Security Policy for Home

Section 1: Risk 1: Client Information Loss

Background Research: The loss of client information by an inside employee is a significant security concern that can result in severe consequences. This typically occurs due to human error, negligence, or malicious intent. A real-life example of such a situation was the 2018 Marriott data breach, where the personal details of nearly 500 million guests were exposed. A significant part of the blame was placed on internal negligence.

Another example is the 2017 Equifax data breach. The personal info of 147 million people was exposed due to an internal error. The root cause was traced back to a failure to install a software patch on time, which highlights the potential for internal human error leading to significant data loss.

Likelihood: While the exact likelihood can depend on specific circumstances like the organization's size, data handling practices, and employee training, generally speaking, the risk is quite high. According to the Ponemon Institute's 2020 Cost of a Data Breach Report, around 30% of data breaches involved internal actors.

Consequences: - **Financial:** The loss of client information can result in considerable financial loss due to litigation, regulatory fines, and loss of business. For instance, Equifax had to pay $575 million in fines and customer restitution due to their breach.

- **Asset:** The company's reputation, a significant intangible asset, can be severely damaged. Loss of trust can lead to loss of clients and potential business opportunities.

- **Client:** Clients can suffer identity theft, financial loss, and other forms of harm if their personal information is misused. This can lead to a breakdown in the client-company relationship.

- **System:** A breach could indicate system vulnerabilities that need addressing, which can be costly and time-consuming.

- **Infrastructure:** Depending on the scale of the breach, there could be substantial impact to the infrastructure, including the need for overhauls or upgrades.

Mitigation Strategies: Not provided.

Section 2: Risk 2: Man In The Middle Attack

Background Research: Man-in-the-middle (MITM) attacks occur when a hacker intercepts the communications between two parties, either to secretly eavesdrop or modify the data traveling between the two. Attackers might use MITM attacks to steal login credentials or personal financial information, or to inject malware into the communication.

Real-life examples of this kind of attack are abundant. A notable incident occurred in 2014 when the Chinese government allegedly executed a MITM attack against Apple's iCloud to gain access to usernames and passwords of encrypted iOS data. Another example is the 2013 Belgian Telecom attack where the UK intelligence agency GCHQ and NSA reportedly intercepted the telecom's communication to spy on their traffic.

Likelihood: The likelihood of this risk is moderate to high. As more businesses migrate to public cloud services and as cyber threats continue to evolve, the probability of such an attack occurring is increasing.

Consequences: - Financial: Financial losses from the theft of banking information, fraudulent transactions, or ransomware payments.
- Asset: Loss or corruption of data assets. Unauthorized access to sensitive business or personal data.
- Client: Loss of trust from clients due to breach of their personal or financial data. Potential lawsuits.
- System: System downtime or malfunction due to malicious software or code injections.
- Infrastructure: Damage to IT infrastructure, which can be costly to repair and cause significant downtime.

Mitigation Strategies: - Financial risks: Implement strong security measures such as encryption and secure payment gateways. Regularly monitor financial transactions for any signs of fraudulent activity.
- Asset Risks: Encryption of data at rest and in transit. Regularly backup data and implement a robust data recovery plan.
- Client Risks: Ensuring end-to-end encryption and using secure communication channels. Regular security awareness training for clients on how to discern and avoid potential threats.
- System Risks: Regular system updates and patches. Implement intrusion detection systems and firewalls. Regularly scrutinize system logs for any abnormal activity.
- Infrastructure Risks: Use of secure and trusted cloud service providers. Implementing robust network security measures like VPNs and firewalls, and regularly auditing these measures for any potential vulnerabilities.

Section 3: Risk 3: Zombie Attack

Background Research: A "Zombie Attack" in the context of cybersecurity refers to

a botnet attack where a group of compromised, or 'zombie', computers are used to launch coordinated attacks on target systems. These attacks can take the form of Distributed Denial of Service (DDoS) attacks, spam campaigns, and more.

Real-life examples include the Mirai botnet that targeted IoT devices in 2016, disrupting services like Twitter, Netflix, CNN, and others. In 2013, a botnet named 'ZeroAccess' was used to commit click fraud and bitcoin mining, affecting millions of systems and causing significant financial loss.

Likelihood: Botnet attacks are fairly common in the cybersecurity landscape. As more devices get connected to the internet (especially insecure IoT devices), the potential for these attacks increases. However, the specific likelihood of such an attack depends on many factors including the target's profile, security measures in place, and the sophistication of potential attackers.

Consequences: - **Financial:** Direct loss due to downtime or service disruption, cost of mitigation, potential fines from data breach, decreased customer trust leading to loss of business.
- **Asset:** Compromised systems and data, loss of sensitive or proprietary information.
- **Client:** Potential loss of private client data, disruption of service, decreased trust in the company's ability to secure their data.
- **System:** Overloaded servers, disrupted services, potential permanent damage to software or hardware.
- **Infrastructure:** Overcrowded network, potential damage to server infrastructure, increased vulnerability to future attacks.

Mitigation Strategies: - **Financial Risks:** Invest in robust cybersecurity infrastructure and practices, obtain cyber insurance, set up a reserve fund for incident response and recovery.
- **Asset Risks:** Regularly update and patch systems, use secure configurations, monitor systems for unusual activity, implement strong access controls.
- **Client Risks:** Implement strong data protection measures, educate clients about potential risks and how to avoid them, provide clear communication in the event of a breach.
- **System Risks:** Regularly update and patch systems, monitor systems for unusual activity, implement strong access controls, invest in DDoS mitigation services.
- **Infrastructure Risks:** Regularly update and patch infrastructure, implement network segmentation to contain potential breaches, use network monitoring tools to detect unusual activity.