TOKENEX

WHITEPAPER

TOKENIZATION FOR INSURERS AND INSUREDS

Resolve your exposure to cyberattacks and optimize your insurance protection

CYBER INSURANCE PRIMER

Cyber risks are not new—they have been around for more than two decades. However, it is only in the past five years that they have become one of the top threats to a company's survival. The frequency of incidents and their related severity are increasing and are driven by a number of factors, notably:

- Modern organizations' reliance on the collection and processing of sensitive data has grown exponentially with no signs of slowing.
- Data is no longer measured only by its financial loss value, but also by its extortion value.
- The ongoing battle between cybersecurity and cybercrime has become profitable for both sides.
- Ineffective data security continues to leave organizations exposed.
- Although cyber insurance protects policyholders, it can unintentionally motivate and reward hackers and other cybercriminals.

The types of threats, who is attacked, and to what purpose is constantly evolving with increasing creativity. Digital transformation has driven the enterprise to be increasingly connected via cloud migration, with integrated services and IoT causing the amount of data consumed to skyrocket. This has increased both the surface area and the incentive for attackers. An organization could be hit by malware, ransomware, social engineering, or hijacking, potentially denying it access to its own data. These attacks could come simply through emails (BEC) or by direct breach of a company's own systems despite having what was thought to be adequate firewalls, antivirus software, threat-detection management, and overall security best practices.

Importantly, the target of these types of attacks is primarily the organization's data—and not just the data used by the business to run its operations. The third-party data constantly flowing through its systems as it transacts business in this modern structured data environment is also a target.

And the risk doesn't end there. This customer and employee data—whether personally identifiable information (PII), personal health information (PHI), non-public personal information (NPI), or other sensitive data types—is also increasingly the subject of global privacy regulations such as the European Union's General Data Protection Regulation (GDPR) and the United States' California Consumer Privacy Act (CCPA). This means the impacts of a breach transcend the disruption of business operations and enter into the regulatory heighted arena of legal liability.

RANSOMWARE HAS BECOME THE NUMBER ONE CYBER THREAT TODAY AND IS A VULNERABILITY ACROSS ORGANIZATIONS OF ALL SIZES

There is a growing body of publicly available data that provides deeper insights into who is targeted and what the average cyber losses look like for each of the main threat categories we describe later. At a high level, we note:

- Although the larger public enterprises experience greater losses and attracts media attention, the threat has silently turned to small and medium enterprises (SMEs) that possess valuable customer data but are less protected than their larger counterparts.
- 96 percent of claims originate from SMEs (annual revenue less than $2 billion)[1]
- Ransomware has become the number one cyber threat today and is a vulnerability across organizations of all sizes, but it increasingly targets smaller companies rich in third-party data.
- Large corporations experience significant brand damage which cannot be adequately measured or compensated by insurance.
- Regulatory advancements bring compliance costs and potential fines that go beyond what is insurable.
- Although the impact of COVID-19 on the insurance market is debated, there is consensus it will only add to the frequency and severity of ransomware, social engineering exposures, and the need for enhanced levels of data protection.

- A number of independent major studies have identified data protection as one of the leading measures to reduce the severity of losses from a data breach. Encryption is the oft-cited measure, but tokenization is demonstrably more secure.

- The U.S. consistently has the highest cost per data breach in the world at more than $8 million per incident.[2]

As previously mentioned, and further elaborated on later, these risks exist because either an organization's own data or its third-party data traverses its systems as part of a larger supply-chain offering. When this data is compromised at any level, the windfall of consequences is swift and severe, with the use of encryption or segmentation providing insufficient protection in the modern era. See "Tokenization vs. Encryption" comparison on pg. 8

Before we focus on cyber-specific insurance, it is essential to understand that the impact on any company from a cyberattack cannot be measured or met by cyber insurance alone. Aside from any form of self-retention (like a deductible), cyber incidents often result in additional losses from:

- Business interruption and loss of income
- Recall costs
- Notification costs
- Professional E&O claims
- Supplier and partners lawsuits against the organization
- Directors & officers lawsuits
- Long-term reputational brand damage
- Regulatory review costs and potential fines

The claims placed on these other insurance policies can often be multiples of the cyber insurance policy losses. It is important to consult with your broker to ensure these other policies will respond to your cyberattacks and that your cybersecurity plan accounts for the broad impact of financial losses that can result from a breach.

THE CYBER INSURANCE MARKET

As a result of the increasing levels of vulnerability alongside the increasing numbers of threats facing organizations, the cyber insurance market is responding with equal measures of enthusiasm and apprehension. Insurance providers recognize the incredible opportunity presented but struggle to quantify the risk to the same level of comfort of more longstanding conventional risks.

U.S. CYBER LOSSES INCREASED FROM **$18 MILLION** IN 2001 TO **$3.5 BILLION** IN 2019

As a result, global cyber premiums have been increasing at over 20 percent per year for the past three years, and estimates for 2020 global premiums indicate they could be closer to $8 billion[3]—representing a 30 percent growth over 2019. Additionally, the United States typically accounts for over 50 percent of global premiums.

And yet, the problem continues to grow. According to U.S. Government records (IC3), U.S. cyber losses increased from $18 million in 2001 to $3.5 billion in 2019.[4] Meanwhile, cyber-related losses more than doubled in two years from 2017 to 2019. Clearly, the cyber insurance market is still unsure if conventional cybersecurity measures are able to assess, quantify, and control the rapid expansion and creativity of cyber-related crimes.

This isn't entirely surprising, as the statistics surrounding the costs of a cyber incident are staggering. Some additional figures include:

- Insurance press regularly estimates ransomware alone will exceed 2019 losses.
- The average cost of a data breach is **$8.19 million** in the U.S. and **$3.92 million** around the globe.[2]
  - The average size of a data breach is **25,57**5 records.
  - The average cost per record lost is **$150**.
- The cost of responding to an incident often exceeds the actual financial loss of the incident itself.

Although the size of company tends to dominate the statistics, of equal importance is recognizing that certain industries' data is more attractive and therefore targeted more frequently by cybercriminals. These include companies working in or with organizations, from these industries:


FINANCIAL INSTITUTIONS


BUSINESS SERVICES


RETAIL & WHOLESALE


TECHNOLOGY


HEALTHCARE


MANUFACTURING

Notwithstanding the growing issues with cyber risks, all the major insurance brokers and some specialized cyber-focused brokers have dedicated teams and expertise to help navigate the market, which has most of the world's major insurers fully engaged. These include:

AIG
ALLIANZ
AXA
AXIS INSURANCE
BCS
BEAZLEY
BERKSHIRE HATHAWAY
CHUBB
CNA
LIBERTY MUTUAL
MUNICH REV
SOMPO INTERNATIONAL
TRAVELERS
XL
ZURICH INSURANCE

WHAT IS YOUR RISK PROFILE?

Adopting a logical, systematic process for evaluating and managing your cyber exposure and then leveraging that information to procure an appropriate policy is critical to your business. Cyber insurers and brokers will either help you in this assessment or expect you to have done so as a prerequisite to purchasing cyber insurance.

Organizations and public entities of all sizes need to address and understand their exposure to cyber risks. The key characteristics of a cyber risk profile are:

- The volume of personal data related to employees and customers that flows into, or is retained by, your organization.
- The sensitivity of personal data related to employees and customers that flows into, or is retained by, your organization.
- The organizational or business dependency on said data.
- The complexity, integrity, and connectivity of technology required to enable the flow of data in your end-to-end supply chain.
- The extent to which you operate in a regulated industry (e.g., financial, healthcare, etc.) or are subject to privacy-related regulations such as GDPR, CCPA, or other similar laws.
- Contractual cybersecurity requirements by your suppliers or customers.
- The potential impact on your business from the failings of your partners' or suppliers' security technology.
- The efficacy of your own IT security. This includes any compliances or certifications with existing data security frameworks such as NIST or ISO, or adherence to the data security frameworks contained within compliance regulations like PCI DSS, CCPA, GDPR, or HIPAA.

Estimating the likely losses your business could experience under each of the risk profile categories (above) will help determine the range of cyber insurance you require and the related limits you should purchase. See pg 9 "Impacting the Cyber Insurance Line with Tokenization"

Further, a thorough risk assessment of your entire IT environment and the internal systems within is valuable in addressing your organization's overall cybersecurity needs. In terms of data storage, processing, and transmission, a cloud tokenization provider such as TokenEx can present an excellent opportunity to understand your data security risk and strategize your approach to reducing exposure to this risk.

TOKENIZATION FOR CYBER RISK REDUCTION

As previously covered, the central issue of cyber risk is the data obtained, stored, and processed by organizations and is the oft-cited measure of the severity and associated cost of a breach. Upon a breach, personal data is often what is accessed and held ransom. It creates the basis upon which regulatory fines are levied and is the subject of expensive and damaging breach-notification requirements. Regardless of the way in which an organization was compromised, it is ultimately the exposure of sensitive data that presents the greatest liability risk.

This reality often puts organizations in the difficult position of choosing between data security and business utility. The visibility and processing of data is required to conduct operations, but paradoxically, it also presents the greatest threat. A common method employed to mitigate this situation is the use of encryption. Although encryption methods can be employed with varying levels of security effectiveness, this presents organizations with another set of problems such as format retention (preserving certain elements of the data) and key management. Poor key management can be an organization's complete undoing if done incorrectly, as it is the proximate cause for many ransomware extortion attacks.

TOKENIZATION		ENCRYTPION
Removes sensitive data entirely swapping it with a mathematically unrelated "token"		Uses complex algorithms to obfuscate sensitive data
Uses a secure database to vault sensitive data, which can then be retrieved according to the token issued		Requires a "key" to decrypt cipher text back into its original form
Cannot be reversed		Can be reversed if key is intercepted or discovered
Advantage is ease of use	VS	Advantage is securing large or unstructured data sets
Reduces PCI DSS, HIPAA, GDPR, GLBA scope		Does not reduce PCI DSS, HIPAA, GDPR, GLBA scope
Secures structured data		Secures structured or unstructured data
Increased business-enablement via analytics		Presents business-as-usual difficulties
No keys required		Key-management required

Unlike encryption, tokenization presents the possibility of removing the sensitive data from the organization's environment entirely, virtually eliminating the risk of data theft and significantly reducing the potential impact of a breach in the event that one occurs. Encryption, however, can be reversed if the keys are revealed in a breach or if they become decrypted via a brute-force attack. Conversely, properly tokenized data is irreversible. If this technology is deployed with a cloud-based third-party vendor, the original data sets can even be securely stored offsite, rendering them inaccessible to any malicious parties.

TOKENIZATION PRESENTS THE POSSIBILITY OF REMOVING SENSITIVE DATA FROM THE ORGANIZATION'S ENVIRONMENT ENTIRELY

Although encryption is a useful tool for data in transit (encrypting it before it's sent to a third party for decryption), encrypting data at rest (data stored for the long term in servers) isn't as effective. The ultimate weakness of encryption is that when the decryption keys are obtained or deciphered, this instantly gives the malicious party full reign over the organization's most sensitive data, allowing it to be intercepted, copied, or erased. This unfettered access to sensitive data gives hackers the leverage they need to make extortion demands.

Proper deployment of format-preserving tokens, on the other hand, to replace the sensitive data stored by modern organizations can significantly reduce the impact of a breach while retaining key aspects of the data that are required for analytics, processing, and other forms of use internally or with third parties. This reduction of risk can present a measurable positive impact on the limits, conditions, or pricing of a cyber policy.

IMPACTING THE CYBER INSURANCE PRODUCT LINE WITH TOKENIZATION

Historically, the market responded to cyber claims as either damage to the insureds' own property (first party) or to defend and compensate them for their liability to other people or corporations (third party). Lately, however, the insurance market has responded to the

growing complexity of cyber threats to keep pace with the nature of the varieties of financial loss experienced by the victims of cybercrimes.

Because the cost of breaches and other forms of cyber exposure can so greatly differ depending on the industry, data type, category of cyberattack involved, and many other complex variables, it can be difficult to anticipate the financial repercussions of a breach and, as a result, accurately determine the terms of a policy and attribute damages for claims. Although the market has greatly improved in this regard—insurers' abilities to understand and respond to cyber incidents are better than they ever have been previously—there's still much uncertainty surrounding these complicated claims and coverage areas. However, that uncertainty can be addressed by using tokenization as a risk-reducing solution for the protection of sensitive data, organizations can better quantify the risk and preparation for cyber events.

As the market has evolved, it is better to view the insurance solutions based on the threat and related expenses or damages payable. **Here is each of these solutions, as well as the positive impact offered via tokenization:**

1. NEW WAVE RISKS

Extortion and Ransomware Coverage for costs associated with ransoms related to cyber intrusions into business systems. This can include a variety of costs: **The actual ransom paid.** **Costs to avoid paying the ransom.** **Costs to remove or reduce scale of the ransom.** **Costs to technologically negate the basis of the extortion.**	**How Tokenization Addresses it** Although tokenization does not prevent extortion and ransomware, it can significantly reduce or eliminate the leverage of the attacker by preventing any sensitive data from being accessed and held in exchange for a payout.
Social Engineering Coverage for losses associated with social engineering incidents including business email compromise (BEC)	**How Tokenization Addresses it** Tokenization restricts access to sensitive data to a select few employees on a need-to-know basis and with very stringent verification protocols, dramatically reducing the threat of social engineering and any resulting compromise.

2. EXPENSE AND INDEMNIFICATION COSTS

Replacement or Restoration Data Coverage for the costs to replace or restore data or programs lost or damaged by the incident.	**How Tokenization Addresses it** Properly tokenized data cannot be lost in the event of a cyber incident. When effectively tokenized and stored offsite, restoration is as simple as reissuing the existing tokens if lost or retokenizing the stored data for new token mappings.
Loss of Business Income Coverage for losses and costs associated with the inability to conduct business due to a cyberattack.	**How Tokenization Addresses it** Once the systems have been restored, business processes that rely upon the processing of sensitive data can largely continue immediately upon simple restoration of the tokens. This greatly minimizes downtime of business operations that rely on payment data or any structured PII or PHI.
Security Breach Coverage for losses and incident-recovery expenses such as forensic investigation or customer notification.	**How Tokenization Addresses it** An organization that has identified, located, and tokenized its sensitive PII is likely in compliance with privacy regulations such as GDPR, CCPA, and HIPAA. By the same rationale, if no customer data is revealed in the instance of a breach, no notification is required.
Post-Breach Remediation Coverage for costs to immediately remediate the security weaknesses and mitigate the loss.	**How Tokenization Addresses it** Although tokenization does not seek to directly prevent a breach of an organization's environment, it can act as a strong deterrent to those contemplating such an attack. Furthermore, it substantially mitigates the loss to the degree in which it is leveraged. Any structured data set, including PII, PCI, PHI, or any form of NPI, can be thoroughly protected from loss and then swiftly retokenized if desired to provide an additional layer of protection and peace of mind.
Public Relations Expenses Coverage for the costs to hire a public relations firm to restore reputation due to a cyberattack.	**How Tokenization Addresses it** Because tokenization protects sensitive data from exposure—even in the event of a breach—organizations leveraging tokenization can shield their customers and their brand from harm, potentially avoiding breach-notification requirements.

3. LIABILITY TO THIRD PARTIES	
Security Breach Liability Coverage for liability damages due to the insured's customers and other third parties because of cyberattack on the insured.	**How Tokenization Addresses it** If sensitive data collected from third parties is tokenized upon ingestion, the possibility of data exposure is eradicated, and the liability of storing the sensitive data is shouldered by the tokenization provider. This can vary based on implementation, but a thorough and well-architected tokenization solution can significantly reduce an organization's exposure to third-party liability.
Computer and Funds Transfer Fraud Coverage for the losses associated with a fraudulent transfer of money, securities, or other property (can be insured's and/or the liability to their customers').	**How Tokenization Addresses it** Fraudulent transactions as a result of a breach, whether ACH or traditional digital payments, require access to sensitive PCI or ACH data as well as the authentication data. If this data has been tokenized, with the tokens being the only values stored, the data required to execute these transactions would not be accessible to the attacker.

TOKENEX REDUCES CYBER RISK, ENABLES CYBER POLICIES

TokenEx is a cloud-based tokenization platform that enables its customers to safely and securely ingest any structured data type through a variety of channels, store it offsite, and securely share it with any third party. The TokenEx platform enables numerous business processes with format- and length-preserving capabilities and protects over 300 organizations, ranging from SME to multinational enterprises across the globe.

By leveraging the power of TokenEx's cloud-based tokenization, your organization can safely and confidently control your risk exposure, measurably lower your premiums across multiple insurance policies (see below), and protect your organization's reputation in a world of ever-increasing cyber risk.

BUSINESS INTERRUPTION AND LOSS OF INCOME

Preventing the loss or corruption of the data removes the resulting BI claims or limits them to minimal increased costs.

NOTIFICATION COSTS

Tokenized PII, PCI, PHI, and other structured sensitive data is protected from hackers. If a breach of your systems occurs, there is no loss of original sensitive data, and therefore, no notification is necessary.

PROFESSIONAL E&O CLAIMS

To the extent that these claims are relying on data that has been corrupted, they are avoided through tokenization of that data. Similarly, where professional firms are working confidentially with clients' data, the tokenization of that data prevents its criminal release to the public or competitors that would trigger the E&O claim. Consider eradicating the risk to consultants, lawyers, and accountants working in the M&A space or with upcoming confidential unreleased audited financial results that were captured by hackers.

SUPPLIER AND PARTNERS LAWSUITS AGAINST THE ORGANIZATION

Any flow of structured data to, through, and out of a company creates risk to the integrity of that data. Tokenization can protect the client and potentially be extended up and down the supply chain to everyone's benefit.

DIRECTORS & OFFICERS LAWSUITS

The natural consequence of any data corruption is a trigger to D&O claims. Avoid the data loss and avoid the D&O.

LONG-TERM REPUTATIONAL BRAND DAMAGE

Regardless of its insurance coverage, a breached company can experience catastrophic damage to its reputation and prosperity. Tokenization can protect that company from the negative impact of that breach, thus protecting it also from the reputational damage associated with it.

REGULATORY REVIEW COSTS AND POTENTIAL FINES

The growing focus on privacy and consumer rights is driving up compliance challenges and related costs. Failure to be compliant and the intentional or accidental release of protected data will bring fines, penalties, and public disdain. Tokenization can address many of these requirements simply by tokenizing the sensitive data in question, which de-identifies it to satisfy certain regulatory compliance obligations.

TokenEx is a solution and a partner in your data risk assessment and protection process. By working alongside our team of cybersecurity and compliance experts to focus on protecting structured data, you can resolve your exposure to many forms of cyberattacks and optimize your insurance protection.

[1]NetDiligence Cyber Claims Study 2019 Report. (n.p.: NetDiligence, 2019), PDF ebook, 5.

[2]IBM Security Cost of a Data Breach Report. (n.p.: Ponemon Institute, 2019), PDF ebook, 3.

[3]2019 Global Cyber Risk Survey. (n.p.: Marsh and Microsoft, 2019), PDF ebook, 22.

[4] "Amount of monetary damage caused by reported cyber crime to the IC3 from 2001 to 2019 (in million U.S. dollars)," Statista online, March 27, 2020, https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/#statisticContainer.