



White Paper

CARDVAULTSM

Stopping Data Cyberthieves in their Tracks

July, 2010

Stopping Data Cyberthieves in their Tracks

Ever wonder why keeping a data center safe from intruders is so difficult? It's not just because you're responsible for making sure server cages are locked, disaster recovery plans are in place and there's enough backup power in case of a citywide blackout. It's also because you're one of the first lines of defense when it comes to safeguarding trillions of bits and bytes of sensitive information that reside on the servers in those cages.

Today's data center is a magnet for criminals trying to hijack, steal or destroy personally identifiable information, medical records and credit card numbers. An IT professional's job now encompasses far more than deploying the latest technologies to deliver peak network performance or ensuring on-demand virtual computing environments are operational 24/7.

Identifying and nullifying cybertheft of information assets – whether targeted denial of service attacks, spear-phishing expeditions by spammers, or worms laden with data-stealing malware – are now an important part of a data center manager's responsibilities. Securing a center's ecosphere means protecting everything – from the network architecture to remote applications to confidential data – against relentless cyber attacks, not just preventing unauthorized physical access to the center itself. But with IT staffs stretched thin, making sure all the physical and digital doors of a data center are locked tight without stalling one's business model can be tricky, especially when networks are a hodgepodge of legacy systems and components stitched together, creating security holes that can be easily compromised.

Hackers have a built-in advantage when it comes to compromising data. They think day and night about how to invent and execute a clever attack, and they gravitate to pathways that offer the least resistance for the greatest payoff. Many work for organized crime syndicates. Yet most companies don't have full-time IT security defense teams with the same intensity and focus on deterring hackers. So the odds of a successful breach are in the hacker's favor.

In the **2009 Verizon Business Data Breach Investigations Report**, security experts who analyzed more than 90 forensic investigations and 285 million compromised records found that 74% of all breaches resulted from external sources. While highly sophisticated attacks accounted for only 17 percent of the breaches, those relatively few cases accounted for 95 percent of the total records breached, proving that motivated hackers know where and what to target.

According to the Ponemon Institute's **U.S. Cost of a Data Breach Study**, data heists during 2009 cost companies an average of \$6.75 million, or \$204 per compromised customer record – up from \$6.65 million, or \$202 per record, in 2008. When the Institute conducted its first data breach study in 2005, the average was \$138 per record. In just five years, the cost of dealing with the consequences of a breach rose nearly 48 percent. The same study found that breaches from malicious attacks and botnets doubled from 12 percent to 24 percent between 2008 and 2009 and cost 40 percent more than those caused by human negligence or IT system glitches.

Understandably, organizations that suffer a breach would rather not disclose their losses. But 498 breaches exposing more than 222 million records containing highly sensitive information such as credit card numbers, passwords, driver licenses and Social Security numbers were tracked by the non-profit **Identity Theft Resource Center** in 2009, up from nearly 36 million records exposed by 656 breaches during 2008. Through the first six months of this year, the IRTC has already chronicled 333 breaches representing over 8.5 million records with confidential personal information.

The fallout from a credit card breach equates not only to lost sales and revenue for a company, but lawsuits, damage to its brand and reputation, the loss of customers who take their business elsewhere, and stiff fines for not complying with requirements known as the **Payment Card Industry Data Security Standards (PCI DSS)**.

The PCI standards require that merchants who process, retain or transmit payment card data protect that information wherever it is stored. This means any business that accepts or processes payment cards online, in a store, by phone or by mail must protect and restrict access to that data or risk penalties from the major payment card brands who make up the PCI Security Standards Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

Safeguarding routine business information is tough enough. But conforming with PCI rules for payment data or federal privacy laws (such as the Health Insurance Portability and Accountability Act) for personal medical information on an internal network – even with state-of-the-art technologies – can be extraordinarily difficult and prohibitively expensive because every point at which that data is handled must be secured.

PCI Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security
Source: PCI Security Standards Council	

We find that many large enterprises keep multiple copies of the same payment data on old legacy systems whose underlying technologies remain solidly rooted in the 1960s. Because these systems are transaction-based rather than customer-based, their interoperability with internal audit and accounting processes is severely limited. To make matters worse, organizations often don't know where sensitive data resides on those systems and have no control over it. But even if a fraction of their revenue is card-based, the company must become PCI-compliant.

The alternative is so obvious it's often overlooked – eliminating the storage of that data altogether.

The premise is simple: if companies don't keep confidential credit card information internally, there's nothing for hackers to steal. And when customer card data is no longer on one's system, the need for other controls is either greatly reduced or eliminated entirely. As a result, moving card data "out of scope" lessens the risk of a data breach, promotes faster and easier PCI compliance for organizations and saves them money.

The technology behind this premise is tokenization.

With tokenization, merchants exchange their customers' confidential card data – or other type of personally identifiable information – for randomly generated

payment "tokens," a process that safely replaces real card numbers with a string of characters which then become useless to would-be hackers. The token provides "contextual security" because the token value only makes sense between the token holder and the provider. It is useless anywhere else. Merchants use only the token key reference for each customer transaction while the real card data remains securely offsite at a PCI-compliant service provider and data center.

In an era of continually cheaper data storage options, it's easy not to think about how much data should be retained, where it makes the most sense to store that data or how best to protect it – until it's too late.

Ask yourself, "Would building and defending our own data fortress conform with best practices for encrypting payment information? Would we save time and money going that route or create a cyclonic funnel that drains resources from other, more productive uses? Or would outsourcing to tokenization experts who specialize in storing, protecting and processing customer card information make more sense?"

When choosing a tokenization partner, be sure the vendor is Tier-1 certified by an independent auditor – assurance that every feature and function of their service meets the highest levels of PCI data security.



1. **World-Class Security and Reliability** – 3DSI’s hosting facilities are housed in state-of-the-art Equinix data centers with exceptional security, infrastructure flexibility and power availability that deliver the utmost in reliability, security, performance and support.
2. **Strict Safety Controls** – Access to the Equinix data center that hosts 3Delta Systems servers is strictly controlled using biometrics and other advanced technologies to immediately screen and authenticate user access.
3. **Mission-Critical Power Backup** – Multiple Equinix power generators ensure 3DSI customers receive a continuous, uninterrupted supply of electrical power for mission-critical data center support.
4. **Around-the-Clock Surveillance by High-Alert People and Systems** – 3DSI’s customer data is monitored around the clock by sophisticated systems and highly trained Equinix network engineers.

Source: All photographs of Equinix IBX Centers are © 2000–2010, Equinix, Inc. All rights reserved. The Equinix logo is a trademark of Equinix, Inc.

Evaluate whether a vendor offers the best combination of low cost, security, flexibility and ease of use for processing card payments. Will the vendor save you money by applying the lowest available credit card interchange rates when customer purchase transactions are accompanied by detailed, invoice-like information known as Level-3 line-item data? How robust are the vendor’s data centers that will house your customers’ payment information?

While no data center on earth is 100 percent hack-proof, every IT manager can and should manage the risk of a potential data breach by solving for the concept of “graceful failure.” By assuming elements of your data center will fail at some point and that perpetrators will gain some form of access, you must plan for a layered, deep-defense approach to secure your system so that if one safeguard fails, other countermeasures can detect and respond to an attack. Toward that end, tokenization can be a formidable tool in your defense arsenal.

Author: Aaron Bills, Chief Operating Officer and Founder, 3Delta Systems, Inc.

About 3Delta Systems

3Delta Systems, Inc. (www.3DSI.com) is a leader in online credit card processing solutions and the makers of CardVault®, an innovative tokenization service that removes a merchant’s risk of keeping confidential customer payment information. 3DSI’s complete suite of payment solutions – each designed from the ground up to be scalable, easy to implement and conform with PCI Data Security Standard best practices – enables enterprise, business-to-business and business-to-government customers to manage, authorize and settle payment transactions in real-time. As a leading Software-as-a-Service (SaaS) provider, 3DSI has processed more than 39 million payment transactions worth more than \$33.5 billion for over 6,000 corporations and government agencies since the company was founded in 1999.

© 2010 3Delta Systems, Inc.® All rights reserved.

Rick Ricker

Vice President of Business Development, Enterprise Payment Solutions

rricker@3DSI.com
P: 703.234.6012

3Delta Systems, Inc.

14151 Newbrook Drive
Suite 200
Chantilly, VA 20151
P: 703.234.6010
F: 703.234.6004

www.3DSI.com