Newsletter 2.2025 | January
4th Newsletter of Suppiah & Partners Newsletter Series

CYBER THREATS UNMASKED: MALAYSIA'S LEGAL SAFEGUARDS

The cybersecurity landscape continues to evolve with various emerging threats, such as AI-driven cyberattacks and deepfake scams that leverage advanced technologies for malicious purposes.

Organisations must remain vigilant against these evolving threats while adhering to local regulations that govern cybersecurity practices in Malaysia.

Brought to you by:

SUPPIAH & PARTNERS
since 2007

suppiahlaw.com

DDOS ATTACK

DESCRIPTION

A Distributed Denial-of-Service (DDoS) attack aims to disrupt normal traffic by overwhelming a web property with massive requests from multiple devices (botnet).

CHARACTERISTICS

- Utilizes multiple compromised devices (bots).
- Targets network bandwidth or application resources.
- Does not require access to internal systems.

OPERATIONAL/ BUSINESS IMPACT

- Service outages.
- Loss of revenue.
- Damage to reputation.

PREVENTIVE MEASURES/ RESPONSES

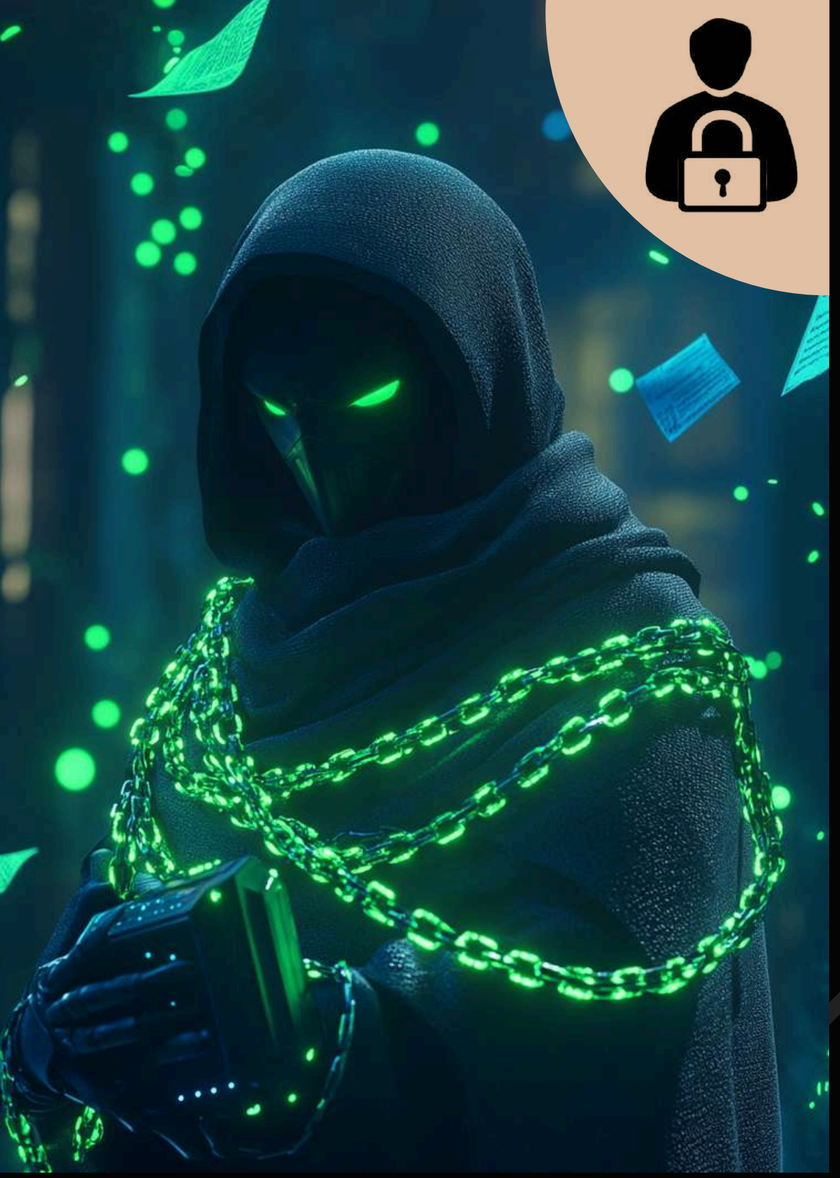
- Use of DDoS mitigation services.
- Traffic filtering and rate limiting.
- Regular system updates.

LEGAL PROTECTIONS/ CONSIDERATIONS IN MALAYSIA

- Governed by the Cyber Security Act 2024, which mandates compliance for NCII sectors.
- Non-compliance can lead to fines up to 500,000 ringgit or imprisonment for up to ten years.

The Hooligan

Like a hooligan, a DDoS attacker causes chaos and disruption, overwhelming systems and services with no intention of directly stealing but instead creating noise and destruction.



The Kidnapper

Encrypting critical data and demanding ransom mirrors a kidnapper holding a victim hostage for financial gain.

RANSOMWARE ATTACK

DESCRIPTION

Ransomware is malicious software that encrypts files and systems, rendering them inaccessible until a ransom is paid.

CHARACTERISTICS

- Encrypts data and demands payment for decryption.
- Requires access to internal systems, often via phishing.
- Typically demands payment in cryptocurrency.

OPERATIONAL/ BUSINESS IMPACT

- Data loss.
- Operational downtime.
- Significant financial costs for recovery and ransom payment.

PREVENTIVE MEASURES/ RESPONSES

- Regular backups and disaster recovery plans.
- Employee training on phishing.
- Endpoint protection solutions.

LEGAL PROTECTIONS/ CONSIDERATIONS IN MALAYSIA

- Subject to the Cyber Security Act 2024; organizations must notify incidents within six hours.
- Penalties for failing to report can include fines up to 500,000 ringgit or imprisonment for up to ten years.
- Subject to the Computer Crimes Act 1997 penalties (fines, imprisonment) could apply for any unauthorised modification of the contents of any computer.

RANSOM DDOS (RDDOS) ATTACK

DESCRIPTION

A Ransom DDoS attack threatens to launch a DDoS attack unless a ransom is paid, without encrypting any data.

CHARACTERISTICS

- Threatens service disruption rather than data encryption.
- May follow an actual DDoS attack or be a threat.
- Payment often requested in untraceable forms like Bitcoin.

OPERATIONAL/ BUSINESS IMPACT

- Service disruption without prior notice.
- Potential financial losses from ransom payments.

PREVENTIVE MEASURES/ RESPONSES

- Implementing robust network security measures.
- Monitoring traffic patterns for anomalies.
- Having an incident response plan in place.

LEGAL PROTECTIONS/ CONSIDERATIONS IN MALAYSIA

- Governed by the Cyber Security Act 2024; compliance with incident reporting is mandatory.
- Legal repercussions for non-compliance include fines and imprisonment.

The Extortionist

The RDDoS attacker threatens service disruption unless a ransom is paid, akin to an extortionist intimidating victims without necessarily carrying out their threat.

The Con Artist

Phishing attackers rely on deception and impersonation to trick victims into revealing sensitive information, much like a skilled con artist manipulates trust to defraud.

PHISHING

DESCRIPTION

Phishing involves tricking individuals into providing sensitive information by masquerading as a trustworthy entity.

CHARACTERISTICS

- Often conducted via email or instant messaging.
- Uses deceptive links or attachments.
- Targets personal and financial information.

OPERATIONAL/ BUSINESS IMPACT

- Financial loss.
- Identity theft.
- Loss of trust in digital communications.

PREVENTIVE MEASURES/ RESPONSES

- User education on recognizing phishing attempts.
- Implementation of email filtering technologies.
- Multi-factor authentication (MFA).
- Software updates.

LEGAL PROTECTIONS/ CONSIDERATIONS IN MALAYSIA

- Governed by the Personal Data Protection Act (PDPA) 2010, which requires organizations to protect personal data. Non-compliance can lead to fines up to RM300,000.
- Subject to Section 17(3) of the Electronic Commerce Act 2006.

SQL INJECTION

DESCRIPTION

SQL Injection involves inserting malicious SQL queries into input fields to manipulate databases.

CHARACTERISTICS

- Targets web applications with database backends.
- Can extract, modify, or delete data.
- Often due to improper input validation.

OPERATIONAL/ BUSINESS IMPACT

- Data breaches.
- Loss of sensitive information.
- Potential legal liabilities.

PREVENTIVE MEASURES/ RESPONSES

- Use of prepared statements and parameterized queries.
- Regular security testing and code reviews.

LEGAL PROTECTIONS/ CONSIDERATIONS IN MALAYSIA

- Subject to the Computer Crimes Act 1997, which criminalizes unauthorized access and data manipulation. Penalties include fines and imprisonment.

The Safecracker

Exploiting vulnerabilities in databases to extract, modify, or delete data is akin to a safecracker breaking into a vault to steal valuables.

The Spy

Intercepting communication and manipulating it without the parties' knowledge resembles a spy or eavesdropper gathering intelligence secretly.

MAN-IN-THE-MIDDLE (MITM)

DESCRIPTION

MITM attacks involve intercepting communication between two parties without their knowledge.

CHARACTERISTICS

- Can occur over unsecured networks (e.g., public Wi-Fi).
- Often uses spoofing techniques.

OPERATIONAL/ BUSINESS IMPACT

- Eavesdropping on sensitive data.
- Data manipulation.

PREVENTIVE MEASURES/ RESPONSES

- Use of encryption protocols (e.g., HTTPS).
- VPN usage on public networks.

LEGAL PROTECTIONS/ CONSIDERATIONS IN MALAYSIA

- Covered under the Computer Crimes Act 1997; unauthorized interception of communications is illegal. Penalties can include fines and imprisonment.

MALWARE

DESCRIPTION

Malware refers to malicious software designed to harm or exploit any programmable device or network.

CHARACTERISTICS

- Includes viruses, worms, trojans, ransomware, etc.
- Can steal data or damage systems.

OPERATIONAL/ BUSINESS IMPACT

- Data loss or corruption.
- System downtime.

PREVENTIVE MEASURES/ RESPONSES

- Antivirus software deployment.
- Regular updates and patches.

LEGAL PROTECTIONS/ CONSIDERATIONS IN MALAYSIA

- The Cyber Security Act 2024 includes provisions against malware distribution; violators may face penalties including fines and imprisonment.

The Saboteur

Malware acts like a saboteur, infiltrating systems and causing damage, stealing information, or corrupting operations from within.

The Opportunist

Exploiting unknown vulnerabilities before they are patched mirrors an opportunist who strikes when their target is unprepared.

ZERO-DAY EXPLOIT

DESCRIPTION

A zero-day exploit takes advantage of a previously unknown vulnerability before it is patched by developers.

CHARACTERISTICS

- Highly effective as there are no defenses available at the time of attack.

OPERATIONAL/ BUSINESS IMPACT

- Significant risk as exploits can lead to unauthorized access or data breaches.

PREVENTIVE MEASURES/ RESPONSES

- Timely software updates and patch management practices.
- The usage of firewalls.

LEGAL PROTECTIONS/ CONSIDERATIONS IN MALAYSIA

- Subject to the Computer Crimes Act 1997; exploitation of vulnerabilities can lead to legal consequences including fines and imprisonment.

SOCIAL ENGINEERING ATTACK

DESCRIPTION

Social engineering involves manipulating individuals into divulging confidential information through deception.

CHARACTERISTICS

- Relies on psychological manipulation rather than technical skills.

OPERATIONAL/ BUSINESS IMPACT

- Compromised sensitive information.
- Financial loss.

PREVENTIVE MEASURES/ RESPONSES

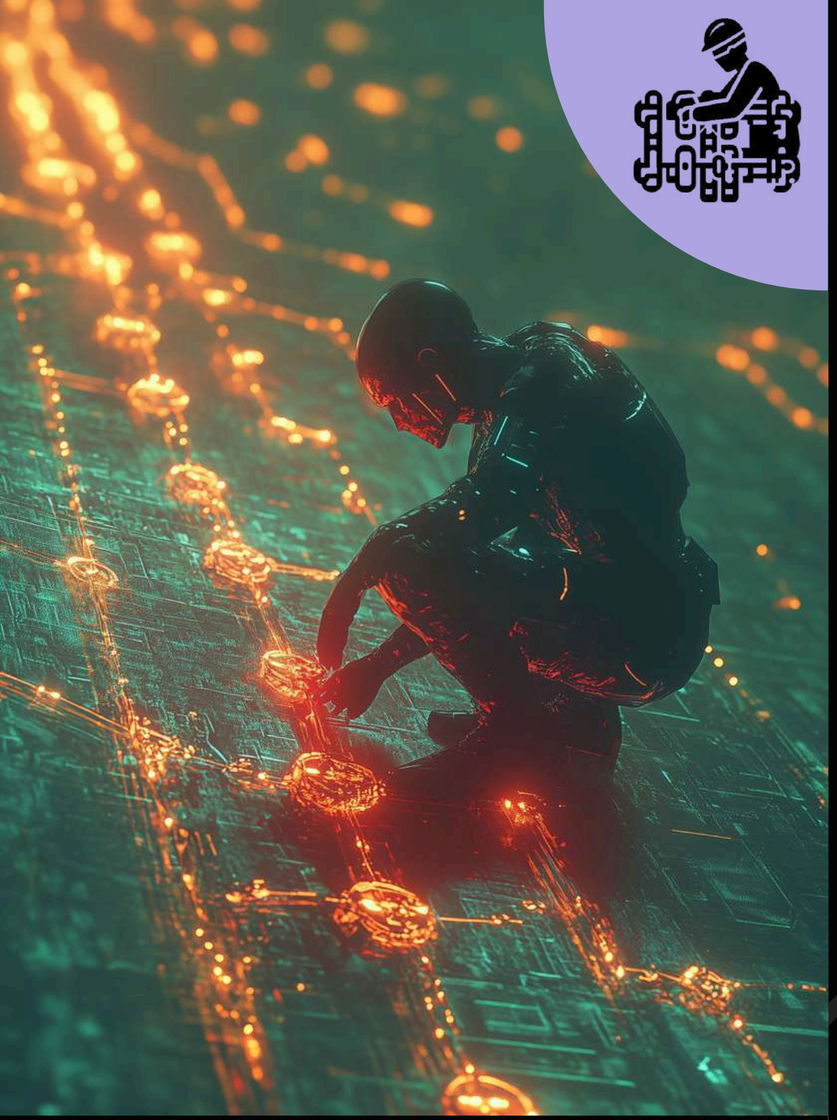
- User awareness training on social engineering tactics.
- Verification processes for sensitive requests.

LEGAL PROTECTIONS/ CONSIDERATIONS IN MALAYSIA

- Covered under various laws including the PDPA; organizations must safeguard personal data against such tactics. Violations may result in legal action and fines.

The Master Manipulator

Using psychological tricks to gain sensitive information mimics a manipulator exploiting trust and emotions for their gain.



The Sabotage Specialist

Targeting trusted suppliers or partners to indirectly harm an organization is similar to a specialist who infiltrates indirectly to cause systemic harm.

SUPPLY CHAIN ATTACK

DESCRIPTION

Supply chain attacks target vulnerabilities within third-party vendors or partners to compromise an organization indirectly.

CHARACTERISTICS

- Exploits trust relationships between organizations.
- Can affect multiple entities simultaneously.

OPERATIONAL/ BUSINESS IMPACT

- Data breaches.
- Operational disruptions.
- Financial losses.

PREVENTIVE MEASURES/ RESPONSES

- Thorough vetting of suppliers.
- Continuous monitoring of third-party security practices.

LEGAL PROTECTIONS/ CONSIDERATIONS IN MALAYSIA

- Subject to the Cyber Security Act 2024; organizations must ensure third-party compliance with cybersecurity standards, with penalties for non-compliance.

AI-DRIVEN CYBERATTACKS

DESCRIPTION

Cybercriminals use AI tools to automate attacks, create personalized phishing emails, and adapt tactics in real-time.

CHARACTERISTICS

- Highly sophisticated attacks that evade traditional detection methods.

OPERATIONAL/ BUSINESS IMPACT

- Increased difficulty in detecting threats.
- Potentially higher success rates for attackers.
- Rapid pace of the attack poses difficulty to effectively respond.

PREVENTIVE MEASURES/ RESPONSES

- Invest in advanced AI-based detection tools.
- Regularly update security protocols.

LEGAL PROTECTIONS/ CONSIDERATIONS IN MALAYSIA

- No specific laws yet; however, general cybersecurity laws apply as AI-driven attacks fall under existing cybercrime regulations.

The High-Tech Fraudster

Leveraging AI for personalized phishing, automation, and real-time adaptability mirrors a high-tech fraudster using advanced tools to outsmart traditional defenses.

The Impersonator

Creating realistic fake identities to deceive others resembles an impersonator or forger who mimics others for fraudulent purposes.

DEEPFAKE SCAMS

DESCRIPTION

Deepfake technology creates realistic audio or video impersonations used in scams or social engineering attacks.

CHARACTERISTICS

- Can convincingly impersonate trusted individuals.
- Exploits trust within organizations.

OPERATIONAL/ BUSINESS IMPACT

- Financial fraud.
- Compromised sensitive information.

PREVENTIVE MEASURES/ RESPONSES

- Employee training on recognizing deepfake content.
- Verification processes for unusual requests.

LEGAL PROTECTIONS/ CONSIDERATIONS IN MALAYSIA

- Not specifically regulated; falls under general fraud laws and PDPA if personal data is involved.
- Subject to Section 211(1) of the Communications and Multimedia Act 1998 penalties could apply for content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person.

REFERENCES

- Cyber Security Act 2024: This act governs cybersecurity measures in Malaysia, particularly for National Critical Information Infrastructure (NCII) sectors.
- Personal Data Protection Act (PDPA) 2010: Regulates the processing of personal data in commercial transactions in Malaysia.
- Computer Crimes Act 1997: Addresses various computer-related offenses including unauthorized access and manipulation of data.

Secure Your Cyber Space, Secure Your Business Future

SUPPIAH & PARTNERS

+603-4142 3766

https://suppiahlaw.com/

thulasy@suppiahlaw.com

UG-13, LEXA Galleria,
No. 45, Jln 34/26, Wangsa Maju,
53300 Kuala Lumpur

Explore more AI newsletters—click here!