



usbank.com

U.S. Bancorp Cybersecurity Overview

Updated January 2019

Contents

Information Protection Services Vision: Strength in Security.....4

Information Protection Services Program4

IDENTIFY5

PROTECT6

DETECT7

RESPOND.....8

RECOVER.....9

Management's Assertion Regarding the Effectiveness of U.S. Bancorp Information Protection Program

As the management of U.S. Bancorp's Information Protection Program, we are responsible for designing, implementing, and maintaining an effective information protection program. As the Chief Information Security Officer (CISO), I have overall management authority and operational responsibility for the U.S. Bancorp Information Protection Program and for the full design, implementation, sustainability, and resiliency of the information security policies, processes, and controls. These policies and processes support the Business Lines in achieving security, confidentiality, integrity, and availability while meeting regulatory and compliance requirements.

U.S. Bancorp Information Protection Management asserts its Information Protection Program has sustainable processes that align with the Cybersecurity NIST framework that attest to the effectiveness of security, availability, and confidentiality policies, processes and controls with reasonable assurance, but not absolute, that controls are implemented to detect, remediate and prevent security events and safeguard customers information in compliance with policies.

Additionally, an independent assessment and opinion can be found in the U.S. Bancorp SOC reports. U.S. Bancorp SOC 2 reports are available upon request from a client that has signed a Non-disclosure agreement with U.S. Bancorp. SOC 3 reports are available upon requests from a client that does not have a signed Non-disclosure agreement.

Sincerely,

A handwritten signature in black ink, appearing to read "Tim J. Heid", written in a cursive style.

Timothy J Heid
Chief Information Security Officer
U.S. Bancorp

Information Protection Services Vision: Strength in Security

The relationship between U.S. Bancorp, its subsidiaries and affiliates (collectively, the Company), and our customers is built on trust. Our customers trust us with their confidential information and assets and expect that we will maintain strength in security in a constantly changing world of sophisticated threats and technology choice. Strong corporate governance, systematic controls, and enterprise processes are designed to protect the Company from loss of customer and company information, data destruction, and system down time, as well as ensure we have a resilient and secure computer environment. The Company is committed to promoting strength in security by protecting the confidentiality, integrity, availability, and privacy of customer information. Our reputation rests upon securely maintaining customer information, and we understand the importance of safeguarding all information within the Company's custody.

Information Protection Services Program

U.S. Bancorp Information Protection Services (IPS) manages access to customer and business assets, ensuring the security of customer and enterprise information, within the Company, as well as for our customers and partners.

The Company's Information Protection Program (the Program) aligns with the National Institute of Standards and Technology (NIST) Cybersecurity Framework, a set of industry standards and best practices to help organizations manage cybersecurity risks. The Program is structured to support compliance with applicable laws, regulations, and contractual requirements, which includes, but is not limited to: Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), Payment Card Industry (PCI) Security Standards, and relevant international data protection standards, such as the General Protection Data Regulation (GDPR). Aligning the Company's cybersecurity practices with the NIST Cybersecurity Framework enhances our ability to sustain compliance with legal requirements and improves our capabilities to prevent, detect, and respond to cybersecurity incidents and events.

The NIST Cybersecurity Framework consists of five main functions: **Identify**, **Protect**, **Detect**, **Respond**, and **Recover**. These functions organize cybersecurity activities at their highest level. The alignment of these functions at the strategic planning level enables IPS to understand existing and emerging risks to the organization, enhance governance and risk management practices, and implement control measures to protect the confidentiality, integrity, and availability of critical business services delivery. Given the ever-changing landscape of cybersecurity threats to financial institutions, the Program continuously monitors for events that can impact the security of our information systems, applies risk mitigating solutions, and utilizes documented procedures for responding to verified incidents. Lessons learned from response activities and post-incident reviews help strengthen the Program.

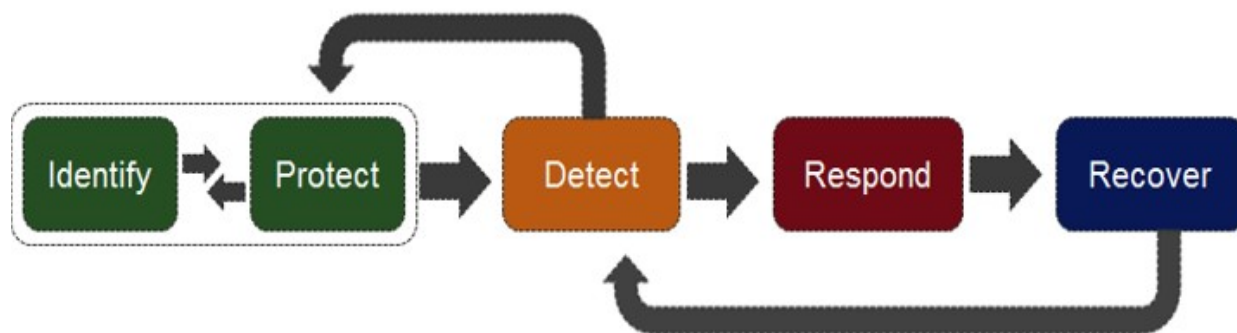


Figure 1: NIST Cybersecurity Framework Flow Diagram¹

¹ Figure 1: NIST Cybersecurity Framework Flow Diagram is custom designed to conceptually illustrate a life cycle of activities using the five main functions for the purpose of informing the intended audience of this document.

IDENTIFY

This function involves managing organizational assets, understanding the business environment, and establishing a governance structure that includes policies, procedures, and process controls. Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy are the main program areas that execute this function in alignment with the NIST Cybersecurity Framework.

Asset Management

The Company's asset management program includes examining policies and practices regarding physical devices and organization systems, communicating policies and practices throughout the company, mapping data flows, prioritizing resources based on classification, criticality and business value, and establishing roles and responsibilities for the workforce and applicable third parties.

Business Environment

The Company's business environment is guided by a program strategy that is communicated to all stakeholders, leadership, and oversight groups. The Company is involved in a wide array of associations and working groups throughout different business lines. Participation in sector trade associations is crucial given Company's place in critical infrastructure and as a leader in the financial sector. The Program is involved in the following security working groups:

- Securities Industry and Financial Markets Association (SIFMA)
- Financial Services Information Security Analysis Center (FS-ISAC)
- Financial Services Sector Coordinating Council (FSSCC)
- American Bankers Association (ABA)
- The Bank Policy Institute
- U.S. Chamber of Commerce
- Financial Services Roundtable
- National Defense ISAC (ND-ISAC)
- The Better Identity Coalition
- Treasury's Cyber Intelligence Group

This enables the Program to stay informed of the latest threat, mitigation trends and information, as well as shape a joint cybersecurity work plan for the financial services industry in partnership with federal agencies and regulators.

FSSCC engagement includes participation in DHS CIPAC meetings, the tri-annual FSSCC-Financial and Banking Information Infrastructure Committee (FBIIC) joint meetings, co-chairing the sector Exercise Program, coordinating across the private sector and with government to improve responses to and monitoring of cybersecurity threats. The Company is a Platinum member of the FS-ISAC where we coordinate tactically on threat intelligence and participate in sharing threat vectors that have the potential to affect the sector.

Governance

The Company works vigilantly to manage and monitor its regulatory, legal, risk, environmental, and operational requirements. Documented policies and procedures are communicated throughout the company and inform management of cybersecurity risk. U.S. Bancorp Information Protection Program aligns with industry-accepted information security guidelines and requirements; where applicable, as provided by the NIST Cybersecurity Framework, the International Organization for Standardization (ISO), General Data Protection Regulation (GDPR), Federal Information Security Management Act (FISMA) and other applicable standards. Information security policies are mapped to applicable legal, regulatory and contractual requirements including, but not limited to: GLBA, PCI, HIPAA, SOX, and the NIST Cybersecurity Framework.

Risk Assessment

The Company conducts a variety of risk assessments to identify new and emerging threats, evaluate Program performance, and set tactical and strategic goals. Through the FSSCC, the Company works with the U.S. Department of Treasury to identify and assess risk and policy issues related to the financial critical infrastructure sector. The Company participates on the FSSCC Sector Exercise Committee, a program designed to jointly

develop and test government and industry processes and capabilities for addressing the full lifecycle of cybersecurity risk management, including identification, protection, detection, response, and recovery mechanisms and the roles and responsibilities involved in responding to cyber incidents. Some examples of internal and external assessment activities include, but are not limited to:

- Self-assessments
- Risk analysis
- Control environment enhancements
- Threat and vulnerability assessments
- Vendor assessments
- Independent audits
- Sector exercises

Risk Management Strategy

The Company's risk management strategy encompasses the organization's priorities, constraints, risk appetite, and assumptions that have been established and used to support its operational risk decisions.

PROTECT

Management of security solutions at the Company is enabled through application of preventive methods and protective technical controls that must comply with policies to ensure the security and resilience of systems and assets. This function provides the foundation for developing and implementing appropriate safeguards to ensure delivery of critical infrastructure services. The main components of this function include: Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology.

Access Control

The Company's Identity and Access Management (IAM) team works to protect customer and Company information by implementing processes, tools, and methods to authenticate users and manage access to data and devices. IAM ensures risks and threats are mitigated or eliminated through strong oversight of access controls. IAM enforces the "least privilege" principle, which requires minimal user profile access privileges based on job requirements.

Awareness and Training

The Company's Security Awareness For Everyone (SAFE) program provides security awareness education to employees and contingent workers. The objective of SAFE is to educate all staff on protecting Company's information, systems, and processes in order to minimize the risk of unauthorized disclosure, alteration, or destruction of Company information and complying with applicable laws and regulations. All Company employees receives monthly phishing exercises that mimic legitimate phishing attacks. These exercises provide immersive training that enforces SAFE education tenets, as well as creating opportunities to demonstrate and reward appropriate staff behaviors, such as reporting phishing attacks to the correct personnel. All new hires, including employees and contractors, are assigned security awareness training which requires completion within 30 days of assignment, and required annually thereafter.

Data Security

The Company's Data Loss Prevention (DLP) program is based on industry best practices and standards to reduce operational and reputational risks. Its mission is to protect against data loss throughout the data lifecycle, from creation to destruction, across three major data categories: Data-at-Rest, Data-in-Motion, and Data-in-Use. The Company safeguards confidential data by implementing control measures to properly dispose of data in electronic and physical formats.

Information Protection Processes and Procedures

The Company publishes and maintains enterprise-wide information security policies establishing requirements to protect information assets. The Company performs vulnerability scans (external and internal), incident, and threat monitoring using applicable security advisories and security baseline management of systems platforms.

Maintenance

The Company's Enterprise Information Technology Service Management Policy establishes enterprise requirements for managing, collecting, and reporting information technology service management information to relevant parties. This policy establishes requirements for elements of information technology service management, including change management, incident management, problem management, configuration management, and service level management.

Protective Technology

The Company provides solutions and services that encompass efficient and effective business processes, security monitoring, detection, prevention, incident response, and centralized reporting and trending. These solutions and services manage risk to support secure and sustainable information technology services to meet the needs of our internal and external customers.

DETECT

Timely detection ensures that the Company is well positioned to limit or contain the impact of potential cybersecurity events. This function includes several layers of detection processes that enable the discovery of cybersecurity events.

Detection Process

The Company utilizes many processes to ensure timely and adequate detection and awareness of anomalous events. Proactive and ongoing detection processes are essential in identifying potential threats and attacks to the organization. These detection processes include, but are not limited to: Continuous Security Monitoring, Cybersecurity Threat Intelligence, Vulnerability Assessment and Management, Penetration Testing, and Automation and Orchestration.

Each information security incident is assessed for its severity and potential impact to the Company. An appropriate course of action is determined by the Computer Security Incident Response Team (CSIRT) during the detection phase.

Anomalies and Events

Detecting anomalies and events requires an advanced incident analysis capability. Cybersecurity events have the ability to disrupt business or result in the loss of customer and Bank information. The Computer Security Incident Response Run Book (the Run Book) maintains consistency in U.S Bancorp's protocol for addressing each information security event. CSIRT utilizes the framework described in the Run Book, which provides an enterprise-level management strategy for the organization and addresses incidents preemptively, proactively, and when necessary, reactively.

Continuous Security Monitoring

Security Incident and Event Management (SIEM) is at the core of the detection phase when remediating cybersecurity threats. The process begins with establishing methodologies and processes to investigate condition based alerts to determine whether a genuine incident or event exists that will require timely risk mitigation steps. A condition establishes a system level baseline threshold for alerting resources to respond to an incident. An alert can be triggered by various sources.

The Company continuously monitors its information systems to proactively detect cybersecurity events. CSIRT monitors day-to-day preventive systems, external notification sources, and performs key containment and investigative functions during incident detection activities. Key roles and leadership are also filled by other members of IPS, Network Security and technical Subject Matter Experts within system administration groups, depending on the needs of specific incidents. Continuous monitoring is supported by other IPS activities, which are detailed in the Run Book.

Cybersecurity Threat Intelligence

The Program collects, analyzes, and publishes timely, objective, and relevant cyber intelligence products on nation-state, hacktivist, cybercriminal, and other cyber threats to Company leadership, lines of business, and operational staff. Continuous monitoring and identification of this broad set of potential cyber threats to the

Company allows management to quickly and accurately assess exposure to risk and respond accordingly.

Orchestration and Automation

The Company is implementing orchestration software to automate processes and tasks. Orchestration allows for the development of workflows to highlight various components. Individual tasks are created as building blocks to be used in the workflows. Some examples of automation tasks include, but are not limited to:

- Threat intelligence ingestion from FS-ISAC and other sources.
- Callouts to various threat platforms for risk scoring/analysis.
- Enrichment of threat intelligence.
- Integration with internal systems to identify threats.
- Summary to threat personnel for actionable intelligence.

The utilization of orchestration and automation increases the volume of cyber threat intelligence that can be examined, vetted, and processed if found actionable.

RESPOND

The Company utilizes a response framework, which provides an enterprise level management strategy for addressing risks resulting from cybersecurity incidents. Respond functions include Response Planning, Reporting, Analysis, Mitigation, and Improvements. Formal responsibility for incident management and response shifts when threats evolve to actual incidents impacting the organization. CSIRT performs initial triage to determine whether an incident requires formation of a specialized team to manage response activities or whether the incident should be handled by business as usual processes.

Response Planning

The Company understands that response planning for incidents is critical. Accordingly, we employ a continuous process of exercising response plans, training, evaluating intelligence, and potential threats to known assets, detecting threats, implementing countermeasures, reviewing events, and incidents, and taking corrective action. To further support this process, the Company periodically engages the Cyber Exercise program which includes a team of trained incident response experts to conduct tabletop exercises that include executive participation.

The Company periodically exercises the CSIRT plan in accordance with regulatory requirements and ensures procedures are sufficient to manage Company's response to cybersecurity incidents and events. The CSIRT plan maintains consistency in Company's response protocol during the execution of response processes which achieves the following:

- Provides a methodology for tracking cybersecurity incidents and events.
- Defines key roles and responsibilities for cybersecurity incidents and event handling participants.
- Identifies external threats with the potential to generate cybersecurity incidents and events.
- Defines processes to provide information to those involved in identifying, analyzing, and responding to incidents.
- Describes internal communication processes for technology management, business line management (as appropriate), Privacy, Corporate Security, and others as necessary.
- Establishes proper external communication to avoid negative publicity and to meet legal, regulatory, and contractual obligations.
- Minimizes the time required to identify and respond to cybersecurity incidents.
- Reduces disruption to business operation during incident response.
- Protects data integrity during evidence collection.
- Minimizes overall recovery time.

Reporting

The Company's security teams produce a variety of information security related reports on a weekly, monthly, and quarterly basis. The reports communicate key metrics to support management decisions and planning activities that focus on risk reduction goals. Key metrics include cybersecurity-focused Risk Appetite Statements, Key Risk Indicators, and Key Performance Indicators.

Company information security reporting can be divided in two major types: 1) executive reporting and 2) operational reporting. Executive reporting takes raw data, often with the addition of analysis and trending, and translates it into a digestible format with the goal of accurately communicating risk to the Company's decision makers. The goal of operational reporting is to communicate performance achievement at all levels to promote continual improvement within the bank's information security environment.

Analysis

Responding to an incident or an event after detection involves balancing several key components to ensure that timely restoration of the integrity, confidentiality, and availability of systems and assets is achieved. The Company employs a risk based approach to prevent threats from impacting the organization and to reduce the severity of an active incident.

The Company's Global Security Operation Center (GSOC) monitors and analyzes alerts from multiple sources, including incident response communications, service platforms and real-time monitoring tools. These inputs are tracked 24 hours a day, seven days a week and are triaged or escalated in accordance with established procedures. Impact analysis and communication guidelines are followed for each cybersecurity incident.

Mitigation

The Company's incident management processes include guidelines for cybersecurity incident containment after an impact and communication assessment has been completed. These processes include testing of containment prior to execution and they specify that affected and relevant parties must be engaged prior to containment.

All identified vulnerabilities are risk rated in the vulnerability tracking database. Tracking, monitoring and remediation ensure identified vulnerabilities successfully move through the incident management process.

Improvements

Following the resolution of every incident rated moderate or above, the Incident Response Team conducts a post incident review to evaluate how the issue was mitigated and contained. These findings generate measurable action items that are tracked. Results following the execution of an incident response process are studied and incorporated to continuously enhance the process. A change in the process or methodology is drafted, reviewed and approved by management prior to updating documentation.

The desired outcome during the Respond phase is the successful execution of incident response procedures by maintaining the security of our information systems, safeguarding our customer information and applying lessons learned to future improvements of the overall response process.

RECOVER

This function supports timely recovery to normal operations and restores affected capabilities or services impacted by a cybersecurity event. Categories within this function include Recovery Planning, Improvement, and Communications.

Recovery Planning

The Company maintains detailed Business Continuity Plans, Disaster Recovery Plans and Service Continuity Plans for the restoration of critical technical support services, environments, processes, applications, infrastructure, networks and operations. Service Continuity Plans cover services residing in U.S. Bancorp environments and services provided by third party providers. The Enterprise Readiness Services Group provides oversight and validation of Plan reviews and approvals. Dedicated resources are allotted to support all contingency planning and disaster recovery processes.

The Business Continuity and Contingency Planning Program is responsible for evaluating the impact of significant events that may adversely affect customers, assets or employees. It is designed to ensure that the Company has the capabilities and capacity to recover mission-critical functions and applications, meet fiduciary obligations to stakeholders and comply with applicable regulatory requirements.

Improvements

Plans are a documented collection of recovery procedures developed to ensure the Company functions and applications are recovered within their predefined recovery time objective in the event of a business disruption. Functional exercises of all Plans are conducted annually and Plans are updated based on the results. Exercise results are reviewed with senior management to ensure accuracy and completeness for use in an actual disruption. Any issues are logged and tracked through resolution.

Communications

The Company has developed a repeatable approach to manage communications and outreach in the event the organization experiences crisis situation. The Company keeps customers at the center, and accounts for its key stakeholders including employees, regulators, legislators, investors, business partners and vendors.