SECURITY BY DESIGN:

Defending our clients by protecting their clients

Cybersecurity breaches are a common news report. Recent highly publicized cybersecurity breaches include Target, Sony, Home Depot, Heartland, Equifax, Marriott-Starwood, and countless others. Businesses that have been fortunate to avoid a cyber breach to date should be careful to not confuse luck with properly vetted and implemented cyber breach protections. For a majority of businesses, their current cybersecurity posture is based more on the former than the latter, and it is likely only a matter of time before the business joins countless others that have suffered a cybersecurity breach.

RIXON TECHNOLOGY

The risk of a cybersecurity breach and the significant financial costs of such a breach should not be taken lightly. As of 2019, the global economic cost of cybercrime exceeds ***six trillion dollars***. Security vendors leverage the fear and shock of these highly publicized security breaches, and many businesses reflexively spend millions of dollars on new security technology, which they have been led to believe would have prevented the breach from happening to them.

The reality is that cyber-defense is an ever-moving target that requires multiple layers of prevention and continual upgrades to existing cyber barriers. To suggest or guarantee that any single cyber tool or solution will keep a business free from a cyber breach is naïve and reckless. It is important for organizations to recognize that the status quo in cybersecurity will not likely be effective. As technology is always advancing, so too are the many methods in which a cyber breach may occur. Security budgets should regularly be re-analyzed to ensure such spending remain proportionate to the serious cyber breach risks facing the organization and its customers.

Such preparation requires recognition by organizations that the cyberworld currently exists in an "already hacked" state. Cyber fraudsters are more sophisticated and resourceful, and have access to faster, more damaging cyber breach tools than ever before. The increasing reliance on Cloud platforms and the ever-growing demand for "anywhere/anytime" access, cyber fraudsters and criminals are presented with a virtual playground of opportunities to exploit. It is also important to note that research is increasingly revealing that existing and former employees are often responsible for cyber theft. Thus, building cyber walls and investing in increased cybersecurity solutions may enhance protection against outsiders, but such protections do not address the vulnerability from internal threats that may have already compromised existing cybersecurity measures.

MARKET DRIVERS

The cost of not protecting your organization can critically terminate business continuity. For instance:

In 2019,
43% of breach victims
were small businesses
of <250 employees.

More importantly, 60%
of small businesses *that experience a data breach incident, or cyber-attack*
are out of business within
6 months of such a breach.

Thus, to a smaller and medium-size organization, a data breach is usually an extinction event.

REALITY

Far from a scare tactic, the reality is that there is a high probability an organization will experience a cyber breach. The question is not ***if*** such a breach will occur, but ***when*** such a breach will occur.

ECONOMIC REALITY

Organizations that fail to meet a minimum threshold of cybersecurity preparation and safeguards can reasonably anticipate massive fines in the event of a cyber breach. Such breaches often result in significant financial losses, as well as the loss of jobs by the organization.

SECURITY OBSTACLES

A major obstacle in protecting against cyber breaches is the fact that such breaches can occur from multiples sources, both external and internal, to the organization. This reality that vulnerabilities can arise from all directions creates a genuine challenge for organizations, particularly when resources are limited.

RECENT HIGH-PROFILE EXAMPLES

$2.2 BILLION in penalties

EQUIFAX **$4 BILLION** in fines and losses

Average cyberattack **cost for a business** **$369,000**

of all small companies attacked in 2019 **47%**

of all medium companies **attacked in 2019** **63%**

Damage related to **cybercrime** is projected to hit **$6 TRILLION annually by 2021**

According to the University of Maryland, **Hackers attack every 39 SECONDS,** on average **2,244** TIMES A DAY

Breaches are getting both more frequent and more severe. *In the first 6 months of 2019 alone,* **3,813 breaches** exposed **4.1 BILLION RECORDS**, *including 3 of the top 10 largest breaches of all time.*

The *global average cost* of data breach in 2019 was nearly $4 MILLION. in the U.S., the average cost of a breach was **over $8M.**

Of the 1,000 IT leaders polled for Invincea's *"2016 Cyber Threat Defense Report,"* three-quarters reported that their networks had been breached in the last year, and **62 PERCENT** said they **expect to suffer a successful cyber attack** at some point this year.

Worldwide spending on cybersecurity is forecasted to reach **$134** BILLION IN 2022

Many data breaches are caused by readily curable cybersecurity weaknesses, such as weak passwords or a lack of essential security awareness within an organization. However, even when such weaknesses are addressed within an organization, a large percentage of ***cyber breaches also arise from the failure to take broader internal and external measures to protect an organization's data.***

OTHER MARKET DRIVER

Compliance Rules and Laws

NIST

ISO
(International Organization for Standardization)

CIS. Center for Internet Security®

HIPAA

PCI-DSS (The Payment Card Industry Data Security Standard)

GDPR (General Data Protection Regulation)

CALIFORNIA CONSUMER PRIVACY ACT

COBIT
(Control Objectives for Information and Related Technologies)

SOX
Sarbanes-Oxley

FISMA
FEDERAL INFORMATION SECURITY MANAGEMENT ACT

GLBA
(Gramm-Leach-Bliley Act)

FedRAMP
Federal Risk Authorization Management Program

COPPA
(Children's Online Privacy Protection Rule)

FERPA
Family Educational Rights & Privacy Act

Organizations must comply with Privacy Laws and compliance standards, accepting this as the cost of doing business. Determining which rule and regulation apply to the unique needs of the organization is no easy task. Rixon Technology compresses the compliance footprint by converting the data into a useless token outside the service provider's environment, which in the simplest terms removes the data from the scope of the law or compliance rule.

WE ARE CUTTING THE COST
OF SECURITY, COMPLIANCE, AND AUDITS.

CYBERSECURITY CHALLENGES AND THE HISTORICAL APPROACH

Analyzing and choosing between the multitudes of data security platforms solutions can be exhausting for an organization. Traditionally, the compromises most organizations face when deciding between products are cost, ease of implementation, and impact on existing information technology systems.

ENCRYPTION

A number of data security platforms and enterprise systems offer encryption as part of their built-in data security strategies. This strategy is in place for good reason, as encryption is well researched and documented, is easy to implement, and can transparently be applied to significant technology layers such as databases and transport protocols. Today, SSL encryption is a standard tool used to protect information transmitted on the Internet. Using built-in encryption capabilities of operating systems or third-party encryption tools, millions of people encrypt data on their computers to protect against the accidental loss of sensitive data through potential theft. ***Encryption is not without its drawbacks, however, the most significant of which is that encrypting data within applications can interfere with the application's functionality such as sorting and searching.*** Because ciphertext is in a different format from the original data, encryption may also break field validation if an application requires specific formats within fields such as payment card numbers or email addresses.

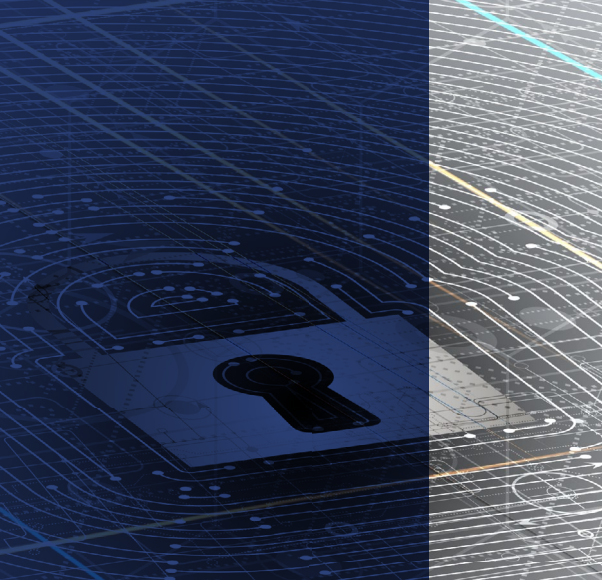
TOKENIZATION

Another data security option that has recently gained adoption is tokenization. Tokenization is the process of turning a meaningful piece of data, such as an account number, into a random string of characters called a token that has no useful value if breached. Tokens serve as the reference to the original data, but cannot be used to guess those values. That's because, ***unlike encryption, tokenization does not use a mathematical process to transform sensitive information into the token. There is no key or algorithm that can be used to derive the original data for a token.*** Instead, tokenization uses a database, called a token vault, which stores the relationship between the sensitive value and the token.

The back-end systems of many organizations rely on Social Security numbers, passport numbers, and driver's license numbers as unique identifiers. Since this unique identifier is woven into these systems, it is very difficult to remove these identifiers from the system. These identifiers are also used to access information for billing, order status, and customer service. Increasingly, tokens are being used to secure such types of confidential or personally identifiable information, including Social Security numbers, telephone numbers, email addresses, account numbers, and so on. **Tokenization offer a way to protect confidential and personally identifiable information, while maintaining the functionality of back-end systems without exposing critical data to cyber attackers.**

Historically, tokenization-based security solutions are implemented as a "Vault." Vaulted tokenization uses a database, called a token vault, which stores the relationship between the sensitive value and the token. The real data in the vault is then secured, often via encryption. Swapping values between tokens and the actual values is merely a matter of retrieving the matched value from the token vault. In practice, however, this extra lookup can require more changes to existing technology systems. Also, vaulted token database solutions encounter scalability and performance issues as the database grows and replication is needed to serve a global audience. Lastly, major concerns linger over whether ultimate data security is achieved with a token that is mapped to a stored value in a different database. In other words, ***is data really secured when it has only been moved to a different, potentially breachable location?***

RIXON TECHNOLOGY



THE REALITY IS that the cost and legal impact, including reputational damage that arises from a data breach, affects the whole organization. Rixon's solution solution offers a revolutionary enterprise vault-less SaaS tokenization solution that does not require an organization to re-engineer or rewrite software, nor require an organization to restructure databases or modify the overall enterprise architecture. The solution offers tokenization capabilities in a way that genuinely addresses data security concerns. The organization's data is not merely transferred from one location to another, such as a vaulted solution. With Rixon's solution, data resides in your architecture and is transformed in such a way that it is useless to those who improperly access it.

RIXON TECHNOLOGY offers patented cloud-based security solution that secures data from unauthorized access, compressing the compliance and security cost to an organization, and is transparent to the authorized user.

OUR PROCESS replaces raw data with tokens. Token architecture is defined and controlled by the client's security & risk tolerance requirements. As a result, only authorized users and applications can access secure data through a multi-factor configuration process.

Vault-less | Format-preserving | Multilingual | Global availability of solution | Smart tokenization | High-speed (2.5+ million tokens per second) | 99.99999% reliability | Seamless | Customizable | Scalable | Transparent to the authorized end-user or application | Configurable Masking

WANT TO LEARN MORE?

United States Contact: 2591 Dallas Pkwy, Frisco, TX 75034

www.RixonTechnology.com

info@RixonTechnology.com
sales@RixonTechnology.com

972-377-0049