



EUROPEAN UNION AGENCY  
FOR CYBERSECURITY

# AR-IN-A-BOX : BUILDING A CUSTOM CYBER AWARENESS PROGRAM

Dimitra Liveri  
Team Leader for Awareness raising and Education

12 | 10 | 2022

# CYBER AWARENESS PROGRAM

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

- 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**.

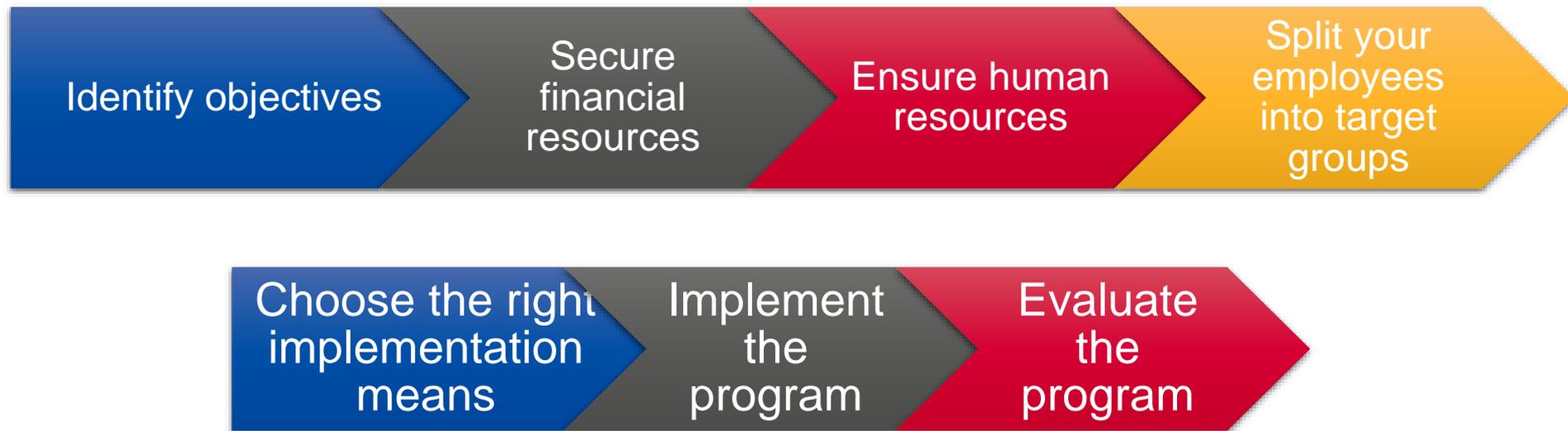
The ISO 27001/2 clause 7.2.2 states:



*'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'.*

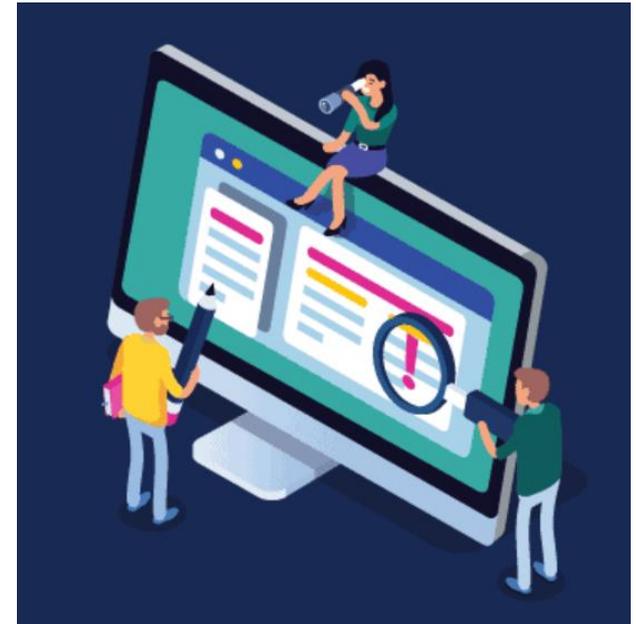


# HOW TO BUILD THE PROGRAM



# IDENTIFY OBJECTIVES

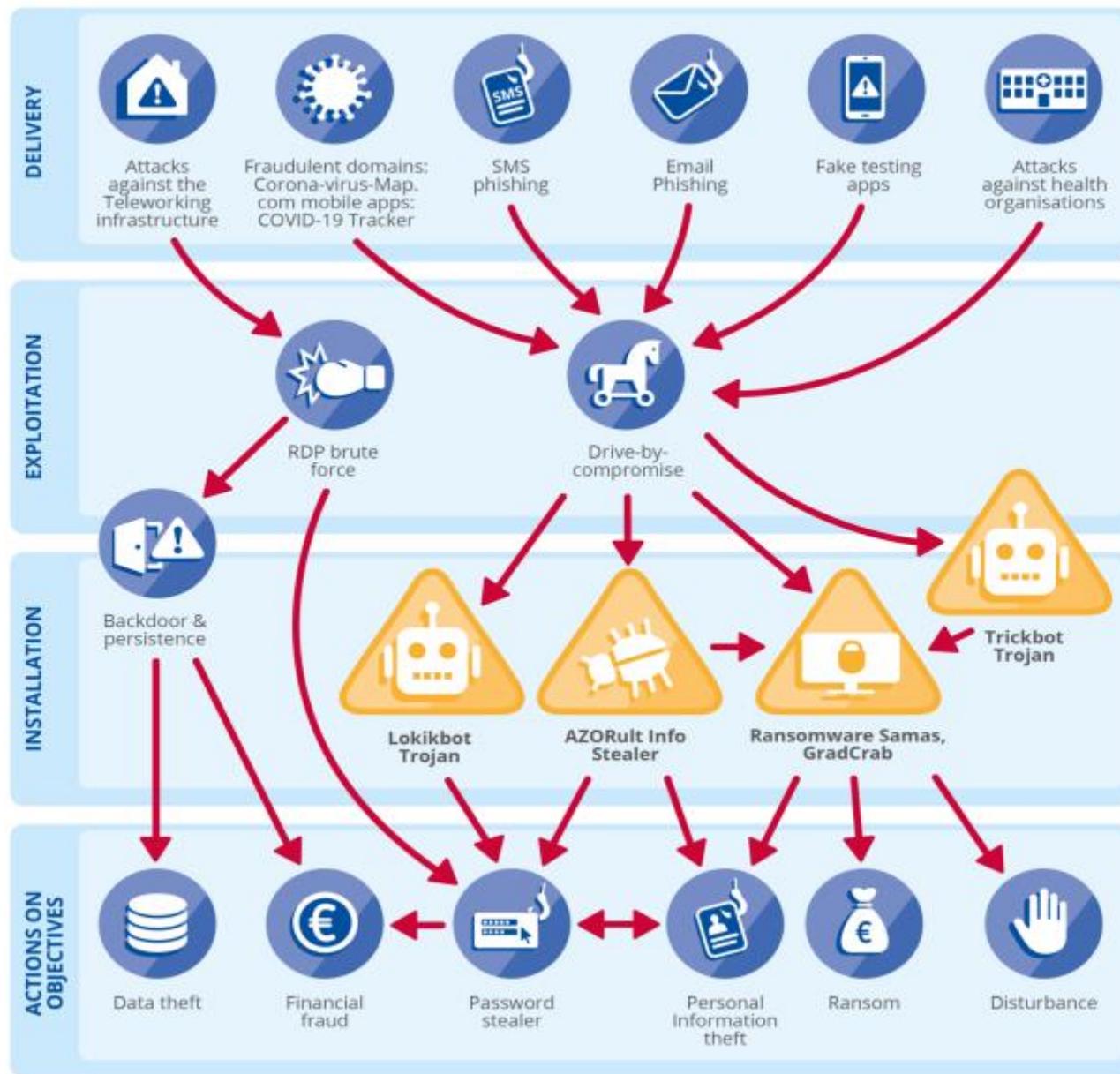
- Evaluate the threat landscape and identifying your top risks.
- Find or develop the right training.
- Every organization has a different threat profile.
- Be sure to cover: phishing, malware, and poor security practices.
- Phishing is behind 71% of all cyber attacks worldwide.



[Threat Landscape — ENISA \(europa.eu\)](https://europa.eu)

# THREAT LANDSCAPE MAPPING

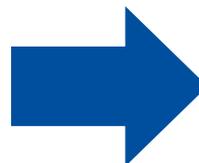
Exploitation by cybercriminals and advanced persistent threat (APT) groups of the current coronavirus (COVID-19) global pandemic.



# ROLES

**Creating a team of Experts cultivates Culture**  
**Use rolling roles!**

- Management
- Cyber Security Officer
- Heads of Departments
- Public Relations
- ICT
- HR
- DPO / LEGAL



# IDENTIFY TARGET AUDIENCE

Audience groups		Clustered audiences
1	Generic Employee	Generic Employee
2	Contractor	
3	HR	
4	Communications & Marketing	
5	Legal	
6	Operations & R&D	
7	Finance & Procurement	C-Level, Decision Makers, Handling budgets
8	Managers, Officers	
9	Head of Unit, Directors	
10	Cybersecurity professionals	Professionals / Horizontal implementors of cybersecurity actions and users of cybersecurity solutions, working for organisations and/or individuals
11	IT professionals	

# CHANGE BEHAVIOR

- We are not in the '00, forget boring classrooms. Employees need to be engaged
- Training needs to be role-specific, tailored, fun, and address daily challenges
- **Make it Audience Specific**
- Provide easily consumable content (videos, realistic scenarios, quizzes, policies and real-world phishing simulation tests)
- Utilize communications & marketing tools such as blogs, awareness posters
- Break the culture barrier that cyber security is an IT thing



# CHOOSE THE RIGHT CHANNEL

#	Mechanism/Activity	Category	Target Audience			Occurrence	Delivery Method	Expected level of Impact	Measurability	Resources
			General	Specific	Target Group					
			X	X	Youth (incl. Students), Kids	Ad hoc, On request	Online	2	1	2
1	Videos	Media	X	X	Youth (incl. Students), Kids	Ad hoc, On request	Online	2	1	2
2	Webinar/Seminar	Training	X			Annual, On request	Online, Instructor led	2	3	3
3	Communication Calendar	Material	X	X	National AR Authorities, SMEs, Large Organizations	Annual	Online	2	2	1
4	Workshop	Training	X			On request	Instructor led, Online	3	3	3
5	Cybersecurity in a Box	Material	X	X	National AR Authorities	On request	Online	3	2	3
6	Surveys/Quizzes	Training	X			Annual	Online	2	3	1
7	Social Media	Media		X	Youth (incl. Students), Employees, Cyber Ignorant, Cyber Savvy	Annual	Online	2	3	1
8	Computer Based Training (CBT)	Training		X	Employees, SMEs, Large Organizations	On request	Online	2	3	2
9	Champions Network	Material		X	SMEs, Large Organizations	Annual	Conventional	3	1	1
10	Physical Material	Material	X			Annual	Conventional	2	1	1
11	One-Day Campaign	Event	X			On request	Conventional	2	2	3

# SCHEDULE DELIVERY

- Security awareness training should be an ongoing process conducted at regular intervals throughout the year.
- Cybercriminals launch scams to coincide with seasonal events, so learn to recognize the devious new attack methods
- Create an annual security awareness campaign
- Keep them wondering when the next test will hit them



# TEST EFFECTIVENESS

- Conduct an initial baseline assessment to determine where the risks lie.
- Execute regular phishing simulations to identify staff that require additional training.
- Execute controlled simulation exercises
- Quizzes and tests can be added to the end of training videos to help reinforce the key messaging and reduce risk.



# MAGNIFY THE EFFECT

- Quick wins count
- Keep it simple
- Identify strategies to magnify the effects of your program
- Train-a-Trainer
- Cyber Awareness Champions
- Inject Cyber Awareness in other events (Ex. team building events)



# MEASURING IMPACT

SCALE OF OUTREACH (KPI)				
Metrics	Number of participating countries	Number of reached individuals	Number of communication partners	Number of mentions in media
FACILITATING THE MULTIPLIERS (KPI)				
Metrics	Number of multipliers	Number of multipliers that contributed to the campaign	Number of multipliers that downloaded the material	
LEVEL OF BEHAVIOURAL CHANGE ACHIEVED (KPI)				
Metrics	Percentage decrease of incidents	Number of reported incidents	Number of positive test results	Level of increased knowledge
	Qualitative feedback on security good practices			
PUBLIC PERCEPTION (KPI)				
Metrics	Qualitative feedback on activities from the participants (on level of satisfaction)	Qualitative feedback from the participating Member States (on level of satisfaction)	Engagement rate (e.g., followers, likes)	
DURABILITY (KPI)				
Metrics	Level of reusability (for example ranging from 1-5)	Resources needed to reach objectives	Costs - Contribution partners/stakeholders	

# ACTUAL MEASUREMENT IS IMPORTANT

## Number of reached individuals

<b>Indicators</b>	<ul style="list-style-type: none"> <li>- Social media impressions and engagement with campaign posts.</li> <li>- Number of people participating in the locally deployed activities and events (i.e., physical vs. online). Possibly on a more fine-grained level with attention to the number of participants of specific target audiences.</li> </ul>
<b>Means of Measurement</b>	<ul style="list-style-type: none"> <li>- Social media analytics provided by the platform (e.g., Twitter, Facebook, Instagram, <a href="#">LinkedIn</a>).</li> <li>- Media monitoring tool.</li> <li>- Measure the number of views, likes, clicks, and shares.</li> <li>- Information from the communication partners on how many people they reach.</li> </ul>
<b>Strengths</b>	<ul style="list-style-type: none"> <li>- Effective way of measuring outreach on a large scale.</li> <li>- Quantitative information to measure the number of citizens or professionals engaged and participating. This is a proof of interest in the security topics discussed.</li> </ul>
<b>Limitations</b>	<ul style="list-style-type: none"> <li>- The use of the appropriate Social Media to disseminate the campaigns according to the target (other than existing accounts on Facebook, LinkedIn, and Twitter).</li> <li>- Media monitoring tool can be costly.</li> <li>- This can only be achieved if the participating Member States collect the information from the events and activities.</li> </ul>
<b>Innovative Suggestions</b>	<ul style="list-style-type: none"> <li>- Ask partners and customers to benchmark activities and track campaigns and the number of individuals reached. Reporting on national activities—and pointing to gaps in that reporting—might motivate less-active entities to increase their efforts.</li> </ul>

# YOUR CYBER AWARENESS PROGRAM

O1. Raise awareness on the cyber threat of Phishing (6 months)					
Target audience	Message/Desired Skills	Means	Materials/Tools	Timeframe	Evaluation
All staff	How aware are we?	Phishing simulation	Email	Jan	
All staff	“Do not open suspicious emails”	Custom training	- Webinar (video tutorial) - Workshops	Jan - Mar	Survey/Quiz
All staff	Do not get phished!	Informative material	- Posters - Stickers	Apr	Survey/Quiz
All staff	What did we learn so far?	Gamification	Quiz	May	Survey/Quiz
All staff	How aware are we now?	Phishing simulation		June	Survey/Quiz
All clientele	“We will never ask for your password via email”	Informative material	Newsletter, videos, leaflets	Mar - Jul	
Business Clients	“We will never ask your credentials via email, sms or call”	Informative material	Newsletter, videos, leaflets	Mar - Jul	
O2. Promote cybersecurity education and culture (1 year)					
Target audience	Message/Desired Skills	Means	Materials/Tools	Timeframe	Evaluation
Public relations team	Actions to follow in case of incident	Custom training	Hands-on table-top exercise	Mar (repeat in Oct)	Survey/Quiz
Financial Dep	Advanced Phishing Attacks	Custom training	- Webinar (video tutorial)	Mar (repeat in Oct)	
New employees	Cyber Hygiene Best Practices	Informative session	Presentation	Every interval	
Board of directors	Whaling Attacks aka Attacks against the C-Level	Custom training	Webinar (video tutorial)	Oct	

# PHISHING SIMULATION

The screenshot displays a 'Phishing Risk Test' interface. On the left, a sidebar contains a list of steps: 'Introduction' (checked), 'Template Selection' (active), 'Create Mailing List' (checked), 'Whitelisting' (checked), and 'Send Phishing Test'. Below this list is an 'Exit Phishing Risk Test' button. The main area is titled 'Select Your Phishing Template' and includes a sub-instruction: 'For the best results, select the phishing template similar to emails your employees frequently interact with.' Three templates are presented in a grid:

- Google - Password Reset:** Features the Google logo and a blue box with the text 'Google Verification Cod'. It has 'Select Template' and 'Preview Template' buttons.
- Starbucks - Free Coffee (Fake Coupons and Deals):** Features a green Starbucks logo and a green banner with the text 'Half-off Frappuccino® drinks—sw'. It has 'Select Template' and 'Preview Template' buttons.
- Your Office 365 password is expiring (with Password Security) PRT template:** Features the Office 365 logo and the text 'Password expiration notice for: {{learner}}'. It has 'Select Template' and 'Preview Template' buttons.

- Think of phishing simulation as a fire drill
- Phishing simulation as part of security awareness training
- Phishing simulation as a security control

## **EXAMPLE:**

[Gophish - Open Source Phishing Framework \(getgophish.com\)](https://getgophish.com)



# CYBER GAMES

(Tabletop) Games help:

- 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
  - Finding missing links in the chain-of-command
  - Ensuring documentation of response plans
  - Finding gaps in your recovery processes
- Testing consequences in a safe environment
- Coordination between different departments
- Save money



# CUSTOM VS READY-MADE AWARENESS PROGRAMS

## CUSTOM

### Pros:

- Fits Organizations needs only
- Engages Employees to collaborate
- Enhances the cyber security culture
- Is cheaper

### Cons:

- Requires time & some expertise
- Material is less professional
- Does not scale fast

## READY-MADE

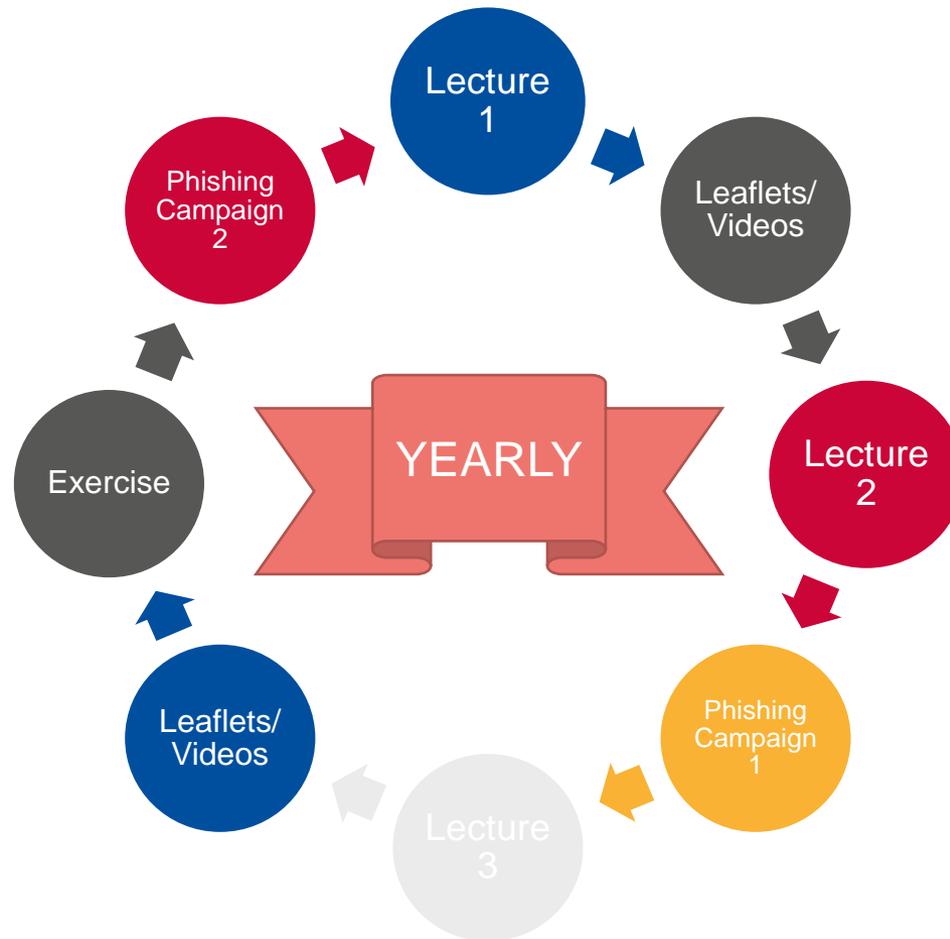
### Pros:

- Deploy & Scale Fast
- Ready Metrics
- Medium Expertise needed
- Updated to current trends

### Cons:

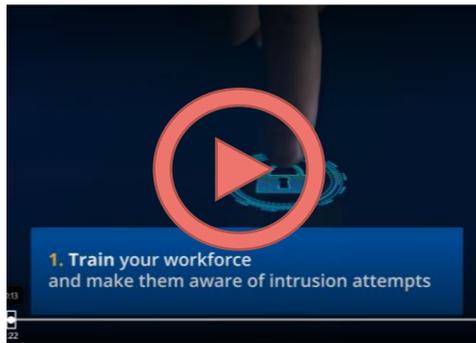
- Expensive
- Not very personalized by default
- Market research is needed to find the suitable product

# AWARENESS ACTIVITY LIFECYCLE





# ENERGY SECTOR EXAMPLE'S



**Focus your energy, prepare for ransomware!**  
Become a human circuit breaker

**RANSOM... WHAT?**

Remember to stop all work when your screen has a red light and don't connect a network to the network if you can't see the screen!

**Ransomware core actions: LEES**

- L**ack of awareness
- E**ncrypted data
- E**xecution of ransomware
- S**tealing of sensitive data

**Ransomware Life Cycle**

1. Initial access: How do you get into the system? (e.g., phishing, remote access, etc.)
2. Execution: How do you execute the ransomware? (e.g., running a file, etc.)
3. Access to objectives: How do you access the data you want? (e.g., accessing a file, etc.)
4. Persistence: How do you stay in the system? (e.g., creating a service, etc.)
5. Exfiltration: How do you steal the data? (e.g., copying files, etc.)
6. Ransom: How do you demand the ransom? (e.g., sending a message, etc.)
7. Payment: How do you pay the ransom? (e.g., sending money, etc.)
8. Recovery: How do you get the data back? (e.g., restoring from backup, etc.)

**Ransomware attacks footprint**

Example of ransomware attacks in the energy sector:

- 2017: Ukraine's power grid was hit by a ransomware attack, causing a power outage.
- 2018: A ransomware attack on a power company in the US caused a power outage.
- 2019: A ransomware attack on a power company in the UK caused a power outage.
- 2020: A ransomware attack on a power company in the US caused a power outage.
- 2021: A ransomware attack on a power company in the US caused a power outage.

**#PowerYourCyber**

**Be the cybersecurity transmitter!**  
Stay safe from ransomware

Did you know that ransomware can affect our company both directly and indirectly? You heard it! Your organization can be directly targeted by an attack, but it can also be the lateral victim of an attack to a third-party provider, particularly a Supply Chain attack. Let's take a look at both cases...

**Your company could be under attack**  
Your company could be the **direct victim** of an attack aimed against your assets

**How can this happen?**

The main entry vectors exploited are **remote services and phishing**

**So... may the entry points be cybersealed... How can you protect your company?**

- Reduce the attack surface
  - Apply Awareness Training Plans
- Protect your perimeter: Run security software, maintain strict security policies, and privacy protection policies up to date keeping personal data encrypted according to the GDPR
- Restrict administrative privileges according to the PLOP (Principle of Least Privilege)
- Stick to good practices (pay special attention to backup policies)
- Have a continuity plan

**A third party is under attack**  
Your company could be affected by an **attack against a third party**

Your organisation is breached through **vulnerabilities in its supply chain**, meaning DSOs or other partnering companies. The attack has affected a supplier, rendering its operations unusable, with **direct repercussions on the services they provide to you**. Or suppliers are used as **stepping stones** to spread the attack.

**By building cyber-secure relations with third parties:**

- Evaluate security policies of third parties (requiring a minimum level of security requirements)
- Apply Awareness Training Plans
- Define obligations of suppliers regarding protection of assets, sharing of information, audit rights, business continuity
- Include all obligations and requirements in contracts, e.g., GDPR
- Restrict administrative privileges according to PLOP (Principle of Least Privilege)
- Monitor service performance and perform routine security audits

**In case of suspicion always REPORT to the corresponding IT Department! if you suffer a ransomware attack...**

- Quarantine affected systems to contain the infection and stop the spread
- Lock down access to backup systems until after the infection gets removed
- Contact the national cybersecurity authorities or law enforcement on how to handle and deal with ransomware
- Visit the No More Ransom Project, a Europol initiative that can decrypt variants of ransomware
- Do not pay the ransom and do not negotiate with the threat actors

**#PowerYourCyber**

**Electricity operators, it is your time!**

We need you to help us **power up cybersecurity knowledge** in your sector!

Together let's lead all your employees into the light! Give them the tools they need to **deal with** the top cyberthreat... **Ransomware!**

...and find ways to **establish cyber-secure relations** with third parties **protecting** the entire supply chain!

Become a cybersecurity conductor and transmit the message, be the light of our cybersecurity community!

**#PowerYourCyber**



# RESOURCES

- **[Cyber Health Week — ENISA \(europa.eu\)](#)**
- **[Cyber Energy Week — ENISA \(europa.eu\)](#)**

# THANK YOU FOR YOUR ATTENTION

**European Union Agency for Cybersecurity**

Vasilissis Sofias Str 1, Maroussi 151 24

Attiki, Greece

 +30 6972765418

 [Alexandros.zacharis@enisa.europa.eu](mailto:Alexandros.zacharis@enisa.europa.eu)

 [www.enisa.europa.eu](http://www.enisa.europa.eu)

