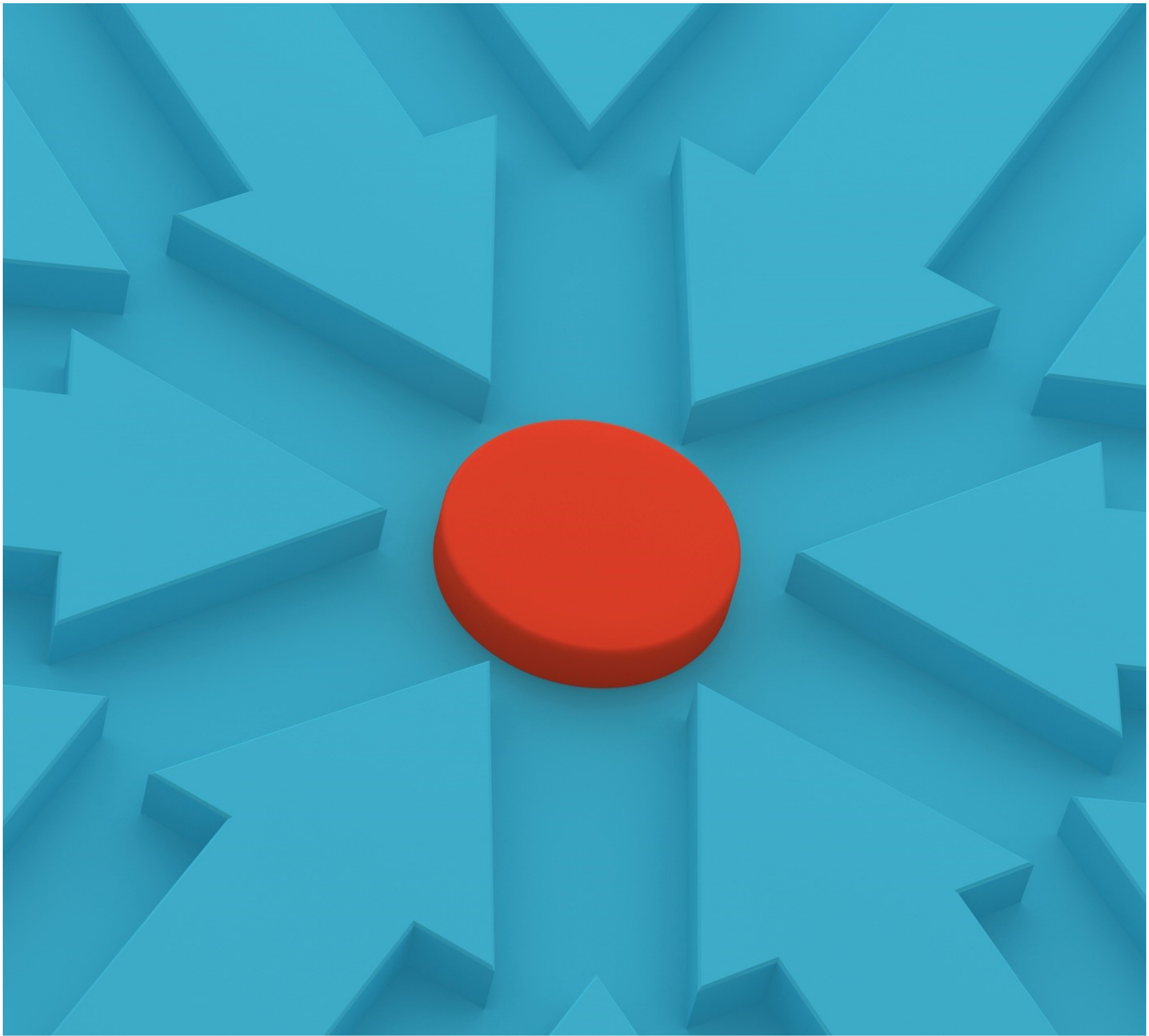
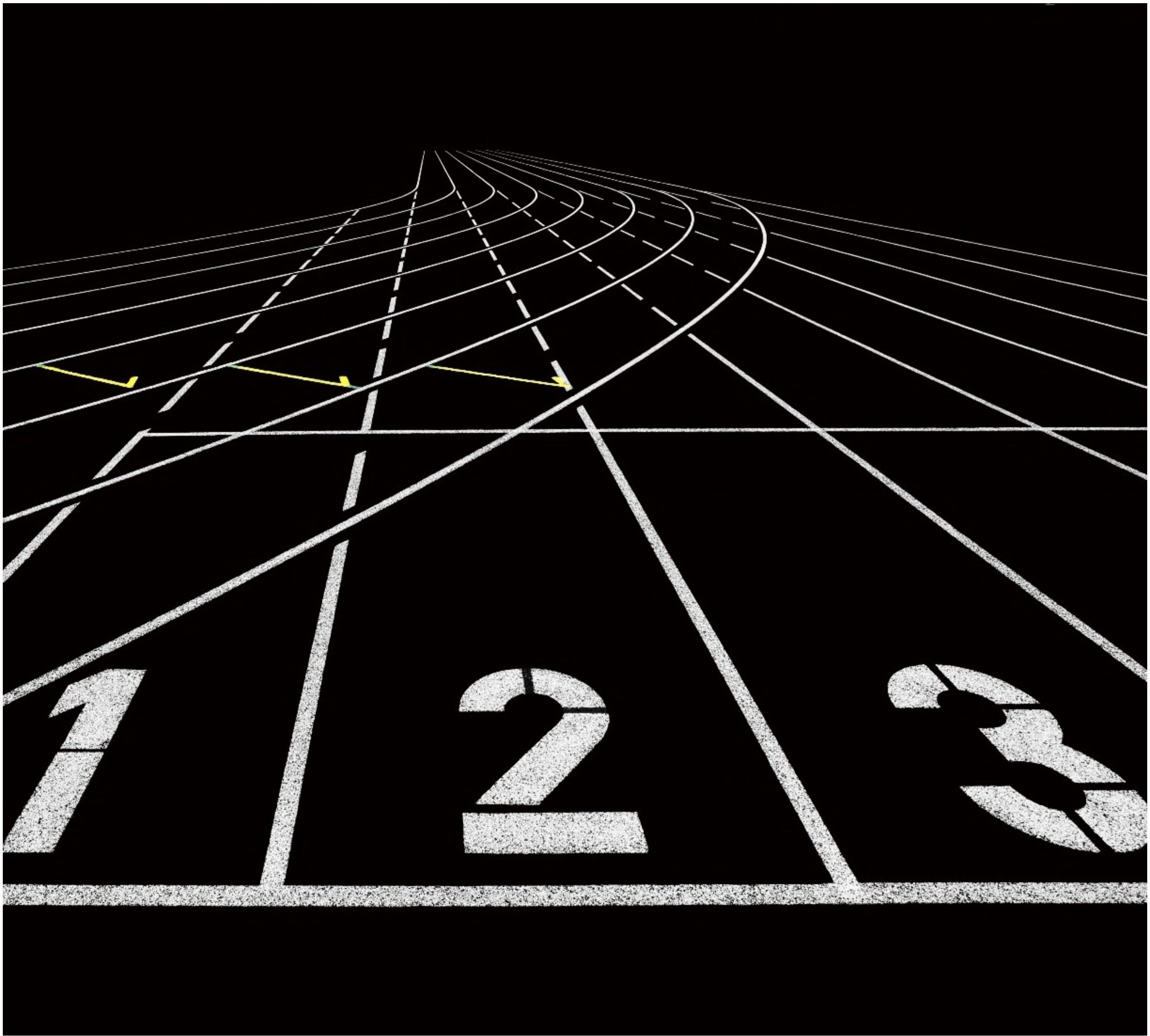


TACKLING CYBERSECURITY IN 2021 UNDER A NEW ADMINISTRATION

PREDICTIONS

SOFTWARE SOLUTIONS CORPORATION™ rgarcia@softwaresolutioncorp.com



CHALLENGES AHEAD 2021

I definetly do not own a crystal ball, nor do I forecast the future; nonetheless, the new administration does have some cybersecurities ahead. Threads are emerging daily which is already having an impact on companies of all sizes. Covid-19 accelerated the digital of most institutions, some, where able to create a solid plan of implementation, other, not so much. Lack of revenue, poorly untrained staff and the fast pace of digitalization are effectevely transforming organizations. If current trends continue, we will see a rise in cybercrime in the coming months and years.

TYPES OF THREADS AHEAD

Poisoning of Machine Learning Data

With the reason cybersecurity attacks which penetrated deep into the heart of our nation to the dissemination of false or misleading news based on poison data, attackers are able to leave the most convincing of deepfakes ever seen before, these criminal activities are all designed to disrupt. The countries unity and democratic harmony. Additionally, the attacker's goal is not just to target the IT systems, extort money, steal identities, no they want more, they want to cause global chaos. It's clear that cybercriminals are scarily good at reinventing themselves to capitalize on the post-pandemic landscape.

Who is the target?

Cyber adversaries do not stop at countries' borders, nor do they comply with different jurisdictions. Organizations, meanwhile, must navigate both a growing number and increasingly complex system of regulations and rules, such as the General Data Protection Regulation, the California Consumer Privacy Act, the Cybersecurity Law of the People's Republic of China and many others worldwide.

Figure 1: Cybercriminal targeting system.

Cloud Platform Risk.

AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations. January 2021, threads alerts by CISA has seen an APT actor using compromised applications in a victim's Microsoft 365 (M365)/Azure environment. The cybercriminal than launches attacks against other tenants. We also are beginning to see APT actor utilizing additional credentials and Application Programming Interface (API) access to cloud resources of private and public sector organizations. These tactics, techniques, and procedures (TTPs) feature three key components: Privilege Escalation and Persistence, User Impersonation, Impossible Logins or impossible travel

NEW ADMINISTRATION CHALLENGES

President Biden administration cybersecurity challenges.

Avril Haines, Biden's nominee for director of national intelligence, told member of the senate intelligence committee; “China is adversarial and an adversary on some issues,” Haines said, “and on other issues, we try to cooperate with them.” This double stance might prove to be difficult as cybercrimes continues to grow. She noted that tackling climate change is one area where the United States has sought Beijing’s cooperation. Concentrating on the positive traits of a relationship is a good starting point, to a challenging partnership. Haines also said the hack was a “major concern” and she has “a lot more to learn about what we know about this.” Biden's first major cybersecurity challenge will be dealing with the fallout and recovery from a Russian hacking campaign that infiltrated at least eight federal agencies and hundreds of companies and organizations.

In 2021 Cybersecurity has become challenging for everyone, from government agencies to private institutions. Staying ahead by is a reasonable expectation which is losing ground; even taking preventive action before any threats exploit the system is difficult since in most cases the bridges in security are internal.

Why the increase in threads?

With the help of the internet, cloud infrastructure is coming online & becoming vulnerable to all sorts of attacks and breaches of personal information. Another example is Easy Jet, where hackers have accessed the travel details of 9 million customers. Another example is the REvil ransomware which attacked a law firm (*Grubman Shire Meiselas& Sacks*) used by the likes of Lady Gaga, Drake and Madonna, Facebook. Sony, HBO, U2, Elton John and many others.

The hackers have allegedly stolen, clients phone numbers, email addresses, personal correspondence, contracts, and non – disclosure agreements made with advertising and modelling firms. So, it’s not only the reputational or monetary loss that is the issue but the risk that businesses can even go bust after paying the penalties. Small firms may not even have the cash to pay or may get indebted. Undoubtedly, cybersecurity is a concern which needs to take care of!

Internet of Things (IoT)

As the adoption of the Internet of things is growing, so will the thread to automated systems.

ML Poisoning

*It describes attacks in which someone purposefully '**poisons**' the training **data** the algorithm uses. The goal: corrupting or weakening it.*

Ransomware Threats

This is the fastest-growing cyberthreat capturing the headlines these days.

GROWING SECURITY TRENDS

2020 brought a flood of new threads into view. COVID-19 has forced companies to create remote workforces and operate off cloud-based platforms. The rollout of 5G has connected devices of all types, very well and in an ever-increasing manner. System, which lived isolated or disconnected are now integrated and available. Cybercriminal, have begun to exploit, the user unwellness to change. A user whose security practices created risk on-premise, will undoubtably be a security risk, vulnerability and attack vector in the Cloud. Cybersecurity experts have never been more important than in 2021. These recent events and the cybersecurity statistics and figures considered, here are some industry trends and also predictions to watch for in 2021 and beyond.

1. Remote workers will continue to be a target for cybercriminals, especially certain age groups, and specific job roles. Cybercriminals will focus on:

    a) New Employees
    b) Younger Employees and Retiring age Employees
    c) Support Staff
    d) Outsourced Staff

2. As a side effect of remote workforces, cloud breaches will increase. Why?
    a) Reluctance to use strong passwords (Length, Complexity)
    b) Unwilling to change current practices such as opening attachments, forwarding emails, downloading content from the internet, consuming media from YouTube and other public sources.
    c) Storing unclassified data in a Classified system, not following internal security policies

3. The cybersecurity skills gap will remain an in 2021 and thru the next four years.

    a) It's not just about certifications, is about proving the skills.
    b) It's not about length of employment in the field, it about running drills and simulations to be ready for an attack.
    c) It's about discipline and well training personal.
    d) It's a cyberarmy, trained in:

        - Patterned detection
        - Intelligence Assessment
        - Counter Intelligence
        - Counter Measures
        - Awareness of attack patterns
        - Awareness of vector-based patterns.
        - Collective recon.

e) Continuous Assessment,
f) Continuous Training
g) Continuous learning.
h) Not about testing, but real knowledge, real skills.
i) Afterall, are all hackers certified in Hackers university with a Blackhat degree? Hardly not!

4. As a result of 5G increasing the bandwidth of connected devices, IoT devices have become more vulnerable, and will continue to be vulnerable to cyber-attacks, until new industry standards are in place.

2021 Covid-19 Pandemic's Will Make Digital Security Even Tougher as emerging threads grow unchallenged!

CyberColdWarfare (CCW) are State Sponsored attacks.
Despite the fact that cyberwarfare can never be won by either side, the Powers of world nation, again begun to clash via proxies on real-world cyber-battlefields.

This new mobilization of cyberarmies, has opened the door for exponentially more combatants in the field of cyberwarfare and cybercrimes. The full might of a Nation-State is usually measured by the accumulation of military hardware. Today a Nation-State full might is measured based on the amount of digital assets and resources, possess by the Nations cyberarmies.

This means that weak nations, even economically and technologically backward can potentially launch deadly attacks toward a perceived enemy, reversing the roles, where a small nation and become a world class player in the cyberwarfare arena, training cyberarmies to conduct state sponsored terrorist acts in the digital space. The small ones able to become great nations able to become formidable adversaries.

(Verma, 2020)

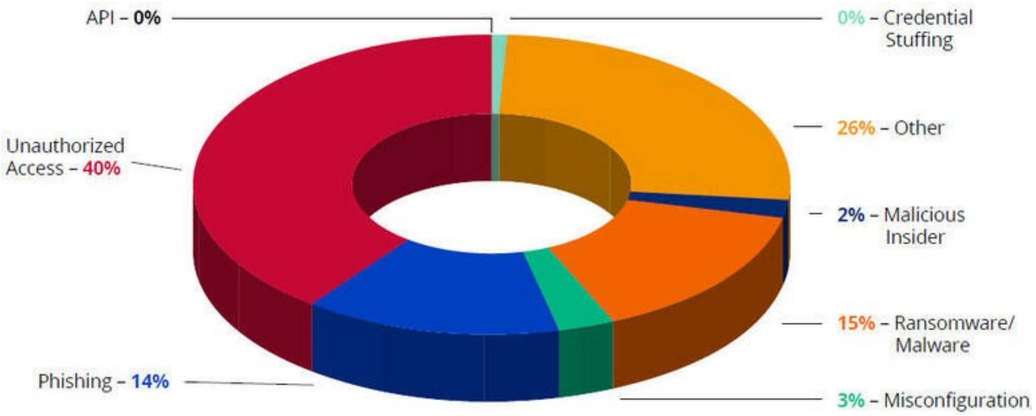
2021 CYBERSECURITY PREDICTIONS

A data breach has inflicted pain worldwide. With customers and user accounts compromised, companies and individuals can suffer financial consequences and can see their reputation, credibility and foundation damaged, sometimes beyond repair. A new report from digital identity platform ForgeRock (ForgeRock, 2020) shows how and where data breaches are affecting US businesses and their customers.

The release of the Garner reports (Gartner, 2019) describes the financial pain data breaches have inflicted. With more than 5 billion records compromised in 2020, breaches cost US organizations more than $1.2 trillion. Combined with the $654 billion in costs in 2018-2019, data breaches have hit organizations to the tune of $1.8 trillion over the past two years and will continue its growth pattern thru 2027 and beyond.

Even prior to the coronavirus pandemic, (The republic, 2020) healthcare was the most targeted sector last year with 382 data breaches leading to costs of more than $2.5 billion--that was a huge jump over the 164 incidents and $633 million in costs seen in 2018. Following healthcare, the banking/insurance/financial industry was the most targeted sector in 2019, accounting for 12% of all breaches. Next were education, government, and retail.

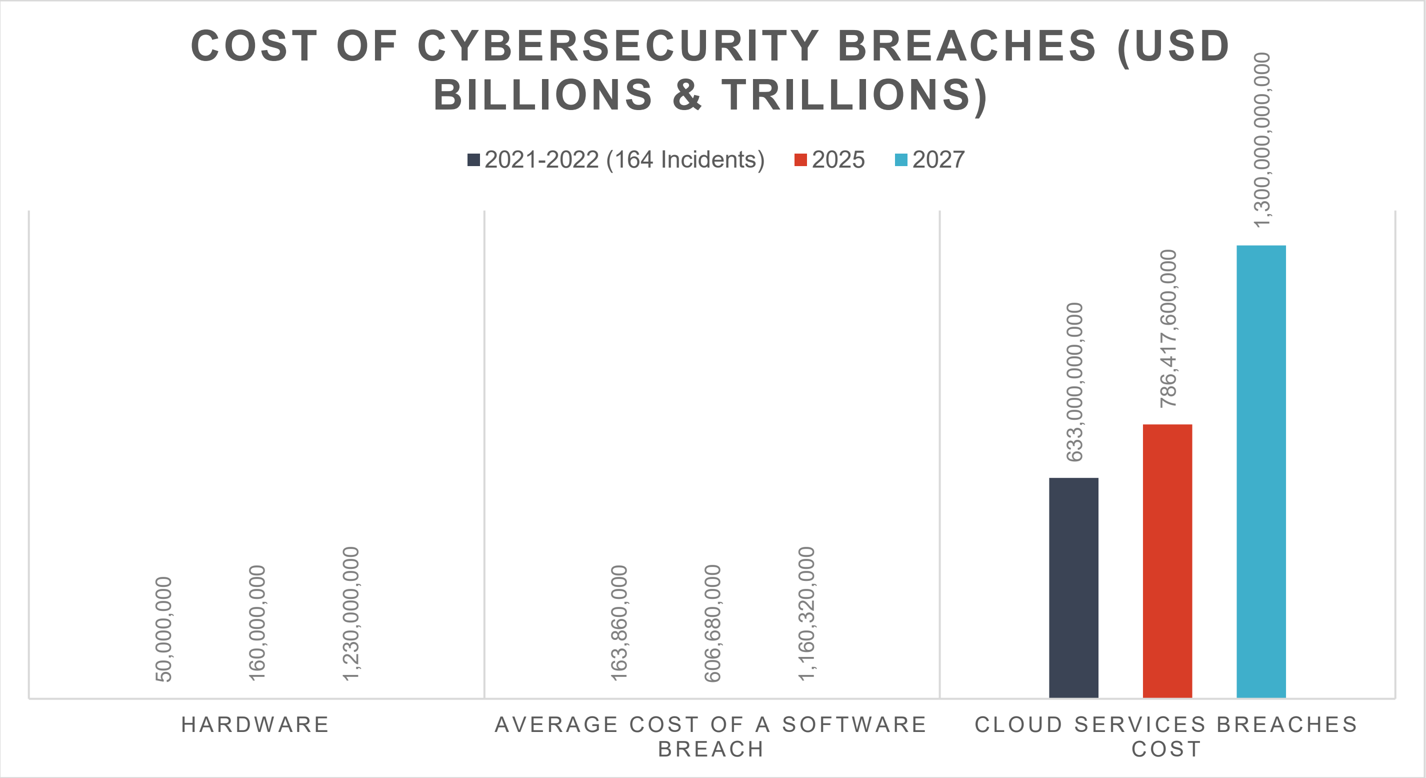
Technology firms saw the largest number of records compromised due to data breaches in 2019. Breaches cost the tech industry more than $250 billion, as more than 1.37 billion records were exposed during the year.



(Garner, 2019)

Personally Identifiable Information (PII) will remain the most targeted type of data sought by attackers. Ninety-eighth percent of the breaches recorded last year were PII. More specifically, social security numbers were the most popular type of breached information, exposing more than 10.88 Billion records, including, SSN and PII data from twenty-two countries. Unauthorized access was the most common type of attack used, playing a role in 40% of last year's breaches. Other popular forms of attack included ransomware, malware, and phishing campaigns.

	2021-2022	2025	2027
Hardware	50.6B	100.7B	175.9B
Software	3.86M	6.6M	160.3M
Cloud Services Attacks	170.4B	250.1B	1.3T



Conclusion
According multiple reports to the report, sixty-eighth percent of surveyed organizations said they do not have a plan to both prevent and respond to a cyber-incident. (Scott Kannry, 2020) Over nine-hundred organizations lack a response plan, only thirty-two percent lack an effective plan of action, or tested solution.

When looking internally at our customers and agencies we serve, we found a relax attitude toward cybercrime. Most organizations do not see the need in development specialized staff, to deal with this problem. The uniform implementation of basic security measures, is disregarded as a fad, or something that larger companies pursue.

In 2021 we will see an increased transparency by organizations and governments, standardization and coordination of cybersecurity requirements, providing cybersecurity awareness training for employees, and developing prevention and response plans. It is our hope, that other take the warning to heart. The security future of your enterprise can change today, if you are willing to follow basic principles to secure your environment.

The response to the eminent security threat is serious, and as such, every organization should take an active role in preserving information security, applying cybersecurity measures, thru training and live drills. Only thru preparation can we change the wave, which threaten the future of our freedom and security.

Every American based company, should do its part to create a unified front and fortify our countries digital boundaries, beginning with our enterprises and moving outward, by protecting the privacy and rights of our customers and partners.

Written by:

Dr. Rigoberto Garcia
Chief Cloud & Security Architect
CEO, Founder
rgarcia@softwaresolutioncorp.com
Software Solutions Corporation™

Translated to Portuguese-Brazil

Damaris Gondim Garcia
Masters in Business Admnistration
President, CFO
dgarcia@softwaresolutioncorp.com
Software Solutions Corporation™

Translated to Latin-American Spanish

Liana Y. Diaz
Masters in Bi-lingual & Bi-Cultural Education
COO
lydiaz@softwaresolutioncorp.com
Software Solutions Corporation™