August 24, 2016

Incident Response Plan Summary

Executive Summary

The objective of Symantec's Security Incident Response Plan is to define and implement an operational framework including the processes, skills, and tools necessary for Symantec to timely detect, contain, investigate and report on cyber security incidents potentially impacting Symantec systems, networks, and data, including customer, partner or supplier information in Symantec's possession. The plan codifies the general procedures for handling information security related incidents from detection through remediation. The plan defines the extended company-wide Security Incident Management Team, departmental roles and responsibilities and also establishes secure communication systems and practices for timely information sharing and coordination in response to a security incident The Symantec Security Incident Response Plan meets PCI requirements, and is consistent with the principles and guidelines described in the NIST Framework for Improving Critical Infrastructure Cybersecurity (v 1.0), while satisfying Symantec's internal control requirements and objectives.

Scope

The Symantec Security Incident Response Plan is an internal facing document for detecting, responding to, investigating, and recovering from "security incidents", which are defined broadly as all events that impact or potentially impact the confidentiality, integrity, or availability of data/information, information systems, and computer assets under Symantec's control. The plan provides for comprehensive company-wide, global processes for handling security incidents from monitoring through containment to recovery and long-term remediation. It designates a single departmental "owner" to manage the end-to-end incident response process, and sets out defined cross-functional roles and responsibilities in order to comprehensively identify and manage all aspects of the security response process.

The plan uses a risk-based approach for initial classification and triage of reported incidents, establishes 24/7 secure communications channels for coordinated containment and investigations and provides guidelines to ensure information relevant to a security incident investigation is shared as appropriate with Symantec's executive management, our board of directors, and our partners, suppliers and customers in a transparent and timely fashion.

Symantec recognizes that the larger Symantec employee community must be actively engaged in securing our data, information, networks, and assets, and understanding employees' respective roles in responding appropriately to security concerns when they arise. Accordingly, our mandate also requires the Global Security Office to provide clear guidance, training and tools to the wider Symantec employee audience to report and respond appropriately to potential security incidents, and to conduct regular exercises and training regarding security incident response.

The Symantec Incident Response Lifecycle

Symantec's plan lays out a four (4) phase incident response lifecycle, consistent with recognized industry standards and practices and the NIST Framework.

1. **The "engagement" phase** includes processes for monitoring systems and events, monitoring the threat landscape, receiving reports from internal and external resources on threats, and making initial assessments to verify, classify and log incidents into our tracking system.

2. **The "detection and analysis" phase** includes processes for assembling the response team, performing initial triage, communicating with appropriate stakeholders, and assigning action items for containment, evidence gathering, risk assessments, and communications.

3. **The "response" phase** includes defined workflows for collection and analysis of evidence following forensic protocols and best practices, identification and execution of a containment strategy, timely information sharing with management and the extended incident response team (for legal assessments and development and execution of risk management strategies), and initiation of recovery plans.

4. **The "post-incident response"** phase provides for a broader investigation and root cause analysis, documentation and evidence archiving, development of remedial action items, and post-mortem review to enable continual improvement of processes and tools.

Conclusion

Symantec's internal Security Incident Response Plan documents repeatable, industry standard procedures for handling actual cyber threats when they arise. It also provides the necessary engagement and information-sharing processes to allow prompt coordination among all relevant stakeholders, and describes the reporting, communication, containment, investigation, and recovery mechanisms that exist to support a comprehensive end-to-end process flow from threat detection through remediation.

The development and implementation of this forward-looking plan supports Symantec's ultimate mission to its customers, partners, shareholders, and employees as a trusted leader in information security risk management.