Funded by the Erasmus+ Programme of the European Union

Overview of Understanding and Handling Cyber-Attacks

Minimizing Damage Through Incident Response

Safeguarding against Phishing in the age of 4th Industrial Revolution
www.cyberphish.eu
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

CyberPhish
Safeguarding your digital future

Learning Goals

Explain design, development and implementation of incident response plans.

Incident response plans:

- GDPR related attacks, Emails, Instant Messaging, Social networks, Websites, Lotteries scams, SMS, Phone calls, Face to face, Shoulder surfing, and other

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Student Workload

Lecture	1.5 h
Further reading	4 h
Preparation for exam	0.5 h

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

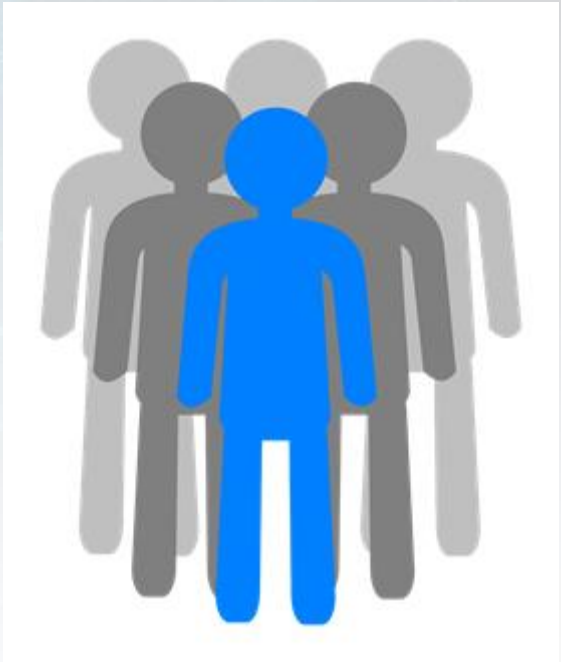
Contents

- **Steps to minimise the damage**
- Actions after cyber attack occurred
- Assess the security breach
- Manage the fallout from your cyber attack
- Post incident response

Funded by the
Erasmus+ Programme
of the European Union

Implement and Follow Cybersecurity Culture in the Organisation

- Aspects of the development of a cybersecurity culture as set out in the EISP (Enterprise information security policy) and relevant complementary policies.
- Leaders must clearly demonstrate through their actions that cybersecurity is critical to the mission of the organisation.

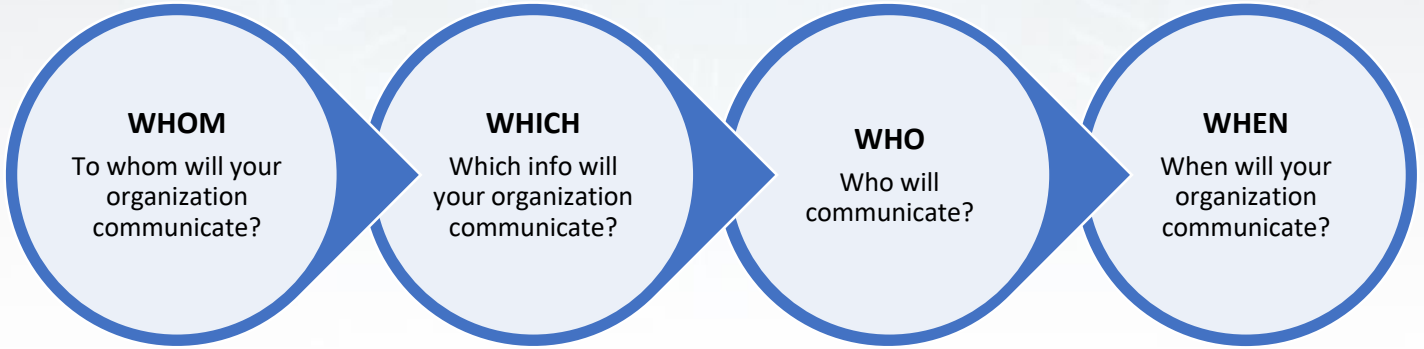


CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Establish Formal Communication Channels

- Communication strategy for issue reporting
- Escalation procedures for reporting issues
- Escalation policy for urgent error reporting or anomaly detection
- At least two formal channels for each of the above occurrences
- Tactics for communication with internal and external stakeholders and any relevant national or regulatory bodies



Source: Cyber Security Incident Management Guide (2017)

Identify Business Critical Assets Assessment

Identify the assets that are essential to the organization ability to accomplish its mission

- MAIN INFORMATION SYSTEMS
  - systems and data collected
  - associated vulnerabilities of information systems
- COMPANY'S NETWORKS
  - companies networks
  - associated vulnerabilities of LANs
- INFORMATION IN THE COMPANY
  - what data are stored (i.e. PII, financial data, credentials…)
  - associated vulnerabilities related with information in the company

Funded by the Erasmus+ Programme of the European Union

Metrics and Measurable Effectiveness

- The responsible person must establish a schedule for providing regular feedback on cybersecurity progress, mitigated risks and changes.
- The policy should define appropriate indicators against which to measure improvement.

Funded by the
Erasmus+ Programme
of the European Union

Security Types

- Different levels of actions in cybersecurity:

Figure from Japanese Ministry of Economy, Trade and Industry Cybersecurity Guidelines

- Remember: the highest security will be achieved using proactive security measures such as raising overall phishing awareness
- But you always must know what to do in the case of attack and especially successful attack
- Remember: even the toughest measures can't guarantee the 100% security

Funded by the Erasmus+ Programme of the European Union

Steps to Minimise the Damage

The first and most important tip is training, which will ensure that all employees, according to their positions, will be able to handle such an incident.

- *Step 1: Identify the Type of Attack*
- *Step 2: Contain the Damage*
- *Step 3: Inform Affected Parties*
- *Step 4: Investigate and Report*
- *Step 5: Safeguard Against Future Attacks*

Funded by the Erasmus+ Programme of the European Union

Contents

- Steps to minimise the damage
- **Actions after cyber attack occurred**
- Assess the security breach
- Manage the fallout from your cyber attack
- Post incident response

Funded by the
Erasmus+ Programme
of the European Union

Actions After Cyber Attack Occurred

Here will be presented main steps what you need to do after cyber attack (potentially successful)

Funded by the Erasmus+ Programme of the European Union

What to Do After Cyber Attack

- If you or your business is the victim of a data breach, follow next steps to help minimize the damage:

- Contain the Breach in Your Cyber Security

- Assess the Security Breach

- Manage the Fallout from Your Cyber Attack

- Report Cyber Crime

Funded by the Erasmus+ Programme of the European Union

Contain the Breach in Your CyberSecurity

- Do not panic !
- Try to clarify the situation: act soon but not fast !

- Remember:

While you may be tempted to delete everything after a data breach occurs, preserving evidence is critical to assessing how the breach happened and who was responsible

Funded by the Erasmus+ Programme of the European Union

Contain the Breach in Your CyberSecurity

- Here are a few immediate things you can and must do to attempt to contain a data breach:

- Disconnect your internet

- Disable remote access

- Maintain your firewall settings

- Install any pending security updates or patches

- Change passwords

Funded by the Erasmus+ Programme of the European Union

Contain the Breach in Your CyberSecurity

- *If you are working in team some suggestions from practitioner:*

- First, assemble a business continuity team, including IT and data forensics experts, and have them determine the size and scope of the vulnerability,
- Then, secure physical areas that could be related to the breach
- Change any access permissions right away.
- Stop any additional data loss by taking all systems affected offline

Funded by the Erasmus+ Programme of the European Union

Contents

- Steps to minimise the damage
- Actions after cyber attack occurred
- ***Assess the security breach***
- Manage the fallout from your cyber attack
- Post incident response

Funded by the
Erasmus+ Programme
of the European Union

Assess the Security Breach

Factors to take into account when assessing the security breach:

- Security (measures that had to be in place),
- Personal data involved,
- Consequences for data subjects,
- Circumstances of the breach,
- Type of controller.

Funded by the
Erasmus+ Programme
of the European Union

Assess the Security Breach

Try to answer next questions:

- How was the attack started ?
- Who had the access to the servers that were infected?
- Which computers were active when the breach occurred?

- E.g., you may be able to pinpoint how the breach was initiated by checking your security data logs through your firewall or email providers, your antivirus program or other way.
- You may need to ask support of cybersecurity professionals.

Funded by the Erasmus+ Programme of the European Union

Assess the Security Breach

Identify those affected by the breach:

- It is very important to find out who may have been affected by the breach, including your employees, customers, and third-party vendors.

- Assess how severe the data breach was by finding what information was accessed or targeted, such as birthdays, mailing addresses, email accounts and credit card numbers.

Funded by the Erasmus+ Programme of the European Union

Assess the Security Breach

Initiate your cyber attack protocol:

- Your employees should be aware of your policies regarding data breaches.
- After discovering the cause of the breach, adjust and communicate your security protocols to help ensure the same type of incident doesn't occur again.

Funded by the Erasmus+ Programme of the European Union

Assess the Security Breach

Initiate your cyber attack protocol:

- Keep in mind not only digital but also physical security measures to avoid new data breach (physical access to the device or workplace).

Funded by the
Erasmus+ Programme
of the European Union

Contents

- Steps to minimise the damage
- Actions after cyber attack occurred
- *Assess the security breach*
- **Manage the fallout from your cyber attack**
- Post incident response

Funded by the
Erasmus+ Programme
of the European Union

Manage the Fallout From Your Cyber Attack

Here are the main guidelines how to went out from the cyber attack with minimum losses

Funded by the
Erasmus+ Programme
of the European Union

Manage the Fallout from Cyber Attack

If attack was on company: notify the managers and employees of the breach and all others that may be affected by the attack

- Communicate with your colleagues to let them know what happened.

- Define clear authorisations for team members on the issue both internally and externally.

- Remaining in the close contact with your team is crucial while recovering from a data breach.

- You may need legal advice on the judicial aspects of the incident

Funded by the Erasmus+ Programme of the European Union

Manage the Fallout from Cyber Attack

If attack was on company: notify the managers and employees of the breach and all others that may be affected by the attack on you.

- If you have cyber liability insurance, notify your carrier

- Cyber liability insurance is designed to help you recover from a data breach or cyber security attack.

- Contact your carrier as soon as possible to see how they can help assist you with what to do after a cyber attack.

Funded by the Erasmus+ Programme of the European Union

Manage the Fallout from Cyber Attack

If attack was on company: Notify customers

- Emphasize your willingness to be transparent

- Communication can be the key to maintaining positive, professional relationships with your clients and could help minimize potential losses.

Funded by the
Erasmus+ Programme
of the European Union

Post Incident Response

- Steps to minimise the damage
- Actions after cyber attack occurred
- Assess the security breach
- Manage the fallout from your cyber attack
- **Post incident response**

Funded by the
Erasmus+ Programme
of the European Union

Post Incident Response

- When the attack is over, lessons identified through the process should be analysed and incorporated into the action plan.
- This is very important and should not be forgotten, due to the tendency to rapidly forget the incident.
- Remember: the time spent in gathering lessons learnt and in adjusting the plans and scenarios is an investment that will pay off in the next crisis.

Funded by the Erasmus+ Programme of the European Union

Post Incident Response

Lessons Learned log:

- Keep a log of lessons learned so not to repeat the same mistakes again.
- This could be useful material for new employees and decision-makers for additional cyber security budget.

Funded by the Erasmus+ Programme of the European Union

Summary

- Best way to minimise the damage is to raise general phishing awareness.
- You need to have a plan what to do in the case of cyber attack.
- Assess the security breach.
- Act in accordance with assessment results.
- Get lessons from attack.

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

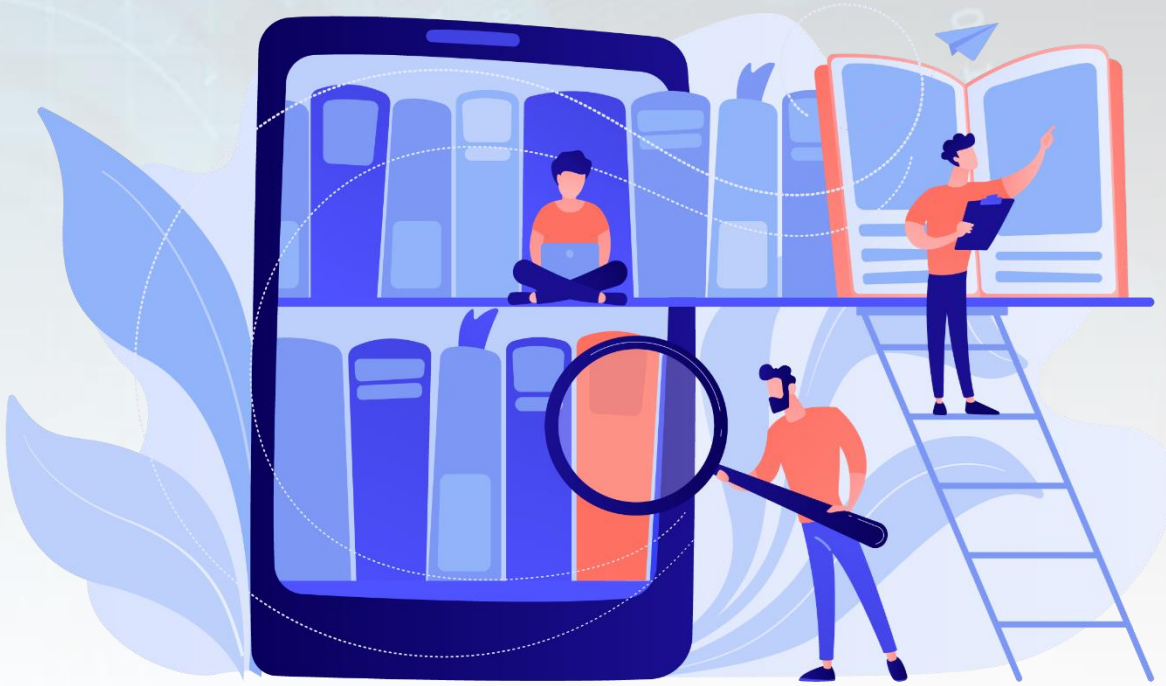
Assignment

- *You are a head of the team of 10 employees. Your systems administrator observed unusual activities in the server.*

- *Describe your immediate actions in the situation.*

Further Reading

- Oguchi Kyohei, Yamazaki Teru, Yamane Masato. Incident Response Solution to Minimize Attack Damage. NEC Tech Reports, 2018
- George Grispos. On The Enhancement of Data Quality in Security Incident Response Investigations. Ph. D. Thesis, University of Glasgow, 2016



Thank you!