6 STEPS TO PREVENT A DATA BREACH

To monitor and protect information from both internal and external threats, organizations should select solutions based on an operational model for security that is risk-based, content-aware, responsive to threats in real time, and workflow-driven to automate data security processes. Here are six steps that any organization can take, using proven solutions to significantly reduce the risk of a data breach.

1 PROACTIVELY PROTECT INFORMATION

In today's connected world, it is no longer enough to defend the perimeter. Now you must accurately identify and proactively protect your most sensitive information wherever it is stored, sent, or used. Only by enforcing unified data protection policies across servers, networks, and endpoints throughout the enterprise can you progressively reduce the risk of a data breach.

2 AUTOMATE THE REVIEW OF ENTITLEMENTS TO SENSITIVE DATA

Improper credentials are the leading cause of data breaches triggered by targeted attacks using malware to find and export data. By automating regular checks on passwords and other entitlement controls, organizations can reduce the risk of such a breach. In addition, failure to lock down the entitlements of terminated employees in a timely manner is a major contributor to breaches caused by malicious insiders. Automated entitlement reviews can stop such breaches before they happen.

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

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

4 STOP INCURSION BY TARGETED ATTACKS

The top three means of hacker incursion into a company's network are default password violations, SQL injections, and targeted malware. To prevent incursions, it is necessary to shut down each of these avenues into the organization's information assets. Controls assessment automation, core systems protection, and messaging security solutions should be combined to stop targeted attacks.

5 PREVENT DATA EXFILTRATION

In the event that a hacker incursion is successful, it is still possible to prevent a data breach by using network software to detect and block the exfiltration of confidential data. Insider breaches can likewise be identified and stopped. Data loss prevention and security event management solutions can combine to prevent data breaches during the outbound transmission phase.

6 INTEGRATE PREVENTION AND RESPONSE STRATEGIES INTO SECURITY OPERATIONS

In order to prevent data breaches, it is essential to have a breach prevention and response plan that is integrated into the day-to-day operations of the security team. The use of technology to monitor and protect information should enable the security team to continuously improve the plan and progressively reduce risk based on a constantly expanding knowledge of threats and vulnerabilities.

SYMANTEC IS
SECURITY.

Confidence in a connected world. symantec.™