Short Question

Name	Midterm
Review	□

Lec 1 - Consider the top cyber-attack(phishing attack, malware and botnet attack) and how to reduce the risk

1. Phishing Attacks: Phishing attacks involve deceiving individuals into providing sensitive information such as usernames, passwords, or credit card details. To reduce the risk:

- Education and Awareness教育和意识: Educate yourself and your employees about phishing techniques and common red flags to look out for, such as suspicious email addresses, spelling errors, and urgent requests for personal information.
- Exercise Caution with Emails注意电子邮件: Be cautious when clicking on links or downloading attachments in emails, especially from unknown or suspicious senders. Verify the legitimacy of the email by contacting the organization directly through their official channels.
- Implement Email Filters实施filter: Utilize spam filters and email authentication protocols like Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) to help identify and block phishing emails.
- Use Two-Factor Authentication (2FA)使用双因素身份验证: Enable 2FA wherever possible to provide an additional layer of security. This helps prevent unauthorized access even if your credentials are compromised.

2. Malware: malicious software designed to disrupt, damage, or gain unauthorized access to computer systems. To reduce the risk:

- Use Antivirus/Anti-Malware Software使用防病毒软件: Install reputable antivirus/anti-malware software on all devices and keep it up to date. Regularly scan for malware and ensure real-time protection is active.
- Regular Software Updates定期软件更新: Keep all software and operating systems patched and up to date. Software updates often include security patches that address vulnerabilities exploited by malware.
- Exercise Caution Online在线时保持警惕,避免点击可疑链接: Avoid clicking on suspicious links, downloading files from untrustworthy sources, or visiting potentially malicious websites. Be careful with email attachments and only download them from trusted senders.
- Enable Firewalls启用防火墙: Activate firewalls on your devices and network to monitor and control incoming and outgoing network traffic, helping to block unauthorized access and potential malware.

3. Botnet Attacks: networks of compromised computers controlled by attackers for various malicious activities. To reduce the risk:

- Strong Passwords强密码: Use strong, unique passwords for all your online accounts, including routers and IoT devices. Avoid using default or easily guessable passwords.
- Network Segmentation网络分割: Segment your network to isolate critical systems and restrict unauthorized access between different network segments. This helps contain potential botnet infections.
- Regular Device Updates定期设备更新: Keep your devices, including routers and IoT devices, updated with the latest firmware. Manufacturers often release updates to address security vulnerabilities.
- Monitor Network Traffic监控网络流量: Regularly monitor your network traffic for any suspicious activity or unusual data transfers. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) can help detect and prevent botnet activity.

Lec 2 - 8 moral theories for three choices. (give reason for all 8 principle)

Relativism

it recognizes the diversity of moral values and beliefs **across different cultures** and individuals. 不同文化和个体之间存在着道德价值观和信仰的多样性 It **acknowledges** that moral judgments are subjective and **depend on individual perspectives.** Relativism promotes tolerance and understanding by acknowledging that there is no universal standard for morality.

Divine Command

based on the belief that moral principles are **derived from a higher power**, such as religious scripture. This theory is chosen because it **provides a clear and absolute moral framework** for those who believe in a divine authority. It asserts that moral obligations are rooted in the commands and teachings of a supreme being.

Utilitarianism

focuses on **maximizing overall happiness or well-being.** This principle considers the **consequences of actions** and aims to bring about the greatest amount of happiness **for the greatest number of people**. 为最多的人带来最大的幸福感 Utilitarianism emphasizes the importance of the overall welfare and utility of individuals.

Kantian Ethics

emphasizes the importance of moral duty and principles. 强调道德义务和原则的重要性 It asserts that actions should be guided by universal moral laws, regardless of consequences. Kantian Ethics places a strong emphasis on rationality, autonomy, and treating individuals as ends in themselves rather than merely as means to an end.

Rights

recognizes the inherent and inalienable rights of individuals. It asserts that individuals possess certain fundamental rights, such as the right to life, liberty, and security. This theory places importance on respecting and protecting the rights of individuals, promoting justice and fairness. 强调尊重和保护个体的权利，促进正义和公平

Virtue Ethics

focuses on the development of virtuous character traits. It emphasizes the importance of cultivating virtues such as honesty, compassion, and courage. Virtue Ethics encourages individuals to **strive for excellence and moral integrity in their actions**, aiming to become virtuous individuals who **contribute positively to society**. 鼓励个体在行动中追求卓越和道德正直

Ethics of Care

emphasizes the significance of **caring relationships and compassion.** 它强调关怀关系和同情心的重要性 It highlights the moral obligations and responsibilities that arise from these relationships, particularly in contexts such as family, community, or healthcare. The Ethics of Care prioritizes **empathy, nurturing, and meeting the needs of others.**共情、培养和满足他人需求

Social Contract

focuses on the idea that moral principles and obligations arise from a social agreement or contract. It asserts that individuals voluntarily enter into a social contract to establish a just and orderly society. 个体自愿进入社会契约以建立一个公正和有秩序的社会 This theory emphasizes the importance of fairness, cooperation, and **fulfilling agreed-upon obligations** for the benefit of society.

Lec 3 - Should Companies Pay Ransomware to Hackers? Pros & Cons for both "To Pay" and "Not to Pay"

To Pay:

Pros:

1. Data Recovery数据恢复: Paying the ransom may result in the decryption key or tools being provided, allowing the company to regain access to their data and systems more quickly.
2. Minimize Downtime减少停机时间: Paying the ransom can potentially minimize the disruption to business operations and reduce financial losses associated with extended downtime.
3. Reputation Management声誉管理: Paying the ransom and resolving the situation quietly can help protect the company's reputation and prevent negative publicity or loss of customer trust.

Cons:

1. No Guarantee没有保证: There is no guarantee that paying the ransom will result in the safe recovery of data or systems. Hackers may take the money and fail to provide the promised decryption tools or may even demand additional payments.
2. Encouraging Criminal Activity鼓励犯罪活动: Paying the ransom reinforces the business model of ransomware attacks, encouraging hackers to continue targeting organizations for financial gain.
3. Legal and Ethical Concerns法律和道德问题: Paying ransomware may potentially violate laws and regulations, as well as ethical principles, supporting criminal activities and potentially funding other illegal operations.

Not to Pay:

Pros:

1. Discourages Future Attacks遏制未来攻击: Refusing to pay the ransom sends a message that the company does not negotiate with hackers and can discourage future attacks, potentially protecting the organization and others from similar threats.
2. Financial Savings节约财务资源: Not paying the ransom eliminates the immediate financial burden and potential for ongoing demands from hackers.

3. Promotes Cybersecurity Preparedness促进网络安全准备: Focusing on preventive measures, such as robust cybersecurity practices and data backups, can help organizations be better prepared for future attacks.

Cons:

1. Data Loss数据丢失: Not paying the ransom may result in the permanent loss of critical data, which can have significant implications for the business, its operations, and its customers.
2. Extended Downtime停机时间延长: Recovering from a ransomware attack without paying can be a time-consuming process, leading to extended downtime, financial losses, and potential damage to the company's reputation.
3. Legal and Regulatory Consequences法律和监管后果: Some jurisdictions may impose legal or regulatory penalties on organizations that fail to adequately protect sensitive data or report security breaches.

considering the specific circumstances, legal implications, and expert advice from cybersecurity professionals.

Lec 4 - autonomous car related question similar to Lec 2

Lec 5 - Choose principles(give reason for all 6 principle)

Principle 1 - Purpose and Manner of Collection

This principle emphasizes the importance of **clearly defining the purpose for which personal data is collected and ensuring that it is collected in a lawful and fair manner.** By adhering to this principle, organizations can **establish transparency and trust with individuals** by providing them with information about how their data will be used and ensuring it is collected with their consent.建立透明度和信任关系。

Principle 2 - Accuracy and duration of retention

This principle highlights the need for organizations to ensure the **accuracy** of personal data and to retain it for only as long as necessary to fulfill the purpose for which it was collected. It promotes the idea that personal data should be **kept up to date and relevant, minimizing the risk of using outdated or unnecessary information.减少使用过时或不必要信息的风险**

Principle 3 - Use of Personal Data

The principle of the use of personal data emphasizes that organizations should use personal data only for the purposes for which it was collected or for other legitimate purposes with the individual's consent. This principle ensures that personal data **is not misused or used in a way that is incompatible with the original purpose, protecting individuals' privacy rights.**确保个人数据不被滥用，保护个人的隐私权。

Principle 4 - Security of Personal Data

This principle highlights the importance of implementing appropriate security measures to protect personal data against unauthorized access, disclosure, or loss. It emphasizes the need for organizations to safeguard personal data through technical and organizational measures, **ensuring its confidentiality, integrity, and availability.**

Principle 5 - Information to be generally available

The principle of information to be generally available promotes transparency by requiring organizations to **provide individuals with information about their data processing practices,** including the purposes, categories of data, recipients, and rights of individuals. This principle ensures individuals have access to information about how their personal data is being handled and **allows them to make informed decisions regarding their privacy.**

Principle 6 - Access to Personal Data

This principle recognizes the right of individuals to access their personal data held by organizations. It ensures that **individuals have the opportunity to review, correct, or delete their personal data** and allows them to have control over their information. This principle promotes accountability and **empowers individuals to manage their own data privacy.**

Lec 6 - Can I install video camera at home to monitor my domestic helper. and how to reduce risk

1. understand the legal requirement: regulations related to video surveillance in your region
2. Obtain informed consent: before install camera, discuss with domestic helper and obtain informed consent. explain purpose of the camera
3. limit camera placements
4. protect recording footage
5. communicate openly
6. regular review and delete footage