Protecting Client Data

An illustrative overview of Fidelity Institutional's cybersecurity program

For any financial services firm, establishing formidable defenses against cyberattacks must be a top priority. This includes not just protecting client data, but protecting all physical, virtual, and cloud-based systems and applications. The challenge of designing a comprehensive and effective cybersecurity program continues to grow with our increased use of digital platforms and data. Fortunately, the fundamentals of effective cybersecurity remain largely unchanged: identify ongoing risks, protect critical infrastructure, detect specific threats, respond to cybersecurity events to mitigate damage, and prepare recovery plans to get back to business as usual after an event. To assist our clients in evaluating our cybersecurity controls—as well as their own—we've outlined our program over the following pages.

A firm's ability to secure critical data and infrastructure depends on the execution of an effective risk management framework. The extensive controls and risk management programs we maintain are aligned to the cybersecurity framework established by the National Institute of Standards and Technology (NIST). We leverage this framework to understand the current state of cybersecurity risks, identify opportunities to achieve a desired future state, and continuously keep up with the ever-changing threat landscape. Within this overview, we describe the components of our program that are aligned to each of the core NIST functions.

Fidelity INVESTMENTS

1. Identify

Fidelity's firm-wide approach to cybersecurity begins with an audit of risks. We systematically work to identify all of our business risks; the related assets, systems, and capabilities we must protect; and the parties dedicated to protecting them. We focus on the following areas:

- **Asset Management**
- **Business Environment**
- **Governance**
- **Risk Assessment**
- **Risk Management Strategy**

Asset Management

Fidelity manages risk across all assets, including our data, personnel, devices, systems, and facilities. This includes:

- **Assigning and tracking asset owners.** Fidelity inventories all applications, databases, and technology infrastructure with an online tracking system. The system can track owners (both technology and business), technology platforms, business criticality and risk rating criteria, and application inter-dependencies. All physical devices are tagged with identifiers (e.g., bar codes) and registered in the inventory system. Dataflow, system, and network diagrams are maintained concurrently by our technology and operational teams.
- **Resource prioritization.** Resources are prioritized based on risk criteria that take into consideration data sensitivity, business criticality and availability requirements, and overall value and importance to the business.
- **Defined Information Security roles and responsibilities.** To protect our assets, Fidelity has an enterprise-wide Chief Information Security Officer (CISO) and cybersecurity team. Information Security Officers (ISOs) with appropriate security staff are also assigned at each business level. We employ over 750 associates in dedicated information security roles; additionally, thousands of technology professionals share responsibility for keeping our systems secure.

Business Environment Alignment

Fidelity Institutional's information security program is directly aligned with our business objectives. Cybersecurity roles and responsibilities and overall risk management policies and procedures are created and implemented with Fidelity's business goals in mind.

- **Security is part of the Fidelity culture.** Fidelity Information Security teams recognize the importance of understanding our distinct businesses in order to better protect our customer's financial data and personal information. Fidelity Institutional's Information Security Office group partners with our business units to help ensure that systems are available to execute trades, that information on holdings is protected, and that unauthorized transactions are prevented. Information security is an executive-level priority and a standing agenda item with our board of directors.
- **Uniform risk management across all business units.** Each Fidelity business unit maintains a risk management program with a common methodology and set of tools to identify and mitigate risks specific to its operations.

- **Robust security policies and procedures.** Fidelity associates follow documented risk management policies and procedures to help ensure that risk events are identified and responded to in a timely manner, and in accordance with the company's risk strategy and objectives. Control policies and procedures are maintained in accordance with industry- and Fidelity-established standards, and they are reviewed on a regular basis and updated as needed. Appropriate personnel are notified when a policy or procedure has been added or modified.
- **Active participation in industry and regulatory groups.** Fidelity is an active member of the financial services industry. We participate in groups such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), as well as in cybersecurity exercises with Securities Industry and Financial Markets Association (SIFMA). We also collaborate with Financial Industry Regulatory Authority (FINRA) and other regulatory agencies.

Governance Practices

Fidelity thoughtfully defines the policies, procedures, and processes to manage its regulatory, legal, risk, environmental, and operational requirements. We also have policies and procedures in place to inform management of cybersecurity risks.

- **Establishing standards for handling company information.** Fidelity's data classification standard, "Securing Private and Proprietary Information (SP2I)," defines specific requirements that all associates must follow for classifying, labeling, handling, and disposing of Fidelity information. Data is classified into four categories: public, internal, confidential, and highly confidential. We provide guidance on handling and protecting all levels of data, and communicate these requirements to all associates.
- **Instituting an Enterprise Risk Management Program.** The Enterprise Risk Management Program aligns our strategy across all categories of risk, including cybersecurity. It also provides a consistent enterprise-wide framework for business units to apply to their risk management programs. Fidelity has 14 enterprise-wide information security policies, each with supporting technical directives and guidelines that govern specific information security controls across the organization. Each business unit has a dedicated Information Security Officer (ISO) who is responsible for compliance with security policies and practices.
- **Executive-level responsibility for security risk governance.** Information security risk governance responsibilities ultimately rest with the FMR LLC Board of Directors, with additional oversight from the FMR LLC Audit Committee. Information security is a standing board-level agenda item, and these two groups oversee independent audit activities and monitor enterprise-wide compliance with legal and regulatory requirements, as well as Fidelity internal policies and standards.
- **Collaborating across the enterprise for risk oversight.** Fidelity has multiple enterprise-level risk groups (e.g., Corporate Security, Corporate Compliance, Compliance Program Management & Governance Group, and Corporate Risk Management) that collaborate to provide oversight of Fidelity's cybersecurity risk management and compliance with federal, state, and internal requirements.
- **Setting standards of conduct.** All Fidelity employees are required to sign a Code of Ethics agreement upon hire and annually thereafter that outlines their responsibility for conducting themselves in an ethical manner and adhering to Fidelity's acceptable use and other information security and HR policies and procedures governing employee behavior.

Risk Assessment Program

Fidelity uses a multi-pronged approach to understanding the cybersecurity risks to its operations, reputation, organizational assets, associates, and clients.

- **Threat Intelligence.** Fidelity has a dedicated Threat Intelligence team responsible for gathering intelligence on new vulnerabilities and emerging

threats from a number of external sources. Fidelity is also a member of FS-ISAC: the only established industry forum for collaboration on critical security threats facing the global financial services sector.

- **Conducting ongoing risk assessments.** Fidelity conducts ongoing risk assessments to identify imminent threats, emerging threats, and how resources should be prioritized and focused. Our risk assessment program methodically gathers input from all Fidelity business units, addressing specific business needs and regulatory requirements.
- **Conducting vendor due diligence.** Fidelity's Vendor Technology Review (VTR) Program works with the Corporate Vendor Management Program to ensure that new and existing vendors are assessed according to their risk to the firm. All vendors who receive highly confidential data are reviewed prior to receiving data. Follow-up reviews are performed at least every two years or when the scope of services changes.
- **24x7x365 monitoring and alerting.** Any issues encountered during daily production processing automatically generate alerts that are monitored by the Fidelity Support Center (FSC). The FSC is responsible for 24x7x365 monitoring of our networks and systems. Fidelity uses an incident management system to escalate alerts to appropriate system owners and business contacts.

Risk Management Strategy

Fidelity employs a series of strategies to manage operational risk based on the priorities, constraints, risk tolerances, and assumptions about the environment in which we operate.

- **Acting on risk assessment program results.** Throughout Fidelity, risk management teams help ensure that we have the right governance and risk management programs in place. The results of their assessments help Fidelity prioritize the systems to protect and the controls to implement. As an example, we perform semiannual resource-level access reviews for resources we have identified as "high risk."
- **Partnering with corporate risk departments.** Corporate risk oversight and audit departments provide assurance that Fidelity's risks are understood and managed in accordance with enterprise-wide and business-unit-specific policies and procedures.

2. Protect

Fidelity develops and implements safeguards beyond fundamental measures to ensure delivery of critical services. To protect our infrastructure, we focus on the follow areas:

- **Access Control**
- **Awareness and Training**
- **Data Security**
- **Information Protection Processes and Procedures**
- **Maintenance**
- **Protective Technology**

Access Control Security

Fidelity allows only authorized users to access assets and associated facilities, perform certain sensitive activities, and conduct transactions.

- **Employing a formal access and registration process.** All users of Fidelity systems are required to submit formal requests for access and role-based privileges through a central, online access management portal. Management approval is required prior to gaining any access. Access is granted based on the principle of least privilege, ensuring that associates have the minimum access necessary to perform the requirements of their job.
- **Automated termination procedures.** When an associate leaves the firm, Fidelity's human resources system automatically initiates a termination request and the associate's access to the Fidelity network is immediately removed. Physical access to the buildings is also immediately disabled in a separate system managed by Corporate Security. Termination procedures are reviewed by both internal audit groups and external audit firms.

- **Annual access reviews for all credentials.** All access for all associates is reviewed at least annually. Access to certain high-risk systems (e.g., trading) and functions (e.g., money movement) requires additional approvals from resource owners and information security. These permissions are also reviewed more frequently.
- **Restricting physical access to our assets.** Fidelity owns and operates our own ISO-certified data centers in Raleigh, NC, and Omaha, NE. Extensive physical security controls (card readers, biometric scanners, alarm sensors, video cameras, 24x7x365 security presence, etc.) protect against unauthorized access, and all data center physical access is reviewed monthly.
- **Securing remote access.** Fidelity uses technology that creates an "always on" virtual private network (VPN) that forces all connections from a Fidelity-managed device to use the Fidelity VPN when the connection originates on a non-Fidelity network. The use of this technology ensures that our network-level controls protect our assets even when an associate is using a public network (e.g., hotel, coffee shop, etc.). All VPN connections require multi-factor authentication.
- **Instituting extensive network-level controls.** Fidelity has multiple layers of defensive infrastructure protecting and segregating our networks. These include firewalls, intrusion detection systems, intrusion prevention systems, distributed denial of service (DDoS) protection, advanced malware detection and prevention programs, and other network-based controls. All Internet-facing resources are located in a secure "DMZ" network and all client data is secured within the internal network.

Awareness and Training Program

Fidelity provides persistent cybersecurity awareness education to help associates perform their duties and participate in the protection of Fidelity resources and data.

- **Requiring cybersecurity training for all associates.** All new hires receive cybersecurity awareness training during orientation, and every associate must attend annual training thereafter. This baseline cybersecurity training is formally tracked, and managers are notified if it is not completed. Associates in certain job functions (e.g., developers) also require training beyond the enterprise-wide baseline curriculum. Further, many of our information security professionals maintain industry certifications, which typically require specific third-party training. Our physical security team also participates in security simulation exercises with local law enforcement and industry groups.
- **Ongoing awareness activities.** In addition to formal training required by all associates, Fidelity also conducts ongoing awareness campaigns, including: "phishing" exercises, security walkthroughs to ensure "clean desk" compliance, daily threat intelligence emails distributed to information security staff, and targeted security bulletins.
- **Protecting our customers.** Fidelity's Customer Protection Program is an executive-level initiative tasked with implementing controls that secure our client-facing systems and working with clients to improve their own controls. We meet regularly with clients to help them become better acquainted with the ways they can implement Fidelity's security offerings (e.g., multi-factor authentication). We are also actively developing and improving our capabilities in areas such as fraud detection and prevention, DDoS attack protection, and addressing "zero-day" vulnerability mitigation.

Data Security Controls

Fidelity leverages technology controls to manage all data consistent with our risk strategy, to protect the confidentiality, integrity, and availability of data.

- **Encrypting data.** Fidelity encrypts all data in transit to and from our networks. For example, our client portals use SHA 256 bit ciphers and RSA 2048 bit encryption keys. We also use full-disk encryption

in our mainframe systems to protect data at rest. Laptop hard drives and mobile devices are also encrypted and can be remotely wiped if a device is lost or stolen.

- **Using secure measures to destroy physical media.** When servers are decommissioned their hard drives are destroyed onsite in our data centers before recycling. A third party securely incinerates all other physical media, and provides certificates of destruction.
- **Constantly monitoring network capacity.** We constantly monitor and test network capacity. A single data center location is capable of handling all Fidelity transaction and Internet traffic should the other location experience an outage.
- **DDoS protection.** Fidelity's DDoS controls include technical capabilities that can block attacks and re-route traffic, and business procedures to ensure Fidelity can continue to service our customers should our networks ever experience a service interruption.
- **Using data loss prevention tools to guard against information loss.** Fidelity has data loss prevention (DLP) tools in place to protect sensitive data from leaving our network. For example, our outbound email filters block emails containing highly confidential data, software code, and social security numbers. All USB and DVD drives are disabled by default, preventing users from copying data to removable media without senior management and information security approval as well as use of an encrypted device. We routinely scan internal servers to detect files containing sensitive information that are not properly restricted, and block access to online storage websites, public email services, instant messaging, and social media sites.
- **Regular scanning of all system configurations.** We scan all server configuration settings on an ongoing basis to ensure compliance with security policies and our secure build templates. Any violations (e.g., an unauthorized open service port) are reported to information security and executive management and tracked through to remediation. Additionally, all employee laptops and desktops are regularly scanned for unauthorized software and local administrative rights have been disabled, preventing associates from downloading and installing software on their PCs.
- **Segregating technology environments.** Fidelity fully segregates development environments from production environments, and developers do not have access to production systems. We also mask data used in test environments. If we ever need to use live data in a non-production environment (e.g., for client acceptance testing), we ensure that the environment has full, production-level security controls in place and is monitored by our security operations center when live data is in use.

Information Protection Controls

Fidelity's information protection processes and procedures ensure the protection of our information systems and assets.

- Certified policies and procedures for information protection. We have formal Enterprise Information Security policies, standards, and technical directives including operating system standards, password management, user accountability, external firewall security, and granting of administrative system privileges. Additionally, we have achieved and maintain the ISO 20000 certification for IT Service Management System across the following programs:

  – Change Management

  – Release Management

  – Problem Management

  – Incident Management

  Each of these programs leverages a centralized tracking system and has formal operating procedures to ensure compliance with all policies and procedures. For example, no changes are implemented into production without formal review and approval from our change review board.

- **Certified business continuity planning (BCP) and disaster recovery (DR) programs.** We have fully redundant systems across multiple sites to ensure continuous service availability and "instantly" mirror client data between our mainframe systems in Raleigh, NC, and Omaha, NE. For business continuity, we have secondary work sites in all of our major regions, key personnel located across regions, and remote work options available to associates if a site is not available. The BCP and DR programs are tested multiple times per year, with tests covering scenarios such as a full production system outage, loss of a site, regional weather event, pandemic outbreak, etc. Fidelity's BCP and DR programs are annually audited and have been certified to comply with the ISO 22301 standard.
- **Data destruction.** All server hard drives are wiped and then physically destroyed within our data centers. No hard drives leave our facilities. All laptop and desktop hard drives are wiped and then incinerated by a third party that provides certificates of destruction. These procedures are audited and meet the guidelines established by the National Institute of Standards and Technology (NIST).
- **Secure System Development Life Cycle (SDLC) process.** Fidelity's SDLC process includes formal security checkpoints throughout all stages of development. Additionally, an information security consultant is made available to all major development projects to ensure security controls are identified and included in the project. We also have security "dev ops" procedures in place to embed security checks into rapid development methodologies (e.g., Agile). We require extensive testing and approval of all software prior to production deployment.
- **Formal vulnerability management program.** Fidelity performs weekly vulnerability scans of its external and internal networks. These scans are part of our comprehensive vulnerability management program that also features a dedicated internal penetration testing team, automated and manual secure code reviews, system configuration scans, and robust reporting on identified issues, with information security teams providing governance and oversight to ensure they are remediated.
- **Human Resources security.** All associates undergo a comprehensive background check that includes a full criminal record search, credit checks, education and employment verification, and drug screening. Checks are re-performed every five years subsequent to initial employment. Fidelity also has formal, automated, and fully audited procedures for processing terminations and transfers, with an update to the HR system automatically triggering removal of network and facility access upon termination.

Maintenance Procedures

Fidelity maintains information systems consistent with industry best practices and internally established policies and procedures.

- **Logging of all service tickets.** All service tickets for software changes and other service requests are centrally logged in an automated system that tracks each request from approval to completion.
- **Requiring change control documentation.** We require change control documentation and an audit trail of each change, including the date and time of change, reason for the change, the name of the person making the change, and the person(s) who authorized the change. All change documentation must also include rollback plans, should the change cause a service interruption or degradation.
- **Formal patching program.** We have a formal patching program and receive change notifications from all our key software and hardware vendors. Patches are tested and deployed according to our formally audited and certified procedures.
- **Creating separate non-production and production environments.** In order to reduce risk of accidental or unauthorized changes to software and data, we require physical and logical separation of non-production and production environments.

All changes to our client-facing platforms are first deployed across various "slices" of the application and on a staggered basis. Taking this approach prior to promoting them across the full production environment eliminates the risk of a software change causing an issue across all production instances and allows for immediate rollback to a known good state.

Protective Technology Controls

Fidelity manages protective technical security solutions in a manner consistent with internally established policies and procedures, as well as industry standards.

- **Ongoing monitoring of networks, systems, and applications.** The Fidelity Support Center (FSC) provides 24x7x365 monitoring of our networks and systems, continuously reviewing system and application audit logs from centralized monitoring systems. Identified issues result in alerts within the system, which are escalated as necessary by FSC staff.
- **Restricting access to sensitive information.** Fidelity restricts access to sensitive system functions (e.g., Administrator and Root accounts) to authorized associates. Additionally, we use firecall procedures and Privileged Account Management (PAM) software to force administrative users to authenticate with their own account before accessing administrative system accounts.
- **Encrypting inbound/outbound email.** We encrypt emails sent to and received from clients, partners, and vendors, and we provide employees with "on-demand" email encryption tools.

3. Detect

Fidelity develops and implements a series of activities to detect cyber threats. Our overall approach ensures that we have the tools and monitoring in place to identify attacks against our infrastructure in real time. To detect cyber threats, we focus on the following areas:

- **Anomalies and Events**
- **Security Continuous Monitoring**
- **Detection Processes**

Anomaly and Event Detection

Fidelity detects, analyzes, and understands the potential impact of any anomalies in a timely manner.

- **Cybersecurity monitoring tools.** Cybersecurity attacks are monitored through the use of an automated Security Incident and Event Monitoring (SIEM) tool, integrated with Fidelity Support Center (FSC) and Cybersecurity Incident Response Team (CSIRT) services. Correlation of system and event logs across applications, servers, and devices allows us to detect anomalies and generate alerts to FSC and CSIRT. Detected incidents are assigned an impact level, and they are escalated and remediated accordingly.
- **Dedicated threat, intelligence, and team.** Our Enterprise Cybersecurity Threat Intelligence team is made up of data scientists and subject matter experts in network topologies, malware decomposition, and endpoint security. The team is responsible for gathering information about new vulnerabilities and emerging threats from external sources, identifying new threats to Fidelity, and providing internal daily threat advisories to all Fidelity business units.
- **Implementing preemptive measures.** We've instituted a preemptive perimeter defense for Fidelity's web presence, with multiple layers of defense against attacks and denial of service attempts before they reach Fidelity's network perimeter. We monitor and inspect web traffic with secure web gateways and traffic proxies, as well as inline traffic assessment. Finally, we leverage extensive tools and systems to monitor for fraudulent transactions in client accounts, and we continuously train our associates to identify and prevent fraud.

Security and Continuous Monitoring Activities

Fidelity continuously monitors information systems and assets in order to identify cybersecurity events and also verifies the effectiveness of its proactive measures.

- **Continuously monitoring system and application logs.** To alert to anomalies, Fidelity uses monitoring and aggregation tools in its U.S., Ireland, and India locations. In addition, Fidelity maps inbound and outbound external IP address requests to applications and systems, ensuring Internet traffic remains within scope of authorized applications and systems. Our systems and networks are monitored 24x7x365 by the FSC. To detect malicious code, we have installed antivirus/anti-malware software on production servers and employee laptops and desktops. Within our office locations, only authorized devices are allowed to connect to the network (e.g., MAC address filtering), and we regularly scan for unauthorized hosts and wireless access points.
- **Continuously monitoring firewalls and IDS/IPS.** Fidelity continuously monitors all firewall configurations and uses intrusion detection systems (IDS) in front of perimeter firewalls to alert to potentially harmful traffic before it enters our network. We also use intrusion prevention systems (IPS) deployed behind the internal DMZ firewalls to block harmful traffic from entering the production networks where client data is processed and stored. Host-based IPS is also installed on all endpoints and servers. This approach provides multiple levels of IDS/IPS protection and helps us accurately identify and mitigate genuine threats.
- **Installing enterprise security agents on all servers.** Fidelity installs security agents on all critical systems to define, measure, and report on the compliance of servers with preset firm-wide security policies. The agents identify security vulnerabilities and deviations from Fidelity's security policies.

Detection Capabilities

Fidelity maintains and tests its detection processes to ensure timely and adequate awareness of anomalous events.

- **Clearly defining roles and responsibilities.** The Fidelity Support Center, our infrastructure teams, and our application owners each understand the role they play in detecting security issues. Policies and procedures are well-defined and communicated. For event escalation purposes, we have identified key stakeholders and contacts for all applications, and we maintain this information in a centralized asset management portal.
- **Maintaining a dedicated security testing team.** A dedicated application security team provides pre-release (secure code reviews, training) and post-release ("Red team" penetration testing) security testing services to all Fidelity business units. The team's scope includes attack simulation to test the ability of our monitoring tools and teams to detect an active attack.
- **Ongoing reviews of detecting and testing procedures.** Our internal and external auditors review our cybersecurity detection procedures. We have certified these procedures to be compliant with the ISO 27001 information security standard. We also conduct—and make available to clients—annual SOC 1 and SOC 3 audits, covering myriad information security controls.

4. Respond

Fidelity is prepared with an array of activities to detect and respond to cybersecurity events. Attacks can occur at any time, and our approach to incident management helps mitigate any significant damage from any particular event. Our cyber threats response focuses on the following areas:

- **Response Planning**
- **Communications**
- **Analysis**
- **Mitigation**
- **Improvements**

Response Planning

Fidelity executes and maintains response procedures to help ensure a timely response to any detected cybersecurity event.

- **Clearly defining incident response personnel and procedures.** Fidelity has a Computer Security Incident Response Team (CSIRT) and cyber incident response procedures in place. Further, we have a "Cyber Event Playbook" that defines the teams that will be involved with various types of cyber events, as well as their roles and responsibilities. The playbook includes event triggers, the event declaration process and decision matrix, roles and responsibilities across all business units (e.g., Legal, Communications and Corporate Affairs, Corporate Risk, Enterprise Business Continuity, Technology Risk, Real Estate, Government Relations, Corporate Security, and Human Resources), escalation procedures, example incident types and response procedures, and after-action reporting and closure procedures.
- **ISO 20000 certified response procedures.** Fidelity's Incident Response (IR) framework is annually certified compliant with the ISO 20000 standards and guidelines. Fidelity's IR framework is a multi-functional approach that dictates our response based on the severity level (business impact) and priority level (urgency) of a security incident.

Communications Procedures

Fidelity coordinates response activities with internal and external stakeholders, and with appropriate law enforcement agencies.

- **Relying on designated communication managers.** In the event of an incident, a designated communications manager identifies all parties (internal and external) that are to be notified. All incidents are assigned an impact level according to predefined criteria that consider the criticality of the asset and the potential impact of the event. Customer notification and regulatory reporting requirements are also identified and processed. If necessary, our Communications and Corporate Affairs department will assist with communicating the impact of an incident to internal or external (clients, regulators, news agencies, etc.) parties.
- **Sharing information with other institutions and law enforcement.** Fidelity's participation in the Financial Services Information Sharing and Analysis Center (FS-ISAC) helps keep other financial institutions informed of ongoing threats and attacks against the industry. Our corporate security officers also maintain contacts with federal and local law enforcement and regularly participate in regional preparedness activities.

Analysis Process

Fidelity conducts analysis to both ensure adequate response and support recovery activities.

- **Relying on established processes to analyze incidents.** During analysis, we take a detailed approach to understanding the nature of the incident. Details include motives, opportunities, and means (MOM), likelihood of the threats, attack vector(s), the source(s) of the attack, the target(s) of the attack, the full scope and extent of the attack, and the security controls in place at the time of the incident.
- **In-house forensics capabilities.** Fidelity has specialized staff trained to perform digital forensics. Our digital forensics teams can image systems and forensically preserve evidence of an attack. Having this expertise helps us to prevent a similar attack in the future. Evidence preserved by our forensic professionals can also be used for legal purposes as needed.

Mitigation Strategy

Fidelity performs activities intended to prevent the expansion of an event, mitigate its risks, and eradicate the incident.

- **Mitigating the impact of an event.** Containment is the first step in mitigating the impact of an event. Fidelity will take any necessary steps, including taking applications offline, to prevent

the compromise of customer data. For more common security events, such as an end user's computer being infected by malware, the system is immediately taken off the Fidelity network and is fully reimaged before being reconnected.

- **Accessing outside experts, as needed.** As part of the response process, Fidelity brings in application, database, server, and network subject matter experts, when needed, to identify possible containment options. Once a course of action is identified, the CSIRT manages the containment process and tracks all tasks to completion.
- **Proactively identifying mitigation strategies.** As new vulnerabilities are identified, especially "zero-day exploits," Fidelity proactively identifies mitigation strategies (e.g., patching systems, implementing new IDS/IPS rules, etc.) to prevent the compromise of Fidelity systems.

Improvements for Detection

Fidelity improves organizational response activities by incorporating lessons learned from current and previous detection/response activities.

- Ongoing learning and improvements. Information security is ever-evolving, and after-action reporting and analysis is critical to ensuring that we are prepared for the next attack. During the incident closure process, the CSIRT drafts the formal incident response report, performs root cause analysis, identifies and tracks mitigation actions, identifies gaps or weaknesses in the incident response process and framework, and initiates improvements to the incident process.

5. Recover

Fidelity has strategies and plans in place to restore and, in a worst case, rebuild any capabilities or services that were impaired due to a cybersecurity event. For recovery, we focus on the following areas:

- **Recovery Planning**
- **Improvements**
- **Communications**

Recovery Planning Program

Fidelity executes and maintains recovery processes and procedures to help ensure timely restoration of any systems or assets affected by cybersecurity events. Our recovery strategy has plans for significant cyber events, large-scale regional events (e.g., a widespread power outage), and full site failures of our major data centers.

- **IT and security recovery procedures.** Our incident recovery capabilities include procedures for reimaging systems, segmenting and isolating systems to limit the impact of an attack, conducting forensic examinations, and after-action reporting.
- **Disaster recovery plan.** Fidelity has a robust disaster recovery program in place to assure continuous operations 24x7x365. This program identifies critical systems, as well as how they are backed up and recovered in the event of an incident. The program is certified compliant with the ISO 22301 standard for business continuity management. Fidelity dedicates significant resources to business continuity management and disaster recovery programs. We test components of these plans throughout the year to ensure effectiveness. Fidelity's continuity plans include the ability to recover from situations including, but not limited to, unplanned evacuations, power outages, major water leaks, fires, severe weather, pandemic outbreaks, cyber events, and any facility failures.
- **Fully redundant data centers.** Our data centers have full redundancy to ensure continuous operations. Any single site can meet the system and capacity requirements for the entire organization, with a recovery time objective (RTO) of eight hours and data recovery point objective (RPO) of five minutes in the event of a total site loss. Other key controls include:
  - Active/active configuration with data replicated in true real time (e.g., within nanoseconds) across our data centers
  - Continuous availability for key application functions such as trading
  - Fully redundant power supply via separate paths into the data centers

- Fully redundant generator and UPS backup power
- Fully redundant HVAC systems
- Multiple network providers via separate paths into the facilities
- Bandwidth capacity such that any single site can accept the full traffic load should all other sites experience an outage

- **Planning for multiple disaster scenarios.** Fidelity mitigates risk to reduce potential issues and impact. In the event of a business disruption, Fidelity has regularly tested plans to ensure continuity of its critical business functions, including:
  - Multi-site strategy for backup of certain critical functions. Fidelity employs multiple recovery strategies, including the use of designated alternate sites where there are tested procedures to address voice and data communications.
  - Alternate site tests. Fidelity conducts alternate site tests for its critical functions at least twice a year. Tests include validation and application functionality of desktops and telecom.
  - Contingencies for inclement weather. If there is a forecasted weather emergency, hotel rooms are obtained for essential personnel. If the weather emergency could result in the inability to access the primary site, Fidelity prepares an alternate site for use and personnel are sent there prior to the event.
  - Employee safety. Fidelity conducts regular evacuation drills, led by trained floor wardens and supervised by on-site security personnel.
  - Site infrastructure. Fidelity strategically locates trading and operations sites in buildings with uninterruptible power supplies (UPS) and backup generators.
  - Notification to clients. Procedures for notifying intermediary clients have been established for relationship managers and client service managers to follow in the event of an outage.
  - Regulatory reporting. Fidelity's business continuity plans ensure that regardless of the length of an outage at a primary location, our ability to meet regulatory requirements will not be impacted.
- **Following established business continuity standards.** Fidelity's Enterprise Business Continuity group maintains corporate standards to which all business units must adhere, and it coordinates response and event management across all Fidelity companies. Each Fidelity business unit also has dedicated business continuity planners to prepare and test its specific plan. Fidelity's program and standards embody, and are certified to comply with, the ISO 22301 standard.

Improvements for Recovery

Fidelity improves organizational response activities by incorporating lessons learned from current and previous detection/response activities.

- **Conducting ongoing plan reviews.** Reviews of our business continuity and disaster recovery plan, as well as our continuous improvement processes, require the following:
  - Plans are reviewed at least annually, or as significant changes occur, and are approved by executive management.
  - Plan reviews coincide with our semiannual mainframe disaster recovery testing.
  - Results from scheduled testing and actual event findings, or after action reviews, are incorporated into plans as needed.

Communications Capabilities

Fidelity uses systems and personnel to coordinate communications with internal and external parties.

- **Emergency notification system.** Fidelity's Business Continuity team has an emergency notification system that can be used to contact all associates during, or leading up to, an emergency situation.

We routinely test the system by calling associates at their office and alternative phone numbers and emailing them with instructions on how to respond during an actual event.

- **Coordinating communications among all stakeholders.** Our Communications and Corporate Affairs business unit is responsible for communicating with clients, news agencies, government officials and regulators, and other parties, as necessary. We also have dedicated Privacy and Compliance departments that determine if clients and end customers need to be notified of an event.

Summary

Maintaining comprehensive controls and risk management programs is the most effective way to combat cybersecurity risks. As the environment and specific risks continue to evolve, we believe that maintaining a robust cybersecurity program—one that executes the fundamentals well, while adapting to evolving risks—is critical for today's financial services firms. Through these programs, we work to mitigate costly financial and reputational risks, and to safeguard the data—and trust—of our clients.

For more information, please contact your Fidelity representative.

Information provided in this document is for informational and educational purposes only. To the extent any investment information in this material is deemed to be a recommendation, it is not meant to be impartial investment advice or advice in a fiduciary capacity and is not intended to be used as a primary basis for you or your client's investment decisions. Fidelity and its representatives may have a conflict of interest in the products or services mentioned in this material because they have a financial interest in them, and receive compensation, directly or indirectly, in connection with the management, distribution, and/or servicing of these products or services, including Fidelity funds, certain third-party funds and products, and certain investment services.

Fidelity Institutional[SM] provides investment products through Fidelity Distributors Company LLC; clearing, custody, or other brokerage services through National Financial Services LLC or Fidelity Brokerage Services LLC (Members NYSE, SIPC); and institutional advisory services through Fidelity Institutional Wealth Adviser LLC.

Personal and workplace investment products are provided by Fidelity Brokerage Services LLC, Member NYSE, SIPC.

Institutional asset management is provided by FIAM LLC and Fidelity Institutional Asset Management Trust Company.

200 Seaport Boulevard, Boston, MA 02210

780463.7.0 1.9898375.101