LAZARD

Information Security and Data Privacy Statement

Table of Contents

Information Security and Data Privacy Statement

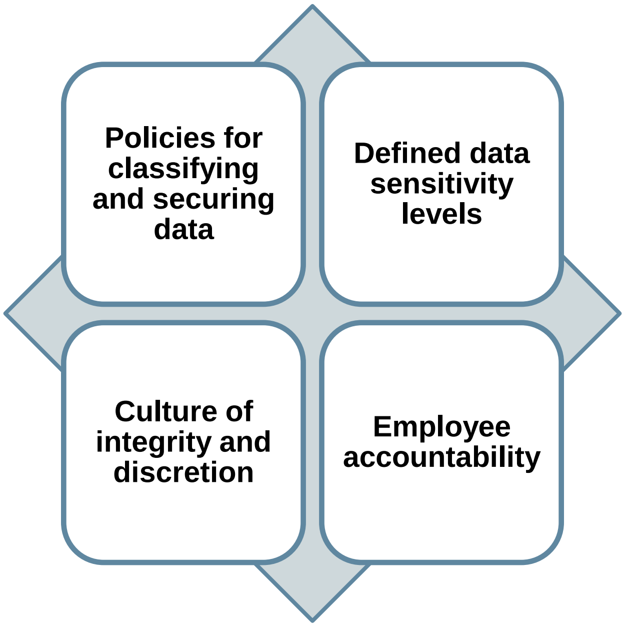
Business growth, technology innovation and increased electronic activity, including vast amounts of data processing and storage, are evolving and reshaping the cybersecurity landscape. We believe the protection and security of sensitive information across each of Lazard's offices and business lines worldwide is an important aspect of our business practices and an integral part of our risk management framework.

Lazard maintains a formal, robust cybersecurity and information security program that is aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). Our Information Security (IS) Program, Policies and Standards are also designed to comply with key global financial regulators and cybersecurity laws in the jurisdictions in which we operate. At the same time, our cybersecurity program incorporates monitoring activities conducted by our Internal Audit team. In February 2021, an independent third-party assessed our cybersecurity program's alignment with the CSF and we plan to have external reviews conducted periodically on an ongoing basis.

Our IS Polices and Standards are applicable to and compliance is required by all Lazard's employees, operations and third-parties with whom data is shared. As part of our third-party vendor due diligence process, we continue to evaluate and monitor cybersecurity policies and practices of vendors who provide critical data services to Lazard or its clients.

Safeguarding data and client information is among our top cybersecurity and information security priorities. Our practices and processes are designed to secure our data, systems, and services in accordance with the NIST CSF framework: **Identify, Protect, Detect and Respond**, and **Recover**. This document is intended to provide an overview of our cybersecurity and data protection practices firm-wide; however specific information security protocols differ across Lazard's businesses and geographic locations.

Lazard Information Security and Data Privacy Framework


Policies for classifying and securing data
Defined data sensitivity levels
Culture of integrity and discretion
Employee accountability

Identify

Governance and Approach

Lazard's cybersecurity program, which includes information security and data privacy, is the responsibility of our Chief Information Security Officer (CISO), who oversees our global information security strategy and program within our Information Technology (IT) and Information Security (IS) departments. The CISO reports monthly to the Global Risk Committee (GRC), which includes our Chairman and Chief Executive Officer (CEO), President, Chief Financial Officer (CFO), Chief Information Officer (CIO), Chief Administrative Officer (CAO) and General Counsel, among other members of senior management. Our CISO reports twice a year to the Board of Directors, including the Board's Audit Committee, on material cyber risks, including those identified in our business and rising threats, and the current state of Lazard's information security. Additionally, our CFO and Head of Risk Management review with the Audit Committee potential cybersecurity risks and exposures as part of Lazard's risk management assessment. Each Lazard office has IT team members responsible for monitoring the unique risks and local management is principally responsible for oversight of business activity risks on a day-to-day basis. Local teams report to corporate IT and IS departments tasked with oversight and auditing, and senior IS and IT management provide regular and, as necessary, elevated reporting to the CISO.

A formal review of the firm's IS Polices and Standards, and Cybersecurity Incident Response Plan (CSIRP) is performed annually by members of the IS department for review by the IS team's senior management and the CISO. Lazard seeks to identify cybersecurity risks to Lazard's information, brand, and assets by soliciting varied industry perspectives and analyzing each identified risk across a variety of factors including likelihood, potential impact, maturity of controls in place and ability to respond or mitigate the risk. The priorities of our IS Program are informed by the risks identified as a result of this annual review together with emerging cybersecurity trends. Ultimately, Lazard's information security and data protection priorities drive multi-year strategic planning for our IS Program.

How We Manage and Handle Data

Collection: Collect relevant reliable information necessary for business objectives

Storage: Store information as needed and necessary for compliance with retention policies and only on firm managed or authorized systems

Labelling: Label information and apply appropriate encryption

Security: Protect Lazard equipment and resources

Distribution: Follow policy guidelines when sharing information internally or publicly, require non-disclosure agreements for third parties as appropriate. Encrypt and protect sensitive files

Disposal: Delete and degauss files no longer required to be retained, laptops and external hard drives wiped clean to reuse

Protect

Training and Awareness

We recognize that the strength and effectiveness of our cybersecurity program relies in part on the vigilance of our employees. Through our intranet portal and 24-hour, 7-day (24/7) IT Help Desk support, our employees have access to our IS Policies and Standards, web-based cybersecurity training and assistance from IT support staff. Our employees participate in mandatory cybersecurity training annually to learn updates on information security protocols and practices, including how to promptly identify and report phishing or other suspicious cyber incidents, recovering lost data, and the importance of contacting the IS team in any high-risk situation. To reinforce training and awareness, throughout the year the IS team sends simulated phishing attempts to our employees and follows up directly with employees who do not properly respond to provide incremental instruction. We provide function-specific security training and role-based security training to IT personnel on an annual and timely basis as necessary.

Cybersecurity training topics offered firm-wide

- Information and Cybersecurity Fundamentals
- Security Awareness
- Data Protection
- Social Engineering and Phishing
- Information and Physical Security Protection
- Safe Use of Lazard Technology
- Data Privacy and Credential Management
- Communication and Media Security

Remote Work

In response to the increased number of employees working remotely, our IT and IS departments implemented a secure remote work solution seamlessly and rapidly and without significant impact to our operations. We proactively engaged and educated our people on cybersecurity awareness through training sessions, global town hall programs, and in-depth resources regarding cybersecurity protocols and procedures on our intranet.

Infrastructure and Software Security

Lazard makes significant investments in information technology that are designed to secure our information and enable the operations of our business across our infrastructure, software platforms, and program applications while simultaneously protecting against cybersecurity threats. Our cloud-based platform and infrastructure is built with data security fundamentally integrated including the security enhanced Bring Your Own Key (BYOK) customer-managed permission vault. In addition to implementing security processes, we also continuously assess, mitigate, and manage Lazard's top risks and vulnerabilities including, for instance, the use of legacy applications.

Lazard maintains a hardware asset inventory which tracks information properties and operational status. Our hardware inventory management is governed by policies and procedures that specify manual and automated processes and controls to track the lifecycle of an asset and ensure the equipment is secure and up to date for optimal use. Our inventory management process undergoes periodic audits by internal or third-party consultants and is reviewed annually or whenever a significant change occurs. Asset decommissioning is critical to protect our information. The secure removal and destruction of sensitive data is managed by our IT department through formal processes and procedures to ensure all assets are securely, and in an environmentally sound manner, disposed, recycled, or wiped clean for reuse when no longer needed.

The firm has established a systems hardening approach designed to reduce vulnerability in technology applications, systems, infrastructure, firmware and other areas. The goal of systems hardening is to reduce security risk by eliminating potential attack vectors and condensing the system's attack surface. Operating systems, applications, servers, databases and networks are hardened on a risk-adjusted basis to meet or exceed industry standards. Baseline security practices, such as password and credential encryption, restricted file access permissions, and mandatory inactivity screen lock is enforced by our IS department via a configuration policy on endpoints.

The firm’s network hosts multiple business zones separated by firewalls and other controls designed to emphasize security, confidentiality and resilience in the event of business disruption. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are deployed across the network to monitor for and block malicious/suspicious activity. Management interfaces on perimeter firewalls, routers and other devices are not accessible from the public internet.

Wireless access to the Lazard network is only permitted from Lazard issued devices and approved and registered employee devices. Network Access Control (NAC) technology is used to monitor compliance with these procedures and unauthorized devices are not permitted access to the Lazard network.

Vulnerability Management

We assess the vulnerability of our systems by applying a lifecycle perspective and conducting full monthly scans. All machines on the Lazard system are also equipped with an agent able to report vulnerabilities in real time. Once a vulnerability is discovered, our IS team implements a structured patch management process to resolve the issue. To facilitate the identification of vulnerabilities, we test our systems internally and utilize external parties to conduct penetration tests for our internet facing systems, online applications, and public websites. We also conduct an annual external penetration test of our entire network, rotating between vendors to rigorously test our systems across a breadth of penetration approaches.

Third-Party Risk Management

Third-Party Risk Management (TPRM) is built into our due diligence process and risk protocol. We are committed to continuously improve our existing processes to ensure that all third-parties that manage Lazard information are evaluated and undergo an initial risk assessment prior to working with the firm with heightened due diligence for vendors providing critical services to the firm. Types of risk assessments include site visits, evaluation of staff and screening practices, employee background and security checks and if necessary, an assessment conducted by an independent third-party. As appropriate, Lazard performs ongoing due diligence during the duration of the contact and third-parties are routinely assessed and re-certified annually. Lazard seeks to remedy any failure by a vendor to meet our standards, but if the vendor is not able to continue to meet our standards, we terminate the relationship.

Prior to the due diligence process, vendors must sign a non-disclosure agreement (NDA) and must sign an NDA once and prior to receiving sensitive information from the firm. When applicable, third-party policies, standards and controls shall be in accordance with Lazard's IT standards and guidelines.

Lazard's Information Security department is responsible for the review, approval and onboarding of any third-party vendors that provide data, information technology or cybersecurity support. Our dedicated TPRM team reports the overall risk score for these third-parties to Senior Management on a regular basis.

Data Protection and Privacy

Due to the nature of our asset management and financial advisory businesses, we have very limited access to and management of end user data. Most of our clients are institutions, brokerages or corporations, and a smaller portion of our business represents individuals directly. However, as part of our overall cybersecurity program, we are committed to, where applicable, implementing data protection protocols; obtaining user data through lawful and transparent means limited to the stated purpose through explicit consent of the data subject where required; providing clear terms for the collection, use, sharing, and retention of user data; and notifying data subjects in a timely manner in case of material policy changes or a data breach that would impact the data subject. Individuals can request that their account information be deleted or amend personal information. Our procedures for collecting, using and sharing user information is in accordance with our Privacy Policies and applicable laws.

In the event government authorities or law enforcement submit data requests to Lazard, our CISO works directly with our Legal and Compliance department to evaluate and respond in compliance with the law. We are committed to privacy in data management with respect to human rights, and therefore would, absent a legal or regulatory restriction, notify data subjects in case of data sharing and disclose to the data subject our processes for evaluating these requests.

Detect

Security events are categorized, prioritized and addressed according to our documented CSIRP. The CSIRP operates three intrusion detection systems and includes detailed procedures and incident management, notification and escalation procedures, including a defined cybersecurity Information Security Incident Communications Response plan. The CSIRP is reviewed at least annually or more frequently, as necessary. The Lazard Cybersecurity Incident Response Team (CSIRT), led by our CISO, has the primary responsibility for the management and resolution of all Lazard-related cybersecurity incidents and is available 24/7 to respond to incidents that are observed through proactive network and system monitoring. The CSIRT also responds to incidents reported by end users.

Logging and Monitoring

Log management is implemented in our cybersecurity program and security management processes. Log files and active monitoring allows surveillance of our IT infrastructure and an assessment and analysis of our security operations.

Log files allows us to detect potentially malicious activity and respond accordingly to eliminate suspicious activity or threats. Logging is enabled for specific events including changes in system configuration, authentication access and administrative activity. Logs are kept in accordance with the firm’s policy and, should an event occur, security logging supports our forensic investigations into the source and results of a successful or failed attempt.

Lazard maintains active monitoring capabilities through global security information and event management (SIEM) technology which provides detection, analytics and real-time security alerts of suspicious activity generated by software applications and network hardware. This provides our security team both insight into and a track record of the activities within our cyber environment by gathering data from antivirus events and firewall logs, sorting data into categories, such as malware activity, and identifying potential threat levels. Our SIEM technology provides enterprise-level security by integrating visibility across our network of devices and applications.

End users, including employees, third parties, and data subjects (where applicable), are encouraged to report potential cybersecurity incidents, suspicious activity or data privacy concerns either directly to Lazard’s IS and IT departments, our 24/7 Help Desk or through Lazard’s Accounting Concern Reporting Procedures, available on our public website and outlined in our Code of Business Conduct and Ethics.

Respond and Recover

Lazard has Business Continuity and Disaster Recovery plans designed to respond to and recover from a disruptive event. Each business line and supporting department is responsible for creating and maintaining its own plan, with oversight coordinated by the CISO. Plans are tested and updated annually, or more frequently as necessary and appropriate.

The firm maintains an alternate data center containing infrastructure to support the firm's business in the case of a catastrophic event. Both the primary and alternate data center facilities have secure access, video surveillance, property management and security detail. In addition, the facilities include redundant power, generators, air conditioning, and fire detection and suppression systems. Our data centers function across geographies and operate 24/7 in normal and distressed circumstances. The firm regularly tests its technology resilience necessary based on business criticality to ensure our network, access to the cloud, software and application components demonstrate operational recovery. Although the firm maintains these alternative data centers, employees are equipped to operate in a remote environment and connect to our secure network from private premises in order to maintain critical business continuity.

To bolster Lazard's response to cybersecurity incidents, we test our incident response procedures and policies through exercises with a third party twice a year. These tests include simulations of communications shared with affected stakeholders on security events and identification of vulnerabilities.

In the event that a cybersecurity incident becomes a breach, Lazard's policy is to provide a timely notification to clients, regulators, and relevant parties such as law enforcement agencies (as necessary and appropriate) involved in the investigation, describing the nature of the event and measures taken to address and mitigate adverse effects. We have established controls that aim to ensure continuous business operations and availability of information in the event of major failures or disasters. We monitor and measure any potential data breaches and report these metrics to the Global Risk Committee and the Board.

Information security is a shared responsibility which involves dedicated efforts of our IT team, as well as investment, training and testing across the firm. Our cybersecurity and data protection program continuously strives to educate our employees on security measures and controls in order to protect client data and our firm systems.

As of December 2021