

# Information Security

## Awareness Training

# Section 1: Information Security Awareness

# What is Information Security?

It's about giving the right people (**Confidentiality**), the right information (**Integrity**), at the right time (**Availability**)

## Confidentiality (C)

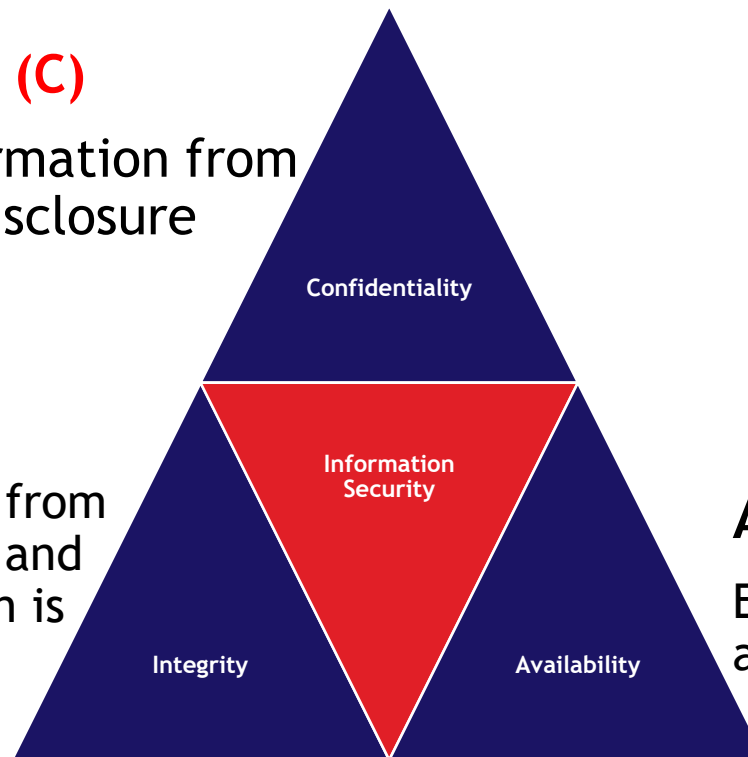
Protecting information from unauthorized disclosure

## Integrity (I)

Protecting information from unauthorized changes, and ensure that information is accurate and complete

## Availability (A)

Ensuring information is available when needed



# Our responsibilities

- ❑ Understand and comply with information security policies, guidelines, procedures, regulatory & legislative requirements.
- ❑ Ensure that information assets entrusted to you are protected properly.
- ❑ Report known or suspected security weakness & breaches immediately to line manager or Information Security Manager.

***Information security is  
everyone's responsibility!***



# Information Classification

MSIG classifies its information under one of four main categories which reflect its sensitivity to the Company. These classifications are:

These are very sensitive information!

## Secret

- Information which if corrupted, disclosed without authority or lost would result in critical loss to the Company. E.g. sensitive business proposals.

Examples: Details of M&A, Price sensitive information, etc.

## Confidential

- Information which if corrupted, disclosed without authority or lost, could result in significant or important loss to the Company and be illegal under certain legislation e.g. Personal Data Protection.

Examples: Personal and customer information, department exclusive information, etc.

Examples: Company policies, handbook, internal memo., etc.

## Internal

- Information that may be made freely available within MSIG-Asia but is inappropriate for general release to the public.

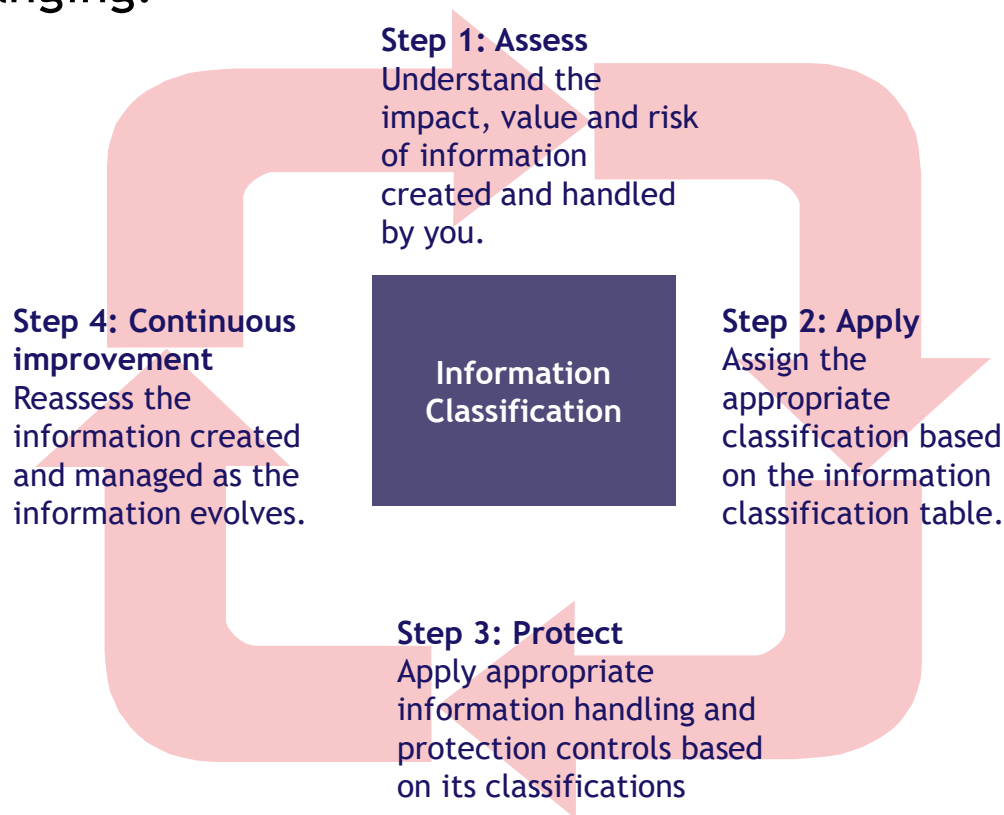
## Public

- Information that can be made available to the public.

Examples: Sales brochures, public FAQ, etc.

# Information Classification

Information classification should not only be performed at the time of information asset generation. It should be evaluated throughout the information lifecycle because data and business needs are dynamic and constantly changing.



## Section 2: Personal Data & Business Data

# What is personal data?

## ❑ Definition of Personal Data:

‘Data, whether true or not, about an individual who can be identified:

- ✓ from that data; or
- ✓ from that data and other information to which the organization has or is likely to have access.

Types of personal data may include a combination following (but not limited to):-





# What is business data?

## □ Definition of Business Data:

- ✓ Business data is important for the company, we usually classify the data into categories based on its sensitivity.
- ✓ Data, e.g new products, customers are classified as confidential, and data that are publicly circulated are “public”.
- ✓ We should all handle business data with care, and only share business data with people with a business need to know.

# Personal Data Protection

- ❑ Comply with local personal data protection legislation, including any related regulations or directions or guidelines.
- ❑ Personal data are considered as **Confidential** information within the company.
- ❑ When dealing with personal data, due care must be taken to protect the information.
- ❑ Ensure such data has adequate protection applied. Such as encryption, sealing of envelopes, secured USB storages, etc.
- ❑ Ensure consent has been acquired prior to obtaining personal data.



- Consent, Purpose & Notification
- Access & Accuracy
- Data Protection
- Retention & Transfer limitation
- Openness / Transparency

Typical principles of privacy requirements

# How to protect your own information and data?

- Don't print documents with confidential information, and if you must print, do not leave it unattended.
- All confidential documents must be secured or destroyed safely. (E.g. shredding)
- Use strong passwords.
- Educate yourself on the latest scams and spams.

# How to protect the business data? (*e.g company information*)

- Erase all information from writing boards, and safely dispose all documents after meetings.
- Never discuss private work information in public places.
- Always backup your data.
- Never leave devices in an unprotected location.
- Lock your device when not in use.
- Never let anyone use your managed devices.

# Section 3: Business Email Compromise (BEC)

# Business Email Compromise (BEC)

What is BEC?

- ❑ A type of scam targeting companies who conduct wire transfers and have suppliers abroad.

Typical targets:

- ❑ High-level employees related to finance/payments or involved with wire transfer payments.
- ❑ But.. Anyone could be targeted!

Method

- ❑ Rely heavily on **social engineering tactics** to trick unsuspecting employees and executives (e.g.: impersonate CEO or any executive authorized to do wire transfers)
- ❑ Email spoofing or compromised through key loggers or phishing attacks.

Motivation for attackers:

- ❑ According to FBI, nearly half of cybercrime losses (\$1.7b) is due to BEC in 2019.
- ❑ 100 times greater net profit compared to ransomware.
- ❑ Globally, cybercriminals scammed more than \$50 million dollars from victims in non-US countries.
- ❑ Easy money for criminals!

# BEC during Covid-19

It is anticipated that BEC attacks will increase during this pandemic. Below are some of the commonly used tactics/themes. Please do not response to any of such emails. You may report through the phishing button and delete the email.

## Email masquerading as government / regulator announcements.

Phishing and BEC emails disguised as government announcements. Fraudulent emails have included logos associated with health officials and/or the World Health Organization (WHO). Include links to items of interest that may look legitimate, but the sites are often malicious and may be designed to steal email credentials. There were also reports of BEC emails pretending to be local regulators providing financial support to businesses, with intend to steal financial information.

## False advise and cures.

Emails purporting to hail from regional medical providers, sent to people in Japan in January and February, were among the first coronavirus-related phishing attacks. Emails enticed recipients to download attachments containing cure for the virus but instead contain malware designed to steal the personal and financial information.

## Relief funds or charities.

The emails appeal to recipients' altruism, urging victims to donate into a Bitcoin wallet or to make other types of payments. Other malicious actors may create fraudulent charities.

---


# Actual BEC attempt on MSIG

Work on matter with legal advisors



ms\_ad\_ir=ms-ad-hd.com@mg.server2655.com

To

 If there are problems with how this message is displayed, click here to view it in a web browser.

**EXTERNAL EMAIL:** Be careful when you click any links or open any attachment(s)..

I would like you to be in charge of a matter that needs to be resolved

with our appointed legal advisors within this week.

Please let me know soonest by email if you can assist in this and I will

provide more details.

Thanks.

Yasuyoshi Karasawa

Sent from my iPhone

Be careful:  
Fictitious email domain

Pay attention:  
External email banner.

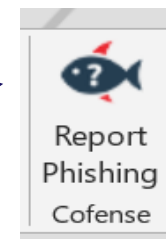
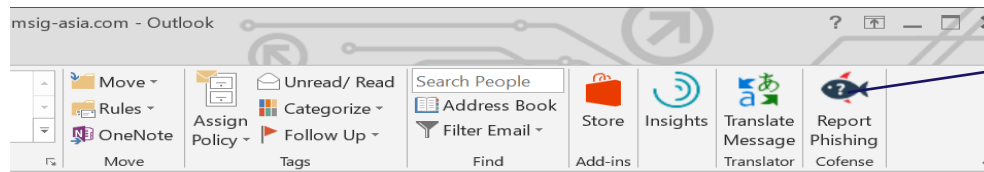
Be alert:  
- Out of context  
email content.  
- Poor formatting



# Business Email Compromise (BEC)

What can we do?

- **Be wary of irregular emails** that are sent from C-suite executives. They may be used to trick employees into acting with urgency.
- **Verify any changes in vendor payment requests** by double checking with the vendor directly to confirm the changes.
- Stay **updated on your customers' habits** including the details, and reasons behind payments.
- **Confirm requests for transfer of funds** when using phone verification as part of two-factor authentication, use known familiar numbers, not just the details provided in an email requests.
- If you suspect that you have been targeted by a BEC email, **do not response to it**, delete the email and/or report the incident through this button below.



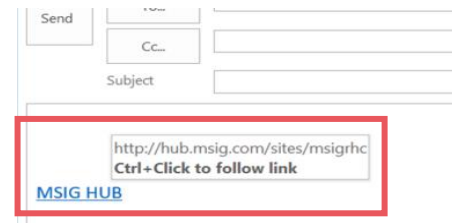
# Be vigilant when responding to emails

- ❑ When receiving emails from unknown sender, double check the validity of the email address.

Examples of fictitious email addresses:

sender@nnsig-asia.com, sender@msig\_asia.com, sender@asia-msig.com, etc.

- ❑ Try not to hastily reply an email. Take a step back and think about the content or request of the email. (even if it is urgent - think about its intent first). **Call the sender** if you need to verify.
- ❑ If you are not sure, **ask!** - Verify with your manager or colleagues, and get clarity.
- ❑ If there is a link in the email from unknown sender **DO NOT CLICK the link!**
- ❑ For known sender, to be safe, hover on top it (not clicking it yet) to verify it is linked to the intended website.



- ❑ Remember, if something looks too good to be true, it probably is.

# Section 4: Malicious Code

# What are malicious code?

❑ Malicious code includes any program which is deliberately created to cause an unexpected and unwanted event on an information system. Using such code, adversaries\* can:

- ✓ Steal information
- ✓ Sabotage systems
- ✓ Take over systems

*\* are anyone that seeks to do you and our organization harm, like insiders from our own organization and hackers.*

❑ Types of malicious code are:

- ✓ Virus: it attach itself to program and propagates copies of itself to other programs.
- ✓ Trojan Horse: it contain unexpected, additional functionality.
- ✓ Logic Bomb: it triggers action when condition occur.
- ✓ Time Bomb: it triggers action when specific time occur.
- ✓ Trapdoor: it allows unauthorized access to functionality.
- ✓ Worm: it propagates copies of itself through network.
- ✓ Rabbit: it work as a virus or worm where it replicates itself without limit to exhaust resources.

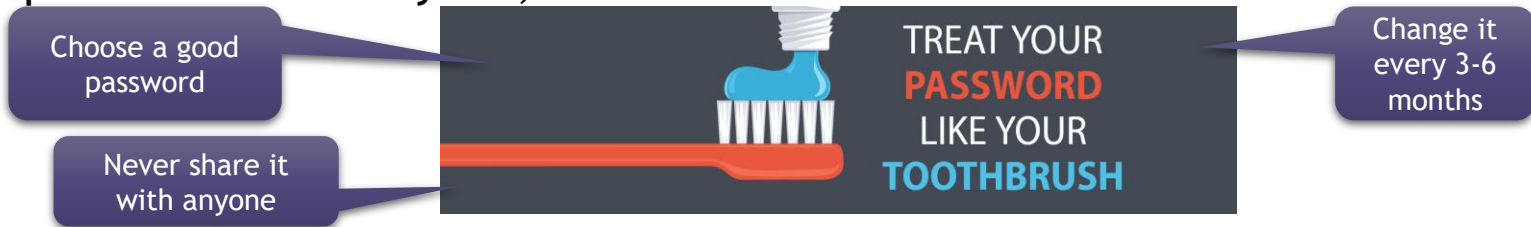
# How to protect yourself from being the victim of malicious code?

- View e-mail messages in plain text.
- Do not view e-mail using the preview pane.
- Use caution when opening e-mail.
- Scan all attachments.
- Delete e-mail from senders you do not know.
- Turn off automatic downloading.

# Section 5: Good practices of Information Security

# Create a robust password

- ❑ Select **quality passwords** with sufficient minimum length (more than 8 digits) which are:
  - ✓ Phrases that means something to you and incorporate symbols as a replacement of alphabets
  - ✓ Not based on anything somebody else could easily guess or obtain using person related information, (e.g. “password”, names, pet’s name, telephone numbers, and dates of birth, etc.)
  - ✓ Free of consecutive identical, all-numeric or all-alphabetic characters. (e.g.: “qwerty12345”, “12345”, “abcde” and etc.)
  - ✓ Change passwords at regular intervals (recommended to have 45 days intervals and even maximum less than 6 months) and avoid re-using or cycling old passwords;
  - ✓ Change temporary passwords at the first log-on;
  - ✓ Not use the same password for business and non-business (personal) purposes.
- ❑ Always **keep your passwords confidential**, and **do not share** your passwords with anyone;



# Handle all information with care

- ❑ Label your information based on the information classification table.
- ❑ Encrypt all confidential data prior to sharing in email.
- ❑ Retrieve your printouts from the printer immediately.
- ❑ Don't leave confidential or personal information on your desk. It's easy for anyone to glance at your desk and see sensitive documents.
- ❑ Keep your desk tidy and documents locked away or shredded when no longer needed.
- ❑ When leaving your desk, always remember to lock your laptop/PC. Press the following keys:



- ❑ Ensure adequate protection is applied for non-public company information that is about to be shared/leaving the company/office premise. Example:



Use secure  
USB drives



Documents  
sealed in  
envelopes



Transfer  
through secure  
connectivity



# Be thoughtful when sending emails and postal mails

- ❑ Always **double check details of the recipient** and ensure that:-
  - ❑ Email address of recipient is genuine and accurate.
  - ❑ Only intended parties are on the email list.
  - ❑ Name and address of postal recipient is accurate.
- ❑ **Password protect** all attachments that contain confidential information/customer's information.
- ❑ Ensure that the email attachment is the right file and is meant to be shared with recipients on the list.
- ❑ Ensure content of the postal mail is accurate and is for the intended person.
- ❑ If you had accidentally sent an email/postal mail containing confidential information to an unintended party, please attempt to recall the message immediately.
- ❑ If you are unable to circumvent the information from reaching the unintended party, please report the incident to your information security manager to assess the situation.

# Information Security “Don’ts”

- ❑ Do not share your password with anyone including your bosses, managers, supervisor, friends, family, or colleagues.
- ❑ Do not share personal data belonging to the company outside of its intended purposes with any unrelated parties.
- ❑ Do not send and store any non-public company information to your personal email, cloud or devices.
- ❑ Do not download and/or install any unauthorised software or applications onto your laptop/PC.
- ❑ Do not share confidential information with unrelated parties.
- ❑ Do not leave sensitive/confidential information on your desk unattended.
- ❑ Do not disclose non-public company information onto any social media platforms.

# Safe internet usage habits - for your own safety!

- Be prudent when sharing personal information online.
- Be wary of the links you click.
- Make sure your internet connection is secure.
- Be Careful of what you download.
- Be Careful of what you post online.
- Be Careful of who you to meet online.
- Keep your antivirus updated.
- When it is too good to be true, it probably is.
- A little more common sense will help along the way.
- If possible, enable two factor authentication (2FA) when logging onto personal social sites.



# THANK YOU