Awareness, Risk Management and Response to Cybersecurity Threats and Vulnerabilities

DIGITAL INSIGHT™
an NCR company

The Federal Financial Institutions Examination Council (FFIEC) has released new cybersecurity guidance to address specific types of cyberattacks and threats. Future IT examinations of financial institutions will include a review of specific cybersecurity initiatives to ensure they are adequately addressing risks and investing in risk-mitigation technologies to safeguard and protect sensitive customer information.

The new FFIEC cybersecurity guidance will focus on the following five domains:

1. Risk Management & and Oversight of Digital Insight Products and Services
2. Threat Intelligence and Information Sharing
3. Cybersecurity Controls
4. External Dependency Management
5. Incident Response Program

This document presents best practices and controls implemented at Digital Insight to combat the inherent risks related to doing business in the information age, which will help financial institutions be aware and better understand how Digital Insight will address the FFIEC's concerns. For information related to risks associated with Mobile Banking, please refer to Digital Insight's Mobile Security FAQ document, located on Admin Platform or through your relationship manager.

Risk Management and Overview of Digital Insight Products and Services

Cybersecurity is a priority for Digital Insight and is routinely discussed in management meetings among our senior leaders, who already have a strong background in security. Expectations are clearly communicated to the entire organization and objectives are set for each team.

In addition to NCR's central security team, Digital Insight has a dedicated security team that is responsible for areas such as application security, fraud prevention, compliance and infrastructure. This team reports to Digital Insight's VP of Engineering and Security and has a dotted line to NCR's Chief Information Security Officer.

Digital Insight uses a modified version of the Microsoft Secure Development Lifecycle (SDL) methodology, which includes a signoff process where all artifacts created during the regular development of products are presented. There are no major surprises expected in this step, as the security team is involved in all phases of the SDL. Steps performed during the SDL include architectural review, data classification, data handling, code reviews, mandatory use of static code analysis in all supported platforms, review of third-party libraries, dynamic analysis and penetration tests.

Infrastructure is regularly scanned for malware, vulnerabilities and misconfigurations. The security teams at Digital Insight and NCR are responsible for the execution of an annual risk assessment to help ensure that relevant threats are identified and effectively addressed. Specifically, threats and associated vulnerabilities that might impact Digital Insight and NCR assets are identified. The potential impact of each vulnerability is assessed along with the likelihood of a related failure occurring. All risks identified are prioritized and reported in a fashion that allows management to implement an appropriate level of training, controls, and the assurances necessary for effective mitigation. Access management is regularly performed on all Digital Insight systems

Security Awareness training is mandatory at Digital Insight and NCR. Employees are our first line of defense for many types of attacks, particularly social engineering, which is discussed at length during training. A dedicated email address monitored by Digital Insight's security team is available for all employees who suspect phishing and social engineering schemes. Digital Insight's dedicated security team gives talks for internal groups and often extends invitations to outside speakers. The team authors white papers and maintains a repository of all presentations. Given the rapidly changing nature of the threat landscape, Digital Insight's security team allocates a significant part of its budget for specialized staff training, focusing on the different threats that each of our product offerings face.

Digital Insight contracts with a third party to perform periodic security reviews and vulnerability assessments. Results are communicated to parties responsible for remediating exceptions identified during the assessments. Remediation is reviewed with and tracked by Digital Insight's security team and the appropriate management teams. Internal monitoring is performed by management and supervisory personnel who monitor performance, quality and controls as a normal part of their activities. Risk-monitoring activities include reviews of operating performance, quality control reviews, and various reports that measure the results of the processes involved in providing services to Digital Insight clients. These reports are reviewed periodically, depending upon the nature of the item being reported, by appropriate levels of management and required actions are taken as necessary

Findings and recommendations made during audits, exams, and reviews are prioritized to help ensure an appropriate level of response. Progress reports that identify current status and delays are provided to Digital Insight's Senior Leadership Team (SLT) to help ensure appropriate levels of awareness and oversight.

Access controls

Financial institutions have numerous access points and use a variety of connection types. Digital Insight has structured its network architecture in such a fashion that financial institution computing resources that store sensitive account information are not Internet facing. Online Banking Web servers handle the requests made through the Internet. End-user information is either housed on the client's host system (for real-time clients), which is connected to Digital Insight using a private Multi-Protocol Label Switching (MPLS) connection, or in secure Digital Insight databases (for batch clients), which are updated with data sent to Digital Insight by the client or Data Processing Vendor (DPV).

The use of a Virtual Private Network (VPN) is mandatory to access the Digital Insight network along with strong credentials and soft token for two-factor authentication. On-site access to employee areas requires a physical access badge and authentication credentials (username/password). Biometric authentication is mandatory to access all Digital Insight data centers.

Network devices (e.g., firewalls) are configured to leverage Terminal Access Controller Access-Control System (TACACS+), a remote authentication protocol, which allows a remote access server to communicate with an authentication server in order to validate access to the network. Only once authenticated via TACACS+, administrative access to the network devices occur.

Network access information is centrally logged and securely submitted to NCR for monitoring and analysis. Management regularly review employee access rights to all Digital Insight systems. Only Digital Insight-owned devices with digital certificates are permitted on the intranet. Bring your own device (BYOD) is only allowed at Digital Insight's guest network.

Firewalls and routers are strategically placed to control and filter traffic between firewalled segments of the network by verifying the source, and destination of network packets. Additionally, fully configured backup firewalls are available for use in the event of a failure of a primary firewall. Firewalls and load balancers provide perimeter security, segment the production network from other areas of the corporate network, and are configured to only allow network traffic between specifically authorized sources and destinations using specifically authorized ports. Web servers are protected from the Internet via firewall and/or routers and are configured to only permit what is required of the business function. All other traffic is dropped and logged.

Wireless networks are only available in employee areas but not in the data centers. Digital Insight uses Wi-Fi Protected Access 2 - Pre-Shared Key (WPA2-PSK). Detection of rogue wireless networks is enabled in all wireless access points in all Digital Insight locations.

Threat Intelligence and Information Sharing

Many financial institutions rely on media reports and third-party service providers to gather information on cyber events and vulnerabilities. Digital Insight's security team is composed of seasoned, industry-acclaimed security experts who delivered significant contributions to the industry by setting best practices, conducting certifications, developing white papers, speaking at conferences and influencing the curriculum of some of America's top universities. Members of Digital Insight's security team contributed to initiatives in communities such as: PCI, Cloud Security Alliance (CSA), Open Web Application Security Project (OWASP) and Information Systems Security Association (ISSA). Because the team is well connected with the security communities worldwide, Digital Insight sometimes hears about zero day attacks before they are published in the specialized media. Digital Insight is also a contributing member of Financial Services Information Sharing and Analysis Center (FS-ISAC) and partners closely with organizations such as IBM, Intel Security, Guardian Analytics, RSA and the FBI to keep abreast of new threats. Lastly, the security team works closely with Digital Insight's communication team to ensure financial institution clients are kept informed.

The team monitors and maintains sufficient awareness of cybersecurity threats and vulnerability information so that risk is evaluated and action is taken accordingly. Digital Insight is also engaged in sharing information with other financial institutions as well as applying proactive blocking controls to defend its clients based on abuse patterns observed in other clients. Points of contact with law enforcement bureaus and regulators have been established as well as a process to respond efficiently.

Digital Insight offerings keep securely centralized logs of all system transactions which is also replicated to NCR facilities to ensure integrity. Logs are analyzed for fraud, intrusion and abuse patterns by internal experts and external partners.

Cybersecurity Controls

Digital Insight systems are secured with multiple layers of firewalls, screening and filtering routers, intrusion detection/prevention systems, strict authentication, and malware defenses. A defensive in-depth strategy is employed using a mix of preventive, detective and corrective controls.

Our network architecture is structured so the data servers are not connected to the Internet and there are two fully redundant data centers. We scale horizontally for host servers, application servers, and database servers. All of our applications and subsystems are designed for high availability with redundancy designed in every layer (e.g., Power, Network, Cooling etc.). Network usage is projected to utilize less than half of the available bandwidth, saving the surplus for unplanned peaks.

Stateless Intelligent DDoS Mitigations Systems (IDMS) are configured to provide staff early alerts about attempted DDoS attacks and blocks malicious network packages. Digital Insight contracts for cloud-based monitoring and mitigation services to combat complex volumetric Distributed Denial of Service (DDoS) services from a major ISP.

Network-based intrusion detection systems are in place to detect and/or prevent unauthorized access attempts. These systems identify and alert attempted malicious access or potential abuse of computer systems by internal or external attackers. When suspicious activity is recognized, an alert is sent for review by security personnel and validated alerts initiate the incident response process.

As a defensive measure, our vulnerability management system scans all assets in our data centers monthly – analyzing vulnerabilities, controls, and configurations. The scan happens from inside our network and the scan agents have full login credentials of all servers. This provides a complete picture of all internally and externally facing vulnerabilities and minimizes the number of false positives. Results are prioritized and presented to management. Once devices are patched, another scan is triggered to validate the resolutions.

Non-Unix servers that have a long history of malware attacks are secured with layered protection and intelligent security at the endpoint that goes beyond traditional definition-based antivirus. Capabilities include hardware-enhanced security against stealthy attacks, behavioral anti-malware and dynamic whitelisting.

Environmental Safeguards

All Digital Insight-managed data centers are situated on raised flooring and are supported by an appropriate number of uninterruptable power supplies (UPS) and redundant diesel generators configured to sustain computer operations and air conditioning systems in the event of a commercial power loss. Separate UPS systems are provided to protect the production data centers in the event of an interruption to power. The diesel generators, which are located in a secured area, provide the capability to assume power within 10 to 30 seconds of commercial power loss. During this start-up time, the UPS devices keep systems running until the generator(s) are online to take the full load.

All of the data centers have environmental safeguards in place to prevent damage to critical systems. At the Westlake Village data center, the entire building is protected by a sprinkler system that is tested annually. In addition, there is a FM-200 fire suppression system backed-up with a double interlock pre-action system.

In the event of a fire detection alarm on the floor, an audible alarm is triggered in each respective data center. In addition, the Fire Department is automatically notified. Hand-held fire extinguishers are on the floor, available for operations personnel in the event of small emergencies.

Computer room air conditioners (CRACs) are the environmental systems that provide computer room air conditioning to the data centers. The systems monitor and control both temperature and humidity above the data center's floor. If there are any problems, the system will immediately alert the maintenance staff at each respective site for immediate action.

To help ensure equipment remains in working order, periodic inspections and preventative maintenance are performed. Established internal controls are in place to schedule and monitor preventive maintenance procedures to help ensure they balance recommended timeframes given against business activity to minimize overall impact.

Online Banking Controls

Security configurations (e.g., password parameters, failed login attempts, and account lockout) are implemented on production web, application, and database servers. Passwords used to access Digital Insight servers and network devices are subject to password composition requirements established including: minimum length, complexity, history, account lockout, and periodic change intervals. Access to perform system administrative functions on Digital Insight production systems and network devices require multi-level authentication. Individuals must be authenticated to the Digital Insight network in order to access systems

Multifactor Authentication (MFA) is federally recommended for financial institutions to increase security for online access and transaction capabilities for banking accounts. In order to be authenticated, end users must successfully validate their user ID with their password and present a One-Time Passcode (OTP) sent to the user's phone or smart device to respond to the challenge.

Access to the Online Banking application is suspended after a financial institution-defined number of consecutive invalid access attempts. Account access can be reset by the financial institution or by the end user. The financial institution should reset the end user's access only after receiving a request from the end user and verifying the end user's identity. The forgotten password feature allows an end user to reset their password without the interaction of a financial institution administrator. The end user must have previously established alternate validation information in order to utilize this feature from a link on the login screen. The end user will be asked to provide their member or user ID and a phone number registered for MFA purposes. Once identified, the system will generate a random password and send it to the end user either via an email, voice call or an SMS text message to the number entered. This password can then be used to access the Online Banking application.

The financial institution administrator can list and disable accounts that are considered inactive or whose accounts have been closed. Disabled accounts are not granted access to the Online Banking application

Financial institutions have the ability to set the time-out interval of an Online Banking session to be anywhere from ten to twenty minutes1, and end users do not have the ability to adjust the time-out interval. If the end user exceeds the time-out interval, the end user must re-authenticate by entering the user ID and password before accessing confidential information.

All Web transactions utilize the Transport Layer Security (TLS) protocol. The TLS protocol helps ensure integrity and confidentiality for the data flowing between the end user's browser and Digital Insight's server, ensuring that the data cannot be altered in route. Digital Insight uses an extended validation (EV) Certificate in all financial institution's domains. To prevent phishing and spoofing, receiving an EV Certificate requires an organization to go through extensive investigation and validation to prove identity. Once the EV Certificate is successfully installed on the Online Banking domain, a green navigation bar with a padlock icon and an organization name is shown.

When processing requests from the end user, the URL displays no information that allows replay attacks, thus protecting accounts and transactions from unauthorized access. Lastly, all data in the browser cache is cleared upon end-user logout to help ensure privacy.

1 Mobile is not configurable by financial institutions or end users and is set for 30 minutes

Security Solutions

Digital Insight offers a set of add-on security solutions for financial institutions to protect the digital channel. Through key partnerships with Guardian Analytics, IBM (Trusteer), RSA, and Symantec, financial institutions have access to products and services for protection, monitoring and remediation – focal points to forming an effective IT security strategy.

Guardian Analytics offers a behavior-based, fraud-detection service. The system automatically analyzes Online Banking user activity and flags suspicious financial activities using advanced heuristics based on user behavior and profile. The service can also be extended to analyze Mobile Banking user activity and monitor small business payments (ACH and Wire transfers). Security analysts are available to assist the financial institution and assess the security alerts flagged by the system.

IBM Trusteer Rapport is a downloadable anti-malware solution that users install prior to accessing Online Banking. The tool prevents keystroke logging and Man-in-the-Browser (MitB) by disabling browser helper objects. IBM Trusteer Pinpoint malware detection is a server-side solution that accurately detects malware-infected devices and determines both the nature of the threat and the risk it represents to the financial institution. Financial institutions are informed about infected users logging into Online Banking so they can manually intervene.

RSA FraudAction is a global, 24x7x365, end-to-end, anti-phishing, anti-pharming and anti-email fraud service. The service proactively detects and shuts down fraudulent phishing sites by monitoring domain name registration, abuse mailbox and Web server access logs. Financial institutions receive secure, real-time reports and phishing alerts. FraudAction includes technical counter measures to dilute the effectiveness of fraudulent attacks.

Symantec provides Extended Validation (EV) Certificates (SHA2) to Digital Insight's financial institution domains. While EV Certificates utilize the same levels of security as conventional certificates, the solution requires more extensive verification of the certificate requestor by the Certificate Authority (CA) issuing the certificate. For this reason, EV Certificates are considered more secure than regular certificates. Websites using EV Certificates have a unique visual indication in a browser's URL bar, such as a green address bar with a padlock, to help users identify the increased security verification measures.

External Dependency Management

Digital Insight uses various subservice organizations for monitoring infrastructure, physical and environmental services, bill payment services, online funds transfer, person-to-person payment solutions, remote deposit check capture and tier one client support. A formal vendor management program is in place for ongoing monitoring of service levels and standard vendor contract requirements.

Quarterly reviews are conducted of critical vendors, such as Bill Pay providers, to review whether vendors are meeting service level agreements (SLAs). All other vendors providing less-critical services are reviewed at least annually. Digital Insight facilitates the distribution of key partner vendor's service organization control reports, but does not otherwise distribute vendor information to clients.

Incident Response Program

Digital Insight has documented corporate policies and procedures that provide guidelines for effective incident response, and help ensure that incidents are escalated to the proper levels of authority. The policies and procedures include guidance on the types of intrusions and security breaches that will be escalated to senior management. Digital Insight Customer Care internal procedures provide additional detail on how an intrusion incident will be communicated to client financial institutions.

If an employee becomes aware of a security incident, that employee is responsible for initiating an appropriate escalation procedure according to the nature of the incident. Those areas within Digital Insight that participate in incident response are required to create and maintain supporting procedures. Internal procedures describe response activities related to events including network-based attacks and intrusion, virus and other malicious software, theft or destruction of company property, abuse or disregard of corporate information security policy and fraud.

For additional information on Digital Insight's disaster recovery program, please see "Digital Insight's Disaster Recovery Executive Summary" document located on Admin Platform or through your relationship manager.

Summary

Digital Insight enables a financial institution to meet its business objectives by implementing systems with due consideration of information technology (IT)-related risks to the organization, business and trading partners, technology service providers and customers.

Financial institutions are critically dependent on information technology to conduct business operations. Digital Insight monitors and maintains awareness of threats and vulnerabilities. Connections to third parties are managed and comprehensive response plans that incorporate cyber incident scenarios are in place and are regularly tested. A best-of-breed, in-depth security approach that is integrated with the entire systems development lifecycle is followed when developing and maintaining all product and services. Lastly, specialized security partners, threat intelligence services, state of the art data centers and strong ties with the security community back Digital Insight's security initiatives.

Banks and credit unions turn to Digital Insight for innovative online and mobile banking technologies that drive growth. For nearly 20 years, our leading solutions have helped financial institutions engage consumers more meaningfully and more profitably.

digitalinsight.com | 888-344-4674

DIGITAL INSIGHT™
an NCR company