SOSA The Open Innovation Company. | FinTLV

InsurLab Germany

Protecting Today's Digital Consumers Report

Prepared in collaboration with
InsurLab Germany Gmbh

FEBRUARY 2023 | CONFIDENTIAL

SOSA | FinTLV

Table of Contents

00

Introduction

The speed and adoption of digital technology since the turn of the 21st century ushered in a new era for consumerism. Last year alone, digital commerce in Germany totaled a record EUR 141B, a figure projected to continue to increase at a CAGR of 11.5% through 2025.

The migration to a digital-first economy was already in full flight prior to the arrival of the COVID-19 pandemic. However, dependency on digital services skyrocketed when the pandemic struck in early 2020, a natural consumer response to lockdown mandates and social distancing guidelines. Unsurprisingly, with that rapid growth in digitalization, came an equally unprecedented increase in cyber crime. By the end of 2020, malware attacks had increased by 358%, according to data from the World Economic Forum.

More recently, a study by PwC reported that nearly 46% of businesses have experienced instances of fraud since the start of 2021, with cyber-based fraud reported as the most prevalent.

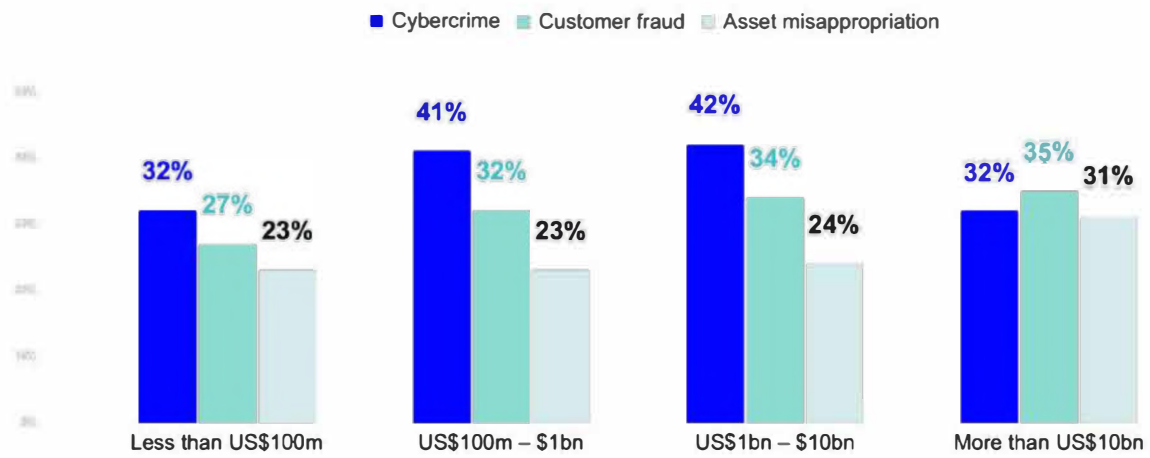


Figure 1:

Types of Fraud by Organization Size

Source: PwC's Global Economic Crime and Fraud Survey 2022

It is clear that as advancements in digital technology continue to materialize, a substantial investment will need to be made to combat the cyber crime that will inevitably follow. By understanding past cyber attacks, uncovering structural vulnerabilities, and investing in innovative technologies to prevent attacks, organizations can begin to build a roadmap that ensures the protection of their digital consumers.

Executive Summary | Key takeaways.

In this report, we discuss some of the steps that organizations, and the insurance industry in particular, can take to protect digital consumers from increasingly sophisticated cyber threats.

The report covers:

1. A case study analysis of recent cyber attacks across various major industries
2. Insights on relevant strategies and technologies to shore up an organization's cybersecurity infrastructure
3. Recommendations on how individuals can protect themselves and their personal data from cyber criminals
4. A showcase of innovative technology startups building the next generation of solutions to fight cyber crime

01
Cyber Threats in the Digital Era

A recent report analyzing corporate data breaches found that ransomware attacks grew by 13% YoY in 2022 - a troubling increase greater than the last 5 years combined. Identifying and analyzing the most prevalent types of cybercrime can help guide organizations through the process of auditing their own digital infrastructures, in an effort to identify known vulnerabilities that have been exposed at other organizations.

Below, we feature case studies of recent, well documented cyber incidents, spanning a wide variety of industries. Each case study reflects a unique vulnerability that was exploited by cyber criminals, and led to significant damages and subsequent reparations by the impacted organizations.

A. Industry Case Studies

Data breaches are one of the most common and lucrative tactics deployed by cyber criminals today. The healthcare industry is particularly prone to targeting by such attacks, due to the sensitive nature of the data that they host, and the consequences of that data getting exposed. Last year, the average cost of healthcare-related data breaches was USD 10M, according to a report from IBM. The financial sector ranked second, with an average cost of USD 6M, followed by pharma (USD 5M), technology (USD 5M), and energy (USD 5M). Stolen or compromised credentials were the most frequently exploited vulnerability that led to data breaches, which also took the longest time to discover - an average of 327 days.

Twitter | Social Media — December 2022

Vulnerability
Open API that lets computer programs connect with Twitter to collect data

Impact
→ 400M accounts compromised, including phone numbers and email addresses
→ Hacker demanded USD 200K to return the stolen data
→ Hacker also provided guidance on how the data could be abused by others to carry out similar attacks

Takeaways & Outcomes
Twitter (like all organizations who collect PII) are subject to Europe's GDPR privacy laws, and face much steeper fines should regulators find them liable for the data leak.

Medibank Australia | Insurance — October 2022

Vulnerability
Leaked credentials on a dark web forum

Impact
- → 3.9M customers' data exposed
- → Expected cost exceeding USD 35M
- → Delayed premium increases will cost approx USD 62M

Takeaways & Outcomes
Since Medibank did not have cyber insurance, the company is still liable for customer compensation and any regulatory or legal costs that may be incurred as a result of the breach.

25%
Increased mortality rate due to ransomware attacks

A 2021 study that surveyed over 600 healthcare facilities found that 25% of respondents reported increased mortality rates due to ransomware attacks.

University Hospital (Düsseldorf, Germany) | Healthcare — October 2022

Vulnerability
Ransomware introduced through well-known vulnerability in the hospital's Citrix application

Impact
- → Ambulances were turned away, leading to patient fatalities
- → 30 servers corrupted
- → Hospital was forced to cancel hundreds of operations and procedures, and capacity was limited to 50%

Takeaways & Outcomes
Healthcare is arguably one of the most important service industries, and the consequences of cyber vulnerabilities are grave. The enormous amounts of sensitive patient data stored in hospital computer systems must be protected. Medical devices that require internet connection are also at risk of being deactivated, compromising patient care.

Microsoft | Technology — March 2022

Vulnerability
SIM swap attack - a tactic where hackers steal phone numbers in order to gain access to other applications related to that individual and their personal cell phone numbers

Impact
- According to Microsoft, only one account was infiltrated, and no data has been obtained
- Microsoft's reputation maintained thanks to quick mitigation

Takeaways & Outcomes
This case study displays the value in proactive monitoring in order to actively mitigate risk and protect consumers. Microsoft's security team was well prepared, as they had been tracking the Lapsus$ organization and their previous attacks against other businesses. Microsoft took the additional step to educate its customers how best to protect personal data such as stronger MFA implementation, authentication of VPNs, and computer settings.

United States Colonial Pipeline | Oil & Gas — May 2021

Vulnerability
Exposed VPN password that led to a ransomware attack, shutting down the pipeline for a number of days

Impact
- Major gas shortages across the Southeast US and sharp increases in gas prices
- 100 GB of data leaked
- USD 4.4M paid in ransom (in Bitcoin)

Takeaways & Outcomes
Cyberattacks targeting critical infrastructure have demonstrated how devastating effects can extend far beyond an organization's digital boundaries. These institutions must be protected, as the cost of a cyber attack directly affects consumers and often national security.

B. Digital Consumers

While corporate cyber attacks tend to grab the headlines, attacks on individuals are just as, if not more prevalent in today's digital age. Targeting organizations may present a more lucrative opportunity for criminals, but individuals, who often lack the know-how to adequately protect themselves, are simply easier targets. Whether you're an employee, an individual, or a digital entrepreneur, it's essential to understand basic data security best practices, in order to protect yourself from unknowingly giving access to cyber criminals.

90%

of all cyber attacks are orchestrated through stolen and/or weak passwords.

Connected Employees

Following an analysis of 23k corporate data breaches, it was found that 82% of incidents involved human error in some shape or form.

Cyber criminals prey on unsuspecting individuals through a variety of means, including fraudulent emails or websites which appear legitimate, luring employees into giving away sensitive information. The attacker will often use the employee's data and compromised credentials as an entry point for malware distribution into an organization, posing a potentially crippling risk to the company's infrastructure. It's imperative that employees remain vigilant, and strictly adhere to their organization's security protocols in order to avoid these types of incidents.

Uber | Mobility — September 2022

Vulnerability
Hacker leveraged "social engineering" to convince an Uber employee to provide a password that gave hacker access to Uber's systems

Impact

- Hacker obtained access to Uber source code, email, and other internal systems, and reconfigured Uber's Open DNS to display images on internal sites
- Breach compromised several internal systems
- Uber was fined almost USD 150M for attempting to cover up the breach
- Uber's top security executive at the time was terminated and charged with obstruction of justice for failing to disclose the breach to regulators

Key Takeaway
Employee negligence was at the core of this attack. With proper protocols, processes, and guardrails in place, this instance may have been avoided.

Some basic best practices for employees to better protect themselves include making use of secure password generator tools (to avoid using easily guessable passwords), not repeating passwords across multiple accounts, not using easily or publicly findable data for identity verification purposes, downloading company sponsored anti-virus software, and leveraging anti-phishing tools to protect their inboxes from becoming the entry point for malicious actors.

42%

of seasonal passwords contained the word "summer"

Individual Users

From online banking, to social media accounts, and online dating apps, individuals are uploading unprecedented amounts of personal data online. This poses an obvious risk for individuals, and an opportunity for criminals to leverage that personal information to commit crimes. And while individuals are becoming more aware of the risks associated with disclosing personal information in digital settings, it's still imperative for individuals to properly educate themselves on how to best protect their data to avoid costly cyber attacks.

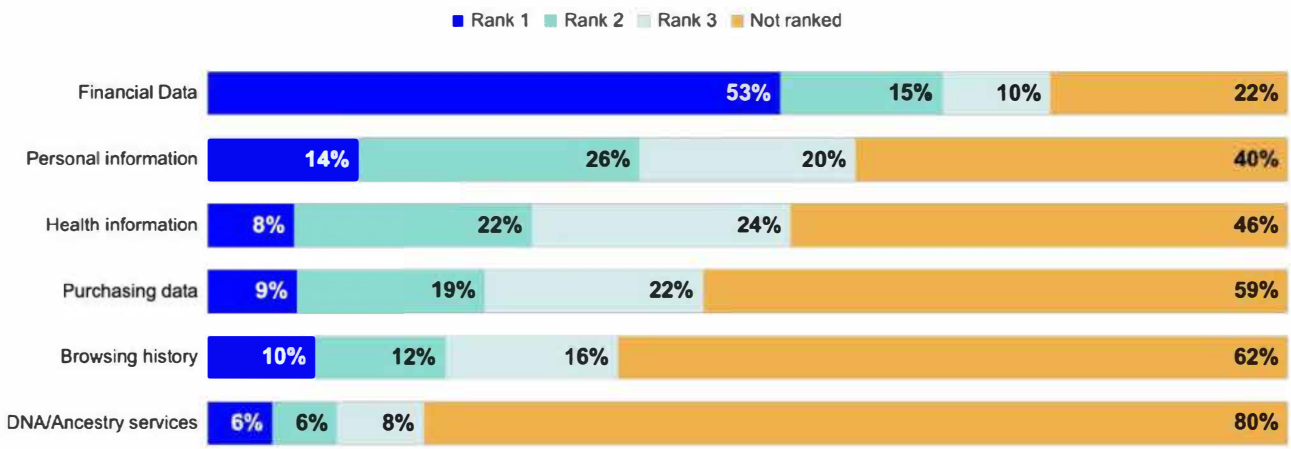


Figure 2:

Top 3 personal data breach concerns

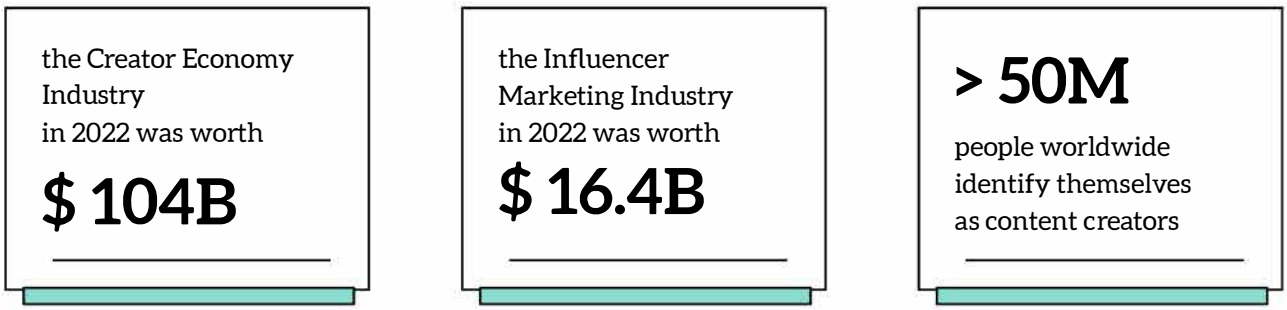
Source: Chubb - Fifth Annual Study on Personal Cyber Risk

According to a recent study on personal cyber risk conducted by Chubb, an increasing number of online users are beginning to implement security measures to protect their personal information and data from cyber attacks. While the progress is encouraging, best practices such as regularly updating operating systems, conducting weekly cloud backups, or using secure browsers, are still left behind by most users (see ch. 3 for specific recommendations for individuals to better protect themselves from cyber crime).

One practical means of protection in the event of an attack is cyber insurance. According to Chubb's above cited personal cyber risk study, of the 1.6k individuals surveyed across the US and Canada, 39% had a personal cyber insurance policy. An equal percentage, however, were unfamiliar with the concept of cyber insurance and what the policy coverages offered.

Digital Entrepreneurs - The Creator Economy & Influencers

Social media-based content creators and "influencers" have recently emerged as a popular trend across all of the major social media platforms. Owners of these well followed accounts can earn considerable income from sponsored content and paid placement of products.



Fraud is a growing concern within the influencer industry. Cyber criminals will either target the take over of established accounts, or generate fake accounts in an attempt to impersonate a celebrity or influencer.

Brands can leverage tools to validate influencer authenticity through detecting anomalies, such as rapid account growth or fake followers, in order to avoid engaging with fraudulent influencers.

In 2021, almost half of Instagram's influencer population was affected by fraud (49.2%), demonstrating how vulnerable digital entrepreneurs are to bots and fake accounts. Falling victim to these scams (crypto related, as an example) can cause irreparable harm to the individual's following and brand.

02
Building the Cybersecurity Infrastructure

The global fraud detection and prevention market, currently worth USD 25.6B, is expected to grow to USD 130B by 2029. The sheer size of the market and the amount of capital that has been invested to fund the next generation of cybersecurity companies, demonstrates the scale of what must be done to keep our digital society safe.

The following chapter provides an overview of existing cybersecurity approaches and technologies, which represent an integral part of the detection, response, and mitigation of cyber threats.

A. Zero Trust Framework

Zero Trust is a security framework centered around the principle of "never trust, always verify." In a zero trust environment, all users are required to be authenticated and authorized before being given access to data and resources, even if they are within the internal network of the organization.

This framework is a departure from traditional cybersecurity models, which assume that company data and assets within an organization's own network are safe by default. Traditional perimeter-based cybersecurity models distinguish "trusted" from "untrusted" communications based on elements like the office firewall and corporate LAN. Because those legacy systems do not address the full scope of security threats, they have since been rendered inadequate.

> Data from Security Intelligence shows that on average, organizations that turn to Zero Trust incur 20.5% lower costs resulting from a data breach than those that do not.

There are four key steps required by an organization to implement a zero trust security framework:

1. **Inventory**. Creating a record of all users, applications, devices, and other services, as well as the specific data and assets to which users have access, enabling the security team to create a unique and traceable identity for all users (internal and external) within the organization.
2. **Micro-Segmentation**. Dividing the network into "areas," each with its own set of access controls, thereby reducing the risk of an attacker infiltrating isolated parts of the network and moving laterally once inside.

3. **Multi-Factor Authentication (MFA).** Authorizing access based on multiple pieces of personal evidence: traditionally relies on information unique to the user (i.e. secret questions), devices possessed by the user (i.e. cell phones), and biometric indicators (i.e. facial recognition).
4. **Continuous, Real-Time Monitoring.** Integrating cyber detection and response solutions to promptly respond to breaches.

   → **AI-driven Endpoint Detection and Response (EDR)** software designed to automatically protect an organization's end users, endpoint devices, and IT assets from cyber threats that go undetected by antivirus software and other traditional endpoint security tools.

   → **AI-driven Extended Detection and Response (XDR)** solution that integrates security tools throughout an organization's hybrid infrastructure, including data from networks, email, applications, and cloud workloads, among others.

   > According to IBM, organizations that utilized XDR solutions decreased the time it took to identify and contain a data breach by one month, compared to organizations that did not use the software.

   → **Dark Web Monitoring** regular scans of the dark web to identify compromised information. Service allows organizations to set up real-time alerts triggered by specific keywords or phrases, allowing an organization to respond quickly.

   → **Phishing Blocking Solutions** phishing refers to criminals impersonating third parties in order to trick victims into disclosing personal information (i.e. bank accounts, passwords, credit card information, and other PII). Phishing blocking solutions scan incoming emails and identify suspicious senders or malicious links and attachments.

B. Digital Identity Verification

Digital identity verification refers to the process by which organizations seek to confirm that a digital individual is in fact who they say they are. A common tactic employed by cyber criminals is fraudulently impersonating an individual in order to gain access to their personal information. Digital identity verification tools seek to make committing those crimes more difficult.

These tools are especially critical for any organization subject to regulations such as KYCs (Know Your Client), and CDDs (Customer Due Diligence).

There are multiple approaches available today to verify digital identities, such as biometric verification, and tools to mitigate fraud, such as deepfake detection technology.

Biometric Technologies

Biometric verification leverages an individual's unique biometric traits to confirm user identity prior to gaining access to a protected network. Unique biometric identifiers can include:

→ **Fingerprint recognition** scans and compares fingerprints with previously recorded minutiae mapped samples.

→ **Facial recognition** ability to identify unique facial structures and confirm that the presenting face is in fact human (as opposed to a digital image or video frame).

→ **Iris recognition** high-contrast image of a person's iris in order to identify its uniqueness using visible and near-infrared light.

→ **Vein recognition** (or vascular biometrics) technique that examines blood artery patterns and assesses unique components of a subject's circulatory system by using optical scanning technology, recording vein images in a person's palm, finger, or eyeball (retina scanning).

→ **Voiceprint** examines a specific person's voice pattern and compares them with previously saved recordings.

Deepfake Detection

Deepfake refers to digitally produced images, videos, and audio files that are able to mimic real human traits. Driven by machine learning, deepfake technology can be used by criminals to commit crimes such as fraud, extortion, and identity theft.

While deepfake technology is still in its infancy, as it develops, it has the potential to severely compromise the cyber integrity of organizations and individuals alike.

→ **Deepfake detection technologies** utilize identification tools to examine picture and video files. APIs can be developed to stay current with the most up to date deepfake manipulation techniques, such as the use of realistic face swaps in videos and the use of false human faces in social media profiles, in order to better detect instances of deepfake fraud.

Once limited to social media, deepfake has emerged as a formidable threat across many industries. Its potential to impact the insurance industry, whose cost of fraud already suffers from over USD 300B in the US alone, is immense.

Deepfake Technology Example	June 2022

The most prevalent form of deepfake technology is a program that supplants facial characteristics of one person onto the face of another.

Voice cloning, a different deepfake approach, duplicates a person's distinctive vocal characteristics to digitally copy and modify their speech.

The viral video of Morgan Freeman (link above), is a prime example of deepfake technology. This particular deepfake was most likely created with the help of a generative adversarial network (GAN), which creates new images from source material, and is then trained to determine whether or not the image is original. Following the training, the generator is capable of producing fake images that can pass as real.

C. Behavioral Analytics

Behavioral analytics is an additional layer of security that can be used as part of a holistic cyber defense strategy to prevent things like identity theft.

Behavioral analytic tools develop digital fingerprints for individuals by collecting and analyzing mass amounts of metadata based on their digital usage patterns, IP addresses, physical locations, device types, typing speeds, and a whole host of other unique digital identifiers. Through machine learning, these tools are then able to detect behavioral anomalies, and notify the respective individual or organization as the fraudulent attempt is occurring in real time. The collection and analysis of interaction data is typically referred to as **behavioral-data mining**.

The behavioral analytics market, also referred to as UEBA (User and Entity Behavioral Analytics), is forecast to grow to USD 1.2B by 2025.

D. Blockchain for Data Security

Data storage infrastructure plays an equally critical role in protecting consumers. Traditionally, data gets stored on centralized databases, making it vulnerable to hacks. The blockchain is one method that can help protect consumers, by decentralizing the storage of data, thereby lowering the risk associated with a single breach giving unwanted access to an entire database.

A blockchain is a digitally distributed, decentralized, public archive that exists across a network and stores data in blocks. Each block can contain one or multiple transactions. Blockchain solutions can be used by both organizations and individuals for transactions and data storage, by creating tamperproof and immutable records based on consensus, cryptography, and decentralization principles. Blockchain technology has paved the way for unprecedented data security, transparency, and accountability.

Blockchains are classified into various categories, mainly distinguished by their restrictions (open or closed to limited participants) and permissions. Closed blockchains (restricted and permissioned) usually offer a higher level of protection by providing better control of activities of its participants.

The blockchain security global market is expected to reach USD 1.6B by 2027.

The main blockchain data security solutions are predicated on the following four technological pillars:

→ **Tracking and verification** (Consensus) - Any change to the blockchain is permanently recorded, preventing third parties from altering the data and claiming it as legitimate. Because every change is recorded in the blockchain, incidents can be traced back to the exact moment that it occurred.

→ **Unique access** (Cryptography) - Data stored on the blockchain is converted into an encrypted code. A unique "private key" belonging to the user is generated when a connection is made, and serves as authenticated proof of the user's identity to access data or funds. This encryption technology protecting consumers private keys makes it harder for criminals to steal personal information.

→ **Self-sovereign identity** (Decentralization) - Blockchains store data in a decentralized network, meaning no single entity owns or controls the data. Importantly, users are able to manage their self-sovereign digital identities, maintaining complete control of their sensitive data. The public key, associated with the private encryption key, is published through a distributed ledger technology (DTL), a solution that is applied to create a secure, private, decentralized, portable, and fully user-controlled online identification system.

→ **Network backup** (Decentralization) - Data is frequently downloaded from multiple computers (or nodes), and duplicates are stored locally. Therefore, multiple sources can be restored from stolen data.

Despite its many advantages, blockchain technology has its weaknesses, mainly related to human vulnerability and social engineering tactics. Attackers can send phishing emails or exploit weak network security to obtain encryption keys, allowing them to intercept sensitive data. This points once again to the importance of individual education on cybersecurity and data protection best practices.

03
Cyber Safety for Digital Consumers

One of the most difficult variables to account for when designing a cybersecurity strategy, is the risk of human error. As demonstrated throughout this report, cyber crime is often initiated by exploiting unsuspecting individuals.

While it's nearly impossible to completely protect an organization from the human risk factor, there are guardrails that can be put into place in order to mitigate some of that risk.

A. Parametric Insurance | The future of cybersecurity coverage

Insurance providers and insurtech companies are developing new coverage offerings to compensate individuals and organizations who may have fallen victim to identity theft, largely through parametric models.

In the traditional insurance model, claims are only paid out once damages are able to be accurately assessed. This often leaves the policyholder in a difficult position during the claim management period, and can lead to higher payouts from the insurance companies. Parametric insurance, on the other hand, is structured to pay a predefined amount to the claimant, based on predefined events (regardless of actual damages). Considering the costs associated with cyber attacks and the need for immediate response, parametric coverage presents an attractive option for both organizations and individuals who are looking for both downside financial protection and a way to respond quickly in the event of a cyber attack.

> The global parametric insurance market is projected to reach USD 29.3B by 2031.

Cyber Insurance for Organizations

Cyber insurance is still in a relatively nascent stage of development. In 2020, less than 1% of global losses related to cyber crime were insured. One of the main roadblocks hindering insurance companies from broadly rolling out more comprehensive cyber policies, is the lack of historical data available to properly underwrite the risk. That challenge is compounded by the fact that the risks that are being underwritten today, will likely evolve and become more sophisticated tomorrow.

This seemingly impossible problem has galvanized incumbent insurance and InsurTech companies to work together to find a way to meet the cybersecurity needs of organizations. Below are two examples of novel cybersecurity products launched in partnership between insurance providers and tech companies.

Allianz + Google Cloud | Cyber risk management	*Insurance and Tech*
Allianz partnered with Google Cloud and Munich Re to provide Cyber Risk Management solutions for its cloud customers. The Risk Protection Program consists of two components: Risk Manager, to determine a customer's security risk posture on the cloud, and Cloud Protection +, a cyber insurance solution built exclusively for Google Cloud customers.	

Lloyd's, Tokio Marine, RenaissanceRe + Parametrix | Cyber-related business interruptions	*Insurance and Insurtech*
Lloyd's launched a cyber business interruption insurance policy for SMEs. Payment under Parametrix Insurance is automatically triggered if a customer's critical IT services, such as cloud, e-commerce or payment systems are disrupted. The new product is led by Tokio Marine Kiln (TMK) and supported by other members, including RenaissanceRe.	

Cyber Insurance for Individuals | Identity theft

Identity theft insurance is designed to cover some of the expenses associated with identity theft. Coverage typically includes the costs incurred after the identity is stolen (eg. legal fees, lost wages and application fees), and not direct financial losses incurred by the policyholder as a result of the attack, such as fraudulent credit card charges.

Some of the expenses that may be covered by identity theft insurance include:

→ Credit application costs

→ Notary and postage fees

→ Legal expenses

→ Fees charged by other financial institutions (eg. fees charged to a victim's account as a result of identity fraud)

→ Lost wages, covering lost income due to days off from work to manage identity theft (eg. meeting with an attorney)

→ Child care services while the victim reclaims the stolen identity

Furthermore, policies frequently include specialists who can help victims navigate the identity restoration process.

Identity theft insurance is provided, and can be applied by users in several ways. The following will provide an overview of which players are already offering this type of protection as a standalone or as an add-on to their existing products.

Individual Cyber & Identity Theft Coverage Examples

Hartford | Add-on to a P&C coverage — *Insurance company*

Product AARP Homeowners Insurance Program

Includes
- Coverage limits ranging from USD 25k to USD 50k
- Access to The Hartford ID Hotline and identity restoration services, as well as fraud specialists to answer questions

Allstate | Standalone coverage — *Insurance company*

Product Allstate Identity Protection

Includes
- Monitoring services
- Reimbursement for expenses related to identity theft restoration

Notch | Standalone or bundle — *Insurtech*

Product Instagram, YouTube, Twitch, NFTs, TikTok, and Twitter insurance

Includes
- If a social media account is compromised, users can be paid on a daily basis based on this coverage
- Notch's retrieval and crisis management team will work to reclaim the account in a timely manner
- Real-time monitoring to ensure that the account is secure, as well as dark web monitoring to see if the user's credentials have been leaked

Wallife | Standalone or bundle

Insurtech

Product Wallet Smart, Wallet Classic, and Wallet Premium for online payment account protection, and social plan for social account protection

Includes

- Wallife App secures end-user biometric identities, reducing the possibility of private data breaches online (eg. VPN and Threat Scan)
- Customers can manage policies and claims using the Wallife App, as the company offers a variety of plans

Discover | Protection plan

Credit Card company

Product Identity Theft Protection Plan

Includes

- Credit monitoring
- Dark web alerts
- Fraud resolution specialists

Experian | Protection service

Credit reporting company

Product Identity Theft and Credit Protection

Includes

- Dark web monitoring
- Credit monitoring
- Fraud resolution assistance
- Up to USD 1M in identity theft insurance

B. The Human Factor | Education is key

While insurance policies protect you from the financial aftermath of a cyber incident, there are proactive steps that can be taken to help individuals become more vigilant about preventing cyber attacks in the first place.

Organizations

According to the 2022 World Economic Forum, 95% of cybersecurity problems are caused by human mistakes, while 43% of breaches are caused by insider threats (either intentionally or accidentally). Cybersecurity training and education, therefore, must become staples in any organization's cybersecurity strategy.

A successful security awareness training program for employees could include the following:

1. **Communication** - Educate users about common attack methods, such as phishing and other social engineering tactics.
2. **Training** - Create security and compliance training seminars to properly educate employees on how to respond in the event of an attack.
3. **Simulations** - Simulate attacks and monitor the internal responses from employees.
4. **Review** - Review and measure the results from the simulations.
5. **Discussion** - Raise awareness by openly discussing the results of the simulations and improvements made over time.

There are multiple third party vendors who will organize professional training seminars and simulations for corporations in order to teach cybersecurity vigilance.

Individuals

Corporations have a very clear and strong incentive to train their employees on the importance of responsible digital etiquette. That incentive should be just as strong for individuals, who need to properly understand the potential impact of cyber crime on their personal lives. Thankfully, there are a number of basic steps that individuals can take to protect themselves from cyber crime.

10 Cybersecurity Tips for Digital Consumers

1. **Disclosing information** - Only disclose personal identifying information to a trusted source online. Lookout for phishing scams through email or phone calls.
2. **Online activity** - Limit the amount of personal information you post about yourself online and/or on social media. Moderate your privacy settings to limit the amount of information that unknown contacts can access.

3. **Content review** - Check that no information is mistakenly disclosed in public forums through images that may contain sensitive information (eg. license plate numbers, addresses).
4. **Connecting with others** - Carefully review a profile when accepting requests on social media platforms (eg. unknown or duplicates of existing contacts). Cybercriminals are known to clone accounts by stealing personal details through friend requests.
5. **Source reliability** - Cross-check information on multiple trustworthy platforms when content has surfaced from an unknown source.
6. **Password management** - Create strong passwords. Use different passwords for different websites. Consider using password management tools to keep your details in a secure place.
7. **Fair skepticism** - Always be cautious when you get an email asking you to follow a link. Verify the sender's email address, and importantly, their email domain.
8. **0.0.0. computers** - Avoid completing sensitive or financial transactions when using public or shared computers. If you do login from a shared computer, make sure to log out when you're done with you session.
9. **ATMs** - Avoid using standalone or remote outdoor ATMs. Indications of tampering can be seen by looking for unusual materials, colors, and images that seem inauthentic.
10. **Education** - Stay informed about advances in personal digital security technology and potential cyber attacks as an additional layer of security.

04
SOSA & FinTLV Picks

How an organization manages and responds to cyber attacks often determines the viability of the impacted business, as showcased throughout this report. In order to properly secure data, a joint effort is required from both corporations and individuals, to implement technological barriers, educate & train the employee base, and ensure digital best practices and habits.

Below, we feature a select list of cybersecurity-focused companies that directly relate to protecting today's digital consumer.

Infrastructure Threat Detection and Prevention

Cynet
Automated security management platform

XDR threat detection and response platform designed to simplify security support. The company's real time monitoring solution undertakes threat analysis, and targets and remediates unknown threats by collecting network activity, establishing a baseline, and correlating indicators to create a risk ranking.

Notable clients: NEC, Catalina, Becker, Carrefour, SPIE Switzerland

Darkowl
Dark web monitoring database solution

Real time dark web monitoring platform, allowing customers to analyze data for specific use cases through a centralized dashboard, with triggers and alarms, and emerging threats tracking. Data is collected using a combination of AI and manual actions, processed using the company's engines, and organized by type.

Notable clients: IBM, Hitachi, Coinbase, Riskiq, Ontic, Babel Street

Deep Instinct

End-to-end deep learning platform

Cybersecurity platform designed to predict, prevent, and analyze cyber attacks at any touchpoint of an organization in real-time. The company's platform provides protection against zero-day threats and APT attacks by identifying malware from any data source through its end-to-end deep learning technology.

Notable clients: SEIKO, Honeywell, T Systems, Tanium, Internet Initiative Japan

Digital Identity Verification

Veriff

AI-powered identity verification solution

Enables commercial sectors to improve fraud prevention and compliance with KYC regulations securing online identity verification. Through authentication and cross-platform fraud detection AI technology over websites and mobile apps, Veriff ensures the validity of drivers' licenses, passports, and other identities.

Notable clients: Trustpilot, Blockchain.com, Mintos, Bolt, Starship

Alchera

Data collection and analysis full-stack AI solution

Specialized in visual anomaly detection, the solution uses AI-based image recognition, allowing computers to recognize and analyze any visual input through deep learning. Core technologies include AI, AR and big data solutions, including image-based hand, face, behaviour and object recognition.

Notable clients: LG, Toss, CGV, KakaoBank, Great Safety Information Laboratory

iProov

Identity verification technology provider

Palm and face authentication solution designed with patented Genuine Presence Assurance technology. iProov applies deep-learning technologies as well as built-in replay-attack and spoof prevention for primary, multi-factor or step-up authentication processes.

Notable clients: Home Office, NHS, ING Group, Eurostar, Rabobank

Behavioural Analytics

Biocatch

Fraud protection solution

Behavioral biometric technology solution able to detect fraud by monitoring mouse activity, touchscreen behaviour, and keystroke and device movement. The risk engine is powered by machine learning technology, collecting and analyzing trillions of digital behavioral interactions globally.

Notable clients: HSBC, Itaú, Barclays, American Express, Citi Ventures

ThetaRay

SaaS AML transaction monitoring solution

Fraud detection solution for financial critical infrastructure institutions and other industries, to control risk and recognize money laundering schemes. AI technology detects anomalies and atypical behavior, including new categorizations through proprietary and patented algorithms.

Notable clients: Santander, Apollo, Payoneer, Qolo, Travelex Bank, Cecabank

BehavioSec

Behavioral biometric fraud prevention solution

Behavioral biometrics and ongoing authentication solution for MFA process, risk-based authentication as well as a Zero Trust approach. BehavioSec is based on machine learning and analysis of contextual variables of users' behavior (eg. how they type, use their devices) compared to previous patterns.

Notable clients: Undisclosed

Blockchain for Data Security

Near Protocol

Blockchain application platform developer

Blockchain-based decentralized application platform that serves as a collective, a foundation, and a development solution. The NEAR protocol is a sharded, proof-of-stake, layer-one blockchain. Users can create coins, applications, and industries without the need for a central authority to oversee the process.

Notable clients: Flux, TessaB, SeatLabNFT, Arroz Estudios, Berry Cards,

Compute North

Blockchain infrastructure and hosting services solution

Blockchain infrastructure and hosting services solution intended to power operations. The company's services offer computing power solutions with miner hosting, repair, quality assurance, logistics, and equipment services, enabling organizations with reliable and cost-efficient power sources.

Notable clients: Undisclosed

Axelar

Key offering

Decentralized interoperability software solution, powered by byzantine consensus, cryptography, and mechanism design protocols. Applications live on different blockchains, enabling clients to get a distributed network, APIs, and tools to make it easy to build cross-chain decentralized applications.

Notable clients: Undisclosed

Insurance solutions and Insurtech companies

Notch

Insurtech solution for web3 assets

Insurtech MGA offering semi parametric coverage to protect SMBs and individuals generating income from their digital presence. The company developed a proprietary actuarial model algorithm to detect account anomalies, and provides loss income coverage, 24/7 real time monitoring and account retrieval services.

Notable clients: Not applicable

Corvus

Insurance risk management and selection SaaS platform

Risk management, breach response, claims handling and post-breach remediation insurance solutions for business. Coverages help policyholders prevent and respond to cyber incidents providing overview dashboards, Corvus Scan reports, alerts, risk management resources, and claim information.

Notable clients: Travelers, Lacework, SiriusPoint, Tarmika, Tarian

Parametrix

Parametric insurance for IT downtime

Parametric policies for external IT service downtime (eg. cloud outages, network failures, system crashes) enabling businesses to edge their external risks. The monitoring systems and risk aggregation capabilities are incorporated with deep actuarial and data science expertise, providing new software services space.

Notable clients: Lloyd's, Tokio Marine, RenaissanceRe, Apollo, Hannover Re, Munich Re, Sompo Japan

Education and Training

Talon

Secure enterprise browser

Designed to protect employees against threats posed by distributed work and accelerated cloud usage, the company's cybersecurity technology isolates web traffic locally on the Chromium-based browser endpoint, through Data Loss Prevention, Threat Protection, SaaS Visibility and Zero Trust approach.

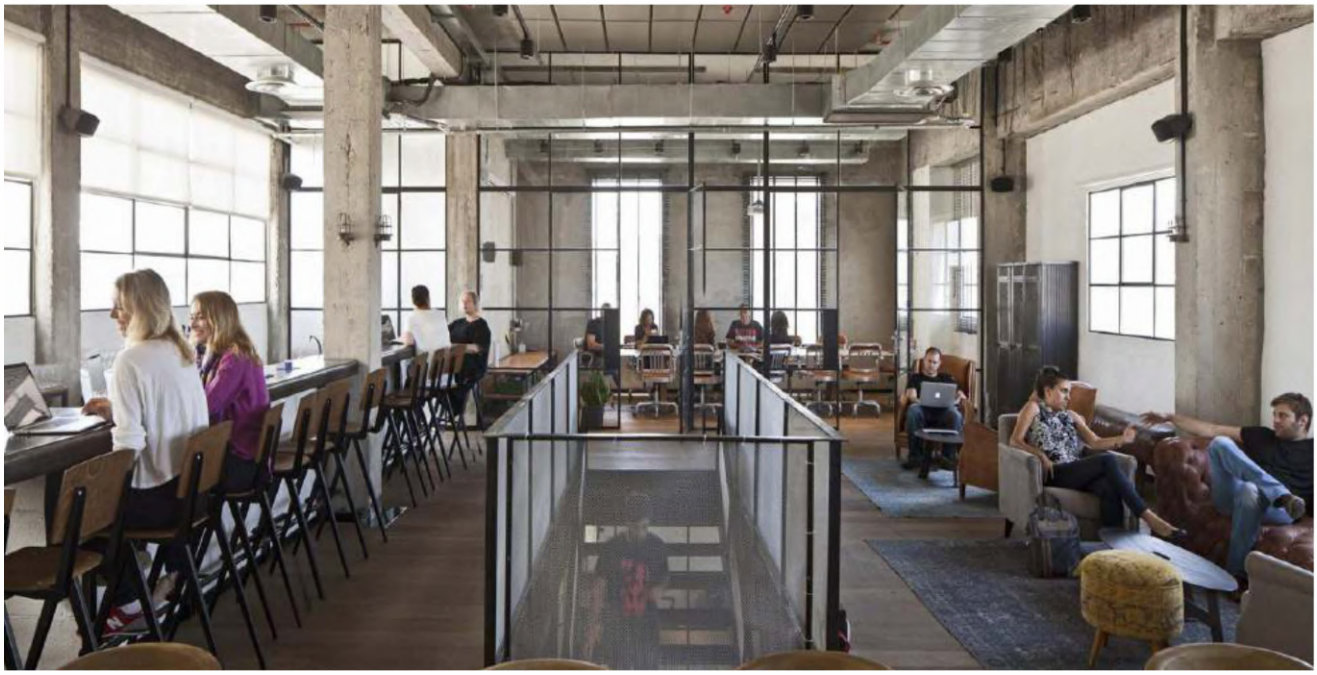
Notable clients: Citi, Symantec, Palo Alto Networks, CrowdStrike

Immersive Labs

Interactive cybersecurity training platform

Human cyber readiness platform designed to empower organizations to increase, measure, and demonstrate cybersecurity human capabilities. The platform helps in interaction, exploration, and incident simulation, enabling organizations to identify potential cyber weaknesses and areas of focus to defend.

Notable clients: Citi, HSBC, Daimler, BCG, Pfizer, Moody's



About SOSA

SOSA is an open innovation company. SOSA works with innovation teams and business units in corporations (like Tokio Marine, Schneider Electric, Swiss Re, LG), and governments (like Australia, Brazil, Canada and Taiwan). The SOSA team scouts and validates startups and technologies in order to bring clients the solutions they need to solve use cases, identify opportunities, or build new products.

About FinTLV

FinTLV is a global venture capital fund focused primarily on Insurtech and Fintech. The VC backs some of the most promising companies in these domains in the US, Europe and Israel and invest across all stages. Furthermore, FinTLV supports its portfolio companies with a rich experience in the insurance field and a global network of tens of insurance and reinsurance partners.

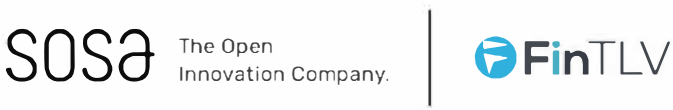
Authors & Contributors

Giulia De Benedetti, Polina Gohman, Dani Forman

Disclaimer & Copyright

Although substantial time and effort have been invested in gathering the information contained in this document, it is provided on an as-is basis, with no expressed or implied warranties, neither with respect to its accuracy nor completeness nor otherwise including the following:

1) The data (including opinions and information) in this document is provided for information purposes only and is not intended for investment purposes. SOSA is not liable for any errors in content, or for any actions taken in reliance on any content.
2) The document reflects SOSA's view on the subject matter of the document, and is intended to provide you with a reference point only, rather than as a basis for making financial or other decisions.
3) SOSA does not guarantee the accuracy of the information provided in this document and shall not be liable for any loss due either to its negligence or to any cause beyond its reasonable control.


sosa
The Open
Innovation Company.
FinTLV