SAMPLE RISK ASSESSMENT

Sample Risk Assessment for Corporate Account Takeover

Threats and mitigating controls related to Corporate Account Takeovers should be addressed in the institution's information security (or GLBA) risk assessment. All reasonably foreseeable threats should be identified along with the likelihood of occurrence and potential impact for each threat.

Below is a sample risk assessment format. Other formats are acceptable as long as the required GLBA components are included. In the sample, the Inherent Risk rating for each threat is derived from the ratings for Probability of Occurrence and Potential Impact *before* controls are considered. The Residual Risk is the remaining risk *after* controls are considered. The ratings system can use either a (H)igh, (M)edium, (L)ow value or a numeric score. In either case, the ratings used for each category should be well defined. Ratings can be influenced by many factors including services offered, customer base, and transaction size and volume; and will change over time, hence annual update is needed.

This risk assessment should be modified to fit your institution's technology capabilities, specific needs, and circumstances.

				Mitigating Controls				
Potential Threats and Vulnerabilities	**Probability of Occurrence (H, M, L)**	**Potential Impact/ Severity (H, M, L)**	**Inherent Risk Rating (H, M, L)**	**Admin./Policy**	**Technical**	**Physical Security**	**Residual Risk Rating (H, M, L)**	**Comments**
Weakness of each third party service provider	M	M	M	Vendor Management policies/procedures are in place. Obtain a SSAE16 (FKA SAS 70) report from the vendor. Obtained vendor's assessment of their vulnerabilities, and mitigating services and controls they offer.	Implementation of technical controls offered by the service provider. Use of other software to mitigate weaknesses in service provider products.		L, M, or H	
Customer's lack of knowledge of the risks associated with online payment systems.	H	H	H	Provide training or training resources to customers.			L, M, or H	
Automated "pass-through" payments sent directly to the wire processor or ACH operator.	H	H	H	Customer education and training program. Customer reconciles account daily. Prior out-of-band notice of intent to deliver wire instructions or an ACH file is required.	Manual or automated anomaly detection system is in place. Use of payee "whitelisting" and/or "blacklisting."		L, M, or H	
Customer can change a wire/ACH transaction without further authentication.	M	H	H	Customer education and training program. (Or) Institution policy requires re-authentication.	IDS/IPS system in place to help thwart man-in-the-middle attacks. Customer reconciles account daily. System configuration requires re-authentication before processing a change. Manual or automated anomaly detection system is in place. Use of payee "whitelisting" and/or "blacklisting."		L, M, or H	

SAMPLE RISK ASSESSMENT

				Mitigating Controls				
Potential Threats and Vulnerabilities	**Probability of Occurrence (H, M, L)**	**Potential Impact/ Severity (H, M, L)**	**Inherent Risk Rating (H, M, L)**	**Admin./Policy**	**Technical**	**Physical Security**	**Residual Risk Rating (H, M, L)**	**Comments**
Inadequate institution staffing and risk awareness.	M	H	H	Periodic review of activity levels and trends. Staff training.	Generation of automated reports for activity level and trends.		L, M, or H	
Inadequate risk management practices	M	H	H	Involvement of management from all functional areas in the risk management process. Resources are used to stay abreast of emerging issues. Consultation with service and security providers and auditors. Periodic review and revision of the risk assessment. Policies/procedures are periodically reviewed, revised, and Board approved.			L, M, or H	
Inadequate insurance coverage	M	M	M	Electronic theft coverage has been purchased and is reviewed periodically.			L, M, or H	
Inadequate customer evaluations	M	H	H	Each commercial customer is evaluated based on type of business, financial strength, institution history, security measures in place, and type and volume of transactions. Policies with appropriate criteria for evaluating customers risk profile (beyond rating them as simply consumer or commercial risks).	Monitoring system generates reports on usage and trends,		L, M, or H	
Inadequate password policies for the institution	M	H	H	Policy requires and system enforces strict password rules. Employee training enforces importance of password security.	Passwords are not stored on the access device for the wire transfer system. System requires password changes every 90 days.		L, M, or H	
Inadequate password policies for the customer	H	H	H	Policy requires and system enforces strict password rules. Employee training enforces importance of password security.	Passwords are not stored on the access devices for online banking. System requires password changes every 90 days.		L, M, or H	

SAMPLE RISK ASSESSMENT

				Mitigating Controls				
Potential Threats and Vulnerabilities	**Probability of Occurrence (H, M, L)**	**Potential Impact/ Severity (H, M, L)**	**Inherent Risk Rating (H, M, L)**	**Admin./Policy**	**Technical**	**Physical Security**	**Residual Risk Rating (H, M, L)**	**Comments**
Lack of dual controls at the business	M	H	H	Policies and procedures outline dual control and segregation of duties requirements, and the consequences for non-compliance. Deposit accounts are reconciled daily.	System requires two individuals to authenticate and approve a transaction. The two approvals must be performed from separate dedicated and isolated devices.		L, M, or H	
Inadequate contact information if an incident occurs	M	H	H	Contact information (including after hours) is incorporated in contracts and training materials.	A secure database for customer contact information is maintained to prevent unauthorized changes.		L, M, or H	
Phishing attempts and phone calls	H	M	M	The FDIC, IRS, NACHA, and many other entities do not contact business customers to request software installation or provide access credentials. Institution and customer staff training. Institution staff will not request account holders to click on links, install software, or require changes to established procedures without securely communicated notification.	Spam email filters are in place.		L, M, or H	
Unauthorized changes using the Admin account (users, password resets, device registration, time of day restrictions, etc.)	H	H	H	Institution must approve addition of new Admin. Institution will suspend the Admin account if the customer fails to adhere to minimum standards. Out-of-bank verification is performed prior to changes taking effect.	Changes require additional authentication and out-of-band verification before changes are implemented. The account holder is automatically sent a notice immediately after the changes are made.		L, M, or H	

SAMPLE RISK ASSESSMENT

				Mitigating Controls				
Potential Threats and Vulnerabilities	**Probability of Occurrence (H, M, L)**	**Potential Impact/ Severity (H, M, L)**	**Inherent Risk Rating (H, M, L)**	**Admin./Policy**	**Technical**	**Physical Security**	**Residual Risk Rating (H, M, L)**	**Comments**
Fraudulent transaction has been initiated.	H	H	H	Dual controls implemented. Daily reconcilement. Out-of-band verification required. Institution policies and procedures for dealing with customers with compromised equipment. Staff will identify potential “suspicious activity” and flag the transactions for further review. High risk customers may utilize a restricted funds transfer recipient list.	Fraud detection and monitoring systems are in place. Manual or automated anomaly detection system is in place. Dual authorization required from separate isolated devices. Software or other techniques are used to restrict transactions to approved limits. Transactions are approved only from authorized IP addresses, or IP addresses associated with fraud are blocked. Complex device identification: One-time cookies are used that detect the PC’s configuration, IP address, geo-location, and other factors. Enhanced challenge questions. Pattern recognition software to detect unusual activity. Transaction aggregation and monitoring system. Transaction limits within the system are appropriate that reduce the risk. Use of payee "whitelisting" and/or		L, M, or H	
Unauthorized physical access to customer’s computer system	M	H	H	The customer’s Acceptable Use Policy is reviewed and signed annually. Information security and social engineering training are performed.	The customer’s access logs are periodically reviewed. Administrative rights are restricted. Manual or automated anomaly detection system is in place.	Computer is in a secured area with restricted access. USB ports and optical drives are disabled. Security cameras are installed.	L, M, or H	

SAMPLE RISK ASSESSMENT

				Mitigating Controls				
Potential Threats and Vulnerabilities	**Probability of Occurrence (H, M, L)**	**Potential Impact/ Severity (H, M, L)**	**Inherent Risk Rating (H, M, L)**	**Admin./Policy**	**Technical**	**Physical Security**	**Residual Risk Rating (H, M, L)**	**Comments**
Unauthorized external access to the customer's computer system	H	H	H	Customer has Firewall, Patch Management, Anti-Virus, and Acceptable Use Policies. Staff trained on Phishing and Social Engineering techniques.	Using dedicated/isolated workstations. Hardware and software firewalls are in place. Commercial anti-virus and malware products are installed and automatically updated. OS and peripheral software is regularly patched. An intrusion detection/prevention system is in place. Multi-layered and multi-factor authentication controls are in place. Manual or automated anomaly detection system is in place. Use of payee "whitelisting" and/or "blacklisting."	Modems are disabled.	L, M, or H	
Fraudulent transfer of customer funds via the online wire/ACH system.	M	H	H	Institution policies and procedures are in place.	The customer's dual control procedure requires two individuals to authenticate a transaction. Multi-factor authentication and multi-layered controls are in place. Strong password requirements are in place. Call-backs or out-of-band verifications are required on all or certain transactions. Transmission of wire or ACH instructions must come from two separate isolated devices. Manual or automated anomaly detection system is in place. Transaction limits within the system are appropriate that reduce the risk. Use of payee "whitelisting" and/or "blacklisting."		L, M, or H	

SAMPLE RISK ASSESSMENT

				Mitigating Controls				
Potential Threats and Vulnerabilities	**Probability of Occurrence (H, M, L)**	**Potential Impact/ Severity (H, M, L)**	**Inherent Risk Rating (H, M, L)**	**Admin./Policy**	**Technical**	**Physical Security**	**Residual Risk Rating (H, M, L)**	**Comments**
Smart phone applications lack security controls	L	M	M	Consumer awareness and education initiatives. Users are encouraged to password protect their phones and have the capability of wiping stored data remotely.	Applications are rigorously tested prior to implementation. Strong passwords are required for access to the Internet Banking platform. Data is encrypted during transmission. An email confirmation is sent to the account's old and new email addresses when the address is changed.		L, M, or H	
Consumers are subject to identity theft when using the Internet Banking / Bill Pay platform.	M	H	H	Users are encouraged to never reveal their login credentials to anyone. Know Your Customer policies help ascertain the true identity of customers. Employees are trained to recognize pretext calls from persons requesting confidential information. A "Welcome" letter is mailed to the address provided to help ensure the authenticity of the new user. Reports monitored: Rejected transactions; Large transactions; Bill pay transactions; Debit card activity; Employee account changes. Institution website has links to Identity Theft resources.	Security questions are "out-of-wallet" questions. The institution truncates account numbers and customer data to hinder internal employee fraud. Manual or automated monitoring can help detect suspicious activity. Real time validation is conducted for accounts opened online. User is locked-out upon three failed login attempts. Password changes are required periodically. An email confirmation is sent to the account's old and new email addresses when the address is changed.		L, M, or H	

SAMPLE RISK ASSESSMENT

				Mitigating Controls				
Potential Threats and Vulnerabilities	**Probability of Occurrence (H, M, L)**	**Potential Impact/ Severity (H, M, L)**	**Inherent Risk Rating (H, M, L)**	**Admin./Policy**	**Technical**	**Physical Security**	**Residual Risk Rating (H, M, L)**	**Comments**
Customer access controls do not match the level of risk for each customer.	M	H	H	The institution has an ongoing customer education and awareness program. Customers are urged or required to install anti-malware software to reduce the risk of key loggers, adware, and spyware. Out-of-band authentication is used when anomalies or suspicious activity is detected.	Controls commensurate with the level of risk include: Initial login and authentication of customers requesting access to the Internet banking system. Additional authentication prior to the transfer of funds to other parties. Use of manual or automated transaction monitoring and/or anomaly detection. Complex device identification: One-time cookies are used that detect the PC's configuration, IP address, geo-location, and other factors. Out-of-wallet challenge questions are used. One-time password tokens are used for high risk customers. Vendor supplied USB devices enable a secure link between the user's PC and the institution.		L, M, or H	
Institution has Inadequate Response Plan or no response plan.	M	H	H	Institution has a appropriate Incident Response Program that addresses corporate account takeover. Designated response coordinator / team is immediately notified.			L, M, or H	
Customer has Inadequate Response Plan or no response plan.	H	H	H	Customer has a appropriate Incident Response Program that addresses corporate account takeover. Customer immediately notifies the institution.			L, M, or H	

SAMPLE RISK ASSESSMENT

				Mitigating Controls				
Potential Threats and Vulnerabilities	Probability of Occurrence (H, M, L)	Potential Impact/ Severity (H, M, L)	Inherent Risk Rating (H, M, L)	Admin./Policy	Technical	Physical Security	Residual Risk Rating (H, M, L)	Comments