White Paper

A Valid Solution for Card Data Security Anxiety

Elavon

Card data is a favorite target for cybercriminals, for obvious reasons. The attacks have typically been easy to carry out and the rewards can be high. Verizon noted in its 2017 Payment Security Report that "point-of-sale environments continue to provide rich pickings for the bad guys, with nearly 98% of all recorded attacks resulting in a confirmed data breach." Furthermore, CSOonline.com security writer Michael Kan observed that:

> **"Retailers, hotels and restaurants have all been victimized through the same Achilles' heel that cybercriminals continue to attack: the point-of-sale system, where customers' payment data is routinely processed."**

With such an irresistible target as financial data – second only to social security numbers – the outlook for breaches isn't positive.

Customer loss from data breaches can total as much as **$4.13 Million**.[1]

[1] Ponemon Institute, "2017 Cost of Data Breach Study," June 2017

The likelihood of a recurring data breach over a two-year period is **27.7%**[2]

Elavon

The number of card data breaches is increasing… again

Breaches that exposed card data dropped significantly in 2012 (to 14.4% from 26.14% in 2011), but are now at almost 20% again.[3] Europay, Mastercard and Visa (EMV) standards for chip cards have curbed authentication fraud. But while card data isn't as valuable on the black market as social security numbers (SSNs) and medical data, thieves will still stop at nothing to get it if they can.

DATA BREACH COSTS ARE STAGGERING

U.S. businesses pay a high price for data breaches, including the costs of detection, escalation and notification, as well as expenses to get back to normal business operations. Customer loss alone can total as much as $4.13 million.[4]

But there is also a largely unknown, perhaps incalculable cost – loss of reputation. Some businesses never overcome the broken trust experienced after a breach, which can impact customers, but also employees, shareholders and suppliers. As the adage goes, there is never a second chance to make a first impression.

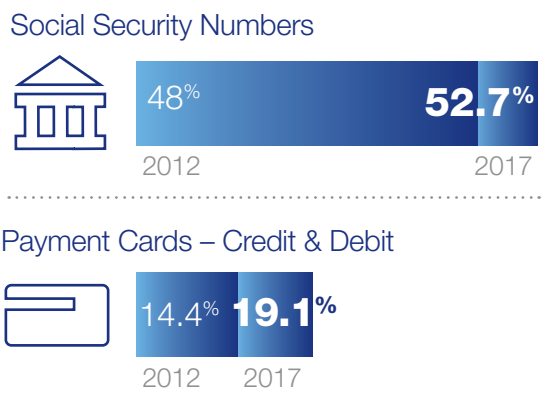
BUSINESSES ARE AT RISK OF SUBSEQUENT ATTACKS

Unfortunately, thieves tend to target low-hanging fruit. The assumption is that if security allows a break one time, it could again. In fact, the likelihood of a recurring data breach over a two-year period is 27.7% if it's a smaller breach.[5] This may seem like a small percentage, until it's compared to the millions of dollars of damaged incurred from a single breach.

Why are businesses at risk of being breached multiple times? Simplify put, many don't understand the importance of cybersecurity. They think it couldn't happen to them – "My business is too small" (A word on that: 61% of breaches in 2017 hit small businesses.)[6] Others think they don't have the resources – financial or personnel – to implement an effective security program. Still others are slow to learn of and react to the initial breach.

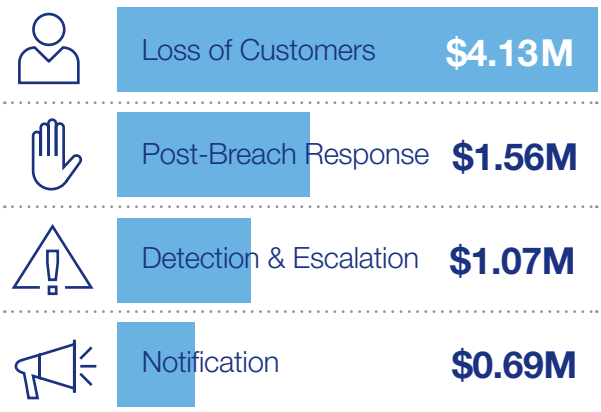
Whatever the reason, some businesses fail to take even the simplest measures – like software patches – to the delight of fraudsters.

Data Breaches Exposing SSNs & Card Data



Source: Identity Theft Resource Center, 2017

Cost of a Data Breach



Source: Ponemon Institute, "Cost of a Data Breach Study," June 2017

[2] Ponemon Institute, "2017 Cost of Data Breach Study," June 2017
[3] Identity Theft Resource Center, "2017 Cost of Data Breach Study," January 18, 2018
[4] Ponemon Institute, "2017 Cost of Data Breach Study," June 2017
[5] Identity Theft Resource Center, "2017 Cost of Data Breach Study," January 22, 2018
[6] Verizon, "2017 Data Breach Investigations Report," June 2017

Elavon

The Payment Card Industry expects you to protect cardholders

Launched in 2004, the Payment Card Industry Data Security Standard (PCI DSS) is now an industry cornerstone that features 12 requirements for safely managing card cardholder data.

> **Nearly half** of businesses that achieved validation in 2016 fell out of compliance within a year.[7]

Although these measures are clear in their direction, how merchants go about achieving and maintaining PCI DSS compliance is a whole other matter. For some, it becomes too costly. For others too complex and time-consuming.

Verizon reports that only around 55.4% of organizations achieved validation in 2016. But of those, nearly half fell out of compliance within a year – most in less than nine months![8]

PCI DSS Goals & 12 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 cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data
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 for all personnel

[7] Verizon, "2017 Data Breach Investigations Report," June 2017
[8] Ibid

Why PCI-validated Point-to-Point Encryption (P2PE) is more than just a good idea

Failure to protect cardholder data can leave businesses open to data breaches. PCI-validated P2PE offers a proactive, systematic strategy for securing cardholder data and continuously adhering to industry mandates – while dramatically reducing the scope of PCI compliance efforts.

What does "scope" really mean?

The PCI Security Standards Council defines "scope" as "the PCI DSS security requirements that apply to all system components included in or connected to the cardholder data environment." This can include networking devices, firewalls, servers, applications, switches, routers – and anything else that stores, processes, or transmits sensitive data, or is connected with systems that do. All are considered "in scope" (translation: requires lots of time and money for compliance).

1. Protects sensitive payment card data. Encrypts and tokenizes card data to render it useless in the event of hacking, and prevents storage in merchant environments.

2. Securely manages devices. Each device must be managed via a chain of custody that includes:

- Ordering from an approved supplier
- Secure receipt at an approved facility for injection with keys
- Secure delivery directly to the merchant

At no time does the merchant have access to the encryption or decryption keys, so card data is undecipherable within the merchant's payment environment.

3. Establishes an ongoing security program. Merchants' employees must be properly trained to manage payment card data according to the PCI DSS. The merchant must also document processes and ensure that quarterly checks and audits are performed. This approach provides for continuing compliance with the standards.

Data breaches have become a fact of life, but that doesn't mean your business has to be the next victim. A PCI-validated solution will help you launch a preemptive strike in the ongoing battle against cybercrime, while saving yourself time and money.

For more information about Elavon's PCI-validated solution, call 1-866-548-6826.