CYBERSECURITY THREAT MANAGEMENT(CSTM)

Garranto Academy

Garranto Academy has been at the leading edge of learning and training since 2016. Garranto Academy is a Singapore-based EdTech that offers skill development training to people globally. Garranto Academy is a trustworthy training partner in the Asia-Pacific region

NATIONAL SKILL DEVELOPMENT

Collaborate with the Ministry of Education on this goal to aid the knowledge gapand skills gap..

CORPORATE TRAINING

Helps organizations in fixing and closing the knowledge gap globally.

EXPERT TALK/MASTER CLASS

Expert Talk is an initiative by the Garranto Academy that will enhance your skills

Address : #11-04, Shaw House Office Building,
350 Orchard Rd, Singapore 238868
Phone： +65 92318743
Mailbox :academy@garranto.com

+65 92318743

CYBERSECURITY THREAT MANAGEMENT PROGRAMME OBJECTIVE

Understanding the Cyber Security & Information Security concepts

Understanding the Cyber Threats

Understanding Cyber Security Management frameworks

Managing the Cyber Security Risks – Governance, Risk, Compliance

Prepare for Cyber Security Professional Certification programs

CYBER SECURITY WORKFORCE GAP

The threat of a cyber attack on Singapore's critical infrastructure services remains low but the maritime sector has been in the cross hairs of hackers, members of an international panel appointed by the Cyber Security Agency of Singapore (CSA) said. 2019 and 2020 threats are increase greatly.

OVERVIEW OF CYBER THREATS IN 2019

PHISHING

47,500

phishing URLs[1] with a Singapore-link were detected.

COMMONLY SPOOFED GOVERNMENT ORGANISATIONS IN SINGAPORE:

- IMMIGRATION & CHECKPOINTS AUTHORITY (ICA)
- MINISTRY OF MANPOWER (MOM)
- SINGAPORE POLICE FORCE (SPF)

70%

of incidents reported to SingCERT by Small and Medium Enterprises (SMEs) and members of the public occurred through phishing attacks.

WEBSITE DEFACEMENT

873

Singapore-linked website defacements were detected.

RANSOMWARE

35 cases of ransomware were reported to SingCERT.

COMMAND AND CONTROL (C&C) SERVERS AND BOTNET DRONES

530 unique C&C servers were observed in Singapore.

2,300

botnet drones (compromised computers infected with malicious programs) with Singapore Internet Protocol (IP) addresses were observed daily, on average.

[1] URLs – Uniform Resource Locators; colloquially termed web addresses.

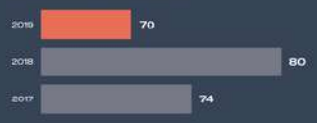
CYBERCRIME IN SINGAPORE

Cybercrime cases accounted for

26.8%

of overall crime in 2019.

CYBER EXTORTION



COMPUTER MISUSE ACT

ONLINE CHEATING

[2] Figures provided by Singapore Police Force (SPF) as of 10 June 2020.

Featured Topic

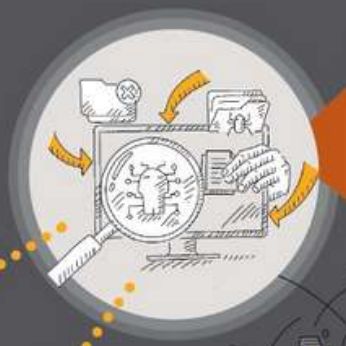
Singapore remains a safe city, but scams remain a concern

Cybercrime continues to be on the rise in Singapore, with 9,430 cases reported in 2019 — this was a 51.7 per cent increase from the 6,215 cases reported in 2018, and it accounted for more than one-quarter of all crime in Singapore last year.[2] Online cheating remains a major concern as cybercriminals continue to leverage the anonymity afforded by the Internet to target unsuspecting victims.

E-commerce scam remains the top scam type in Singapore and recorded a 30 per cent increase to 2,809 cases from 2,161 cases in 2018. The total amount cheated in e-commerce scams also increased to S$2.3 million, from S$1.9 million in 2018. Unsuspecting victims continue to be enticed by online deals, such as electronic gadgets and event tickets, which are often too good to be true.

Fighting crime is a community effort. Even while the Police continues to educate the public on crime prevention measures and work with relevant stakeholders to disrupt scam operations, members of the public must also play their part by taking active steps to safeguard themselves online. They should use trusted payment services provided by the e-commerce platforms to mitigate the risk of falling prey to e-commerce scams.

Overview of Cyber Threats in 2020



CYBERCRIME IN SINGAPORE

16,117

Cybercrime cases accounted for

43%

of overall crime in 2020

ONLINE CHEATING
2020: 12,251
2019: 7,580
2018: 4,928

COMPUTER MISUSE ACT
2020: 3,621
2019: 1,701
2018: 1,207

CYBER EXTORTION
2020: 245
2019: 68
2018: 80

WEBSITE DEFACEMENTS

495

'.sg' websites were defaced, a sharp decrease of 43% from 873 cases in 2019

RANSOMWARE

89 ransomware cases were reported to CSA, with cases hailing from the manufacturing, retail and healthcare sectors. This was a significant rise of 154% in cases over the whole of 2019

C&C SERVERS AND BOTNET DRONES

1,026 unique and locally hosted C&C servers were discovered, a spike from 530 recorded in 2019

About **6,600**

botnet drones were observed daily on average in 2020, also a significant increase from 2019's daily average of 2,300

PHISHING

47,000 phishing URLs[1] with a Singapore-link were detected. A slight decrease of 1% as compared to 2019

NUMBER OF CASES SINGCERT HANDLED IN
2020: 9,080
2019: 8,491

COMMONLY SPOOFED GOVERNMENT ORGANISATIONS IN SINGAPORE:
- MINISTRY OF EDUCATION (MOE)
- MINISTRY OF MANPOWER (MOM)
- SINGAPORE POLICE FORCE (SPF)

COMMONLY SPOOFED SECTORS
- TECHNOLOGY
- BANKING AND FINANCIAL SERVICES
- SOCIAL NETWORKING FIRMS

AMAZON, PAYPAL AND FACEBOOK ARE COMMONLY SPOOFED BRANDS

1 URLs – Uniform Resource Locators; colloquially termed web addresses.

MARITIME USECASE 2017 MAERSK CYBER INCIDENT

The 2017 MAERSK Cyber Incident

Learning from and applying the Lessons of a Major Cyber Incident

Maarten van Hees, MSc Eng.
CISSP, CISA, CISM, CCSP

Cyber Security Officer for OT, Maersk

In 2017: Cyber Security Manager for APM Terminals

With APM Terminals since 2011, moved to Maersk in 2018.

Previously worked for IBM, AT&T, Seneca, QNH, and DNB

MAERSK

The marine industry being an attractive target for hackers is not new. Since Maersk suffered a devastating US$300 million ransomware attack in 2017, the maritime industry has earned the unfortunate distinction of being the only sector to have all four of the world's largest shipping companies being hit by cyber attacks in the last four years, namely – Maersk, Mediterranean Shipping Company, CMA CGM and COSCO.

Programme contents

- Introduction to Information Security
- Threats that were Real
- Understanding Cyber Eco System
- Emerging Trends –Cyber Risks
- Security & Risk Management
- Protection of Information Assets
- Data Protection & Privacy Principles
- Identity & Access Control Management
- Software Development Life Cycle – Security Considerations

Programme contents

- Enterprise Security Architecture
- Threat Intelligence, Threat Hunting
- & Threat Monitoring
- Communication & Network Security
- Security Assessment & Testing
- Operational Resilience
- Security Incident Management
- Security Operations
- Cyber Security Strategy Development
- 2017 Maersk cyber incident use-case
- Cyber security Table Topic
- Open Discussion

THE FUTURE OF JOBS AND SKILLS FOR EVERYONE

Contact us

+65 92318743

Email

academy@garranto.com

Main Office

#11-04, Shaw House Office Building, 350 Orchard Rd, Singapore 238868