Carbon Black.

10 Ways to Protect Your Company From a Data Breach

As a result of the recent spate of high-profile data breaches at brand name retailers, compromising credit and debit card and other personally identifiable information for hundreds of millions of consumers in the process, data security has become priority No. 1 for many retailers in 2014. And for good reason: The consequences of suffering a data breach are numerous, and none of them are positive — consumer mistrust, a drop in traffic and a decrease in sales, to name just a few.

With retailers recently testifying before Congress that they're facing increasingly sophisticated threats from cyber criminals, and no end to those in sight, it's become apparent that your company needs to implement strategies that will protect itself from a costly data breach. Here are 10 ways you can more easily achieve that goal while maintaining required PCI compliance (all of these tips fall within one of five buckets — visibility; asset control; enforcement; trust policy; advance measurement.)

1. MINIMIZE THE CUSTOMER DATA YOU COLLECT AND STORE.

Acquire and keep only data required for legitimate business purposes (e.g., marketing, billing, shipping), and only for as long as necessary. When data is no longer of business value, properly dispose of it. For example, shred paper documents before recycling and remove hard drives from computers before disposing of them. Take your security efforts a step further by encrypting the sensitive data that you collect. Encryption makes it more difficult for unauthorized parties to read lost or stolen data. Install encryption on all laptops, mobile devices, flash drives and backup tapes.

2. MANAGE THE COSTS AND ADMINISTRATIVE BURDEN OF THE PCI COMPLIANCE VALIDATION PROCESS.

Try segmenting your infrastructure among multiple teams to minimize the complexity associated with the applicable compliance metrics. Having full visibility into all enterprise assets (e.g., network systems, point-of-sale system) along with the templates to determine PCI-relevant data gives you a snapshot of the corporate assets that are affected.

3. MAINTAIN PCI COMPLIANCE THROUGHOUT THE CHECKOUT PROCESS.

If you're able to detect transactional data point infractions in real time and stop anything introduced into your infrastructure that's outside of known software (e.g., advanced threats),
you can ensure that transactional data (e.g., a credit card number) is protected at every stage in the process.

4. DEVELOP A STRATEGY TO PROTECT YOUR INFRASTRUCTURE ON MULTIPLE LEVELS.

This includes closing every opportunity for cybercriminals to exploit your point-of-sale terminals, kiosks, workstations and servers. The ability to collect endpoint information in real time provides retailers with the information to assess the risk that any asset may pose to its security and PCI compliance. Monitor traffic and create a central log of security-related information to alert you to suspicious activity on your network.

5. MAINTAIN REAL-TIME INVENTORY AND ACTIONABLE INTELLIGENCE ON ALL ENDPOINTS AND SERVERS, AS WELL AS CONTROL THE OVERALL SECURITY OF YOUR INFRASTRUCTURE TO MAINTAIN PCI COMPLIANCE.

Employ multiple layers of security technology — e.g., firewalls, up-to-date anti-malware programs — to stymie sophisticated hackers. Establish a baseline for the software inventory that should reside on your endpoints, schedule security patches on your own timetable and eliminate the need for constant profile scanning that can bring the performance of an endpoint to a halt.

6. EXTEND THE LIFE OF YOUR SYSTEMS.

Oftentimes you can't upgrade or pay for extended support after an operating systems' end of life. For example, you may have critical applications that won't run on the newer operating system, your hardware can't run the newer operating system or your organization can't afford to pay the high cost for out-of-band support. By implementing a positive security model, you can stay compliant in any end-of-life situation and get protection from zero-day and other attacks for all of your servers and endpoints. You know at any given time what's running on every in-scope system across your organization; you can determine on a real-time basis if you have any vulnerabilities and whether any in-scope systems have fallen out of scope. You have all the parameters set up that matter to your business.

7. USE REAL-TIME SENSORS TO TEST YOUR SECURITY SYSTEM REGULARLY.

By maintaining continuous, real-time file integrity monitoring and control, retailers can protect critical configuration files from unauthorized changes and meet file integrity monitoring and audit trail rules. You'll be able to identify all suspected vulnerabilities across your infrastructure and proactively take action against specific versions and types of files based on your company's policies. By giving individual employees' file rights and approvals into the trust metrics for your company, you'll have complete visibility into all changes and vulnerabilities that software updates may introduce. This increased visibility provides a wealth of information for the penetration test and will expose all known and potential vulnerabilities prior to the commencement of testing. This also will help you determine what penetration tests to execute because the coordinates can be created against a set of known possibilities rather than a negative set of data.

8. BUILD MEASURABLE BUSINESS INTELLIGENCE AROUND YOUR BUSINESS ASSETS.

By understanding and having visibility into real-time file asset inventory information, you can build intelligence around all of your file assets, including their prevalence, trust rating, threat and inherited vulnerabilities. Having a high level of visibility enhances your ability to report on any asset at audit time or during pre-compliance assessment and security intelligence gathering. This enables you to take a proactive stance against anything running within your enterprise, sifting out anything that's deemed untrustworthy.

9. CONDUCT REGULAR AUDITS OF SECURITY MEASURES, ESPECIALLY CONNECTIONS COMMONLY USED AS GATEWAYS FOR ATTACKS, AND MAKE APPROPRIATE ADJUSTMENTS.

A full audit of all significant PCI data and the surrounding events associated with the attempted file alteration is necessary so auditors can quickly assess your compliance stance and produce the necessary reporting for PCI compliance validation.

10. EDUCATE EMPLOYEES ABOUT THEIR ROLE IN DATA SECURITY.

Inform all of your employees of the potential threats to customer data as well as the legal requirements for securing it. This should include designating an employee to serve as information security coordinator, who is responsible for overseeing the company's security efforts. Having a clear data security policy in place will help guide employees on the proper use of data, creating a more secure environment.

Some guidelines to consider including in your security policy include the following:

- allow access to sensitive employee or customer data only to those employees whose positions require access to it;
- Require employees to store laptops and other mobile devices in a secure place;
- direct employees to give no security information over the phone;
- require the use of multiple, unique passwords on computers and any personal devices used for work purposes;
- implement a system for retrieving information from departing employees and vendors/contractors at the end of their relationship with the company;
- verify the security controls of any third-party vendors that you work with to ensure they meet your requirements and that you have the right to audit them;
- require that employees and vendors/contractors promptly report any potential data security breach to the company; and
- employ policies outlining the proper disposal methods for data.

ABOUT CARBON BLACK

Carbon Black is the leading provider of a next-generation endpoint-security platform designed to enable organizations to stop the most attacks, see every threat, close security gaps, and evolve their defenses. The Cb Endpoint Security Platform helps organizations of all sizes replace legacy antivirus technology, lock down systems, and arm incident response teams with advanced tools to proactively hunt down threats. Today, Carbon Black has approximately 2,000 worldwide customers, including 25 of the Fortune 100 and more than 650 employees. Carbon Black was voted Best Endpoint Protection by security professionals in the SANS Institute's Best of 2015 Awards.

Carbon Black.

1100 Winter Street
Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499
www.carbonblack.com