AR-IN-A-BOX

HOW TO PROMOTE CYBER SECURITY AWARENESS TO C-LEVEL: A GUIDE

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

CONTACT

For contacting ENISA please use the following details:
info@enisa.europa.eu
website: www.enisa.europa.eu

LEGAL NOTICE

COPYRIGHT NOTICE

Catalogue number: TP-09-22-595-EN-N
ISBN: 978-92-9204-596-8
DOI: 10.2824/65774

1. SCOPE

Cybersecurity awareness programmes are key to eliminating the human risk inherent in any organisation.Often, higher management can become a blocker, as they fail to see the value of awareness-raising against cybersecurity attacks. Senior management typically have little or no knowledge of how cybersecurity-related human risks can negatively impact their organisation. In addition, due to limited availability and attention span, the C-suite is one of the hardest groups to engage.

This guide will help you secure C-suite support for the deployment of cybersecurity awareness programmes through concrete steps.It provides good practices and tips to ease the introduction and conversion of C-level staff from initial supporters to eventual ambassadors of your cybersecurity awareness programme.Fostering a strong understanding of cybersecurity at the C-level,will emphasise its importance and push it higher on the organisation's list of priorities, thereby increasing overall maturity in this area. The entire company's culture and behaviour regarding cybersecurity can be influenced and improved.

Overall, C-level ambassadorship will significantly enhance the effectiveness of your awareness programme and ensure strategic business alignment. Furthermore, it can support cultural transformation, compliance with internal or external requirements, overall resilience, resource allocation, and business continuity.

2. HOW TO GET THE C-LEVEL ON BOARD

Studies have shown that one of the most difficult target audiences for cyber awareness programs are the C-level executives. There are various reasons for this:

- Lack of time i.e. Managers have busy agendas full of meetings or important discussions; awareness trainings requiring 1 hour are very hard to fit in the busy schedule.
- Business goals not aligned i.e. The cyber awareness training is not as important as the board meeting of directors or the customers' meetings.
- Cost vs investment i.e.They don't see the value of having a training for all staff on such a "niche" topic.
- Risk tolerance i.e. Nothing so bad will happen if a cyber incident takes place, is it such big of a deal?
- Power of delegation i.e. Information is handled by assistants, the knowledge should be on them.

Taking all the above into account, achieving the goal of not only informing but also involving the C-suite in cybersecurity practices requires a smart approach, especially when there are limited resources. It's essential tobe efficient and, where possible, creative.

Below are a few steps to help you better prepare and pique the interest of C-level executives.

This process may be revised and restarted from Phase 1 every three years, particularly when there is a change in C-level executives or when a new awareness programme is introduced.

PHASE 1: GET INFORMED

Measure & Understand Organisational Maturity

Assess the current maturity level of the organisation's cybersecurity practices. Prepare realistic examples (if you havecases, it is better to use specific cases as scenarios), as these are important to build narratives.

Align Organisational Objectives

Understand the organisation's vision, mission, and strategy, along with the perspectives of its executives regarding cybersecurity.

Understand and Clarify the Type of Support

The type of C-level support required is closely related to the organisation's maturity level.

However, some types of support, such as strategic support, may always be necessary, as C-level executives are important ambassadors for the organisation. Before reaching out to C-level personnel, ensure you understand what type of support you really need.

Type of engagement/role/objective(what do I expect from my c-suite?)		
1. Strategic support	1.1 Endorsement and advocacy	• Endorse the cyber awareness program and forge a partnership. • Act as champions and ambassadors for the cybersecurity initiatives
	1.2 Integration with Business Strategy	• Ensure cybersecurity is embedded into overall strategy, think security by design • Align cybersecurity goals with business objectives, thinksustainable
2. Resource allocation	2.1 Financial resources	• Allocate sufficient budget for cybersecurity awareness initiatives, including training, tools, and other campaign materials. Review periodically
	2.2 Human Resources	• Dedicate personnel to manage and execute the cyber awareness program • Hire or consult with cybersecurity experts
3. Training and Development	3.1 Executive Training	• Participate in cybersecurity training specific c-level executives, like decision making in case of cyber incident on the organisation. • Encourage other executives to undergo similar training
	3.2 Organization-Wide Training	• Promote and support continuous cybersecurity education for all employees
4. Communication & Culture	4.1 Internal Communication	• Regularly communicate the importance of cybersecurity to all employees • Share success stories and lessons learned from cybersecurity initiatives
	4.2 Culture Building	• Foster a cultureof security awareness and proactive behaviour • Recognize and reward good cybersecurity practices among employees

PHASE 2: CREATE UNDERSTANDING OF CYBER SECURITY AND BUILD PARTNERSHIP

Common concerns among executives should be carefully considered in order to effectively advocate for the implementation of a cyber awareness program. Depending on the organization's maturity, keep the following in mind:

1. Facts & Figures

Argument: "How does a cyber awareness campaign align with our company strategic goals?" "Why is it crucial?"

Response:

1. Demonstrate Human Risk

- Share real-world examples by using industry-specific case studies that illustrate the potential damage caused by human errors or social engineering attacks.

- Highlight the financial impact of a breach. Where possible, show the financial losses incurred due to human error in recent breaches, or emphasise the cost savings achieved through awareness training that prevents attacks.

2. Demonstrate Alignment with Strategic Goals

- Use data to demonstrate how improving cybersecurity through awareness aligns with key strategic goals, such as protecting intellectual property, maintaining customer trust, and avoiding costly data breaches or GDPR fines.

- Cite industry benchmarks and competitors. If competitors are investing in cybersecurity awareness, present this as a strategic advantage that your company should also leverage to remain competitive.

2. Legislation

Argument: "How does this align with legal and regulatory requirements?"

Response:
Use cybersecurity regulations or frameworks (e.g., GDPR, CCPA, ISO 27001) to highlight the need for compliance. Emphasise how non-compliance could result in significant fines or reputational damage.

3. Role & Influence

Argument: "How does this programme leverage our employees?" "Why do I have a role in this?"

Response:

- Clarify the roles and influence of executives in enhancing cybersecurity. Describe their function as both the first and last line of defence, and explain their impact on fosteringa cyber-aware workforce culture.

- Use non-technical language and avoid jargon. Frame discussions around how cybersecurity contributes to business continuity, regulatory compliance, and maintaining customer trust.

- Tailor the message to their specific focus areas. Each executive has different priorities (e.g., the CFO focuses on cost savings, the CEO on reputation). Customise your pitch accordingly.

4. Company objectives

Argument: "How does this support our business objectives?"

Response:

- Align Cybersecurity with Business Objectives.

- Translate cybersecurity risks into business risks. Senior management is focused on business outcomes, so demonstrate how cybersecurity incidents can lead to financial loss, reputational damage, operational disruptions, and legal liabilities.

- Use metrics that matter to them. Focus on key performance indicators (KPIs) such as financial loss, downtime, or productivity impacts resulting from cyber incidents, rather than technical metrics.

- Present cybersecurity as a competitive advantage. Emphasise how strong cybersecurity can protect intellectual property, ensure customer trust, and facilitate regulatory compliance, ultimately enhancing the company's market position.

5. Resilience

Argument: "How does this enhance our organisational resilience?"

Response:

Explain how robust cybersecurity strengthens the organisation's resilience, helping it withstand and recover from cyber threats and other disruptions.

PHASE 3: MAINTAIN AND INCREASE SUPPORT

Take into account the following advice to maintain and increase C-level support for the cyber awareness programme, ensuring its long-term effectiveness and fostering a resilient cybersecurity culture within the organisation.

1. Consider AR-in-the-Box general tips for the design and implementation of an effective cybersecurity awareness programme

2. Develop a clear strategy and objectives for C-level executives in the awareness programme

- Formulate a strategy outlining the role of C-level executives in the awareness programme, or as part of a standalone campaign.
- Break the programme down into manageable steps. Present a roadmap with clear milestones, timelines, and expected outcomes to minimise the perception that awareness programmes are complex or disruptive.
- Define key performance indicators (KPIs).

3. Continuous engagement and communication

- Review performance, gather feedback, and analyse it to make necessary adjustments.
- Regularly update the cybersecurity awareness programme and topic-specific campaigns.
- Provide regular updates and reports to C-level executives on the programme's status and successes, including performance, feedback, and improvements.
- Demonstrate early successes. As the programme progresses, showcase improvements such as reduced phishing susceptibility or quicker incident response times. Regularly share reports highlighting progress and return on investment.
- Involve C-level executives in decision-making. Seek their input on key decisions, such as which departments to prioritise, which KPIs to track, and who should oversee the programme.
- Turn executives into ambassadors. Once you have their support, encourage them to champion the programme internally by promoting it in communications and emphasising its importance in meetings.
- Create visible engagement. Encourage C-suite participation in cybersecurity events, town halls, or awareness campaigns to reinforce the significance of cybersecurity across the organisation.

3. C-LEVEL INTERACTION TIPS

Find below a list of tips on howtoengage or respond in the usually expected questions that will rise during your conversation with C-Level managers. The statistics used below are an extract of real C-Level interviewed on the topic by our experts in order to better understand their mindset and expectations.Take the following recommendations on board for future engagements.

Which approach would convince a C-LEVEL about the gravity of having a cybersecurity awareness raising programme in place, for her/ his organization?

Being presented with the dangers of negligence, as well as examples of attacks on organisations and their implications.	38.89 %
Being presented with the statistics of how much money was saved and/ or how many threats were averted, in organisations where cybersecurity policies were systematically communicated and implemented.	27.78 %
A list of the top human threats your organization is facing and the impact of each one (in terms of cost, reputation etc.) if not mitigated through cyber awareness.	27.78 %
Being presented with the amount of money your organization will lose, in the case ofan attack, as well as the damage that its reputation will suffer.	5.56 %

Which would be a follow up question expected after the above?

Human Risk-related questionsto better understand the problem? Is it something I can force my team or the organization to do?	50.00 %
Inquiry about the amount of engagement required. What does the C-Level have to do and how often?	39 %
Cost-related questions. Does this affect the C-Levels budget?	11%

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu