Qualitative and Quantitative

The most common type of attacks in cybercrime is phishing emails. Phishing emails use email spoofing to trick users/employees. The likelihood of a spoofing attack in email form is very likely and would have high impact. An employee could end up clicking a link from a trusted email and give credentials to company accounts.

Tampering is an attack in cybersecurity where the malicious actor changes data. An attacker could do this through a Man-In-the-Middle Attack, SQL injection, or cross-site scripting. The likelihood of this attack is high as malicious actors will try to change the SQL database in Real Estates Wealth Network with SQL injection. The impact of this threat is high as well, as customers need their Personal Identifiable Information or PII to be accurate. If the SQL database gets changed and customer cant use their information it could lead to reputational damage for the company, loss of customer trust, and revenue loss.

Repudiation attacks are very uncommon and not likely to happen. This attack is still impactful if executed by an attacker because you could make changes to SQL database and cybersecurity team would never know. However, the likelihood of this attack being performed is low. This attack is when an actor can deny performing malicious actions on an organization by covering their tracks. These attacks are not as common as malware or phishing attacks. The audit log in Real Estates Wealth Network can track the actions of any malicious actor along with timestamps and digital signatures (What Is Non-Repudiation in Cyber Security? | Bitsight, 2024). While there are no estimates online of the exact number of times this attack occurs, it is less likely to happen than phishing and malware attacks.

Information disclosure can happen multiple times a year depending upon how many major cybersecurity incidents happened (Gerding, 2023). The likelihood of this is low but an

organization can be attacked at any time. The impact of not complying with information disclosure can ruin your company. This would lead to customer trust being lost, reputation loss, fines for not complying, and revenue loss (PricewaterhouseCoopers, 2023). So, to reiterate, even though few information disclosure notices are needed because of how often cyber security incidents happen. Malicious actors are always planning and coming up with new ways to get customers PII. Information disclosure is low likelihood to happen but the impacts of this are high.

Denial of service attacks are very likely to happen. The impact of a denial-of-service attack is high as customers can not use the organization's services, leading to loss of revenue. The likelihood of this happening is high as well because in recent years the trend of denial-of-service attacks are getting more and more frequent (Warburton, 2024).

Elevation of privileges would have a high impact if successfully done as this could lead to insider threat to expose vulnerabilities and gain unauthorized access. A way this could happen in Real Estates Wealth Network’s database is an insider threat exposing vulnerabilities in software because it was not patched by the IT team. Another way this threat could happen is by social engineering gaining access credentials to a higher security level an insider threat does not have access to.

Insight

According to (Smith, 2024) 3.4 billion emails a day are sent from cybercriminals and are made to look from a trusted source. According to (SentinelOne, 2024) a tampering attack occurs every 39 seconds, making it average to 2,244 tampering attacks a day. There are no estimates online of the exact number of times Repudiation attacks have occurred, it is less likely to happen than phishing and malware attacks.

The likelihood of information disclosure is low as an organization can be attacked at any time, but this happens only a few times per year. Denial of service attacks are very likely to happen as thousands of these attacks happen per year and according to (Warburton, 2024) they doubled in 2022 to 2023. Elevation of privileges is likely to happen as according to (Elevation of Privilege Is Top Microsoft Vulnerability: BeyondTrust 2024 Report, 2024) this attack accounts for "40 percent of total vulnerabilities seen in 2023."

Trend in Resources

The trend in resources from gathering this kind of data is to implement zero trust architecture for Real Estate Wealth Network. Installing this architecture would help by not trusting any entity and instead focusing on verification for the user no matter the location of where this entity is located (Kumar, 2023). This architecture/model is best suited for Real Estate Wealth Network because it helps against insider threats, external breaches, and lateral movement inside the network (Kumar, 2023). This security model will help against unauthorized access to the organization which in turn can help against insider threat gaining access to PII and to the SQL database (Kumar, 2023).

Another trend in resources is to use AI and machine learning for better detection of threats and vulnerabilities (Kumar, 2023). Not only can AI and machine learning detect threats and vulnerabilities, but they can help prevent them by identifying patterns and detecting anomalies (Kumar, 2023). Using these resources for Real Estate Wealth Network can better help predict an attack for the organization. The end result of using these resources can be the difference in being prepared for an attack or being exposed to one.

Evaluate

The trends identified in the threats and vulnerabilities is that an organization needs to implement policies and procedures to each threat and vulnerability. This is so then when this attack happens the cybersecurity team can take the necessary protocols to mitigate the damage to the organization. Using AI and machine learning to give an edge to better detection and prevention for the organization. Also, implementing zero trust is a great move to help better in the event of an insider threat.

Having all users, not just customers, or employees authorize themselves to the organizations systems is better for security. In the trends of threats and vulnerabilities training to employees for phishing could help against protection of email spoofing. The threats of tampering, elevation of privileges, and repudiation could be mitigated by authorization to any entity regardless of location (zero trust architecture). The attack of denial of service could be mitigated by load balancing servers' whether that be from the cloud or physical servers the organization has. Also, machine learning or AI can help against denial-of-service attacks. Finally, implementing procedure and policies for sending information disclosures to customers when a data breach has happened.

References

Smith, G. (2024, April 10). *Top Phishing Statistics for 2023: Latest Figures and Trends*. StationX. https://www.stationx.net/phishing-statistics/

SentinelOne. (2024, September 16). *Key cyber security statistics for 2024*. SentinelOne. https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/

https://www.bitsight.com/glossary/non-repudiation-cyber-security#:~:text=Repudiation%20in%20cybersecurity%20refers%20to%20the%20denial%20by%20a%20party,making%20changes%20to%20a%20system.

What is Non-repudiation in Cyber Security? | Bitsight. (2024). Bitsight. https://www.bitsight.com/glossary/non-repudiation-cyber-security

Gerding, E. (2023, December 14). *SEC.gov | Cybersecurity Disclosure [*]*. Www.sec.gov. https://www.sec.gov/newsroom/speeches-statements/gerding-cybersecurity-disclosure-20231214

PricewaterhouseCoopers. (2023). SEC's new cyber disclosure rule. PwC. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/sec-final-cybersecurity-disclosure-rules.html

Warburton, D. (2024, July 16). 2024 DDoS Attack Trends. F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/2024-ddos-attack-trends

Elevation of privilege is top Microsoft vulnerability: BeyondTrust 2024 report. (2024). Govinsider.asia. https://govinsider.asia/intl-en/article/elevation-of-privilege-is-top-microsoft-vulnerability-beyondtrust-2024-report

Kumar, S. (2023, October 13). Top 11 Trends in Cybersecurity For 2025. CEI | Consulting. Solutions. Results. https://www.ceiamerica.com/blog/top-11-trends-in-cyber-security-for-2025/