INFORMATION SECURITY 101

Learning Module

Topics

- Introduction
- Threats and Impacts
- Workstation Security
- Email and Web Security
- Physical Security
- Incident Response
- Customer and Supplier Security

INTRODUCTION

Welcome & Module Overview

- This is a self paced training module designed to familiarize you with good security practices within the work environment.
- It is to be communicated for all staff including contractor employees/ freelancers across all locations.

Learning Objectives

By the end of this module you will be able to:

- Identify and understand the different types of threats that we face.
- Act in a secure manner when dealing with internal or client systems and data.
- Protect the data that you are handling.
- Protect yourself when communicating or browsing online.
- Know what to do if there is a security incident.

Threats and Impacts

Types of Threats

Below is a table containing the types of threats that we may face. It is important to understand these threats so that we know how acting in a secure manner can protect us from them.

Threat	Description
Intrusion	Unauthorized persons accessing computer systems.
Virus/Worm	Programs that infect a system and run malicious code that allow an attacker to take over your machine.
Ransomware	Programs that encrypt files and ask for payment for the decryption key.
Phishing	Attackers using emails or fake websites to trick a recipient into providing personal information or performing an action.
Spam	Bulk emails containing unsolicited advertising or phishing attacks.
Scams	Attackers attempt to trick recipients into paying money or financial information.
Physical	Attackers may physically steal business property.

These threats may lead to a number of impacts that will be detailed on the next slide

Impacts

Data Loss / Data Theft

Personal Information

Personal information about employee's, clients, or members of the public could be exposed by a security incident. Not only does this potentially damage our brand and reputation, but it also has potential Privacy or personal information transmission implications. Additionally, a data breach containing PII may require disclosure and even incur fines under data breach legislations, depending on the country or geography.

Chainsys IP

Chainsys Intellectual Property produced internally could be exposed or stolen. This has the potential to cause a financial impact to Chainsys

Client Information

Clients entrust us with their important data. The exposure or theft of this data can damage the relationship with the client, as well as our reputation.

Denial of Service

The destruction of data or degradation of service caused by malicious activity could impact our reputation and relationship with clients.

Repudiation or identity spoofing

Attackers could perform actions, including committing crimes or using the identity of somebody else. This could have legal, reputational, relationship, and human resources impacts.

Cyber Security Facts

- 1 in 5 Small and Medium sized businesses never got their data back from a ransomware attack.

  https://securelist.com/kaspersky-security-bulletin-2016-story-of-the-year/76757/

- An individual is attacked by ransomware once every 10 seconds

  https://securelist.com/kaspersky-security-bulletin-2016-story-of-the-year/76757/

- More than 400 businesses are targeted by BEC/CEO Scams every day

  https://blog.barkly.com/phishing-statistics-2017

Workstations Security

Employees have access to sensitive information from our workstations.
It is important we know how to properly protect them.

Password Security

- Create strong passwords for all accounts.
  - Use a password that does not contain easily guessable personal information (Names, pets, locations, hobbies, etc).
  - Consider using a long pass phrase as a password, provided it meets complexity requirements and is not easily guessable.
- Never disclose your password to another person in any way.
- Avoid storing passwords where others can see it OR in an un-encrypted form electronically. (Post it notes, SNAP, OneNote, Word documents)

Computer Security

- Lock your computer whenever you leave your desk, no matter for how long it will be.
- Leave patching, anti-virus, and firewall services enabled on your workstation.
- Do not lower User Account Control (UAC) settings on your workstation.
- Avoid installing unnecessary software onto your workstation.
- Avoid connecting to public unsecured networks such as free Wi-Fi hotspots as far as possible.
- Keep installed software up to date with any updates and patches.
- If you notice any strange or unexplained behavior contact Chainsys Infosec and Infra support immediately.

Data Security

- Understand the types of data you have stored on your workstation.
- Avoid storing personal information of peers, clients, or members of the public on your workstation unless necessary e.g. CVs, test data with personal information.
- Avoid storing important data on your local workstation, using instead managed file servers and SharePoint Sites as workstations are not backed up.
- Storing personal files on your workstation.
- If possible, do not store IP and other important information on your workstation. If there's an immediate need to do so, delete the local copy once you've moved it to a more appropriate location.

Email and Web Security

Most of the threats we face will use the web or email as an attack mechanism

Email Security

- Do not open attachments or open links from an untrusted source.
- Be on the lookout for phishing scams, especially emails that appear to come from banks or social media websites.
- Be wary of emails that appear to come from people within the business asking for information or actions to be done that seem out of the ordinary. Ensure you confirm via a second factor if you receive such a request.
- Avoid sending passwords over email.
- Avoid using personal accounts for business purposes

Web Security

- Be conscious of phishing websites.
- Do not download / install software that isn't required for work purposes.
- Be careful when typing addresses into a browser to ensure you go to the correct site.
- Avoid responding to messages received via pop-up windows on web sites.

Physical Security

Not all security incidents are technology related

Physical Security

- Be wary of ‘coat tailing’. Make sure you know someone before letting them through security doors, or to floors on the elevators when in the office.

- Remember to lock your computer when you leave your desk.

- Report lost or stolen devices to Support as soon as possible.

- Dispose of sensitive materials properly in the secure places situated around the office and use of shredders for destroying sensitive data.

Incident Response

When a security incident happens, it is important to react quickly to ensure we can limit the impact.

Incident Response

- If you suspect that there has been a data breach, notify Chainsys IT support and Infosec as soon as possible.
- If you suspect you have opened a malicious attachment, downloaded a malicious file, or clicked on a malicious link, notify Support as soon as possible.
- If you are unsure of anything security or privacy related, ask your Manager
- In the event of a major security incident. Avoid sharing the details with unrelated parties until the investigation and communications have been completed.

Customer Security

Please be aware of the additional security requirements of our customers

Customer Security

- In addition to our internal security policies, please ensure you are aware of any additional requirements on projects, especially working on customer sites or projects.
- Customers often have additional policies around the use of email, intellectual property, storing data, using USB drives, displaying identification etc.
- Ensure you ask the question of your Manager for each project – “Are there any additional security requirements I need to be aware of?”

Supplier Security

- Vendors often have additional policies around the use of email, intellectual property, storing data, using USB drives, displaying identification etc. and Chainsys should adhere to the same while on the vendor premises.

- Access to restricted/ confidential/ internal information or data of Chainsys shall be provided to third-party suppliers only if they have a legitimate business need for the same and shall be controlled to avoid intentional / unintentional disclosure

- All requests for access to restricted / confidential / internal information coming from a third-party are to be forwarded to the information owner who shall decide whether the request should be granted and level of access to be granted.

Thank You

Reach out for any queries
infosec@chainsys.com