The Global Security Office (GSO)

At Symantec, we are dedicated to each other, our customers, our business, and society. We believe that information protection is a central element of our responsibility. The very nature of our business—ensuring the confidentiality, availability and integrity of your information—requires a culture of security responsibility.

Symantec's **Global Security Office (GSO)** is responsible for maturing Symantec's Information Security posture by supporting our global culture of security and protecting information assets and technologies to secure your information wherever it lives. The GSO is comprised of teams such as Security Governance, Risk and Compliance (GRC), Security Architecture and Engineering, Physical Security, Defensive Cyber Operations, Offensive Security, and Enterprise Resilience. These teams work together to provide visibility and continuously enhance the security over Symantec's applications and networks.

The **Governance, Risk & Compliance (GRC) team** facilitates, monitors and evaluates compliance with information security policies and regulatory standards to protect Symantec's information technology, brand, intellectual property, personal information and customer data from misuse or compromise. Governing information security policies and monitoring the environment for operational effectiveness and compliance helps Symantec maintain an accurate and sensible picture of security risk posture. The Third-Party Assurance team performs security reviews of all third-party suppliers during the various lifecycle stages of the supplier relationship. The Customer Trust Office partners with Legal, Sales and Product teams to solve customer security and compliance needs.

The **Security Architecture and Engineering (SAE) team** works together to ensure security is built into Symantec's development and operations. The architecture team performs reviews over application and network designs, while the software security team ensures appropriate reviews are performed at all stages of the software systems development lifecycle.

The **Physical Security and Safety team** is committed to protecting our employees, assets, facilities and brand reputation from compromise, loss or destruction. They ensure our employees and guests are provided the safest, most secure environment within which to operate. They have the tools and resources to efficiently manage proactive and rapid reactive security responses at facilities worldwide.

The **Defensive Cyber Operations (DCO) team** provides continuous monitoring of all Symantec information systems and assets to identify cyber security events and verify the effectiveness of all protective measures deployed. They are focused on the detection of anomalous activities and understanding the potential impacts in a timely manner. Our vulnerability management program is designed to proactively prevent the exploitation of vulnerabilities and reduce threats to Symantec's infrastructure. To promote security situational awareness, our Threat Intelligence team provides a framework of Indicators of Compromises (IOCs) from a collection of proprietary threat intelligence feeds. These are critical to maintaining the operational availability, confidentiality and integrity of information technology systems used internally by Symantec employees and to support customers.

The **Offensive Security team** protects Symantec and its customers by applying adversarial methods to improve our security posture and resilience to current and emerging threats. To ensure adequate security controls and processes are in place, they conduct general penetration tests against all of Symantec's assets and infrastructure. This may involve penetration testing, external network, internal network, wireless network, etc. The Offensive Security team continually challengs the status quo, innovating new ways to emulate malicious adversaries and their tactics, techniques and procedures. This understanding of how attacks operate improves our detection capabilities and effectiveness of our security posture.

The **Enterprise Resilience team** manages operational and technology risks that could impact Symantec's ability to deliver services to customers. Our Business Continuity and Disaster Recovery program focuses on identifying actual and potential risks to business functions, partnering with the business to mitigate those risks. The Crisis Management program supports consistent and effective responses when there is an interruption to business, safeguarding the interests of employees, customers, partners and shareholders.