MIS761
Cyber Security Strategies

Dept. of Information Systems & Business Analytics

Deakin Business School

Week 2: Cyber Threats

DEAKIN
BUSINESS SCHOOL

AACSB ACCREDITED

EQUIS ACCREDITED

C-I-A Triad

- **Confidentiality:** refers to limited observation and disclosure of an asset (or data).
  - A loss of confidentiality implies that data were actually observed or disclosed to an unauthorized actor rather than endangered, at-risk or potentially exposed.
  - Short definition: limited access, observation and disclosure.
- **Integrity:** refers to an asset (or data) being complete and unchanged from the original or authorized state, content and function.
  - Losses to integrity include unauthorized insertion, modification and manipulation.
  - Short definition: complete and unchanged from original.
- **Availability:** refers to an asset (or data) being present, accessible and ready for use when needed.
  - Losses to availability include destruction, deletion, movement, performance impact (delay or acceleration) and interruption.
  - Short definition: accessible and ready for use when needed.

https://verisframework.org/attributes.html

Threat, Vulnerability, and Risk

- Threat is anything that can harm, damage, steal your assets
  - internal/external; human-related/technology-related; intentional/unintentional
- Vulnerability is a weakness/flaw within your systems (tech, process, people)
- Risk is the likelihood of a threat exploiting a vulnerability within your system.

➢ Leaving your car unlocked in a neighborhood known for thefts increases the probability of your car being stolen.

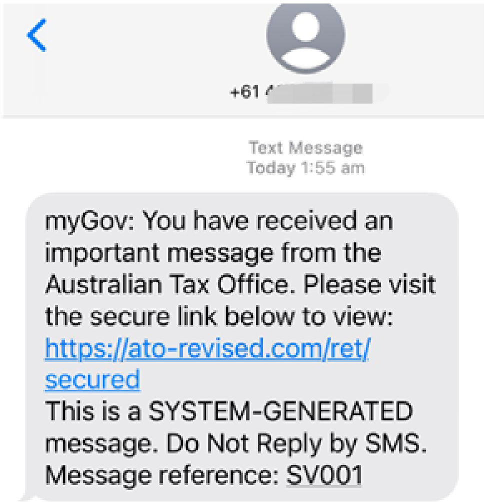
➢ A poorly configured firewall allows a malware attack to succeed, raising the chance of unauthorized data access.

Social Engineering

Social engineering is the act of tricking someone into divulging information or taking action, usually through technology. The idea behind social engineering is to take advantage of a potential victim's natural tendencies and emotional reactions.

https://www.ibm.com/topics/social-engineering

Social Engineering-Phishing



+61 4[redacted]

Text Message
Today 1:55 am

myGov: You have received an important message from the Australian Tax Office. Please visit the secure link below to view: https://ato-revised.com/ret/secured
This is a SYSTEM-GENERATED message. Do Not Reply by SMS. Message reference: SV001

A webpage displaying a tax return amount
Asking for updating account details
Not really urging for quick action

A page mimicking my bank's login screen
Asking for account username and password

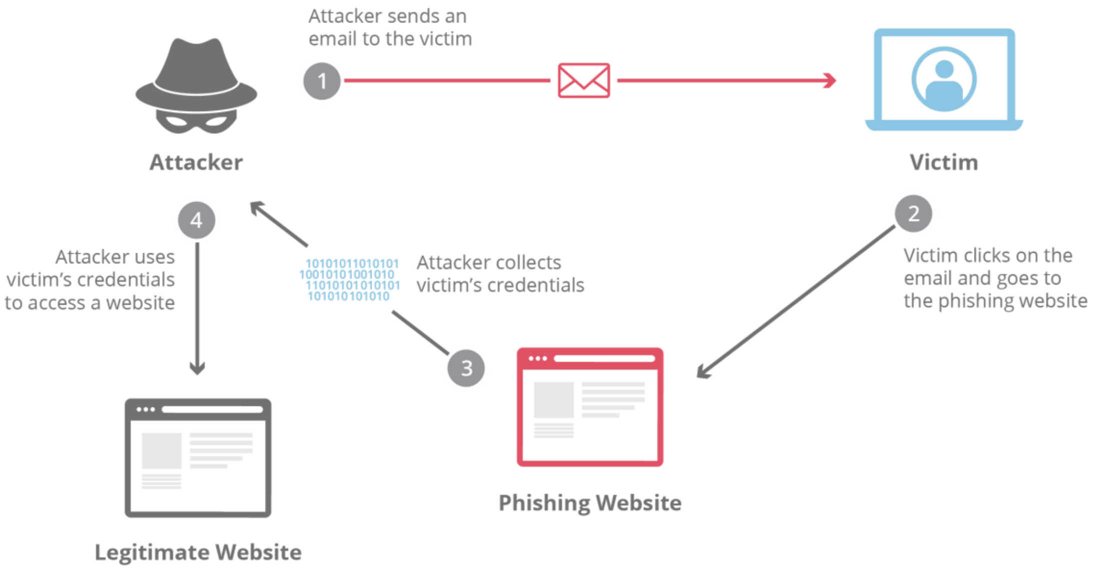
Impersonating
Imitating
Right Timing

Convincing Information
Authentic Design
Subtle Coercion

Evolving manipulation

Social Engineering-Phishing

- **What is Phishing?**
  - A **cyberattack** that uses deceptive communications to steal sensitive information.
  - Impersonates trustworthy sources to trick victims.
  - In forms of emails, SMSs, phone calls, QR codes, etc.
- **How Phishing Works:**
  1. **Impersonation:** Hacker poses as a familiar contact (e.g., colleague, authority figure).
  2. **Deceptive Message:** Instructs victim to click links, download attachments, or pay invoices.
  3. **Execution:** Victim's actions lead to malware installation, data theft, or financial loss.
- **Intent & Impact of Phishing:**
  - Deploys ransomware.
  - Steals account credentials.
  - Compromises personal and organizational security.


Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim's credentials to access a website
10101011010101
10010101001010
11010101010101
101010101010
Attacker collects victim's credentials
3
Phishing Website
Legitimate Website

https://www.cloudflare.com/en-gb/learning/access-management/phishing-attack/

Social Engineering-Pretexting

- **What is Pretexting?**
  - A **social engineering technique** where attackers use fabricated stories (pretexts) to manipulate individuals into divulging sensitive information, transferring funds, or executing harmful actions.
  - Methods: Impersonating via spoofed emails, hacked accounts, phone calls, or in-person interactions.
- **Key Elements of Pretexting:**
  1. **Character:** The role the attacker assumes, often someone with authority or trustworthiness (e.g., boss, IT specialist, HR representative).
  2. **Situation:** The scenario or story used to justify the request or action, ranging from routine (update your account) to specific (urgent task from a supervisor).
- **Making Pretexts Believable:**
  - Extensive research on victims using social media and public records.
  - Techniques include email and phone number spoofing, or unauthorized access to personal communication channels.

https://www.ibm.com/topics/pretexting
https://www.crowdstrike.com/cybersecurity-101/pretexting/

Social Engineering- BEC

- Business email compromise (BEC)
  - an attacker falsifies an email message to trick the victim into performing some action — most often, transferring money to an account or location the attacker controls.
  - BEC attacks differ from other types of email-based attacks in a couple of key areas:
    - They do not contain malware, malicious links, or email attachments
      - often bypass traditional email filters
    - They target specific individuals within organizations
      - personalized to the intended victim and often involve advance research of the organization in question
      - harder to block
        - low-volume
        - use a legitimate source or domain
        - may actually from a legitimate (while previously compromised) email account

https://www.cloudflare.com/en-gb/learning/email-security/business-email-compromise-bec/

Scenario 1

You receive an email that appears to come from the unit coordinator of your MIS761 course. The subject line reads, "Urgent: Secure Your Spot in Exclusive Workshop." The email includes the university's official logo and mimics the style and tone of previous communications you've received from the coordinator.

The message enthusiastically details a new, exclusive workshop in collaboration with a leading tech company. This event is described as a key component of the course, designed to enhance your skills through direct industry engagement. Participation is highly encouraged as it will count towards your final grade.

However, there’s a logistical issue: the workshop requires a specialized software license not covered by the university. The coordinator explains that due to the time-sensitive nature of this arrangement, they’ve negotiated a discounted bulk purchase directly with the supplier.

To facilitate this, students are asked to contribute their share of the cost upfront. Instead of using the usual university payment systems, which might delay the process, the coordinator provides a bank account number where students should transfer their contributions. The email emphasizes that this quick action is necessary to ensure all participating students benefit from the discounted rate and that receipts of transactions should be sent to a new finance officer’s email for record-keeping and prompt reimbursement from the department's budget.

The email closes with a note of urgency and excitement about the learning opportunity, urging immediate action to secure the necessary resources and your place in the workshop.

Scenario 2

- You receive a phone call from someone who claims to be your tutor for the course MIS761. The caller sounds concerned and explains that during a routine check, your recent assignment was flagged for potential issues with academic integrity. Specifically, they mention that a paragraph in your work appears to have been copied almost verbatim from a journal article.
- However, the caller reassures you that Deakin University adopts an educational approach to academic integrity issues, especially for first-year students. They explain that instead of penalizing you immediately, Deakin prefers to offer a chance for early intervention. This involves giving you the opportunity to revise the problematic sections of your assignment and resubmit it within seven days to avoid any marks deduction.
- To facilitate this, the caller claims they need to check if you qualify for this intervention through a specific university system. For this purpose, they ask for your university login and password to verify your identity and access the necessary details on the system.

Scenario 3

- You receive an email claiming to be from the unit chair, stating that there was an error with your assignment format. The email warns that the regular submission system is temporarily unavailable and provides a link for you to submit your work immediately to avoid a late submission penalty.

Ransomware

- **What is Ransomware?**
  - A type of malware that encrypts or locks access to victim’s data or devices.
  - Demands ransom, often in cryptocurrency, to restore access or prevent data leakage.
  - **Double Extortion**: Involves not only encrypting the victim’s data but also stealing it. Attackers threaten to release the stolen data publicly if the ransom is not paid.
  - **Triple Extortion:** Exploiting the stolen data to attack the victim’s customers or business partners.
  - **Quadruple Extortion**: Adds further complexity by including threats to harm the victim’s reputation through other means, such as threatening to inform customers, business partners, employees, media or even law enforcement and regulatory bodies about potential legal violations
- **Impact of Ransomware:**
  - Financial losses from ransom payments and breach mitigation.
  - Lost revenue and/or temporary closure due to significant operational downtime
  - Potential reputational damage if data is leaked.
  - C-level resignations, Layoffs

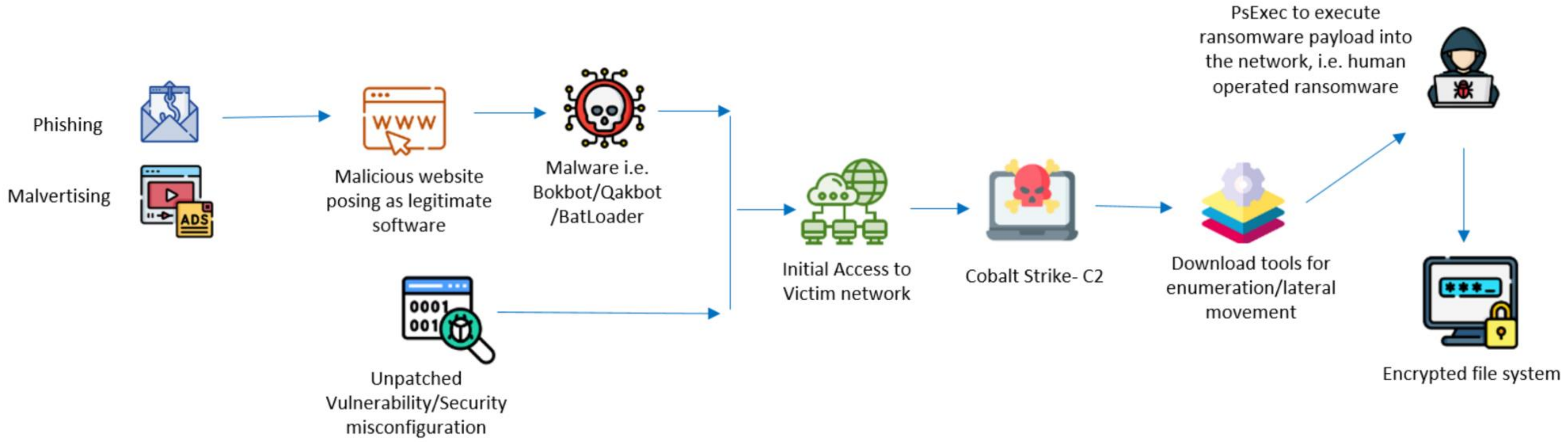
https://www.ibm.com/topics/ransomware?mhsrc=ibmsearch_a&mhq=ransomware
https://www.crowdstrike.com/cybersecurity-101/ransomware/
https://www.cloudflare.com/en-gb/learning/security/ransomware/what-is-ransomware/

Ransomware

How Ransomware Operates:

1. **Infection:** Often initiated through a combination of social engineering, system vulnerabilities, credential theft, drive-by downloads and other malware to infiltrate systems, leading victims to unknowingly download the ransomware.
2. **Encryption:** After infection, ransomware encrypts valuable files and data, rendering them inaccessible.
3. **Ransom Demand:** Victims receive a ransom note demanding payment for a decryption key or to prevent data exposure.

- **Types of Ransomware:**
  - **Encrypting Ransomware:** Locks data with encryption.
  - **Screen Lockers:** Blocks access to the device with a lock screen.
  - **Leakware/Doxware:** Threatens to publish stolen data online.
  - **Scareware:** Tricks users into paying ransoms by posing as legitimate security warnings.


Phishing
Malvertising
Malicious website posing as legitimate software
Malware i.e. Bokbot/Qakbot /BatLoader
Unpatched Vulnerability/Security misconfiguration
Initial Access to Victim network
Cobalt Strike- C2
Download tools for enumeration/lateral movement
PsExec to execute ransomware payload into the network, i.e. human operated ransomware
Encrypted file system

https://www.ibm.com/topics/ransomware?mhsrc=ibmsearch_a&mhq=ransomware
https://www.crowdstrike.com/cybersecurity-101/ransomware/
https://www.cloudflare.com/en-gb/learning/security/ransomware/what-is-ransomware/

Figure-1: Royal Ransomware Infection Chain

Denial of Service, and Distributed DoS

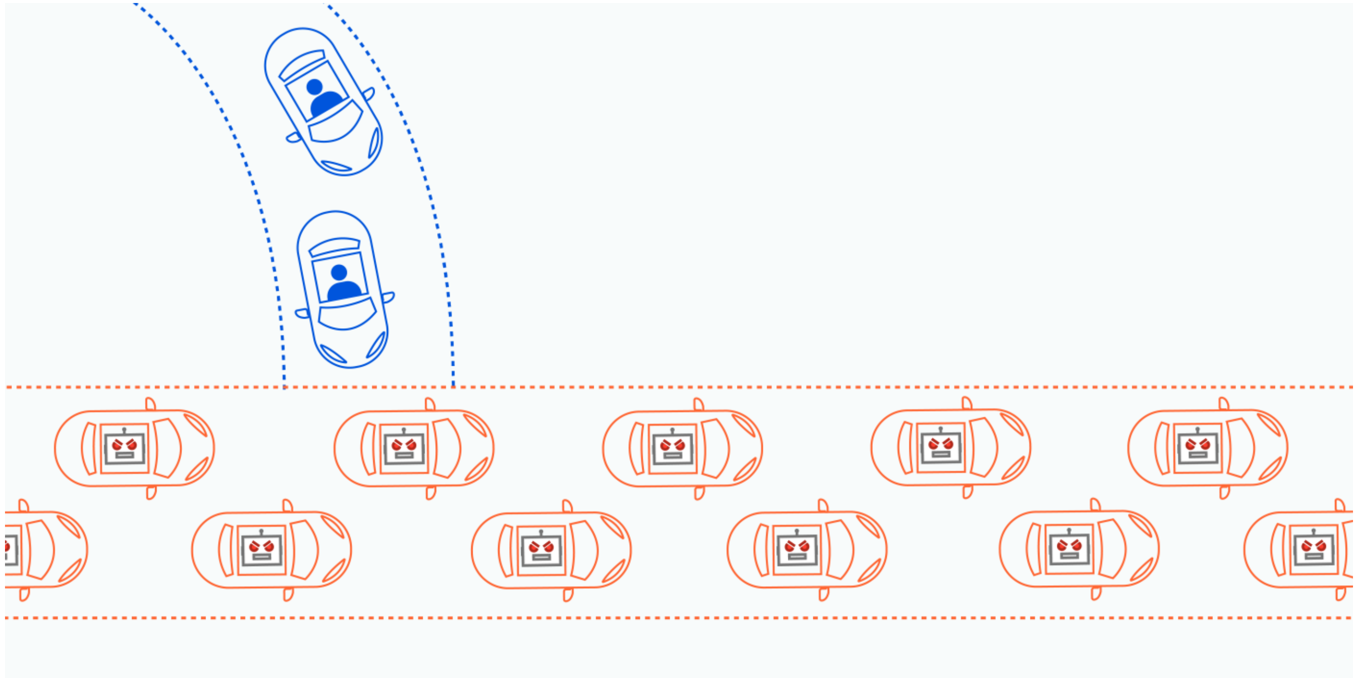
- **What Are DoS and DDoS Attacks?**
  - **DoS (Denial-of-Service) Attack:** Floods a target with excessive requests to disrupt normal operations, typically launched from a single source.
  - **DDoS (Distributed Denial-of-Service) Attack:** Similar to DoS but executed from multiple compromised systems (a botnet) across various locations, significantly amplifying the attack's scale and impact.
- **How Do These Attacks Work?**
  1. **Infection Phase:** Attackers infect multiple devices with malware to form a botnet. Devices can range from computers to IoT devices.
  2. **Attack Launch:** Each compromised device (bot) sends numerous requests to the target's IP address, overwhelming the system.
  3. **Result:** The target server or network is overloaded, leading to slowed service or complete unavailability for legitimate users.
- **Key Differences:**
  - **Scale and Complexity:** DDoS attacks use multiple systems (botnet), making them more disruptive and harder to mitigate than single-source DoS attacks.
  - **Detection Difficulty:** DDoS traffic often mimics legitimate user traffic, complicating the differentiation between harmful and normal interactions.
- **Mitigation Philosophy (but also the challenge):** Distinguish between legitimate user traffic and attack vectors without disrupting normal operations.

https://www.crowdstrike.com/cybersecurity-101/denial-of-service-dos-attacks/
https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/

Carpet Bomb DDoS

- **What is a Carpet Bomb DDoS Attack?**
  - **Definition:** A type of DDoS attack that distributes malicious traffic across a wide range of IP addresses within the same network or service provider.
  - **Analogy:** Similar to aerial carpet bombing in warfare, this attack spreads its effects broadly rather than targeting a specific point, aiming to overwhelm not just one target but an entire network segment.
- **How Carpet Bomb Attacks Work:**
  1. **Wide Distribution:** Attacks simultaneously target multiple IP addresses within a network, diluting the focus of the attack but aggregating to a significant overall volume.
  2. **Evasion Techniques:** By spreading the attack across many IPs, it becomes harder for traditional DDoS mitigation systems to pinpoint and address the threat without affecting legitimate traffic.
  3. **Challenges for Mitigation:**
  - **Threshold Confusion:** Spreading the attack makes it difficult for systems to set clear thresholds for normal vs. attack traffic, potentially allowing more attack traffic to slip through.
  - **Mitigation Overload:** Traditional mitigation strategies like IP blackholing become ineffective, as they would require shutting down too much legitimate traffic, harming the network.
- **Unique Impacts of Carpet Bombing:**
  - **Operational Disruption:** Can cause significant disruption to a network's operations by forcing defensive measures that may inadvertently block legitimate traffic.
  - **Resource Strain:** Overwhelms both the targeted network and the mitigation resources, such as scrubbing centers or cloud-based defenses, which are not designed to handle high volumes of distributed attacks.

https://www.juniper.net/content/dam/www/assets/analyst-reports/us/en/2023/corero-ddos-threat-intelligence-report.pdf



DoS: A single truck breaks down in a one-lane road, blocking all traffic.

DDoS: Hundreds of cars swarming a highway, completely halting traffic across multiple lanes.

Carpet Bomb DDoS: Hundreds of cars simultaneously causing smaller jams on numerous roads throughout an entire city

Fake Threat, True Fear and Impacts?

- **What is Fake Extortion?**
  - Fake extortion involves scammers posing as hackers or ransomware groups, threatening organizations with data leaks or DDoS attacks without actual access to the organization's systems or data.
- **How Do Fake Extortion Groups Operate?**
  1. **False Claims of Control:** Send emails claiming to have compromised systems or stolen sensitive data.
  2. **Impersonation:** Often mimic known ransomware groups or use names similar to notorious cybercriminals to enhance the credibility of their threats.
  3. **Urgency and Fear:** Create a sense of urgency with deadlines for ransom payments, using social engineering to induce panic.
- **Tactics Used by Fake Extortionists:**
  - **Manipulate Perception:** Rely on the victim's lack of technical knowledge to discern real threats from fabricated ones.
    - **Show Real Data**: Scammers compile publicly available or previously breached data, presenting it as freshly stolen to convince victims of a credible threat.
    - **Use Malware to Simulate Encryption**: Deploy simple malware via phishing that renames or relocates files on the victim's system without actually encrypting them.
  - **DDoS Threats:** Threaten to disable services through DDoS attacks to pressure victims into paying ransoms.
  - **Data Leak Threats:** Claim they will release stolen data to the public if the ransom is not paid.
- **Responding to Fake Extortion Attempts:**
  1. **Verify Threats:** Investigate the authenticity of the claim. Check if the data breach or DDoS potential is real.
  2. **Seek Professional Advice:** Consult with cybersecurity experts to analyze the threat and advise on proper actions.
  3. **Implement Robust Security Measures:** Ensure regular backups, strong password policies, and multi-factor authentication are in place.
  4. **Educate and Train:** Raise awareness among employees about fake extortion and other phishing tactics.

https://securityintelligence.com/news/spot-fake-extortion-attacks-without-wasting-time-and-money/
https://socradar.io/fake-extortion-how-to-tackle-and-how-to-verify/

ICT supply chain threat

- ICT supply chain threats arise when cyber actors exploit vulnerabilities within the network of third-party services and products that organizations rely on, from hardware suppliers to cloud hosts and software-as-a-service providers.
- **How Attacks Occur:**

  Dual Attack Vector: Cyber actors initially compromise a supplier, gaining access to their products and services, and subsequently attack the customers using those compromised elements.

  Exploitation Techniques: Common methods include abusing misconfigurations, phishing, exploiting vulnerabilities (CVEs), and leveraging the inherent trust between suppliers and customers.
- **Impact of Supply Chain Compromises:**

  Broad Reach: A single breach at a supplier level can impact hundreds or thousands of downstream customers.

  Data Theft and Extortion: Attackers can steal sensitive information or disrupt services, leading to financial and reputational damage for both suppliers and their customers.
- **Mitigation Strategies:**
  - **Supplier Security Assurance:** Customers should demand high cybersecurity standards and clear security practices from their suppliers, including secure-by-design products and regular security audits.
  - **Robust Contractual Agreements:** Include cybersecurity expectations and standards as part of procurement contracts.
  - **Continuous Vigilance:** Regularly assess and update the security measures in place to respond to evolving threats in the supply chain.

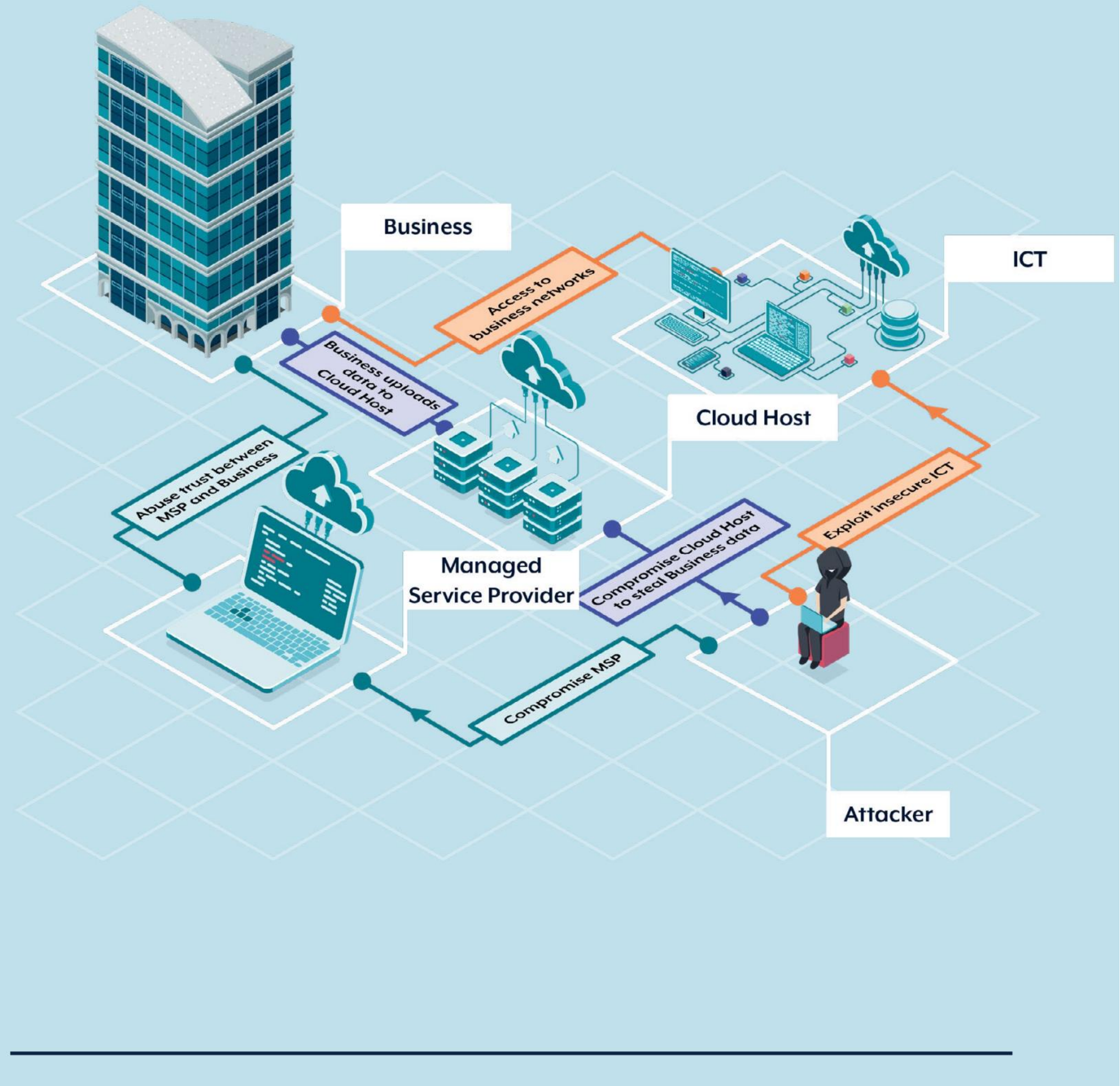

Business
ICT
Access to business networks
Business uploads data to Cloud Host
Cloud Host
Abuse trust between MSP and Business
Managed Service Provider
Compromise Cloud Host to steal Business data
Exploit insecure ICT
Compromise MSP
Attacker

Figure 6: ICT supply chain threats

https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023