Group 1 Assignment

Topic:

Discuss Cybersecurity Risk Faced by the Financial Sector and Risk Assessment Analysis.

Group Members

Emmanuel	Macaulay	08137615856
Adedamola	Babafemi	09050999112
Adu	Olamilekan	08181491119
Ayanbode	Olanrewaju O.	08103364487
Folanke	Abayomi S.	07033410061
Sulaiman	Basirat A	08135286479
Hadiza	Oladipupo	07068590954

Cybersecurity Risks Faced by the Financial Sector:

The financial sector is a prime target for cyberattacks due to the sensitive nature of financial information and the potential for significant financial gains. Some common cybersecurity risks faced by the financial sector include:

1. Phishing and Social Engineering: Attackers use emails, phone calls, or text messages to trick employees or customers into divulging sensitive information.
2. Ransomware and Malware: Malicious software that encrypts or destroys data, disrupting operations and demanding ransom payments.
3. Denial of Service (DoS) and Distributed Denial of Service (DDoS): Overwhelming network traffic to make online services unavailable.
4. Data Breaches: Unauthorized access to sensitive customer information, such as credit card numbers or account details.
5. Insider Threats: Malicious employees or contractors with authorized access to sensitive data.
6. Advanced Persistent Threats (APTs): Sophisticated, targeted attacks by nation-state actors or organized crime groups.
7. Mobile Banking Vulnerabilities: Security risks associated with mobile banking apps and devices.
8. Cloud Computing Risks: Data breaches or unauthorized access to cloud-stored financial information.
9. Third-Party Risks: Vulnerabilities in third-party vendors or suppliers.
10. Cryptographic Risks: Weaknesses in encryption algorithms or key management.

Risk Assessment:

Asset	Threat	Likelihood	Impact	Risk	Justification	Mitigation Strategies
Customer Data	Data Breach	High (4)	Critical (5)	(20)	Sensitive information susceptible to unauthorized access	Implement robust access controls, Encrypt sensitive data
Network Systems	Ransomware/Malware	Medium (3)	High (4)	(12)	Disruption to operations and potential data loss	Regular software updates, Advanced threat detection
Employee Accounts	Phishing/Social Engineering	High (4)	Medium (3)	(12)	Employees may divulge sensitive information	Conduct security awareness training
Financial Databases	Insider Threats	Medium (3)	Critical (5)	(15)	Authorized access could lead to data tampering	Implement insider threat detection, Limit access
Online Banking	DDoS Attacks	Medium (3)	Medium (3)	(9)	Disruption to online services	Implement DDoS protection, Scalable infrastructure
Mobile Banking Apps	Vulnerabilities	Medium (3)	Medium (3)	(9)	Unsecured apps may expose sensitive customer information	Secure coding practices, Regular security audits

Cloud Storage	Unauthorized Access	Low (2)	High (4)	(8)	Cloud storage providers may experience security breaches	Monitor cloud storage security, Encrypt data in transit
Third-Party Vendors	Data Breach	Low (2)	Medium (3)	(6)	Vendors may have inadequate security measures	Conduct vendor risk assessments, Monitor vendor security
Encryption Keys	Cryptographic Exploits	Low (2)	Critical (5)	(10)	Weak encryption algorithms or key management	Implement secure key management, Regularly update encryption

Risk Categories:

By understanding these cybersecurity risks and implementing effective mitigation strategies, financial institutions can protect their sensitive information and maintain the trust of their customers.