crisis communications management.**



# SOME GOOD EXAMPLES... ON WHAT TO AVOID

**Yahoo:** In 2016, Yahoo experienced a series of data breaches that affected billions of user accounts. The company's crisis communication response was criticised for its delayed disclosure of the breaches. Yahoo faced backlash for not promptly notifying affected users, which led to a loss of trust. The lack of timely communication and transparency damaged Yahoo's reputation and raised concerns about user data protection.

**Link:** [Yahoo Data Breaches](#) and [analysis](#)

**Sony Pictures:** In 2014, Sony Pictures experienced a cyber-attack that resulted in the leak of sensitive emails, employee data, and unreleased movies. Sony's crisis communication was criticised for downplaying the severity of the breach initially and not adequately informing employees about the situation. The leaked emails revealed internal discussions that were damaging to the company's reputation. Sony's communication lacked transparency and failed to effectively manage the crisis.

**Link:** [Sony Pictures Cyber Attack](#)



# BETTER DO THIS

**Equifax:** In 2017, Equifax, a credit reporting agency, suffered a massive data breach that exposed sensitive personal information of millions of consumers. Equifax's crisis communication response was swift and proactive. The company established a dedicated website to provide clear and timely information about the breach, including details on the incident, steps to check if one's data was affected, and instructions on how to enrol in credit monitoring. Equifax's CEO issued a public statement acknowledging the breach, and the company offered free credit monitoring and identity theft protection services to affected individuals. The communication was transparent, informative, and included consistent updates.

**Link:** [Equifax Data Breach Response](#)

**Maersk:** In 2017, global shipping company Maersk fell victim to the NotPetya ransomware attack, causing significant disruptions to its operations. Maersk's crisis communication was effective in conveying the severity of the situation, without disclosing sensitive details. The company utilised social media platforms to share updates on its response efforts, openly acknowledging the impact on its operations, while reassuring customers about its commitment to resolving the issue. Maersk's CEO communicated directly with stakeholders through video messages, providing a human touch to the crisis response.

**Link:** [Maersk Twitter Updates](#)



# WHAT ARE THE INGREDIENTS TO SUCCESS?

- ✓ **SPEED**
- ✓ **TRANSPARENCY**
- ✓ **CONSISTENCY**
- ✓ **PROFICIENCY**
- ✓ **HUMAN ELEMENT**
- ✓ **SENSE OF CONTROL**

# SCALING YOUR CYBER CRISIS COMMUNICATION PLAN



Assess  
cybersecurity  
risks



Review regulatory  
requirements



Evaluate  
organisational size  
and complexity



Identify key  
stakeholders



Analyse reputation  
and brand risk



Conduct a gap  
analysis



Consult with  
cybersecurity and  
communication  
experts



Consider Lessons  
learned and best  
practices



# SETTING CLEAR OBJECTIVES

- ✓ **Protect the organisation's reputation**
- ✓ **Provide timely and accurate information**
- ✓ **Ensure customers or stakeholders are informed**
- ✓ **Mitigate the impact of the crisis**

# TRADITIONAL CRISIS MANAGEMENT





# YOUR TEAM

- ✓ **The Incident Manager**
- ✓ **The Spokesperson or Communications coordinator**
- ✓ **Technical Expert**
- ✓ **Legal Advisor**
- ✓ **Human Resources Representative**





# INTERNAL AUDIENCE AND COMMUNICATION CHANNELS

Audience groups	Channels
<b>Generic Employees</b>	<b>Email communications, company-wide meetings or town halls, intranet portals, and employee communication platforms or apps.</b>
<b>Executives and Management</b>	<b>Targeted email communications, leadership meetings or conference calls, dedicated executive communication channels, and secure messaging platforms.</b>
<b>IT and Security Teams</b>	<b>Channels such as dedicated incident response platforms, secure collaboration tools, and direct communication channels should be utilised to reach these teams.</b>
<b>Internal Stakeholders</b>	<b>Tailored communication channels, including targeted email communications, team meetings, or designated communication liaisons, should be utilised to reach them effectively.</b>

# EXTERNAL AUDIENCE AND COMMUNICATION CHANNELS

Audience groups	Channels
Customers	Direct communication line via email or SMS, few hours after the incident have been identified. In some cases, the IT can contact them directly to provide advice or mitigation measures.
Partners and Suppliers	Targeted email communications, designated communication liaisons and in some cases direct communication channels between IT and Security Teams (point of contact – PoC).
Regulatory Authorities	A dedicated platform, or via email or direct phone call. The organisation must be informed and hold this information in the incident response policy.
Media	Designated communication liaisons or communication lead should reach targeted channels or media with tailor made statements and messages.
Investors and Shareholders	Tailored communication channels, including targeted email communications, shareholders meetings, or designated communication liaisons, should be utilised to reach them effectively.
General public	Communication via the mass media can have great outreach to the local community and general public. Tailor made messages to ensure mitigation measures are important.



# ASSESS & CUSTOMIZE

## What to assess in an incident:

- **Affecting safety and wellbeing of people**
- **Affecting the reputation of the organisation**
- **Possible political implications**
- **Affecting the establishment of the organisation**
- **Legal implications or lack of compliance with current regulation**
- **Affecting the confidence of the organisation towards stakeholders**

**This step can define SEVERITY!**



# SOME PRINCIPLES TO SOLIDIFY ACTIONS

- **Acknowledge the crisis:** Do not try to hide if/when there is an incident developing, but be careful not to take ownership or responsibility for a crisis that is not the organisation's responsibility.
- **Act swiftly and decisively:** As soon as the incident is identified, activate the crisis communication plan, delays lead to speculation, misinformation and reputational damage.
- **Communicate what the organisation knows:** Provide factual information only, without judgment, emotion or guessing.
- **Clear and Transparent:** Responses should be timely, accurate and consistency, despite the likely external media and stakeholder pressure.
- **Show empathy:** It is important to express concern for any affected parties, whether internal or external; take responsibility and apologise if it is demonstrably at fault.
- **Action-oriented:** Detail the steps being taken to remedy the situation and avoid it happening again in order to reassure key stakeholders.
- **Provide perspective:** Place the situation into context.
- **Tailor messages to different stakeholders:** provide each group with necessary information, guidance and support.
- **Establish clear lines of communication:** Provide contact information, such as dedicated hotlines or email addresses, to facilitate communication and ensure that queries and concerns are addressed promptly.
- **Leverage social media and online platforms:** Monitor relevant hashtags and keywords to stay aware of public sentiment and address any emerging issues or misinformation proactively.
- **Manage media effectively:** Maintain a proactive approach in managing media inquiries, providing accurate information, and promptly correcting any inaccuracies or misleading reports.
- **Provide ongoing updates:** Acknowledge the need for ongoing communication to maintain engagement and reassure stakeholders that the issue is being addressed.
- **Conduct "Hot wash/ Cold wash" exercises after the crisis is resolved to capture findings and comments.**



# ACTION TIME

## USE CASE

**An energy service provider's servers have been compromised by a ransomware attack, resulting in significant data loss and production downtime.**

**Internal COM Actions:**

1. Activate the cyber crisis communication team and establish a clear chain of command.
2. Assess the severity of the incident and prioritise the Comm response effort.
3. Notify employees of the incident and provide guidance on how to respond.
4. Provide regular updates to employees and stakeholders as the situation evolves.

**External COM Actions:**

1. Notify customers and suppliers of the incident and provide guidance on any impact on their operations.
2. Contact law enforcement and report the incident.
3. Work with legal counsel to ensure compliance with data protection regulations and other legal requirements.
4. Draft and disseminate public statements to media outlets and manage media relations.
5. Monitor social media channels and respond to inquiries from stakeholders.
6. Notify insurance providers and work with them to file a claim.

## INTERNAL COMMUNICATION EMAIL EXAMPLE

*Subject: Cyber Incident Update*

*Dear Employees,*

*As you may be aware, we recently experienced a cyber incident that has impacted our systems and operations. Our IT team is actively working to restore systems and data and minimise the impact of the incident.*

*We want to assure you that the safety and security of our employees, customers, and stakeholders is our top priority, and we are taking all necessary steps to address this incident. We have activated our cyber crisis communication team and are working closely with IT and other stakeholders to manage the incident.*

*We will provide regular updates as the situation evolves and appreciate your patience and understanding during this challenging time.*

*Sincerely,*

*[Your Name]*



## EXTERNAL COMMUNICATION EXAMPLES

### External Communication Website News Post Example:

*Subject: Important Update: Cyber Incident Notification*

*We want to inform our customers and stakeholders that we have experienced a cyber incident that has impacted our operations. We are actively working to restore systems and data and minimise the impact of the incident. Our cyber crisis communication team is working closely with IT and other stakeholders to manage the incident. The safety and security of our customers, employees, and stakeholders is our top priority. We will provide regular updates as the situation evolves. Thank you for your understanding and support*

### External communication tweet example:

*Important Update: We have experienced a cyber incident impacting our operations. We're working to restore systems & data with the safety & security of our customers, employees, and stakeholders as our top priority. Regular updates to follow. #cybersecurity #incidentresponse*



# EXERCISING THE PLAN

Tabletop Exercises

Functional Exercises

Full-Scale Exercises

Lessons learnt and lines to take



# KEY TAKEAWAYS

1. Conduct regular risk assessments
2. Have clear communication protocols and from a team
3. Train employees

## How to prepare

1. Set activation thresholds for the team
2. Communicate clearly and transparently
3. Manage the media pressure by prioritizing & Triaging

## How to react

### Key Don'ts:

1. **Don't assume that your organisation is immune to cyber-attacks.**
2. **Don't delay in responding and communicate with stakeholders in a timely and transparent manner.**
3. **Don't rely solely on technology to protect you**

## How to learn

1. Review case studies
2. Conduct an aftermath assessment
3. Regularly update and review the plan



**AR-IN-A-BOX**

**Thank you**

**BE THE STRONGEST LINK  
BREAK THE KILLCHAIN**

