NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Module 03 – Managing Cybersecurity in Real-life

Learning Objectives

- By the end of this lesson, you will be able to:
- Apply strategies learnt and play a part in keeping the wider NTU community safe
- Illustrate how Singapore and its citizens can protect themselves against cyber attacks

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Cybersecurity in NTU

What CITS cyber security team is doing to keep NTU Cybersafe

- With the increasing of the cyber-attacks to many organisations, NTU has not been spared from these attacks.
- The NTU Cyber Security team maintained strong cyber security postures with 3 main objectives in mind:

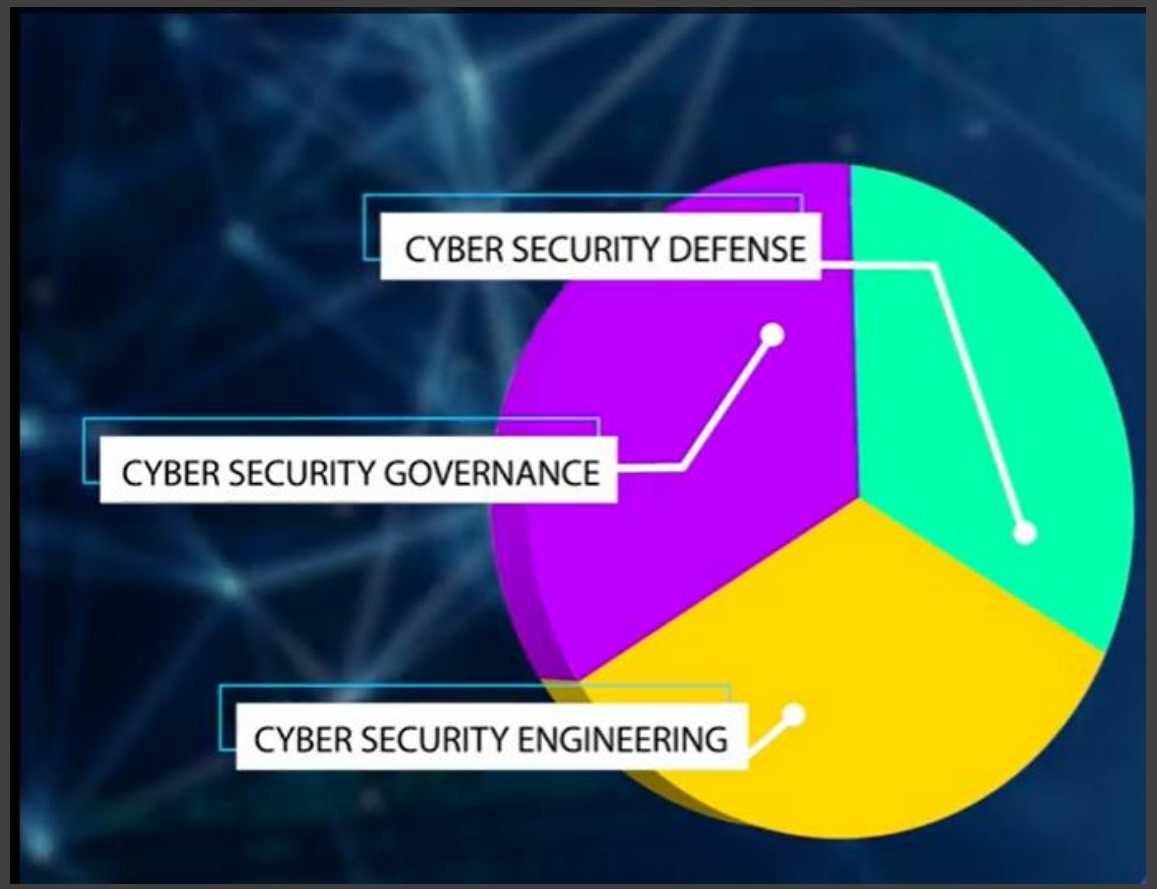
  Confidentiality – Ensuring data or information cannot be read by unauthorised personnel.

  Integrity – Data or information held by NTU remains accurate and unmodified by unauthorised personnel.

  Availability – Data or service remains usable with sufficient capability to deliver our educational services.

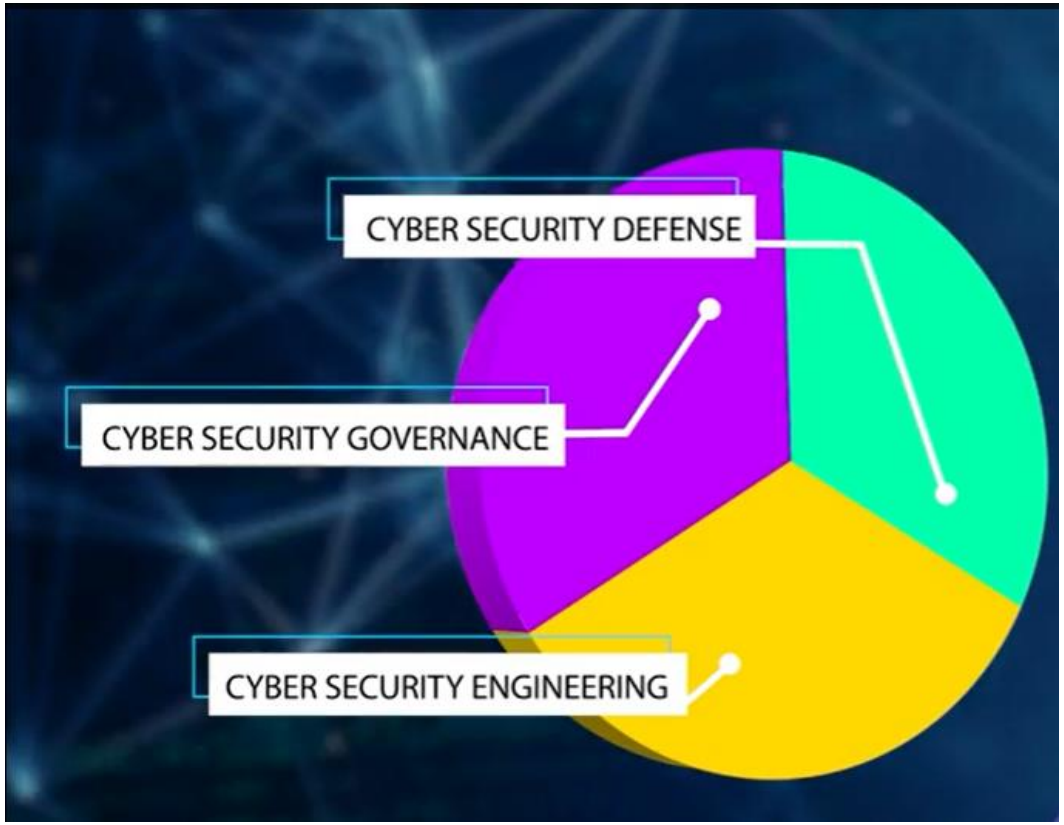
What CITS cyber security team is doing to keep NTU Cybersafe

- To achieve the cyber security objectives, we are organised into 3 main functions:



What CITS cyber security team is doing to keep NTU Cybersafe

- The Cyber Security Governance team is responsible for the development and maintenance of the NTU cyber security policies, standards, and procedures.
- The Cyber Security Engineering team is responsible to explore different technologies to enhance the NTU security capabilities.
- The Cyber Security Defense team manage the University wise security operations centre (SOC). SOC operates 24X7 and 365 days throughout the year to detect and respond to any cyber-attacks against NTU.



Cybersecurity in NTU

Cyber Security and Me is a series of informative sessions to help you understand the importance of cyber security to the NTU community.

- As we live in the digital age, it is inevitable that we are subject to cyber threats which threaten the confidentiality, integrity, and availability of the University's systems.
- Universities are targets for cyber attackers with he large collection of personal information and intellectual properties. However, we believe that through the implementation of an information security management system which emphasise on the upholding the confidentiality, integrity and availability, we can play a vital role in securing the University's digital assets.

- AIUP, which stands for acceptable IT usage policy – it serves to protect University information and IT resources, and helps to minimize risks and damages to the University by governing the usage of all its IT resources.

DO’s

- Update your passwords regularly
- Always ensure that you keep your password safe
- Use the NTU email for all official communications
- Use Blind Carbon Copy (BCC) for mass emails
- Keep your software updated with security patches

DON’Ts

- Don’t share your password with anyone
- Don’t forward any University document to your personal email address or online storage that’s not approved by the University
- Don’t install software without appropriate licenses
- Don’t turn off your anti-virus software or cancel any software updates
- Don’t over share information in social media

- Spot the signs of phishing emails
- Use strong passwords and
- Enable multiple factor authentication (MFA)
- Secure your sensitive digital information through encryption
- Follow the AIUP and conform to the security best practices

No part of this video shall be filmed, recorded, downloaded, reproduced, distributed, republished or transmitted in any form or by any means without written approval from the University.