MetLife's Commitment to Information Security

Overview

As part of the normal operation of our business, MetLife is entrusted with personal and confidential information every day. Consistent with our purpose of helping people build a more confident future, we view data security as a critical part of financial security – our customers are counting on us for both.

MetLife is firmly committed to protecting the confidential information of our customers, partners, and suppliers. We meet or exceed the security standards set by all applicable laws and regulations governing our business. No cybersecurity incident or attack to date has had a material impact on MetLife, Inc., business.

MetLife's Information Security Program is overseen by our enterprise Chief Information Security Officer (CISO), with collaboration across businesses and functions. The CISO is a senior-level executive responsible for establishing and executing the company's information security strategy. The primary goal is to protect information and technology assets. This includes monitoring, reporting, managing and remediating cyber threats.

The Information Security Program aims to prevent data exfiltration, manipulation, and destruction, as well as system and transactional disruption. Our threat-centric and risk-based approach for securing our environment is based on the Cybersecurity Framework (CSF) developed by the U.S. government's National Institute of Standards and Technology. The elements of the Information Security Program are:

- *Prepare:* Drive preparedness through dynamic analysis. We maintain organizational controls to anticipate and identify threats to critical systems, assets, data, and capabilities.
- *Prevent:* Stay ahead of adversaries and reduce number of incidents. We maintain safeguards to address critical vulnerabilities and ensure delivery of critical infrastructure services.
- *Detect:* Limit exposure through continuous monitoring of staff, applications, data, systems and networks. We undertake activities to enable timely discovery of potential cybersecurity events.
- *Respond:* Mitigate incidents through a coordinated response capability. We employ robust measures to contain and respond to potential cybersecurity events.
- *Recover:* Improve security posture through forensics, investigations and lessons-learned capabilities. We restore capabilities or services that were impaired, and we strengthen resiliency against future events.

Cybersecurity Safeguards

MetLife regularly reviews and updates its policies and procedures to keep them current in light of cybersecurity laws and regulation, emerging threats, new and changing technologies, and other information technology risks. MetLife's Information Security Program works with IT and business management to institute controls for IT systems, applications and databases, and for vendor and application service provider arrangements.

As an additional component of the CSF "Prepare" objective, MetLife, Inc., and its subsidiaries maintain primary cybersecurity and privacy liability insurance policy coverages.

As a component of the CSF "Respond" objective, MetLife has a Cyber Security Incident Response Team (CSIRT) that is charged with responding to internal and external threats and taking action. The CSIRT is responsible for establishing and maintaining situational awareness of threats, vulnerabilities and incidents. The team implements proactive measures in

response to changes in the threat environment. The primary goals of the CSIRT are to detect, triage, contain, eradicate and recover from cybersecurity incidents, working with other teams across MetLife throughout the incident lifecycle.

The CISO along with other senior leaders presents to the Audit Committee of the company's Board of Directors at least once per quarter, and to the full Board as necessary. The Board is promptly updated and provided information if a security incident may pose significant risk to our company.

Monitoring, Testing, and Auditing

MetLife routinely monitors the effectiveness of its information security practices. Business applications that are either new or undergoing major enhancements are evaluated through an internal application assessments process.

As a regulated financial services company, MetLife also monitors its compliance with applicable law and regulation, such as, in the United States, the following laws and regulations that relate to cybersecurity practices: HIPAA, Sarbanes-Oxley, Gramm-Leach Bliley Act, and the New York State Department of Financial Services Cybersecurity Regulation, and the laws and regulations overseen by the insurance commissioners of all fifty states.

MetLife engages leading third-party security companies to assess prevalent threats and vulnerabilities through, among other things, periodic network and application penetration testing, capability maturity reviews and controls assessments that help to enhance our Information Security Program.

MetLife employs network surveillance software to determine if any abnormal activity occurs, such as an attempt to gain unauthorized access to MetLife's internal systems from outside MetLife's network. Incidents are escalated to MetLife executive management in accordance with incident handling procedures. On top of internal measures, Security Information and Event Management (SIEM) components are centrally monitored by a managed security services supplier 24 hours a day, seven days a week. Appropriate IT security personnel are alerted to suspicious or abnormal network traffic.

In addition, MetLife undertakes: (i) periodic security reviews to assess the adequacy of its controls, including an SSAE 18 SOC 2 annual review of its information technology infrastructure and key financial applications; and (ii) through its Internal Audit organization, a variety of financial and IT audit reviews across the Enterprise each year, including periodic audits of the security and confidentiality of MetLife nonpublic information.

Staff Training

MetLife requires information security awareness and privacy training to be completed annually by our staff, including all new hires. In addition to required trainings, targeted secure developer trainings are provided to application development teams and a comprehensive library of on-line security trainings is available to all associates. MetLife also embeds security awareness training into its institutional culture, including banner messages on the MetLife intranet home page, email communications to staff, periodic speakers, and lobby monitor displays. Further, the Information Security team maintains dedicated intranet site, that is available to all associates to reinforce security awareness and information security best practice references and archived documentation.