6 STEPS TO PREVENT A DATA BREACH:

WHAT YOUR CUSTOMERS SHOULD KNOW ABOUT BREACHES, AND HOW YOU CAN HELP PREVENT THEM.

Data breaches can severely impact business operations for customers with intellectual property, proprietary information, and other valuable assets stored on desktops and databases. For protection, Symantec offers data loss prevention, IT compliance, and endpoint security and management solutions that are risk-based and content-aware. By leveraging these solutions to implement a program along the six steps listed here, you can help your customers significantly reduce the risk of data breach.

1 STOP INCURSION BY TARGETED ATTACKS

The top four means of incursion into a customer's information assets are: exploiting system vulnerabilities, default password violations, SQL injections, and targeted malware attacks. To prevent incursions, you need to shut down every avenue. Core systems protection, IT compliance controls assessment automation, and endpoint management, plus endpoint, Web, and messaging security solutions should be combined to stop hacker attacks.

2 IDENTIFY THREATS BY CORRELATING REAL-TIME ALERTS WITH GLOBAL INTELLIGENCE

To identify and respond to the threat of a targeted attack, security information and event management systems should be used to flag suspicious network activity for investigation. The value of real-time alerts is much greater when the information they provide is correlated with current research and analysis of the worldwide threat environment from Symantec.

3 PROACTIVELY PROTECT INFORMATION

It is no longer enough to defend the perimeter. In today's connected world, customers need to identify and proactively protect sensitive information wherever it is stored, sent, or used. By enforcing unified data protection policies across servers, networks, and endpoints throughout the enterprise, you can help them progressively reduce the risk of a data breach.

4 AUTOMATE SECURITY THROUGH IT COMPLIANCE CONTROLS

To prevent data breaches caused hackers or insiders, organizations need to develop and enforce IT policies across their networks and data protection systems. By assessing the effectiveness of procedural and technical controls and automating regular checks on controls such as password settings, server and firewall configurations, and patch management, customers can reduce the risk of exposing sensitive information.

5 PREVENT DATA EXFILTRATION

Even if an incursion is successful, network software can still be used to detect an attempted breach and block data exfiltration. Well-meaning insider breaches caused by broken business processes can likewise be identified and stopped. Data loss prevention and security event management solutions can combine to prevent breaches during the outbound transmission phase.

6 INTEGRATE PREVENTION AND RESPONSE STRATEGIES INTO SECURITY OPERATIONS

It's essential to have a data breach prevention and response plan that is integrated into day-to-day operations of the customer's security team. Using technology to monitor and protect information lets security teams continuously improve their strategy and reduce risk based on constantly expanding knowledge of threats and vulnerabilities.

SYMANTEC IS
SECURITY.

WHY SYMANTEC TO PREVENT DATA BREACHES?

Symantec is a global leader in providing security, storage, and systems management solutions to help protect our information-driven world. Symantec software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. For customers that need to protect their vital information, respond to threats rapidly, demonstrate compliance, and manage security efficiently, Symantec is the proven leader.

Confidence in a connected world. symantec™