



6 STEPS TO PREVENT A DATA BREACH

For companies that have critical information assets such as customer data, intellectual property, trade secrets, and proprietary corporate data, the risk of a data breach is now higher than ever before. To monitor and protect information from hackers, malicious and well-meaning insiders, organizations should select solutions based on an operational model for security that is risk-based and content-aware. Here are six steps that any organization can take, using proven solutions to significantly reduce the risk of a data breach.

1

STOP INCURSION BY TARGETED ATTACKS

The top four means of hacker incursion into a company's network are through exploiting system vulnerabilities, default password violations, SQL injections, and targeted malware attacks. To prevent incursions, it is necessary to shut down each of these avenues into the organization's information assets. Core systems protection, IT compliance controls assessment automation, and endpoint management, in addition to endpoint, Web, and messaging security solutions, should be combined to stop targeted attacks.

2

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.

3

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. By enforcing unified data protection policies across servers, networks, and endpoints throughout the enterprise, you can progressively reduce the risk of a data breach.

4

AUTOMATE SECURITY THROUGH IT COMPLIANCE CONTROLS

To prevent a data breach caused by a hacker or a well-meaning or malicious insider, organizations must start by developing and enforcing IT policies across their networks and data protection systems. By assessing the effectiveness of the procedural and technical controls in place and automating regular checks on technical controls such as password settings, server and firewall configurations, and patch management, organizations can reduce the risk of exposing sensitive information.

5

PREVENT DATA EXFILTRATION

In the event 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. Well-meaning insider breaches that are caused by broken business processes 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 their strategy and progressively reduce risk, based on a constantly expanding knowledge of threats and vulnerabilities.



**SYMANTEC IS
SECURITY.**

WHY SYMANTEC

Symantec is a global leader in providing security, storage, and systems management solutions to help organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. For organizations 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.

