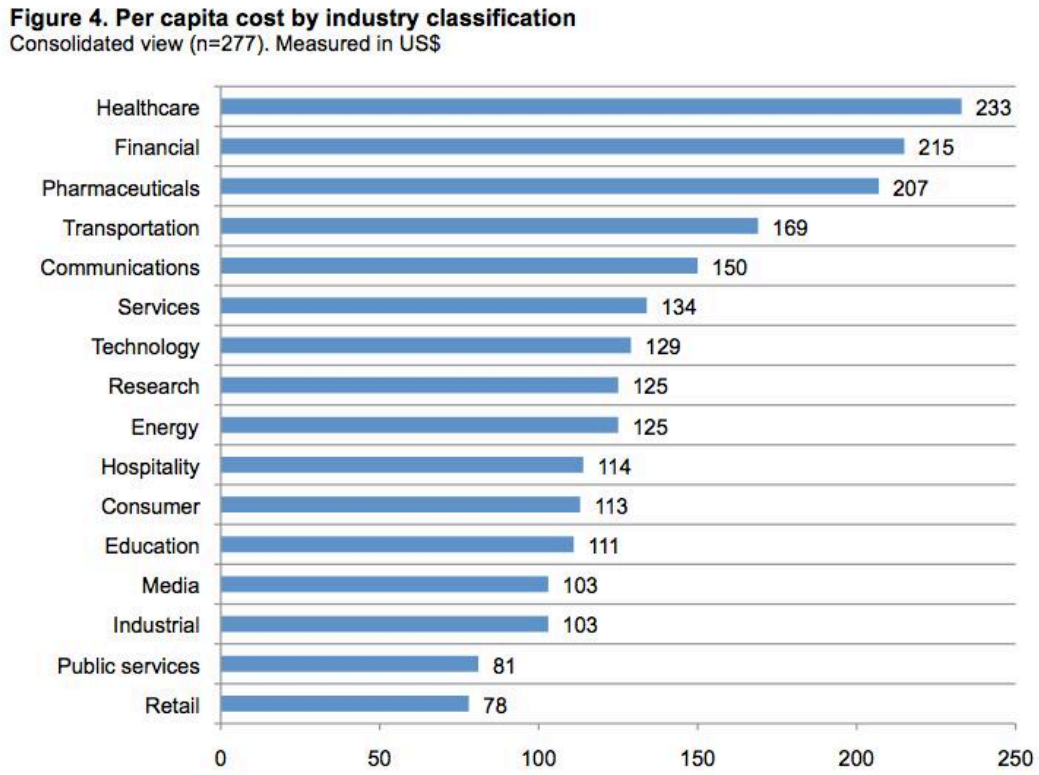
Thieves in Plain Sight: No One is Immune to Data Attacks

Asif Ramji, President and CEO, Paymetric, Inc.

To some executives, the idea of crime against merchants and high-volume data breaches might seem like the latest Hollywood action movie. While it is a reality for retailers because those are the companies we see on the front page of the Wall Street Journal, it seems like fiction for everyone else. Certainly, it's hard to miss the latest data breaches in the news and the associated high-profile retailers: Target, Nieman Marcus and Michael's. All three companies have been hit with extensive breaches of consumers' sensitive cardholder information. But other industries are feeling the cost of data breaches – both financial and reputational -- at an even more aggressive level. And smaller companies aren't immune. In a Verizon 2013 Data Breach Investigations Report survey, nearly half of all breaches occurred at companies with fewer than 1,000 employees. It's time that we all think beyond retail (and beyond the CIO's office) as being most at risk. If your company handles any sensitive personally identifiable information (PII), you are at risk of a data breach.

When a breach occurs, damage can be swift . . . and it appears to be getting worse. According to a recent report released in February 2014, 2,164 incidents reported during 2013 exposed more than 822 million records, nearly doubling the previous highest year on record (2011). Four of the breaches from 2013 secured a place on the Top 10 All Time Breach List.



This seemingly ever growing threat cannot be ignored. Companies in virtually every industry that handle sensitive data are targets. According to a recent study by the Ponemon Institute, healthcare, financial and pharmaceutical organizations top the list of the most expensive breaches. And while retail may be making the headlines, it’s actually the least expensive data breach per customer record.

American companies seem to be particularly at risk. That same Ponemon study showed that U.S. companies experienced data breaches that resulted in the greatest number of exposed or compromised records worldwide (an average of 28,765 records) and the average loss of business per breach was $3 million.

This rise in data breaches and their resulting cost have companies asking “Am I doing enough to protect my data?” As breaches are expected to continue escalating, taking the proper steps to protect your data has never been more relevant or more important. And while data breaches certainly are a PR and CIO’s nightmare, the cost associated with fines, customer churn, litigation fees and auditing processes span nearly every facet of an organization. Data breaches are an ongoing daily risk for every company that handles credit card data and other sensitive information. For that reason, data breaches are not just the CIO’s problem, but the C-level executives as well. Data security must involve commitment from every department across the enterprise.

While all sensitive data is at risk, payment card data remains one of the easiest types of data to convert to cash, and therefore the preferred choice of criminals. As payment card data becomes more and more important with cards supplanting cash, there is a clear path of action for businesses that can help prevent the compromise of payment card data: the Payment Card Industry Data Security Standard (PCI

DSS).

Prior to 2004, each card brand had a unique security program that merchants were required to adhere to including: Visa's Card Information Security program, MasterCard Site Data Protection, American Express Data Security Operating Policy, Discover Information and Compliance and the JCB Data Security program. These five card brands realized it was becoming very confusing for merchants to comply with multiple regulations and decided to develop a uniform security standard called the Payment Card industry Security Standard Council (PCI SSC). The PCI SSC is responsible for the management, education and awareness of security standards including the PCI DSS, which provides guidelines to keep sensitive cardholder data safe from exploitation. Compliance is mandatory for any business that transmits, processes or stores payment card data; even if it's just one transaction.

Failure to be compliant to PCI DSS regulations may result in fines and the loss of a merchant's license to accept card payments. Unfortunately, compliance with PCI DSS is far from universal. For example, according to the Verizon 2014 PCI Compliance Report, 64.4 percent of organizations in 2013 failed to restrict each account with access to cardholder data to just one user.

We recommend a careful, well-designed outsourcing strategy for both the management of security technologies and business processes. The aforementioned Verizon PCI Compliance Report recommends that your choice of provider should be made not just on IT security knowledge, but on business and payment-industry knowledge as well.

Leveraging tokenization technology is a best practice approach for securing sensitive data in enterprise systems and applications. It's a common misperception that tokenization and encryption are equal. Tokenization works by replacing payment card numbers with a surrogate, or "token," ensuring sensitive data is never stored in your environment. The real data is stored off-site in Paymetric's secure data vault. A solution like Paymetric's Data Intercept captures card data and tokenizes it before they enter enterprise systems, ensuring raw cards never even touch those systems. At its core, tokenization is protecting data throughout every

PRINCIPLE	REQUIREMENT
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration
	2. Do not use vendor-supplied defaults for system passwords
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data
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 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 card data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

Because of this, tokenization greatly reduces risk of breach, operational expenses and customer churn – all of which ultimately improves an organization's bottom line. Not only are you limiting your risk of a costly data breach by deploying a tokenization solution, but you can also reduce, and even remove systems from the scope of your annual PCI audit, saving you time and money. Utilizing a tokenization technology enables companies to:

•Eliminate Systems from PCI Audit Scope

•Minimize PCI compliance Costs

point along the transaction – while it is at rest and in transit.
•Drastically Reduce Risk

•Secure Personally Identifiable Information

An additional option some companies are turning to in order to protect themselves from breaches is the purchase of insurance. Last year, cyber insurance policies sold to retailers, hospitals, banks and other businesses jumped 20 percent, according to Marsh LLC, a New York insurance brokerage firm that tracks the market. But companies should be very aware of what the policy covers as many might not cover all of the costs and risks a company faces. Credit card companies, for example, often sue the organization that has been hacked for the cost of all the consumer card replacements that need to be issued. Some policies don't cover this expense.

The bottom line? Businesses must look at data breaches not from the "if," but from the "when" perspective. It's time for executives in every branch of the C-suite, in every industry that takes cards-not-present payment from customers or that handles sensitive PII, to pay attention to the potential loss of business, the compliance requirements and both short and long term risks of a data breach. The statistics show that data breaches are not going away and likely may continue to rise. Protect your business and sleep better at night by finding the right partner to keep your company safe.

Source URL (retrieved on *09/03/2014 - 4:08am*):
http://www.wirelessweek.com/articles/2014/04/thieves-plain-sight-no-one-immune-data-attacks