Ensuring Compliance with Data-centric Security: a Primer

CONTENTS

Introduction 2

Standards and Regulations Driving Change 4

> GDPR3 4

> PCI DSS 5

> HIPAA 5

> NIST 800-53 6

Data-Centric Security 7

> Tokenization 7

> Encryption 7

Conclusion 8

About the author 8

Introduction

Over the last 20 years, the way people find and consume information has changed significantly, thanks to the internet. Digital connectivity has become so widely adopted that many take it for granted as they would electricity or indoor plumbing. Prominent newspapers are considering discontinuing their print publications in favor of digital media. Many children today have never used or even seen a print encyclopedia and instead choose online resources such as Wikipedia or Google when searching for information. Despite the obvious advantages of digital connectivity, there are pitfalls that cannot be underestimated, such as the risks posed to sensitive data. Everything online is hackable; if information is on a computer connected to the internet, it is vulnerable.

High profile data breaches have recently become a reoccurring theme in the news. In the last few months, the TSA, Verizon, Equifax, the NSA, Uber, the CIA, the US Air Force, Deloitte and Alteryx, among many others, have all lost billions of sensitive data elements. In most cases, individuals whose data had been lost did not consent or know that their personally identifiable information (PII) was stored by these organizations.

Upon closer examination of the Equifax and Alternyx breaches it is evident that nearly every adult living in the United States may have been impacted. Equifax lost 140 million records and Alteryx lost 123 million records, each of which contained Personally Identifiable Information about US citizens. Compared to the U.S. Census Bureau's estimate of approximately 248 million adults living in the United States, more than half were affected by the Equifax breach alone.

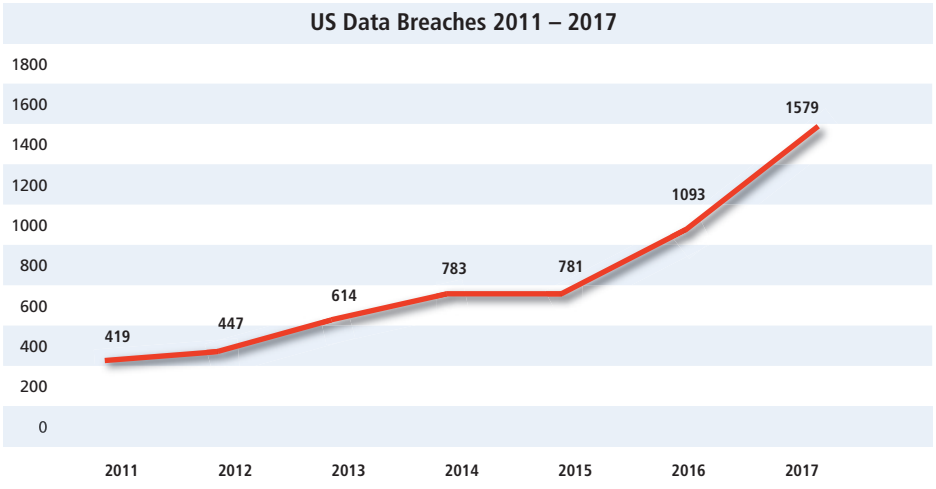
Everything online is hackable; if information is on a computer connected to the internet, it is vulnerable.

Introduction

The latest threats to data security, Meltdown, Spectre, Ryzenfall, Masterkey, Fallout and Chimera – enable hackers to steal sensitive information from a computer's memory or install malware during startup. These are an entirely new class of attacks and likely represent only the tip of the spear for this type of vulnerability. These flaws are seismic events because even though there are software patches being deployed by the CPU manufacturers, they are not perfect. A new generation of computer processing chips will be required to completely eliminate these flaws.

Every second of every day 59 records are lost or stolen. Leading analysts predict that by 2020, the average cost of a data breach will reach $150M. Since 2013, approximately 10 billion data records have been lost or stolen, of which only about 4% were encrypted or tokenized rendering them useless. The rest may very well be for sale on the dark web. In this environment, it is not a question of if you will be attacked, but when.

To help companies deal with these breaches, numerous standards have evolved over the last few years which describe how data should be protected. Legislators and industry leaders are constantly updating their standards and regulations as new threats and new counter measures emerge.



It is not a question of **if** you will be attacked, but **when.**

Standards and Regulations Driving Change

Data Security Standard V 3.2

Requirement 3.4

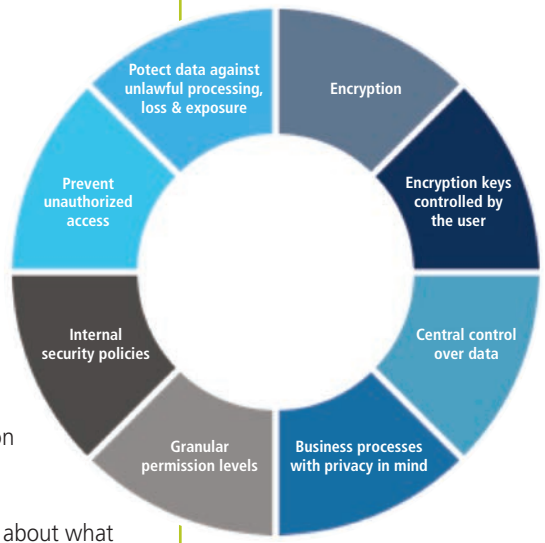
Render PAN data unreadable anywhere it is stored. Technology solutions may include strong oneway hash functions of the entire PAN, truncation, index tokens with securely stored pads, or strong cryptography.

General Data Protection Regulation

Article 32

Data Security measures should, at a minimum, allow: Pseudonymizing (tokenization) or encrypting personal data.

GDPR

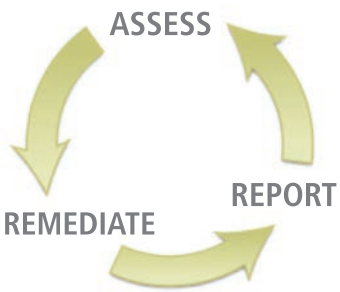


Starting on May 25, 2018, a new set of rules takes effect in the European Union that can carry significant financial consequences if organizations suffer a data breach without having taken the necessary preventative measures. These rules, called the General Data Protection Regulation (GDPR), define and strengthen the rights that EU residents have when they are impacted by a data breach.
Most corporations limit the data fields they consider sensitive to data elements such as name, address, date of birth, Social Security number and driver's license number. The GDPR Includes any data elements that can be traced to a specific person, including GPS data, genetic and Biometric data, browser cookies, mobile identification identifiers (UDID and IMEI), IP addresses, MAC addresses and application user IDs, among many others.

Additionally, the GDPR will require corporations to provide information to their users about what personal data they collect and how it is processed. Any data they collect must be managed in a way that ensures the privacy of that data. Companies with over 250 employees will be required to have a Data Protection Officer (DPO) who will be responsible for securing a corporation's data assets. The GDPR has substantial penalties for companies that experience a data breach with minimum fines of €10 million or 2% of its gross sales worldwide, whichever is higher. Once the GDPR goes into effect, companies will need to either encrypt or tokenize almost all of their data to be compliant (Data protection by Design and by Default). They will need to be able to remove a user's data upon request, known as the right to erasure, or face fines and public backlash.
While the GDPR requires companies to completely overhaul their data security strategy, it will make the general public much safer. GDPR requires companies to document their security controls and to demonstrate that they are compliant with them. Corporations will need to proactively monitor, detect and defend their data assets.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that process, store, or transmit credit cards. The PCI standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council.
The standard was created to increase controls around cardholder data to reduce credit card fraud. Requirements 3.3 and 3.4 are of particular interest as they directly discuss how credit card numbers, referred to as Primary Account Numbers (PAN), can be used.



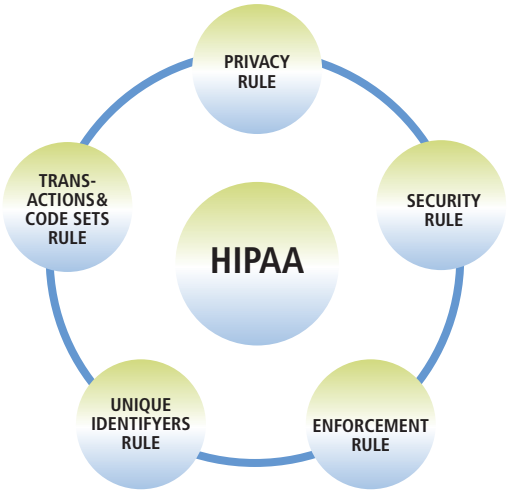
Requirement 3.3 states: Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the of the PAN.

Requirement 3.4 states: Render PAN unreadable anywhere it is stored (including on portable digital media, backup media and in logs).

Industry best practice is to tokenize the PAN which allows a business to perform the tasks that it deems necessary while protecting the card number.

HIPAA

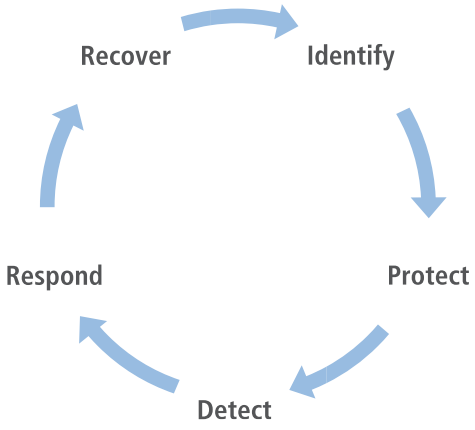
The United States Health Insurance Portability and Accountability Act of 1996 (HIPAA) established standards to protect individuals' medical and personal health information. It applies to health plans, health care clearinghouses and health care providers that conduct transactions electronically. HIPPA requires companies that deal with personal health information to fully protect those records from unauthorized access while at rest and in motion. Since 2015, over 200M patient records have been lost.



NIST 800-53

In the United States the National Institute of Standards and Technology (NIST) has issued standard 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations, a 450-page document that has a simple and logical framework to help prioritize and address key risks. The five main points of this framework are:

1. Identify – Asset, Governance and Risk Management
2. Protect – Access Controls, Training, Processes and Policies
3. Detect – Monitoring, Event Management and Detection Processes
4. Respond – Analysis, Communications and Mitigation
5. Recover – Improvements, Communications and Planning



While all 5 points of the framework are important, number 2 – Protect, is the one that many companies struggle with. If the data is properly protected, the consequences of a data breach are greatly reduced.

In most cases, data breaches are not a result of neglect on the part of the affected organization. Malicious actors are constantly devising new methods to gain unauthorized access to sensitive data and it is extremely difficult for risk analysts to detect every possible vulnerability and foresee which will be exploited and how. Digital connectivity affords many advantages over paper based file systems, but it also requires significantly more security measures. The best approach is a layered defense with tokenization and encryption at the core.

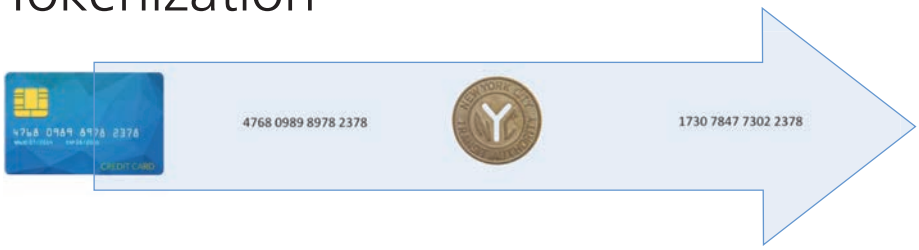
Tokenization replaces sensitive data with random characters and preserves the format of the original data element. The token has no value, if a data breach does occur the tokenized data elements are worthless to the thief.

No matter how many cyber-attacks you manage to prevent, you can never assume you are stopping them all.

Data-Centric Security

Data-centric security is an approach to security that emphasizes the security of the data, rather than the security of the networks, servers or applications where the data lives. There are two common methods used to protect data: tokenization and encryption. Tokenization replaces the sensitive data with tokens that are meaningless without compromising security. Encryption renders the data useless without the key that was used to encrypt it. Companies should use both tokenization and encryption to protect their digital assets.

Tokenization



Tokenization allows for the preserving of the characteristics of the data
such as the type (numeric, alpha, alphanumeric) and length, which makes implementation easier.

Encryption

Encryption does not preserve the format of the data, so it requires more computer processing resources to implement, such as field size changes, encrypting/decrypting when the data is used, adding a hash to be able to search the data, etc.

Data is a critical asset that crosses traditional boundaries (on-premises, hybrid and cloud) and requires a scalable, fault-tolerant solution that can both tokenize and encrypt it to ensure that it stays protected. Once data has been properly protected, a corporation maintains its regulatory compliance while protecting it from hacking, fraud and ransomware.
With both the PCI DSS and GDPR requiring security measures such as tokenization, one company, comforte, has emerged as having best in class solutions. They enable organizations to integrate business applications without having to rewrite existing applications, while also providing intelligent APIs. Their sophisticated and flexible framework allows multiple layers of data protection for both new and existing applications. In many cases, data protection can be achieved without any application changes.

For a real-word example of how comforte's products work, you can find a success story at: https://comforte.com/resources/success-stories/success-story-article/global-payments-technology-company-achieves-pci-compliance-and-protects-the-data-of-their-customers/

Conclusion

No matter how many cyber-attacks you manage to prevent, you can never assume you are stopping them all. Data security technology and regulations are constantly evolving to confront the dynamic threats to sensitive data. As with all forms of security, a multi-layered approach is the best method to prevent breaches. For enterprise data security, tokenization and encryption are proven tools for protecting the center of a multi-layered approach.

About the Author

Marty Edelman has been involved in the IT field for more than 30 years. As an independent consultant, he founded a small consultancy firm that specialized in developing high-volume mission-critical solutions for Fortune 500 companies. He and his team built the UPS Tracking System, the NYSE Consolidated Trade and Quote systems, and the S.W.I.F.T. next-generation computing platform.

While at The Home Depot, the world's leading home improvement retailer, he was the leader of the interconnected payments team and helped to introduce modern software development practices to the IT team which produces software used by over 300,000 associates and millions of customers. Furthermore, Marty was responsible for all aspects of payment processing (credit, debit, gift card, check, and PayPal) and accountable for ensuring that the organization's payment infrastructure was fully PCI compliant and secure.