

RESTECH SOLUTIONS | HOUSTON, TX
713-936-6855 | INFO@RESTECH.SOLUTIONS |
HTTPS://RESTECH.SOLUTIONS



Cybersecuring Our Future

QUARTERLY

ed. 2

7

How Reliant Are We On Technology?

14

7 Steps to Cybersecurity

20

How QR & AI Revolutionized Daily Life



03
INTRODUCTION

Thank-you for subscribiing
and about the author

06
THE RISE OF
DIGITIZATION

News & analysis of the trend taking
place around the world

14
7 STEPS TO
CYBERSECURITY

How to stay safe online while avoiding
digital threats

20
QR & AI

How these two hands-off forces
revolutionized daily life

30
DATA BREACHES

Statistics in 2021, real life threat
examples and more

CONTENTS



INTRODUCTION

Hi,

By picking up this magazine, you've already taken the first step to becoming more cyber-secure in your everyday life! ResTech Solutions is happy to bring you the latest updates in the cybersecurity industry EVERY QUARTER because the more you know, the better protected you'll be - in your personal and professional life!

Remember when you couldn't use the dial-up computer if someone else was on the phone? Or the bulky desktop that would dominate a room in your house, that everyone traded off as needed? Before laptops shrunk to the size of tablets, and tablets grew keyboards?

Life isn't like that anymore. Technology reigns supreme. On an average day, you might order a breakfast sandwich with DoorDash and watch your Smart TV while you eat. Then, you go to work in your office, at the desk with your multi-screen setup; Google Maps the closest place to stop for lunch; and use Bluetooth headphones for the rest of the afternoon before calling a Lyft to meet a Bumble date. At the restaurant, the table already has a QR code sticker for you to pull up the menu. Later, you settle the bill with your Apple Wallet and the date drives you home with their smart car. No need to give directions, either, with the pre-installed GPS guiding the way.

Quite literally, we can't go a day without encountering the Internet at every turn!

Technology is not just here to stay, but constantly advancing and evolving. In *Cybersecuring the Future* ed. 2, we're investigating how and why digitization has increased, the effects it's had on businesses, and what you can expect from technology moving forward into the future.

LET'S GET STARTED



ABOUT

Hi there! I'm a cybersecurity expert with ResTech Solutions who is dedicated to fighting the never-ending threat of cyberattacks on behalf of you and your data. We're dedicated to keeping your private information, private!

First, I want to thank you for picking up this magazine and joining the fight against cyber-threats to you and your business! Education is the first (and most important) step toward preventing insider and outsider threats from attacking your personal data.

That's what we do here at ResTech Solutions, along with our standard IT services to help keep your business running and secure.

Bringing you this magazine every quarter is my way of bringing accessible cybersecurity tips and industry knowledge right to your front door — and your coffee table!

For a sense of cybersecurity now and going forward, here is *Cybersecuring Our Future Quarterly*.

David Levine
Founder & CEO



"When digital transformation is done right, it's like a caterpillar turning into a butterfly, but when done wrong, all you have is a really fast caterpillar."

- *George Westerman*

THE RISE OF DIGITIZATION

NEWS & ANALYSIS OF THE
TRENDS TAKING PLACE
around the world

HOW RELIANT ARE WE ON TECHNO LOGY?

The internet is a useful tool. It connects people all around the world and lets you find information with the click of a button. It's convenient, fast and available – no wonder its influence grows every year as experts invent new games, tools and security measures to make daily life simpler, not to mention more fun. Even money has become digitized, in the form of cryptocurrency and digital wallets rendering dollar bills a relic.

These trends suggest that the interest in digitization is neither going away, nor decreasing.

Who knows what will become digitized next? We can already go to a restaurant, shop retail, make bank transactions, communicate with loved ones and do so many more things on a daily basis which would be incomparably arduous without the aid of smart technology and the digital sphere.

What does all of this mean about the direction that the world is headed, exactly?

Based on trends from the past few years, we know it's not just cybersecurity that's changing. It's cybercriminals' capabilities, too. Increased digitization continues to spur bad actors to invent more complex threats that they can weaponize against businesses like yours, sneaking in through new avenues and social engineering tactics.

”

WITH NEW
DIGITAL
CAPABILITIES
COME RISK,
LIKE
NEWFOUND
OPPORTUN-
ITIES FOR
THEFT.

THE DARK SIDE OF SCREEN RELIANCE

Anything that connects online is a potential target for a hacker. As your online presence grows (with new social media accounts, connecting smart devices to your local network and more), you face increased risk from cyberthreats.

The more places you appear online, the more opportunities you have to make new connections - including bad actors in disguise. The more places you're visible online, the more targeted social engineering schemes will be, and hackers have more chances to catch you slip-up with your privacy settings, even for a few minutes.

OUTSIDER THREATS

Report any scams you encounter, like sketchy emails from unknown senders. Report suspicious behavior from strangers, online and in person; as well as any proposals of collusion you might receive.

INSIDER THREATS

Other people inside or adjacent to your job could pose a risk whether by accident, coercion or malice. Always abide your security awareness training and don't stray outside of your clearance level.



THE TRUTH ABOUT INSIDER THREATS

the trouble with insider threats

As more businesses see the benefits of regular cybersecurity training, you may notice upper management sending out more phishing tests and holding more security awareness meetings. Yet despite these becoming more common, you may notice that people's performances tend to slip over time, or maybe there are a few employees who just can't seem to get the hang of the security protocol system. Whatever the exact issue, you just can't understand why employees don't seem to care as much as you do about the organization's protection.

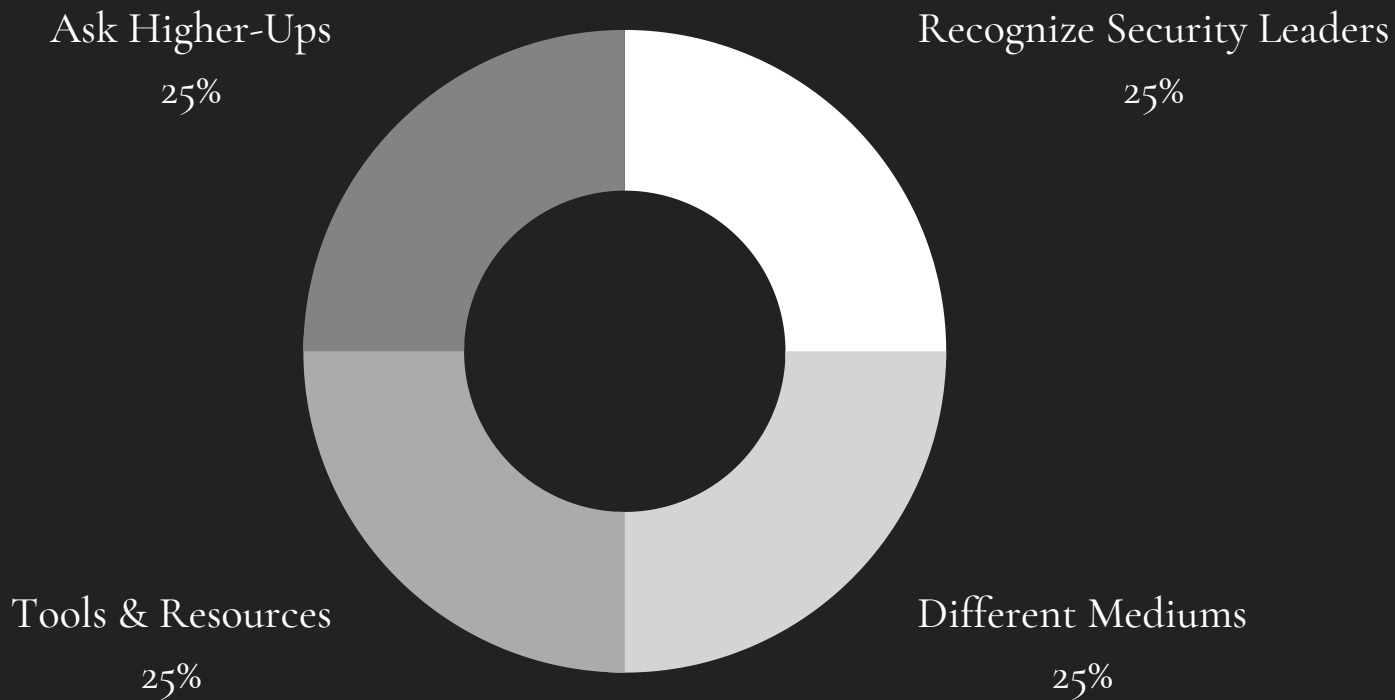
There's a reason why you can't seem to get your staff 100% invested in cybersecurity, and it's not carelessness.

Most of the time, employees don't want to do the organization any harm. They have genuine intentions to follow their cybersecurity training and report threats as noticed. The problem is that they're often way too busy to notice very much.

One Harvard Business review study found that **67% of workers insufficiently comply with at least one cybersecurity standard** or policy on a regular basis. It wasn't out of laziness but usually to provide better output, get or give help, or due to stress from both inside and outside the company.

Stress from the job can cause reckless behavior, cutting corners out of necessity, and missteps that wouldn't be made with rest and a good quality work-life balance. Make sure you're taking the time to reset after a long day so you can come back ready to fight cyber-crime (or at least recognize and report it!).

what you can do about insider threats



- Find the 'security leaders' of your team, those people who you know you can approach with day-to-day questions about security protocol when you need a gentle reminder.
- Everyone's memories work differently. Find the best way to retain your Security Awareness Training and don't worry if it doesn't work for anyone else!
- Ask for and utilize tools to streamline issues at work, from interpersonal conflict to stress at home that carries over.
- Why not talk to your supervisor about getting the tools and resources that you need to protect your systems? You never know until you ask!

THREE TYPES

OF INSIDER THREATS TO YOUR DATA

Unintentional Threats

This person does not intend to cause a threat, but they do so through carelessness. They may misplace their laptop or flash drive, fail to update software, or ignore instructions when setting up software or cloud storage. Their attention to detail may be poor and they can make mistakes that damage the organization, such as causing a breach by emailing data to the wrong person. Vigilance and attention to detail can prevent this from being you!

Intentional Threats

This person intends to harm their organization and is often called a “malicious insider”. They may be in it for financial gain, to get revenge for some perceived slight, or for some other motivation. They may leak information to third parties for money or political beliefs, steal or destroy information to hurt the company. If you see someone you know acting suspicious, say something.

Collusive Threats

Collusive threats occur when an insider collaborates with an outsider to compromise an organization. The outsider may recruit an insider to obtain information to commit fraud, intellectual property theft, espionage, or some other crime. Some insiders may be manipulated into becoming a threat and may not recognize that what they are doing is harmful. ALWAYS report to superiors when someone, whether a stranger or not, asks you to help them commit cyber-crime.



OUTSIDER THREATS

what they are

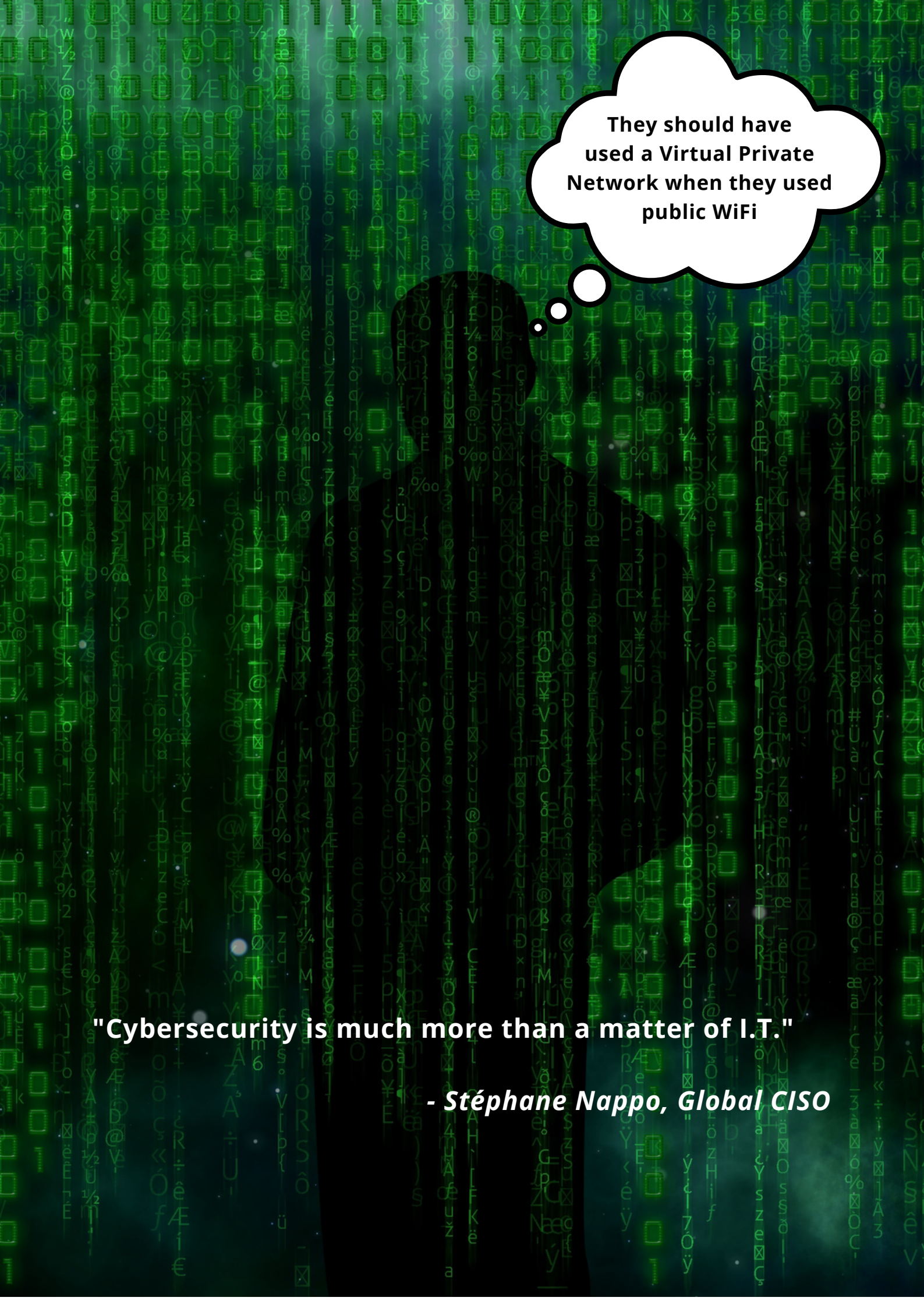
When you think of a cyberattack, these are what people tend to imagine: Some anonymous hacker, masked and miles away behind a screen on the Dark Web. Sometimes, it's just what you picture. Outsider threats refer to any kind of attack that originates from somebody unconnected with the organization.

what risks they pose

The motivation behind outsider threats are less likely to be for spite or vengeance (although it's not impossible), but rather financial gain. Outside threat actors don't typically know their targets, though of course they perform studious surveillance in order to craft a viable ruse.

the threats you face

How often do you hear news stories about a disgruntled ex-employee hacking his former company for revenge? Surely it happens, but the hard-hitters that tend to make news are those aimed at weak security postures with rich potential (literally). Cyber-threats aren't random. Criminals know how to seek out and pin down the weakest link, which is why EVERYONE needs cybersecurity awareness. Even you!



**They should have
used a Virtual Private
Network when they used
public WiFi**

"Cybersecurity is much more than a matter of I.T."

- Stéphane Nappo, Global CISO

7 STEPS TO CYBER- SECURITY

HOW TO STAY SAFE ONLINE

*while avoiding
digital threats*



WHY DIGITAL SECURITY MATTERS

*every second of
every day*

Cybersecurity (and all that entails) is a lot to keep in mind every moment that you spend on the Internet. Unfortunately, cybercriminals don't rest. They have access to the same tools as security professionals, including artificial intelligence. That means they can create their own automation to try and break into your accounts around the clock. This is just one of the many ways that they're leveraging advanced technology against your accounts.

As a result, you need to be just as vigilant and aggressive in your security practices. Password managers, which you may have heard of and even used before, keep your credentials secure and safely generate new ones on a regular basis to make it harder for hackers to get in - keeping the same credentials for years is just as dangerous as having a very simple password, without any combination of numbers and symbols to make it more difficult to guess. This is just one example of how technology has evolved to make daily security much easier to practice.



We all make mistakes: That's why you need backup security to make sure that YOU are not the first and only line of defense. Security teams and services can scan the network for abnormalities to take swift action after a breach. Automated processes stop the hacker from getting into certain areas of the network and notify you about the attempted access so that you can take steps to re-secure your account.

All of these are *in addition* to your hard work. Our online engagement must be tempered with caution to avoid catastrophic consequences.

STAYING SAFE

on a daily basis

PASS WORDS

Weak passwords are the basis for 81% of cyberattacks around the world, according to a WatchGuard Technologies. Creating complex passcodes, using different alphanumerical combinations for each account, and storing them in an encrypted Password Manager are simple preventative measures that can delay or offset the vast majority of breaches.

LOCK DOWN

When you leave your desk for even a second, you risk someone happening by and accessing private files on your computer, glancing at physical reports strewn about your desk or even stealing USBs.

Whether it's a cybercriminal who **piggybacked** into the building or a coworker who's been compromised and now poses an **insider threat**, lock up your workspace when you leave - even just for a coffee break.

RETYPE RETYPE RETYPE

Autofill is a convenient friend to those who visit the same websites often, and like their browser to save and input their log-in credentials, and even credit card info, when prompted in applicable textboxes.

A danger lies therein: A hacked database spills all your secrets, and a webpage that's been compromised could have invisible frames autofilling data that you don't want cybercriminals to know. Though painstaking, it's safest to retype your account information, personal and financial data every time.

VIGILANCE

When it comes down to more advanced social engineering scams, it can be extremely difficult to differentiate a valid email from a trap.

Pay attention to little signs. Is the domain name right? Is it from .com when it should be .org? Does the landing page show any company contact info? These are all little signs that it might be a scam.

AUTO-SCANS

In this day and age, automation is your best friend. In-depth and automated scans of the network notify you about suspicious activity. Advanced systems will immediately launch the appropriate response plan to start recuperation ASAP.

PRE-EMPTIVE TESTS

Why wait until a hacker tries to break into your important files? Run regular checks on your security posture to guarantee it's always up to date.

Penetration Tests, Risk Assessments and Vulnerability Assessments can help determine the weak points in your cybersecurity and the likelihood of a breach given common attacks at the time.

MFA

MFA, or Multi-Factor Authentication, has swept across the Internet in the past several years. Additional methods of proving your identity creates an extra obstacle for hackers, and extra security for you.

Face ID, fingerprint scans, one-time passwords (OTP), QR codes and voice recognition are all examples of MFA.



Bots hurt
your
system
with
malware,
data theft
and even
bringing
your
devices
into a
botnet!

Websites get visits from more than 2,600 bots every week.

Source: SiteLock

Automated bot attacks increased 894% in the second half of 2021.

Source: Statista Research Department

60% of botnets are dedicated to stealing your credentials.

Source: Enisa's 2020 Botnet report

BROWSING SECURELY

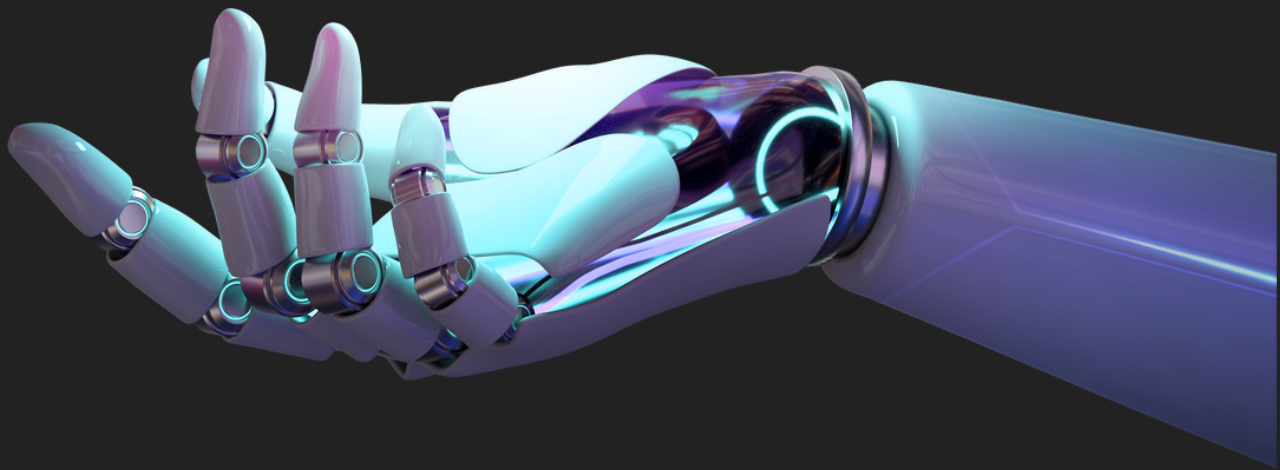
It's all well and good to be careful about preventing entry to your network, but what can you do to stay safe as you're browsing the web? So many devices connect to the Internet these days and so many businesses rely on WiFi to operate, it's inevitable to spend at least part of your day on the web. Thus it's crucial to be able to recognize signs that a website is not quite what it seems.

For example, most URLs begin with HTTPS:// or HTTP. The S stands for *secure*. Hypertext Transfer Protocol transfers and, when secure, encrypts the information on the page so you can safely view the content. It's a series of behind-the-scenes processes going on, to show you a screen that's simple and easy to navigate.

Beside the URL, secure sites often display an icon that resembles the outline of a padlock, indicating that it's been adequately vetted and received a digital certificate from a trusted third party company.

Websites created by reputable companies won't just throw you onto a landing page with their branding and a box for you to give away private data. Safe sites also display contact information for the company; such as their address, email, phone number and a way to "Contact Us." They'll advertise their social media and try to get you to browse their services or products. If none of that is visible, it's likely a phishing scam.

It can be difficult to use the world wide web as much as you want and simultaneously protect your privacy while browsing. Ensuring that the sites you're visiting are safe and secure will help you avoid a very common mistake that leads to more cyber breaches than need be. With widespread education, greater cyberattack prevention is possible. Reading this far means you've taken the first step!



"Machine intelligence is the last invention that humanity will ever need to make."

- *Nick Bostrom*

THE MORE YOU KNOW...

Rather than replacing jobs, AI increases productivity
(Source: PwC 2022 AI Business Survey)

Security solutions that include AI are more cost-effective - and just plain more effective!

AI increases leads by up to 50%
(Source: Harvard Business Review)

Still worried about losing your job to computers? AI is anticipated to create 2M jobs by 2045

AI is self-learning; the more data you input, the more accurate and efficient it becomes

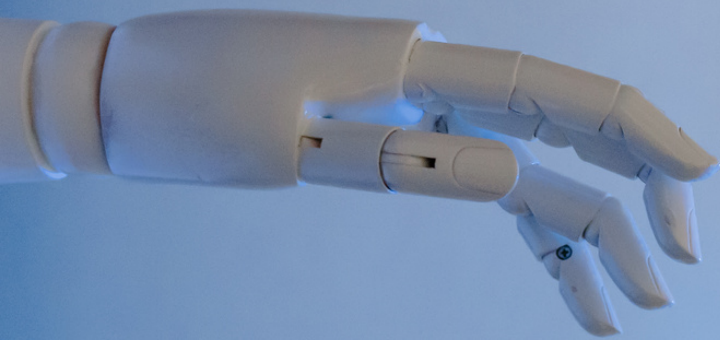


QR & AI

how these two
hands-off forces

revolutionized

our daily lives



The goal of mass digitization is to make information security easy to implement and strong enough to fight off cyberattacks. To do this, you must focus on securing those vulnerable areas of their network as it stands.

Vulnerability management is a very effective tool to mitigate the risk of a cyber-attack. Security vulnerabilities such as misconfigurations and missing patches can open gaping holes in the attack surface and cause data breaches. Vulnerability management attempts to help you secure your systems by identifying such weak points in their cybersecurity posture so that these weaknesses can be rectified before they are exposed and exploited, causing a nightmare scenario. To achieve this goal, you need a strong vulnerability management solution that is built on a solid security foundation with desired outcomes and well-established goals.

Gartner, Inc, a technological research and consulting firm, recommends that enhancing efficiency and remediation windows by employing technology that can automate vulnerability analysis. Automating vulnerability can significantly save time and effort.

This is where QR and AI come in.

QR, short for "quick response," are those squares of code you can find on most restaurant tables these days and even on bus stop advertisements! Smart phones cameras scan these codes and instantly redirect you to the appropriate landing page. Considering the past several years, it's no surprise that QR codes have become a popular tool for assuaging concerns about social distance while also providing faster service than supply disruptions and short-staffed places may otherwise be able to offer.

At the same time, digitization has also hastened the development of AI. Businesses use artificial intelligence to scan for abnormalities on the network, including users accessing unauthorized areas or activity at unusual hours. It can even scan the Dark Web for signs of your personally identifiable information (PII).

Together, these advancements in hands-off digital technology have changed the game for everyone who uses the Internet - so, just about everyone.

BEWARE!

TOO MUCH OF A GOOD THING?

#1

Cybercriminals are just as capable of creating a QR code and pinning it on the nearest signpost. Check the URL before clicking ahead!

#2

AI can be used for good just as easily as evil. Threat actors relying on AI can often be thwarted by smarter, better AI working to protect your systems.

WHY HAVE QR CODES BEEN SUCH A HIT?



With massive amounts of data stored within that code, it can access and display the correct information for the user in seconds. Just like a barcode. Each associated landing page or product is unique, making it easier for the system to identify the correct place to redirect the user.

Unlike a barcode, QR codes store more information. Barcodes store enough information to be read horizontally, but also include repeated information so that they work even when partially destroyed (how easy is it for library barcodes to get scuffed from putting books back on the shelves?); but QR codes can be read in multiple additional directions.

TFA

Two-factor authentication is a great place to implement QR. You can download a specific app to reads the codes and generate a OTP (one-time password). This is a great way to protect yourself and your data from malicious AI.

QR CODES IN 2022



Juniper Research:

This year, an expected total of 5.3B codes will be scanned.

eMarketer:

QR code users will increase from \$83M this year to \$99.5M by 2025.

Better Business Bureau:

The amount of fake QR codes set up to scam users out of financial information has risen in the past year.

Error correction:

QR codes can sustain up to 30% of damage to their physical structure and still work, because of what's known as "error correction."

Kleiner Perkins Caufield & Byers, Visa Inc., and GfK:

4% of all global consumer transactions take place with the use of QR codes.

ARTIFICIAL INTELLIGENCE

a leader in threat detection

Artificial intelligence, known better as AI, refers to the technological advancements that give computers the capability to self-learn tasks and functions. AI has exploded since the early 2010s and is expected to become a **\$35B industry by 2028**, three times what its current worth. What may have started as Facebook suggesting friends to tag in photos has now spawned facial recognition software, automated services that detect suspicious behavior on your network, Dark Web monitoring and so much more.

Machine learning makes AI capable of identifying patterns and making the smartest possible choices, so they can keep running without too much manual oversight.

If an AI that was created with good intentions uses machine learning to understand what a "real" user looks like before allowing them onto the platform, then that profile is based on the legitimate people in the system, new visitors, common spam for your industry, and other logistics that add up to determine whether the web traffic is a threat and respond appropriately.

You've likely come across this concept before. Think about your email platform of choice. Does it automatically detect and filter spam into a separate Junk folder? How do you think it makes those determinations?

Essentially, AI learns by programmers feeding it "good" and "bad" code, and then it learns on its own how to identify threats versus safe web traffic based on that foundational knowledge.

AVOIDING CYBERCRIMINAL AI

what is poisoned AI and how to combat it

When cybercriminals are skilled and inclined, they can create malicious code and feed it into larger datasets, where the poisoned data will be more or less lost in the overwhelming mass of information. Thus artificial intelligence will believe that these snippets of code are, in fact, harmless when they're not; hackers can later trick those so-called "poisoned AIs" into opening a backdoor for easy infiltration into your network.

Of course, ideally you have more safeguards in place than one single AI machine, but nonetheless the threat of poisoned AI is a blow to front-line defenses. Recent data suggests that backdoors can bypass security defenses just by poisoning as little as 0.7% of inputted data.

"Machine learning makes AI capable of identifying patterns and making best-case choices, so they can keep running without too much manual oversight."

It's just short of impossible to sort through every dataset your AI encounters, and would also be incredibly time-consuming to find a needle in that big of a haystack. Nevertheless, security specialists should check in on their AI inputs now and then to guarantee that the information is properly labeled and sorted.

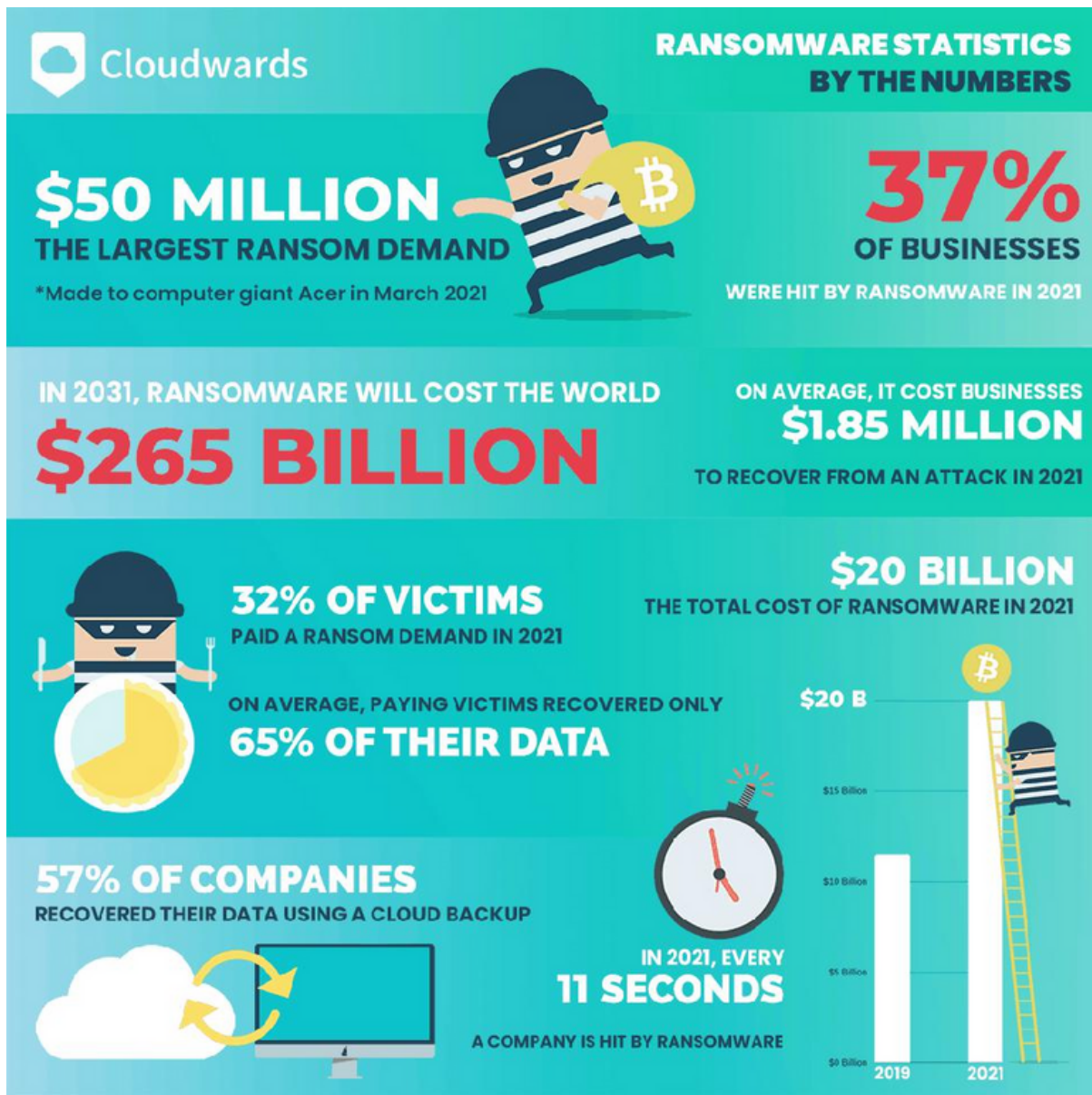
Although it builds accuracy to train AI with a larger database, that often means using open source code which is exactly how the cybercriminal would pass on their poisoned data. Companies can, instead, use less data which they can guarantee is "clean" from malicious code, and extrapolate from there.

"When digital transformation is done right, it's like a caterpillar turning into a butterfly, but when done wrong, all you have is a really fast caterpillar."

- *George Westerman, MIT Sloan Initiative*



DID YOU KNOW?



80% of victims who pay ransomware never get their data back anyway.

Source: Cybereason's 2022 report Ransomware: The True Cost to Business



DATA BREACHES IN 2021

| 212
M

users affected

| 6B

records exposed

| 10K

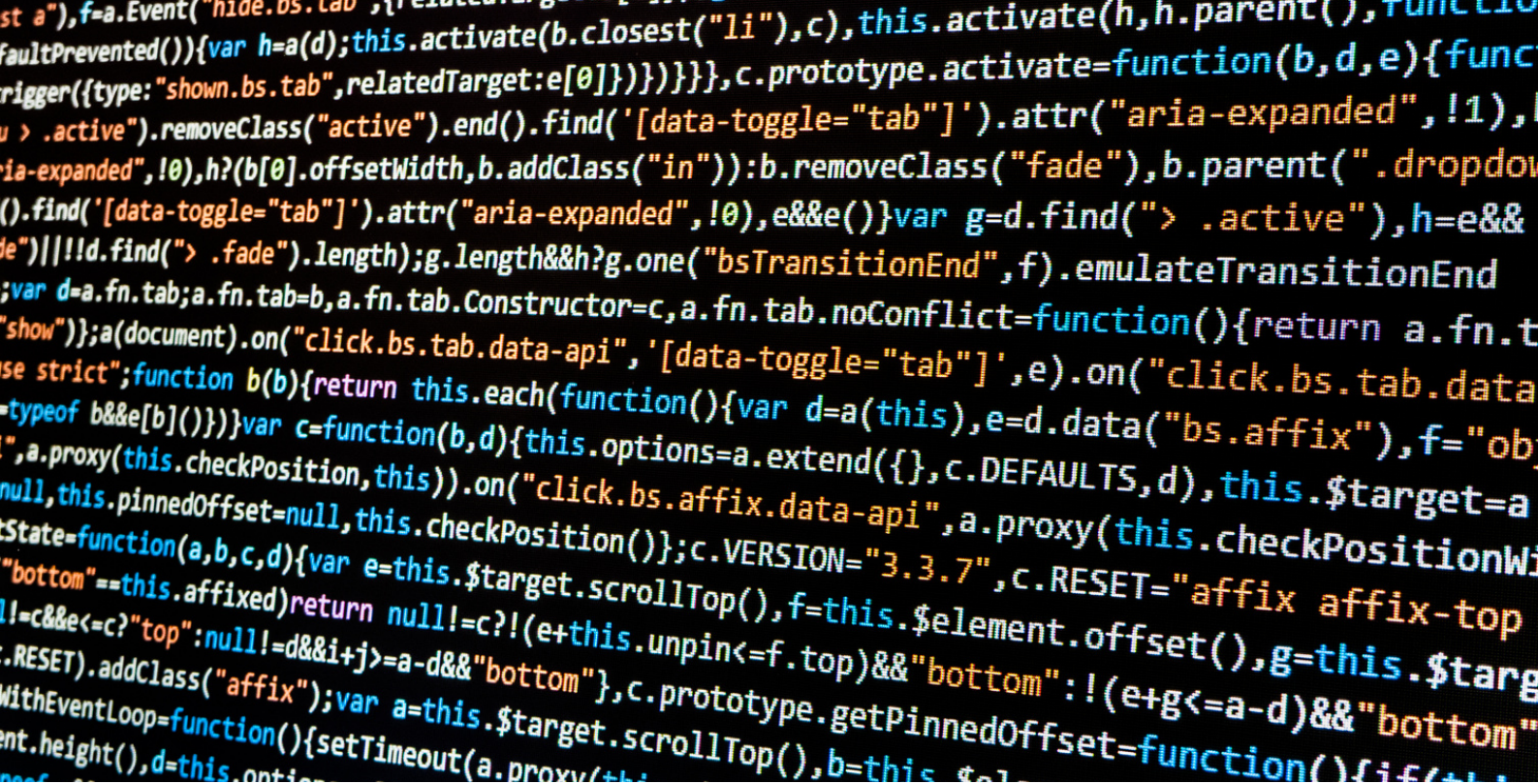
*dollars average
in ransom*

SO FAR, TOO LATE: DATA BREACHES IN 2022

Hackers are only getting more audacious with every new trick they gain. Botnets, which are connected webs of infected devices, are weaponized in Distributed Denial-of-Service (DDoS) attacks. Ransomware demands rise every year. Hackers can get \$30-80 per social media account on the Dark Web!

Their ambitions, and hence the stakes, are getting higher. Heeding your Security Awareness Training and refreshing your knowledge regularly can help keep your accounts protected from hackers.

Never give out private information on public profiles, stop to assess emails encouraging you to act quickly, and keep your personal and professional accounts separate.



REAL DATA LEAK EXAMPLE

*the breach that sent
Australia reeling*

In September 2022, the Australian telecom company, Optus, experienced a data breach that compromised nearly 10M customer records. Nearly 40% of Australia's population might have had their names, birthdays, phone number, email and home addresses, driver's licenses, and even passport numbers leaked in the event.

Optus launched an investigation and notified authorities, as well as financial institutions, about the breach. The event throws into question our data's security when we entrust so much personally identifying information (PII) to telecom companies.

You may have heard about various cybersecurity laws being passed throughout multiple countries in the past few years. Many of them, like the U.S. Cyber Incident Reporting for Critical Infrastructure Act of 2022, are aimed directly at protecting those systems necessary to our day to day lives. Everything from communication to transportation comprises the "critical infrastructure" that has been experiencing more online attacks and, thus, beholden to the subsequent laws made to protect these various industries.

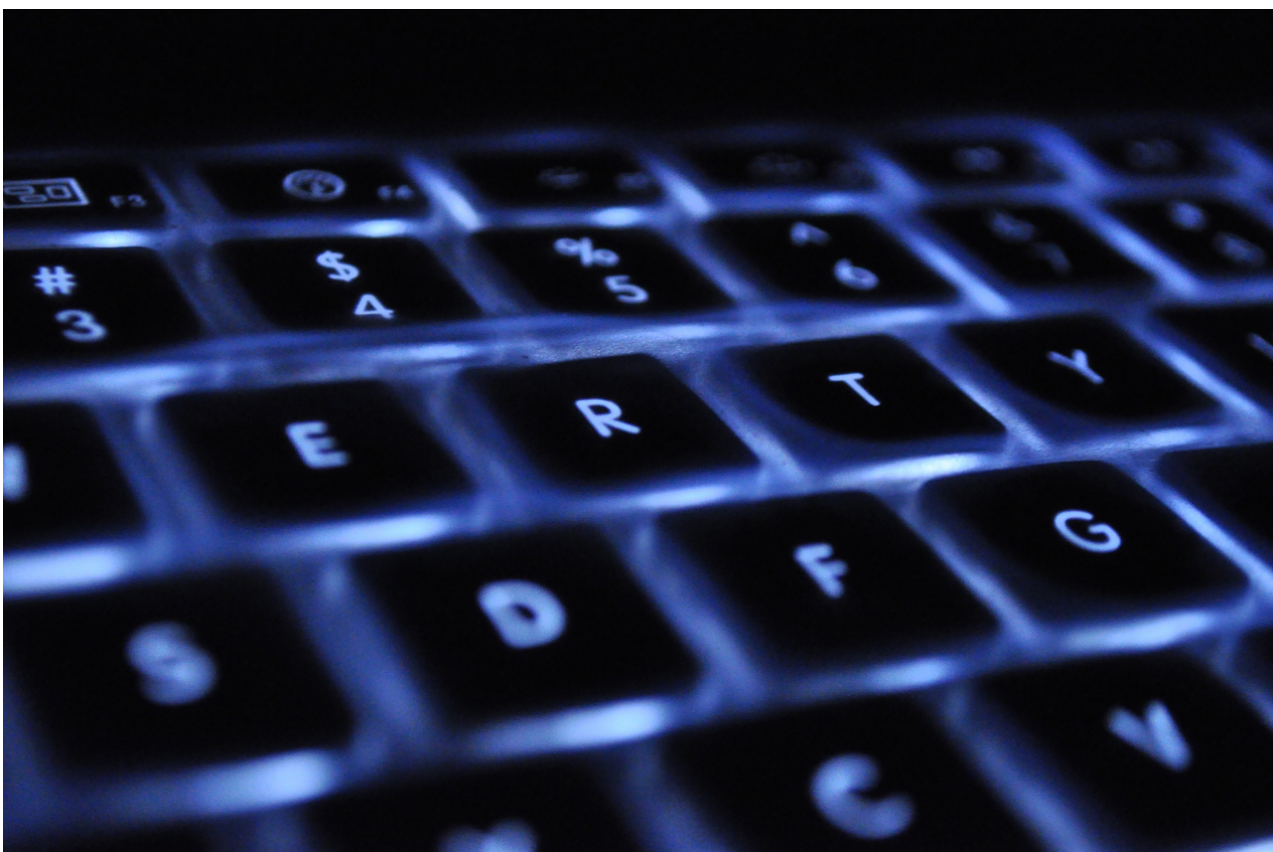
Cyber-attacks against critical infrastructure pose a risk to national security as well as being a frustrating disruption to our lives. Given the capabilities of today's technology, consumers expect ultimate efficiency in every online interaction. Organizations of ALL sizes need to beware what cyber-threats they're opening themselves up to when investing in later and greater technology; and especially those, like Optus, who hold valuable information on millions of people.

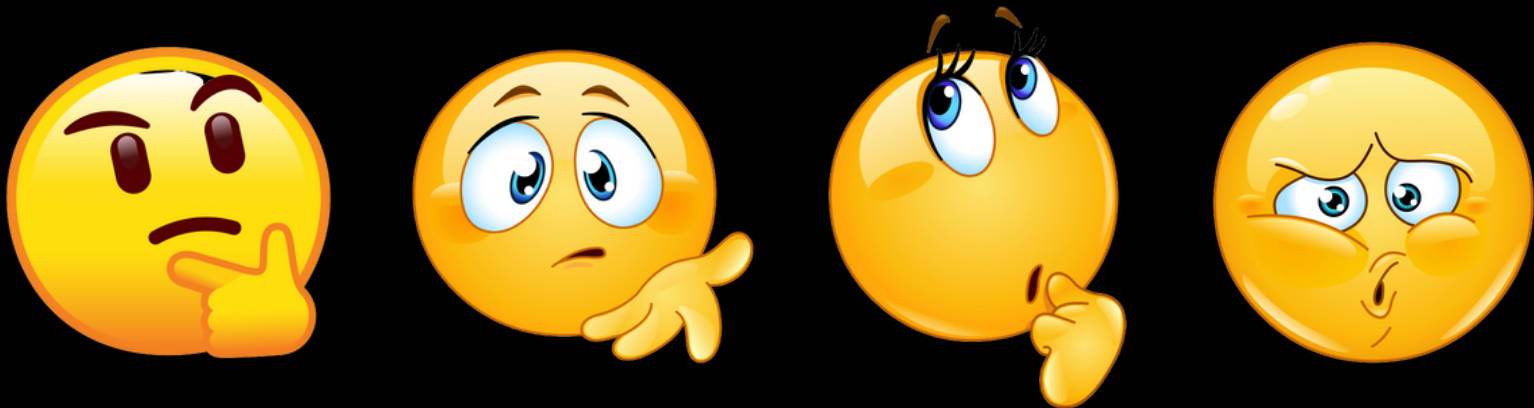
To safely store and retrieve your account information as needed, telecom companies save customer data in a remote and encrypted cloud server. This means that theoretically only those with your password and log-in can access those files. For cloud services just getting on their feet, this introduces room for Zero-day attacks and new vulnerabilities.

How can we defend against these risks? Enable multi-factor authentication to verify your identity elsewhere, like SMS message or one-time passwords, before accessing any account information. Additionally, you should always choose vendors who invest as much into cybersecurity as they do in shiny new devices.

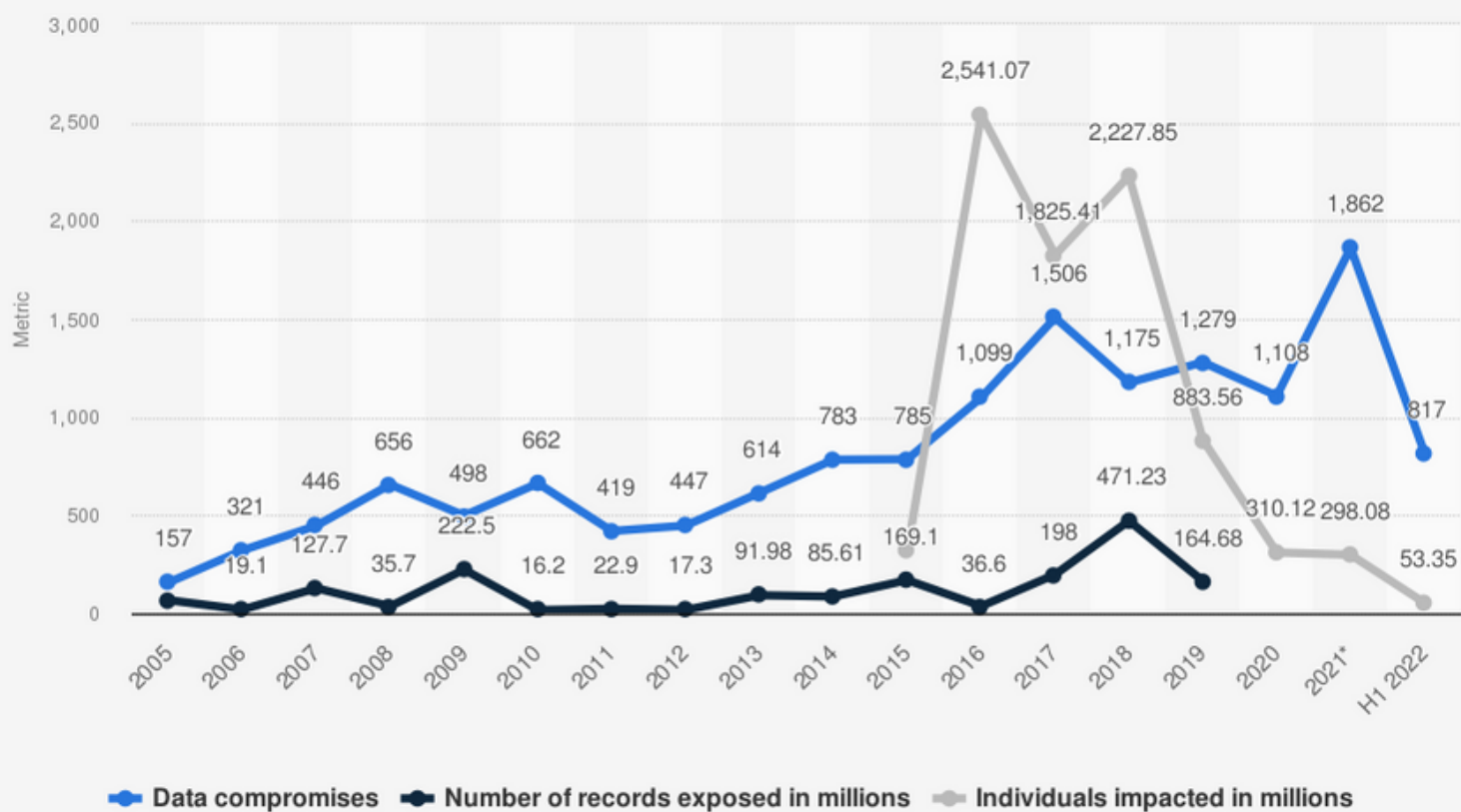
Optus was one of the latest telecom companies to experience a data breach, but they aren't the first and won't be the last database to get hacked. Any service provider that you give access to so much personal information is an additional avenue for hackers to find it. While you can't avoid a phone plan in 2022, you can take steps to safeguard your accounts and choose service providers that invest in threat mitigation before they explode into data breaches.

In the meantime, you can do little things every day to improve the security of all your favorite screens. Add extra security measures to your accounts or use single sign-on so compromised credentials don't necessarily equal data theft. Use different emails and passwords for all your profiles so if one is found on the Dark Web, the rest are still protected.





Annual number of data compromises and individuals impacted in the United States from 2005 to first half 2022

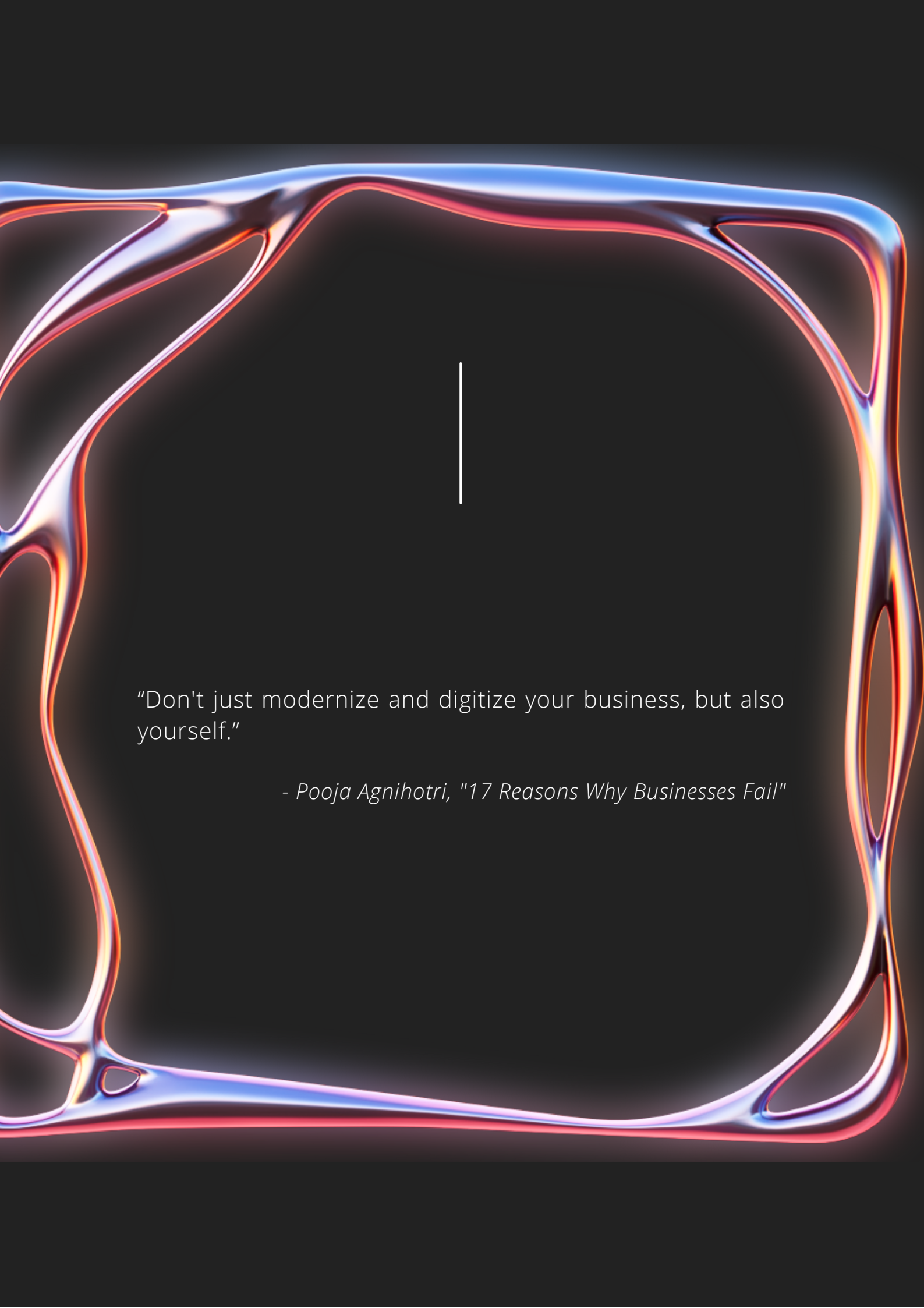


Source
Identity Theft Resource Center
© Statista 2022

Additional Information:
United States; Identity Theft Resource Center; 2005 to H1 2022; data compromises include data breaches, data exposure
impacted may go beyond the United States

It doesn't take a genius mathematician to read this graph and tell that the total number of people impacted and data exposed has been rising every year for the past two decades. It suggests that we're not likely to see cybercriminals back off as we get closer to 2030!





"Don't just modernize and digitize your business, but also yourself."

- Pooja Agnihotri, "17 Reasons Why Businesses Fail"

REAL REVIEWS FROM CLIENTS!



<https://restech.solutions>

Bob Pohl

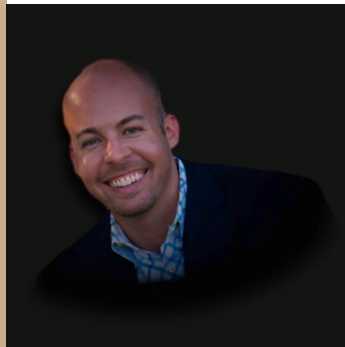


— Furnishings Unlimited



We are confident any issue will be taken care of and know our issues will be resolved in a timely manner. ResTech delivers what they promise.

Eric Spillane



— Performance Seals



ResTech has a wide range of knowledge and is willing and able to roll up their sleeves and assist with managing our IT environment. This sets ResTech apart from all other firms.

Melissa Brown



— Brown Bookkeeping Services



ResTech has been amazing to work with. When I would reach out with an issue ResTech would respond with straight forward and honest communications.

CYBERSECURITY YOU CAN TRUST!



We believe in providing YOU the best-in-class security suite to keep you cyber-secure in the face of the ever-changing threat landscape.

Call us today at **713-936-6855** and let us help you wrap a security blanket around your business.