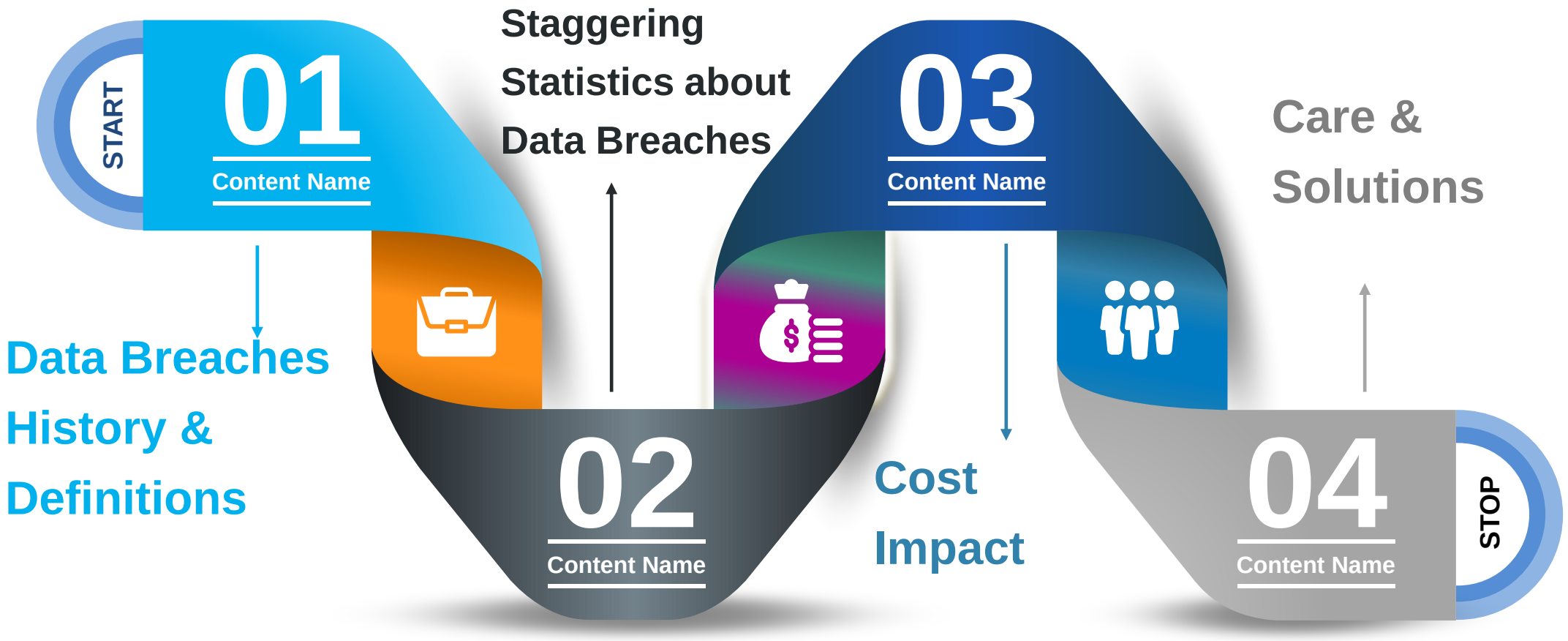
Data Breaches
Facts and Impacts

A short discussion with FDPPI Members

By
S.P. Arya

Presentation Flow



History of Cyber Threats

01

History of Cyber Threats

When it comes to cyber Threat/Security, there are few terms with more name recognition than “Computer Viruses." Despite the prevalence of these threats and their wide-spread impact, however, many users don't know about the basic nature of viruses. Here is a brief history of the Computer Virus, and which is the origin of widespread cyber threats we see today.

Theory of Self-Replicating Automata

What is a computer virus? This idea was first discussed in a series of lectures by mathematician John von Neumann in the late 1940s and a paper published in 1966, Theory of Self-Reproducing Automata. The paper was effectively a thought experiment that speculated that it would be possible for a "mechanical" organism—such as a piece of computer code—to damage machines, copy itself and infect new hosts, just like a biological virus.

The Creeper Program

As noted by Discovery, the Creeper program, often regarded as the first virus, was created in 1971 by Bob Thomas of BBN. Creeper was actually designed as a security test to see if a self-replicating program was possible. It was—sort of. With each new hard drive infected, Creeper would try to remove itself from the previous host. Creeper had no malicious intent and only displayed a simple message: "I'M THE CREEPER. CATCH ME IF YOU CAN!"

The Rabbit Virus

According to InfoCarnivore, the Rabbit (or Wabbit) virus was developed in 1974, did have malicious intent and was able to duplicate itself. Once on a computer, it made multiple copies of itself, severely reducing system performance and eventually crashing the machine. The speed of replication gave the virus its name.

The Brain Boot Sector Virus

Brain, the first PC virus, began infecting 5.2" floppy disks in 1986. As Securelist reports, it was the work of two brothers, Basit and Amjad Farooq Alvi, who ran a computer store in Pakistan. Tired of customers making illegal copies of their software, they developed Brain, which replaced the boot sector of a floppy disk with a virus. The virus, which was also the first stealth virus, contained a hidden copyright message, but did not actually corrupt any data.

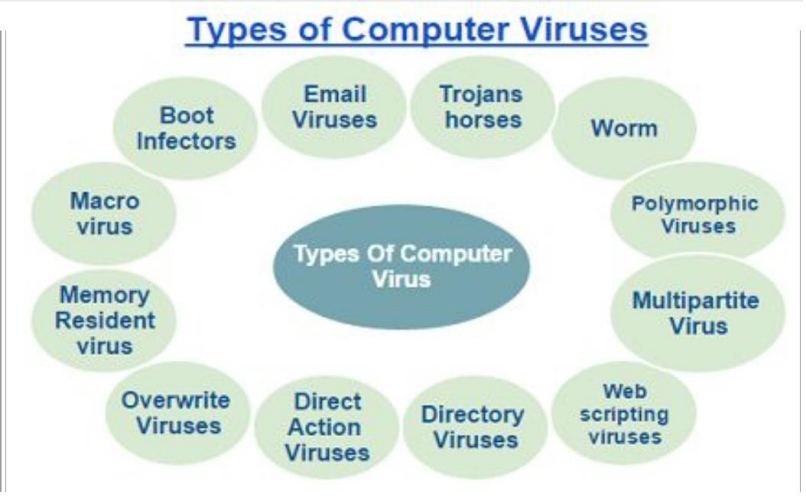
History of Cyber Threats

In 1991, the "Michelangelo" virus was first discovered in Australia. It would lay dormant until 6th March every year and then overwrite the first one hundred sectors on the storage devices with zeros, preventing the computer from booting. Only 20,000 computers were reported infected.

In 1998, CIH was released. It infected around 60 million computers and caused significant damages by overwriting important system files. It was written by a Taiwanese student.

In 1999, "Melissa" was released. This one, was the first wide spread Word Macro Virus. It was distributed via email and would automatically send itself to the first 50 people in the Outlook address book. It did not harm the computer as it was sending out passwords for some erotic websites which required membership. It caused so much email traffic resulting in email servers to crash.

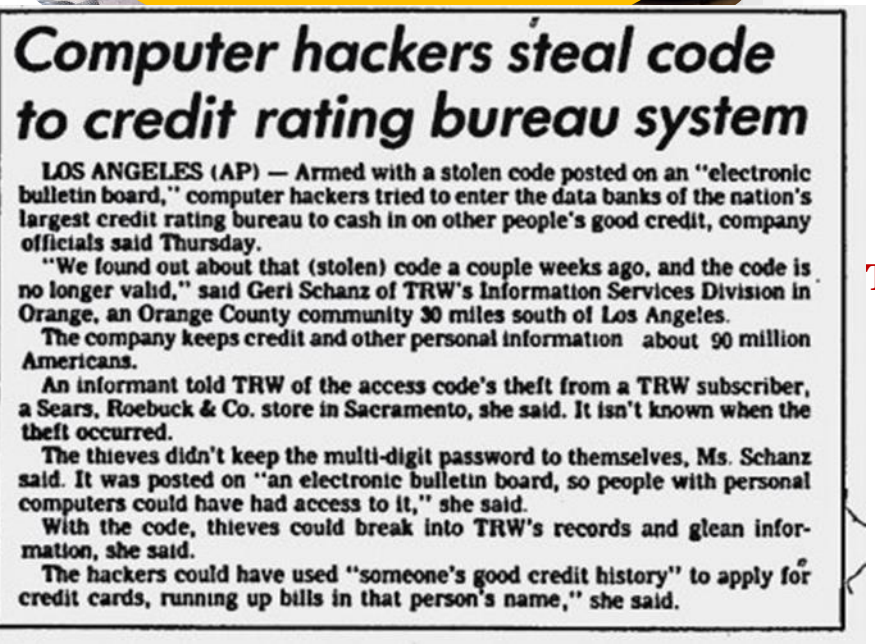
2000 was the year of "iloveyou". Again, it came via email however it sent itself to all contacts. It also overwrote office, image, and audio files. The virus came from the Philippines and infected over 50 million computers in less than 10 days. Most companies back then decided to turn off their email servers to stop spreading the virus.



The Code Red Virus

The Code Red worm was a "file less" worm—it existed only in memory and made no attempt to infect files on the system.

Evolution of Data Breach



Computer hackers steal code to credit rating bureau system

LOS ANGELES (AP) — Armed with a stolen code posted on an "electronic bulletin board," computer hackers tried to enter the data banks of the nation's largest credit rating bureau to cash in on other people's good credit, company officials said Thursday.

"We found out about that (stolen) code a couple weeks ago, and the code is no longer valid," said Geri Schanz of TRW's Information Services Division in Orange, an Orange County community 30 miles south of Los Angeles.

The company keeps credit and other personal information about 90 million Americans.

An informant told TRW of the access code's theft from a TRW subscriber, a Sears, Roebuck & Co. store in Sacramento, she said. It isn't known when the theft occurred.

The thieves didn't keep the multi-digit password to themselves, Ms. Schanz said. It was posted on "an electronic bulletin board, so people with personal computers could have had access to it," she said.

With the code, thieves could break into TRW's records and glean information, she said.

The hackers could have used "someone's good credit history" to apply for credit cards, running up bills in that person's name," she said.

The start of the era of Cyber Crimes (Data Breach/Theft)

- **The earliest case, of data breach, was identified, when an incident occurred with credit reporting agency TRW Information Systems. In 1984, they were informed that the password of one of their databases had been stolen and posted online on an electronic bulletin board, exposing the personal data and credit histories of 90 million Americans.**

- Historically most sources cite **2005** as the year that the current era of frequent large-scale data breaches began. As high as **136 data breaches** were reported that year, which included **George Mason University** (names, pictures, and Social Security numbers of 32,000 students and staff), **DSW Designer** Shoe Warehouse (1.4 million credit card numbers), and CardSystems Solutions (40 million credit card numbers), among others.

- **2005** was also the year that hacker Albert Gonzalez masterminded a breach of retail giant TJX Companies where **45.6 million** credit card numbers were stolen from one of its systems over a period of more than **18 months**, culminating in **2007.**

And it was in 2007 when Gonzalez launched "Operation Get Rich or Die Tryin", another set of data breaches that targeted Heartland Payment Systems (130 million credit card numbers), Hannaford Brothers (4.2 million credit card numbers), and other organizations.

The big one

More major data breaches continued to make headlines into the 2010s, media outlets were throwing around the label "the largest to date" quite a lot, But the true "largest data breach to date" was right around the corner.

Evolution of Data Breach

Continued….Evolution of the cybersecurity threat

In 2013 the new form of ransomware started with the CryptoLocker virus. There have been many new versions of this virus including Locky and WannaCry, as well as Petya (not the latest version). The original CryptoLocker virus infected about half a million computers in its original version. Some of these clones, such as TorrentLocker or CryptoWall, were specifically designed to target computers in Australia.

- In September 2016, Yahoo! disclosed that a data breach had taken place some time in late 2014. 500 million user accounts, including account names, email addresses, telephone numbers, dates of birth, hashed passwords, and in some cases, encrypted or unencrypted security questions and answers had been compromised.
- In 2017 year we have had virus attacks which spread very fast:
- WannaCry and NotPetya. Both of these viruses used a security hole within the protocol Windows uses to access files over the network (SMB).
- This security hole, named EternalBlue, was made public by a Hacker group called "Shadow Brokers", who stole it from the US National Security Agency (NSA).
- Microsoft later released a patch for this vulnerability in March 2017, the number of systems worldwide based on obsolete/unsupported software, or that had not yet applied the latest updates, allowed WannaCry to gain a strong foothold through a phishing email attack.
- WannaCry infected around 200,000 computers across 150 countries before the "Kill switch" was discovered and stopped the virus from spreading further.

While above viruses and malware were used to either block the data uses or destroy the same but these later evolved into data breach or theft gradually. **Malware** and **Ransomware** lead it from front in creating havoc across the world.

01a

About Data Breaches

The definition

A **data breach** is an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner.

Technically, there's a distinction between a **security breach** and a **data breach**. A security breach is effectively a break-in, whereas a data breach is defined as the cybercriminal getting away with Data/ information.

- Stolen data may involve sensitive, personal, proprietary, or confidential information such as credit card data, customer data, health records, trade secrets, or matters of national security, payment card information (PCI), personal health information (PHI) and **personally identifiable information (PIIs)**
- A small company or large organization or an individual may suffer a data breach.

How Data Breach Happens

Most data breaches are attributed to **hacking** or **malware attacks**. Other frequently observed breach methods include the following:

Insider leak: A trusted individual or person of authority with access privileges steals data.

Payment card fraud: Payment card data is stolen using physical skimming devices.

Unknown: In a small of number of cases, the actual breach method is unknown or undisclosed

Unintended disclosure: Through mistakes or negligence, sensitive data is exposed.

Loss or theft: Portable drives, laptops, office computers, files, mobiles and other physical properties are lost or stolen.

Ransomware

Ransomware is software that gains access to and locks down access to vital data. Files and systems are locked down and a ransom is demanded commonly in the form of cryptocurrency.

How data breaches happen..

•**Research:** The attacker, having picked a target, looks for weaknesses to exploit: employees, systems, or the network. This entails long hours of research on the attacker's part and may involve stalking employees' social media profiles to find what sort of infrastructure the company has.

•**Attack :**Having scoped a target's weaknesses, the attacker makes initial contact either through a network-based or social attack.

- In a **network-based** attack, the attacker exploits weaknesses in the target's infrastructure to instigate a breach. These weaknesses may include, but are not limited to SQL injection, vulnerability exploitation, and/or session hijacking.
- In a **social** attack, the attacker uses social engineering tactics to infiltrate the target network. This may involve a maliciously crafted email sent to an employee, tailor-made to catch that specific employee's attention. The email can phish for information, fooling the reader into supplying personal data to the sender, or come with a malware attachment set to execute when downloaded.

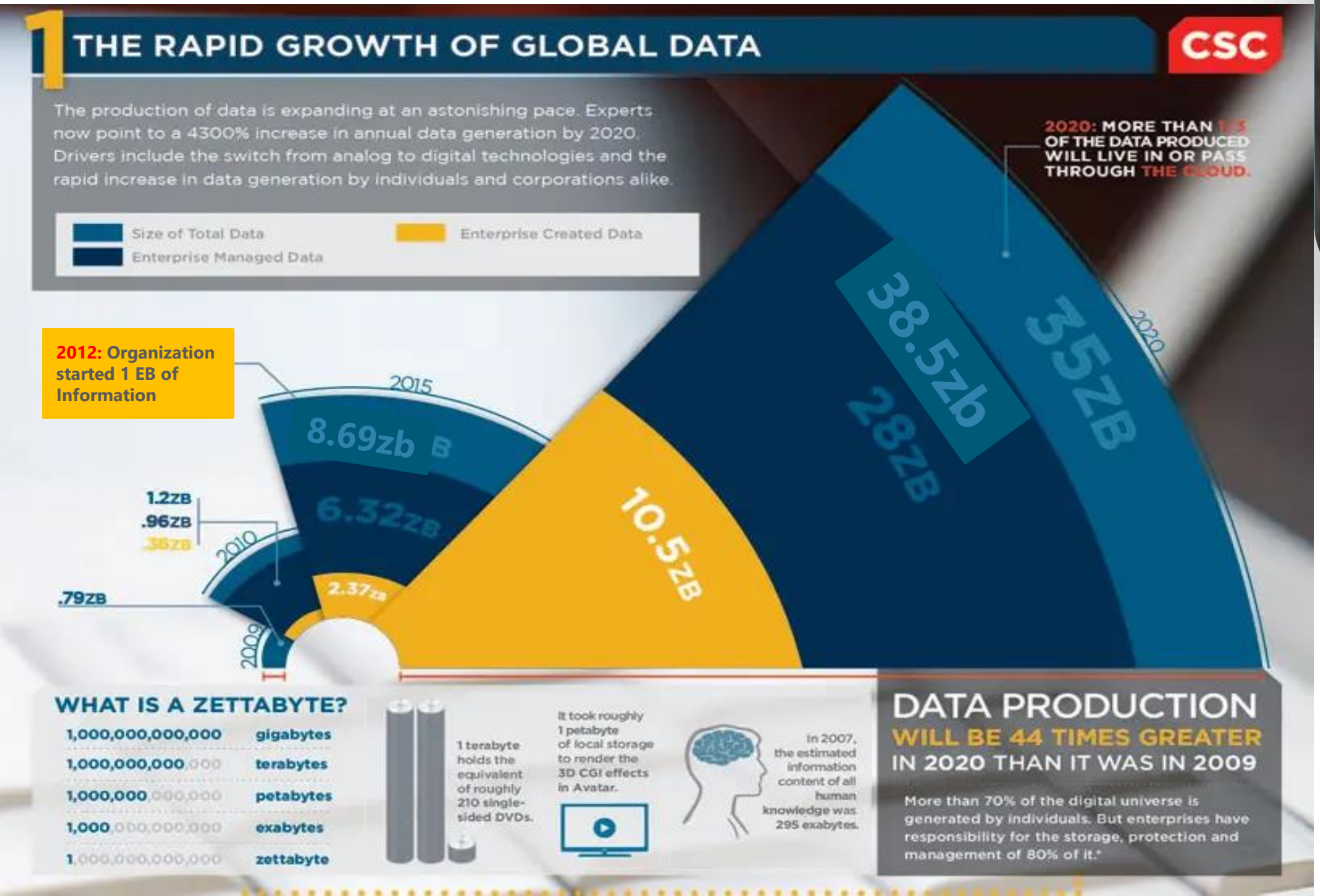
•**Exfiltrate**

Once inside the network, the attacker is free to extract data from the company's network. This data may be used for either blackmail or cyber propaganda. The information an attacker collects can also be used to execute more damaging attacks on the target's infrastructure.

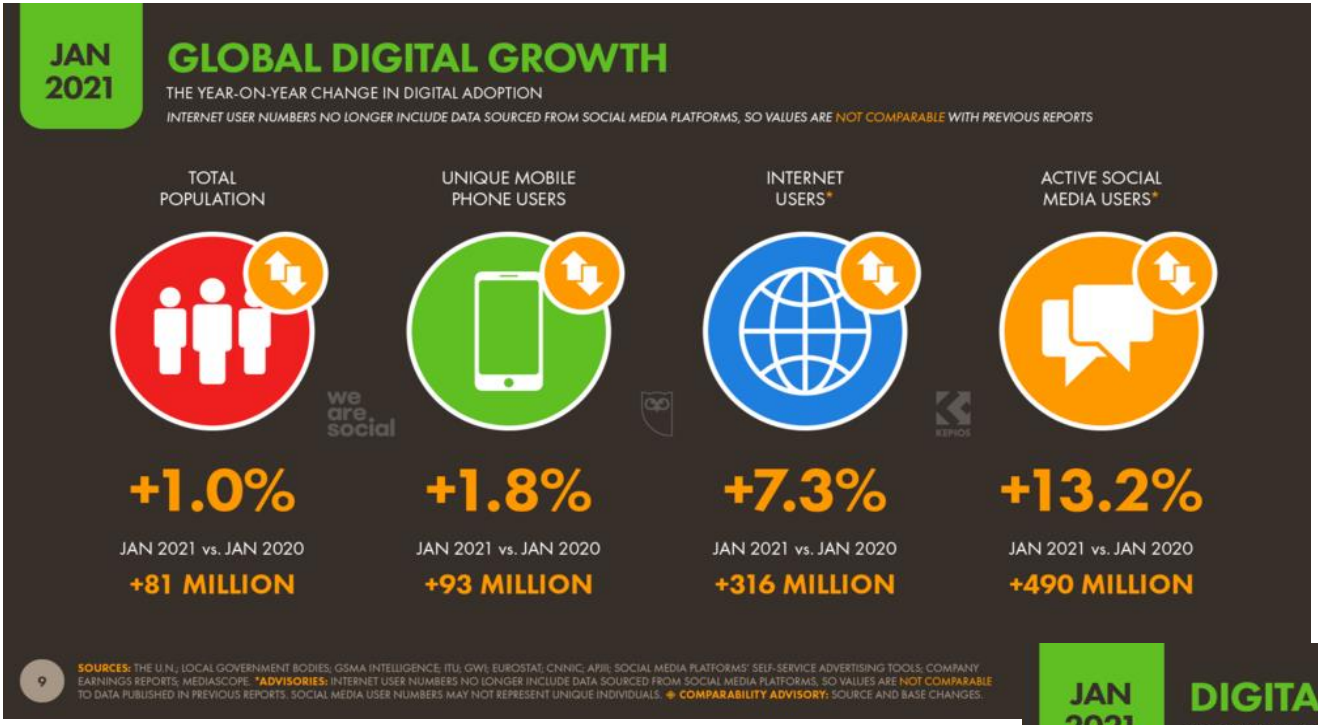
02

Staggering Statistics

Data size world is generating



Some important Data breaches Stats



Some important Data breach Stats

JAN 2021

SHARE OF WEB TRAFFIC BY DEVICE

EACH DEVICE'S SHARE OF TOTAL WEB PAGES SERVED TO WEB BROWSERS

⚠ THE FIGURES ON THIS CHART ARE BASED ON TRAFFIC TO WEB BROWSERS ONLY, AND DO NOT INCLUDE DATA FOR OTHER CONNECTED ACTIVITIES (E.G. USE OF NATIVE MOBILE APPS)

MOBILE PHONES	LAPTOPS & DESKTOPS	TABLET COMPUTERS	OTHER DEVICES
55.7%	41.4%	2.8%	0.07%
DEC 2020 vs. DEC 2019:	DEC 2020 vs. DEC 2019:	DEC 2020 vs. DEC 2019:	DEC 2020 vs. DEC 2019:
+4.6%	-5.8%	+3.3%	[UNCHANGED]
+244 BPS	-253 BPS	+9 BPS	

44 SOURCE: STATCOUNTER (ACCESSED JAN 2021). FIGURES REPRESENT EACH DEVICE'S SHARE OF WEB PAGES SERVED TO WEB BROWSERS ONLY. NOTES: FIGURES FOR DEVICE SHARE ARE FOR DECEMBER 2020; ANNUAL CHANGE FIGURES COMPARE MONTHLY SHARE VALUES FOR DECEMBER 2020 TO DECEMBER 2019. PERCENTAGE CHANGE VALUES REPRESENT RELATIVE CHANGE (I.E. AN INCREASE OF 20% FROM A STARTING VALUE OF 50% WOULD EQUAL 60%, NOT 70%). 'BPS' VALUES REPRESENT BASIS POINTS, AND INDICATE THE ABSOLUTE CHANGE IN SHARE VALUES.

JAN 2021

SOCIAL MEDIA USE AROUND THE WORLD

USE OF SOCIAL NETWORKS AND MESSENGER SERVICES, WITH DETAIL FOR MOBILE SOCIAL MEDIA USE

⚠ SOCIAL MEDIA USER NUMBERS MAY NOT REPRESENT UNIQUE INDIVIDUALS

TOTAL NUMBER OF ACTIVE SOCIAL MEDIA USERS*	SOCIAL MEDIA USERS AS A PERCENTAGE OF THE GLOBAL POPULATION	ANNUAL CHANGE IN THE NUMBER OF GLOBAL SOCIAL MEDIA USERS	TOTAL NUMBER OF SOCIAL MEDIA USERS ACCESSING VIA MOBILE PHONES	PERCENTAGE OF TOTAL SOCIAL MEDIA USERS ACCESSING VIA MOBILE
4.20 BILLION	53.6%	+13.2% +490 MILLION	4.15 BILLION	98.8%

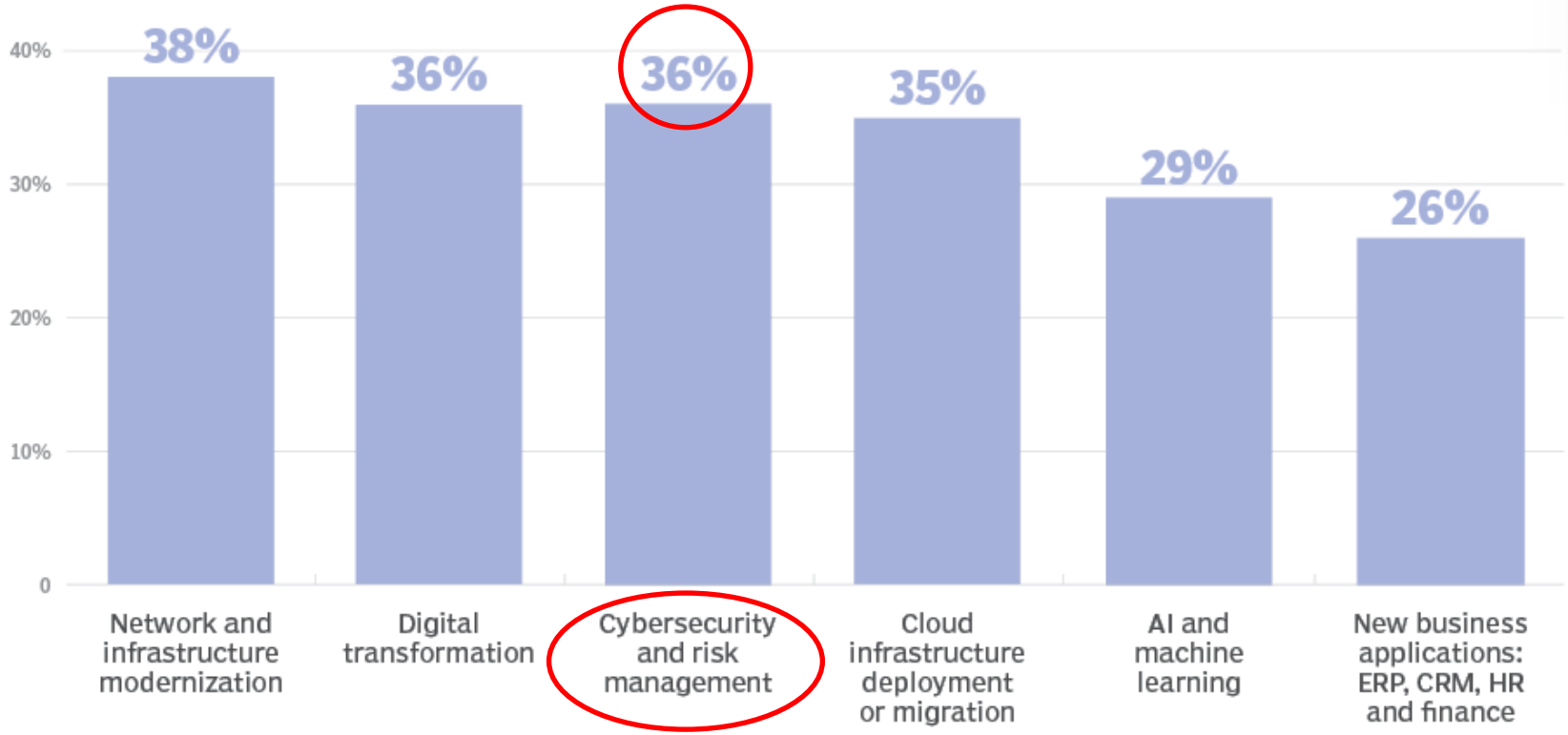
79 SOURCES: KEPIOS (JAN 2021), BASED ON EXTRAPOLATIONS OF DATA FROM: COMPANY EARNINGS ANNOUNCEMENTS; PLATFORMS' SELF-SERVICE ADVERTISING TOOLS; CNNIC; MEDIASCOPE. *ADVISORY: SOCIAL MEDIA USERS MAY NOT REPRESENT UNIQUE INDIVIDUALS, AND MAY EXCEED INTERNET USER NUMBERS IN SOME COUNTRIES. ◆ COMPARABILITY ADVISORY: BASE CHANGES AND HISTORICAL REVISIONS. DATA MAY NOT CORRELATE WITH FIGURES PUBLISHED IN PREVIOUS REPORTS.

we are social Hootsuite

Data breached Contd……

Top IT spending drivers

Before the COVID-19 outbreak became a global pandemic, survey respondents said these technology initiatives would have the biggest impact on their IT spending plans in 2020



SOURCE: TECHTARGET'S 2020 IT PRIORITIES SURVEY
BASED ON RESPONSES FROM 2,437 IT AND BUSINESS EXECUTIVES, MANAGERS AND STAFFERS WORLDWIDE SURVEYED BETWEEN NOVEMBER 2019 AND FEBRUARY 2020.

10 Largest data breaches

(in terns of number of users affected)

1

Yahoo : Date: August 2013 but was revealed in 2016

Impact: 3 billion yahoo accounts were exposed.

Securing the number one spot – almost seven years after the initial breach and four since the true number of records exposed was revealed – is the attack on Yahoo. The company first publicly announced the incident – which it said took place in 2013 – in December 2016.

2

Alibaba: Date: November 2019

Impact: 1.1 billion pieces of user data

Over an eight-month period, a developer working for an affiliate marketer scraped customer data, including usernames and mobile numbers, from the Alibaba Chinese shopping website, Taobao, using crawler software that he created.

3

LinkedIn : Date: June 2021

Impact: 700 million users

Professional networking giant LinkedIn saw data associated with 700 million of its users posted on a dark web forum in June 2021, impacting more than 90% of its user base.

4

Sina Weibo : Date: March 2020

Impact: 538 million accounts

With over 600 million users, Sina Weibo is one of China's largest social media platforms. In March 2020, the company announced that an attacker obtained part of its database, impacting 538 million Weibo users and their personal details including real names, site usernames, gender, location, and phone numbers.

5

Facebook : Date: April 2019

Impact: 533 million users

In April 2019, it was revealed that two datasets from Facebook apps had been exposed to the public internet. The information related to more than 530 million Facebook users and included phone numbers, account names, and Facebook IDs.

10 Largest data breaches

(in terns of number of users affected)

6

Marriott International (Starwood) : Date: September 2018

Impact: 500 million customers

Hotel Marriot International announced the exposure of sensitive details belonging to half a million Starwood guests following an attack on its systems in September 2018. Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database and net work was compromised in 2014

7

Adult Friend Finder : Date: October 2016

Impact: 412.2 million accounts

The adult-oriented social networking service The FriendFinder Network had 20 years' worth of user data across six databases stolen by cyber-thieves in October 2016. Given the sensitive nature of the services offered by the company it was quite sensitive breach. It was offered on sale on dark web.

8

MySpace : Date: 2013

Impact: 360 million user accounts

Though it had long stopped being the powerhouse that it once was, social media site MySpace hit the headlines in 2016 after 360 million user accounts were leaked onto both LeakedSource.com and put up for sale on dark web market

9

NetEase : Date: October 2015

Impact: 235 million user accounts

NetEase, a provider of mailbox services through the likes of 163.com and 126.com, reportedly suffered a breach in October 2015 when email addresses and plaintext passwords relating to 235 million accounts were being sold by dark web marketplace vendor DoubleFlag. Being Chinese site it remained unverified.

10

Court Ventures (Experian) : Date: October 2013

Impact: 200 million personal records

Experian subsidiary Court Ventures fell victim in 2013 when a Vietnamese man tricked it into giving him access to a database containing 200 million personal records by posing as a private investigator from Singapore. The details of Hieu Minh Ngo's exploits only came to light following his arrest for selling personal information of US residents

The 10 Most Expensive Data Breaches in Corporate History

1

Epsilon – $4 Billion

The single most expensive breach so far, in 2011 hackers hit Epsilon. They stole an unknown number of names and emails, affecting up to 75 clients of Epsilon's, including Best Buy, JPMorgan Chase and Target. The hack caused a headache to the tune of up to $4 billion.

2

Veterans Administration – $500 Million

If you leave the records of 26.5 million veterans, military personnel and their families unencrypted you're playing with fire. In 2006 the Veterans Administration got burned when the database containing all 26.5 million records was stolen. There was quite a public backlash when it was revealed all of the data was not only unencrypted but on a laptop and external hard drive.

3

Hannaford Bros – $252 Million

Crafty hackers hit the Hannaford Bros main servers in 2007, and the malware spread to all 300 of their stores as well as independent stores who sold Hannaford products. All in all the hackers made off with 4.2 million debit and credit card numbers costing an estimated $252 million.

4

Sony PlayStation – $171 Million

This is one list you don't want to be on twice! Sony PlayStation got hit in 2011, a few years before the Guardians set their sights on the entertainment division. This cost them a massive $171 million and the public's opinion of them soured after it was discovered Sony knew of the hack a full 6 days before they announced it to the public

5

Target – $162 Million

More recently, Target was the victim of a major attack in late 2013. Hackers compromised the retailer's credit card readers just before Thanksgiving and it wasn't detected until well after Black Friday. All said, 110 million Target shoppers had their card numbers stolen costing them $162 million and lost sales after the public lost faith in their business.

The 10 Most Expensive Data Breaches in Corporate History

6

TJ Maxx – $162 Million

Beginning their attack in 2007, hackers hit the fashionable retailer TJ Maxx over an unbelievable 18 month period. This is the same thief who would go on to cause our #7 pick, the Heartland Payment Systems hack, a year later. The TJ Maxx hack originally caused $118 million in damages but has since ballooned to $162 million as they continue to deal with the after effects.

7

Heartland Payment Systems – $140 Million

Back in 2008, Heartland Payment Systems was hit by a nasty piece of malware that broke into their data room and stole over 130 million debit and credit card numbers. The company didn't even know about it until early 2009! At the time it was the most expensive breach, totally around $140 million in legal fees and overall costs.

8

Anthem – $100 Million

Health insurer Anthem's cloud storage was hit hard in February of 2015. A cyber attack stole and later revealed personal information for nearly 80 million people. The real danger is in the fallout, the information included everything from names to social security numbers so all of those people are in danger of identity theft. It's estimated this slip-up will cost Anthem more than $100 million.

9

Sony Pictures Entertainment – $100 Million

Striking at the end of 2014, a collective of hackers calling themselves the 'Guardians of Peace' managed to slip malware into Sony's servers. Although no official numbers have been released, the guardians claim to have stolen 100 terabytes of data from Sony's servers. They must have had a grudge, because once they were finished they erased all of the company's data! Cleanup and data recovery have cost Sony $100 million.

10

The Home Depot – $56 Million

Utilizing a cloud computing setup to launch malware onto Home Depot's servers, a group of hackers hit the home improvement chain in 2014. They got away with 56 million debit and credit card numbers before getting shut out of the servers. This is going to cost Home Depot up to $56 Million dollars in restitution.

Some important Data breached

Entity	Year	Records	Organization type	Method	Sources
21st Century Oncology	2020	2,200,000	healthcare	hacked	[5][6]
500px	2020	14,870,304	social networking	hacked	[7]
Accendo Insurance Co.	2020	175,350	healthcare	poor security	[8][9]
Adobe Systems	2021	152,000,000	tech	hacked	[10][11]
Adobe Inc.	2019	7,500,000	tech	poor security	[12]
Advocate Medical Group	2017	4,000,000	healthcare	lost / stolen media	[13][14]
AerServ (subsidiary of InMobi)	2018	75,000	advertising	hacked	[15]
Affinity Health Plan, Inc.	2021	344,579	healthcare	lost / stolen media	[16]
Airtel	2019	320,000,000	telecommunications	poor security	[17]
Air Canada	2018	20,000	transport	hacked	[18]
Amazon Japan G.K.	2019	unknown	web	accidentally published	[19][20]
TD Ameritrade	2021	200,000	financial	lost / stolen media	[21]
Ancestry.com	2021	300,000	web	poor security	[22]
Animal Jam	2020	46,000,000	gaming	hacked	[23]
Ankle & Foot Center of Tampa Bay, Inc.	2021	156,000	healthcare	hacked	[24]
Anthem Inc.	2021	80,000,000	healthcare	hacked	[25][26]
AOL	2021	92,000,000	web	inside job, hacked	[27][28]
AOL	2021	20,000,000	web	accidentally published	[29]
AOL	2014	2,400,000	web	hacked	[30]
Apple, Inc./BlueToad	2021	12,367,232	tech, retail	accidentally published	[31]
Apple	2021	275,000	tech	hacked	[32]
Apple Health Medicaid	2021	91,000	healthcare	poor security	[33]
Ashley Madison	2021	32,000,000	web	hacked	[34]

03

Cost Impact of Data Breaches

Data breach Statistics

2020

S.No.	COUNTRY	Avg Cost ($Millions)
1	**United States**	**8.64**
2	Middle east	6.52
3	Canada	4.50
4	Germany	4.45
5	France	4.19
6	United Kingdom	4.01
7	Global Average	3.90
8	Italy	3.86
9	South Korea	3.19
10	ASEAN	3.12
11	Scandinavia	2.71
12	Australia	2.51
13	South Africa	2.15
14	India	2.14
15	Turkey	2.00
16	Latin America	1.77
17	Brazil	1.68
18	**Middle East**	**1.12**

Global cost of cybercrime is expected to peak at US $6 trillion p.a. by end of 2021 and $10 Trillion by e.o. 2025.

Ransomware attacks to be worth $20 billion by e.o. 2021. (By Cybersecurity Ventures)

The worldwide information security market is forecast to reach $170.4 billion in 2022. (Gartner)

2020

S.No.	INDUSTRY	Avg Cost ($Millions)
1	**Healthcare**	**7.13**
2	Energy	6.39
3	Financial	5.85
4	Pharma	5.06
5	Technology	5.04
6	Industrial	4.99
7	Services	4.23
8	Entertainment	4.08
9	Education	3.90
10	Global Average	3.86
11	Transportation	3.58
12	Communication	3.01
13	Consumer	2.59
14	Retail	2.01
15	Hospitality	1.72
16	Media	1.65
17	Research	1.53
18	**Public**	**1.08**

Source IBM Data breach report 2020

Data breach Statistics

$3.86 millions Avg. cost of Breach

US as a country has the highest Cost

Healthcare as Industry has highest cost

286 days avg. time to identify & contain

52% breaches caused by malicious attacks

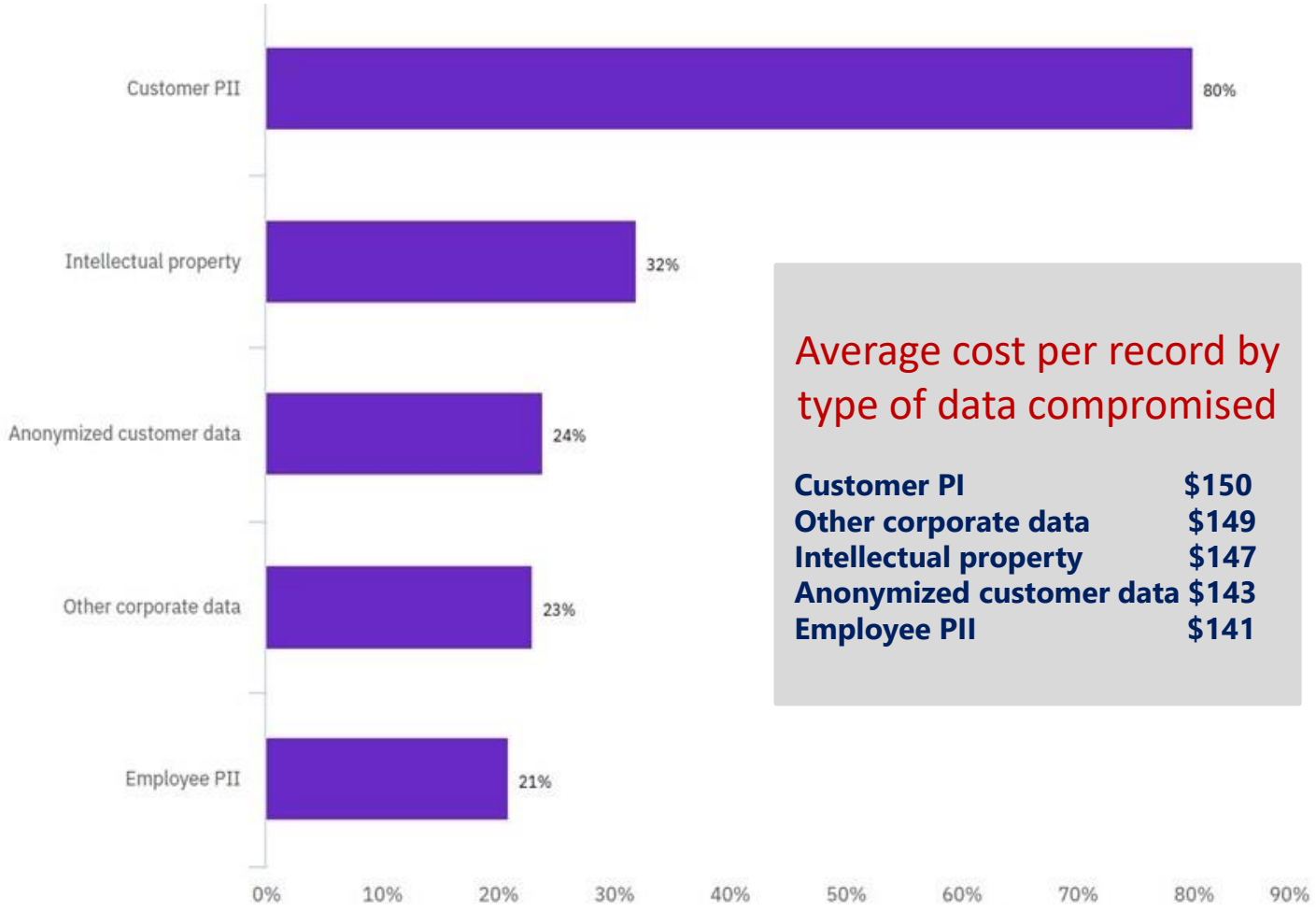
80% breaches with Customer PII

Source IBM Data breach report 2020

Data Breach Statistics Continued….

Types of records compromised

Percentage of breaches involving data in each category



Average cost per record by type of data compromised

Customer PI	**$150**
Other corporate data	**$149**
Intellectual property	**$147**
Anonymized customer data	**$143**
Employee PII	**$141**

$5.52 million

Average total cost of a breach at enterprises of more than 25,000 employees, compared to $2.64 million for organizations under 500 employees

$7.13 millions

The average cost of a data breach in the healthcare industry, an increase of 10% compared to the 2019 study

80%

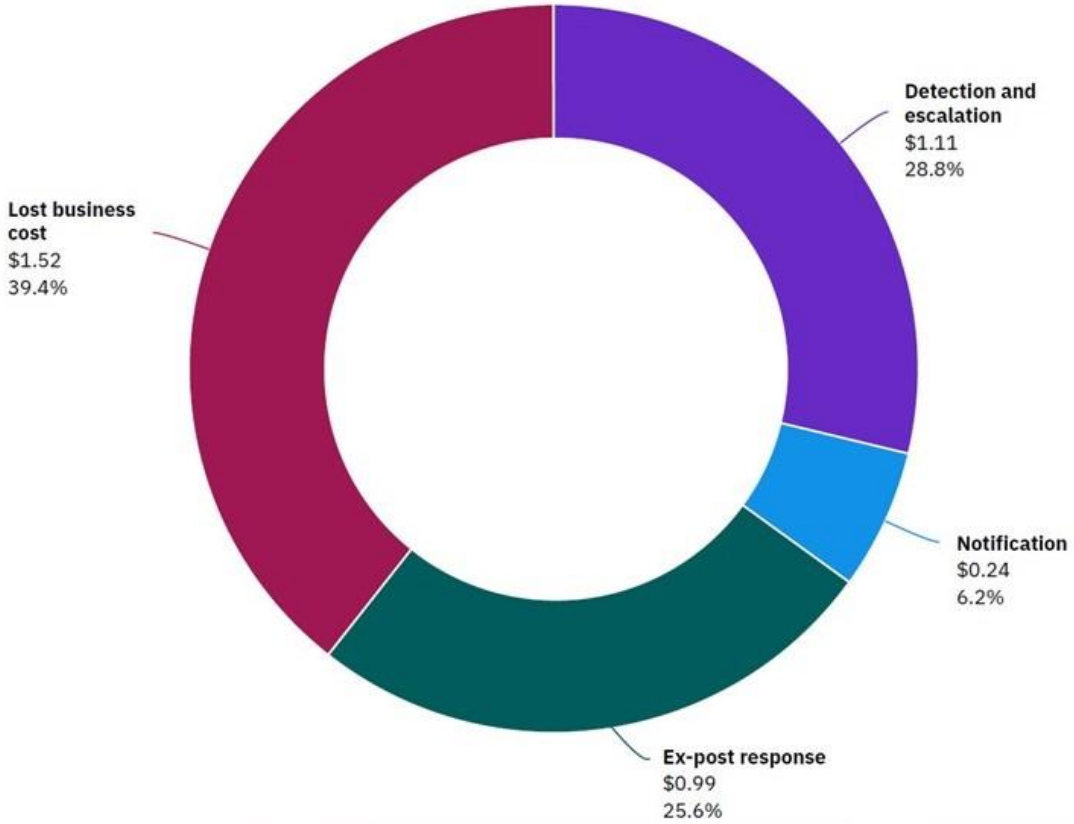
Share of breaches that included records containing customer PII, at an average cost of $150 per record

Source IBM Data breach report 2020

Statistics Continued….

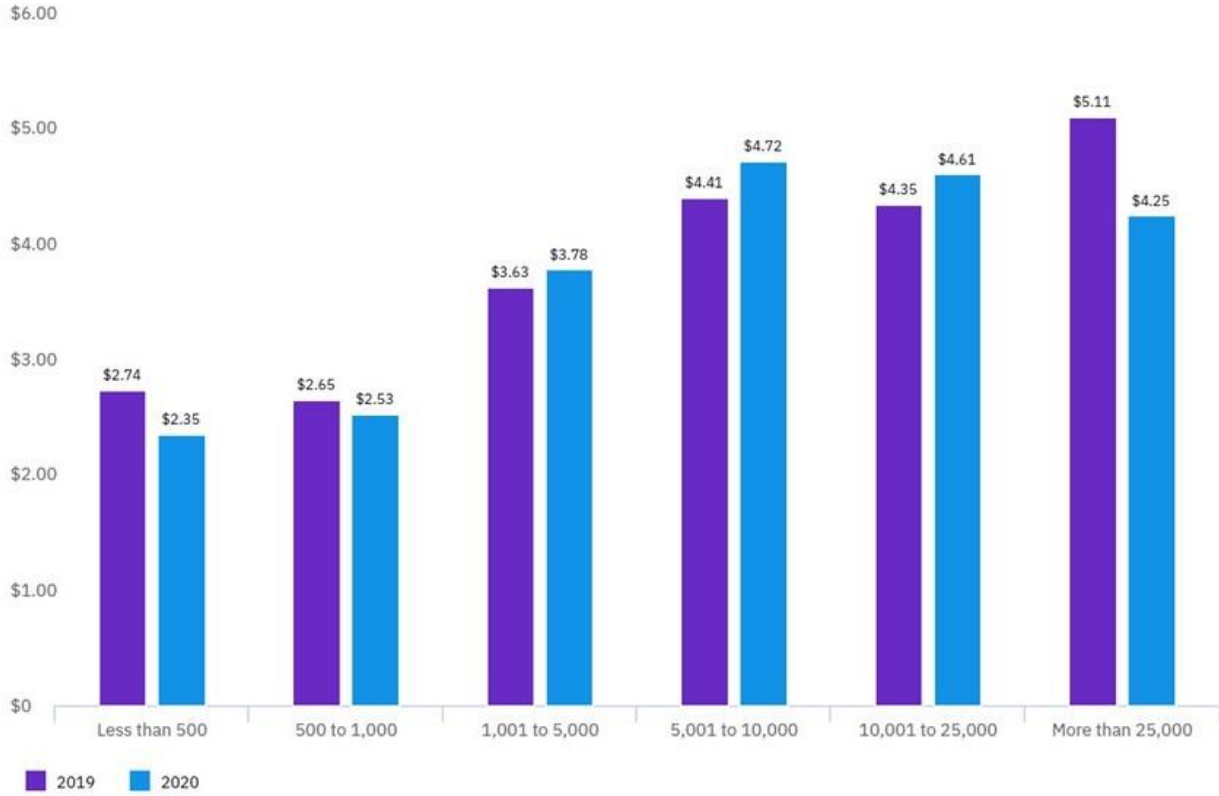
Data breach average total cost divided into four categories

Measured in US$ millions



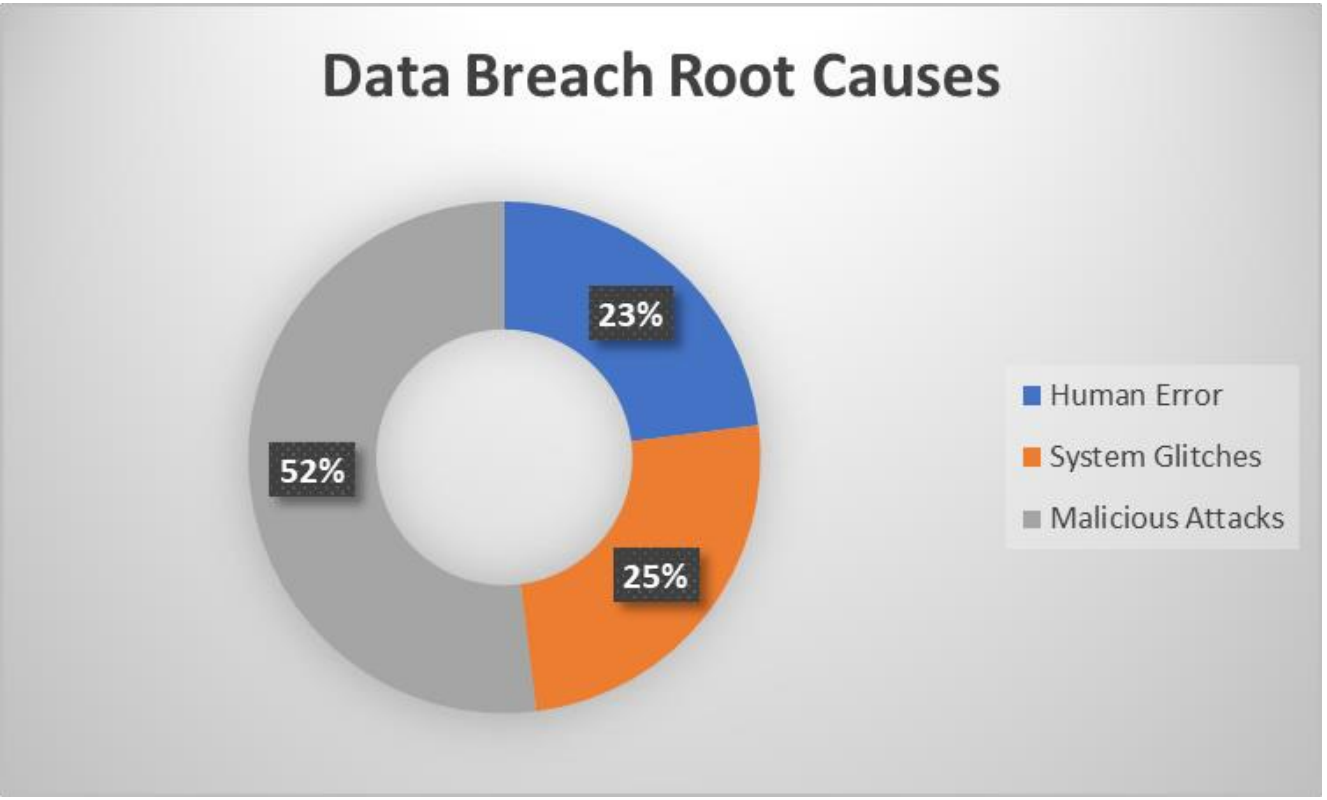
Average total cost of a data breach by organizational size

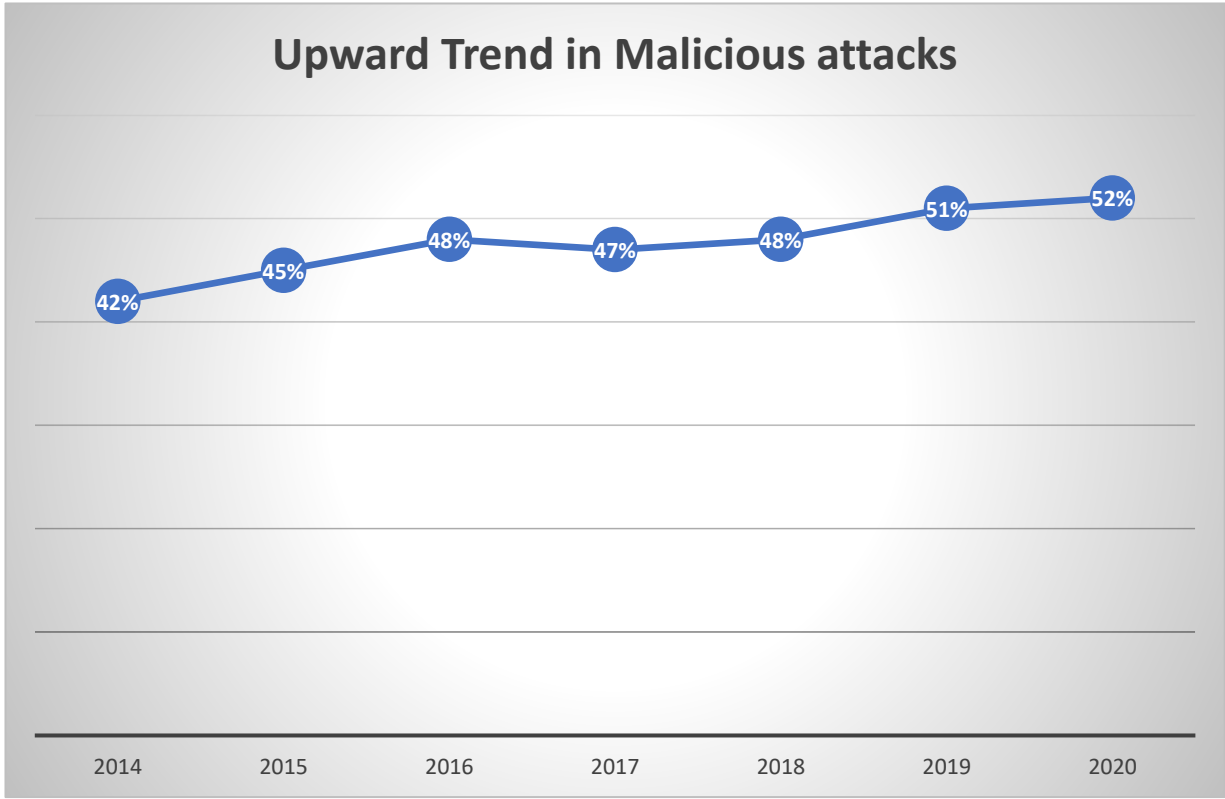
Measured in US$ millions



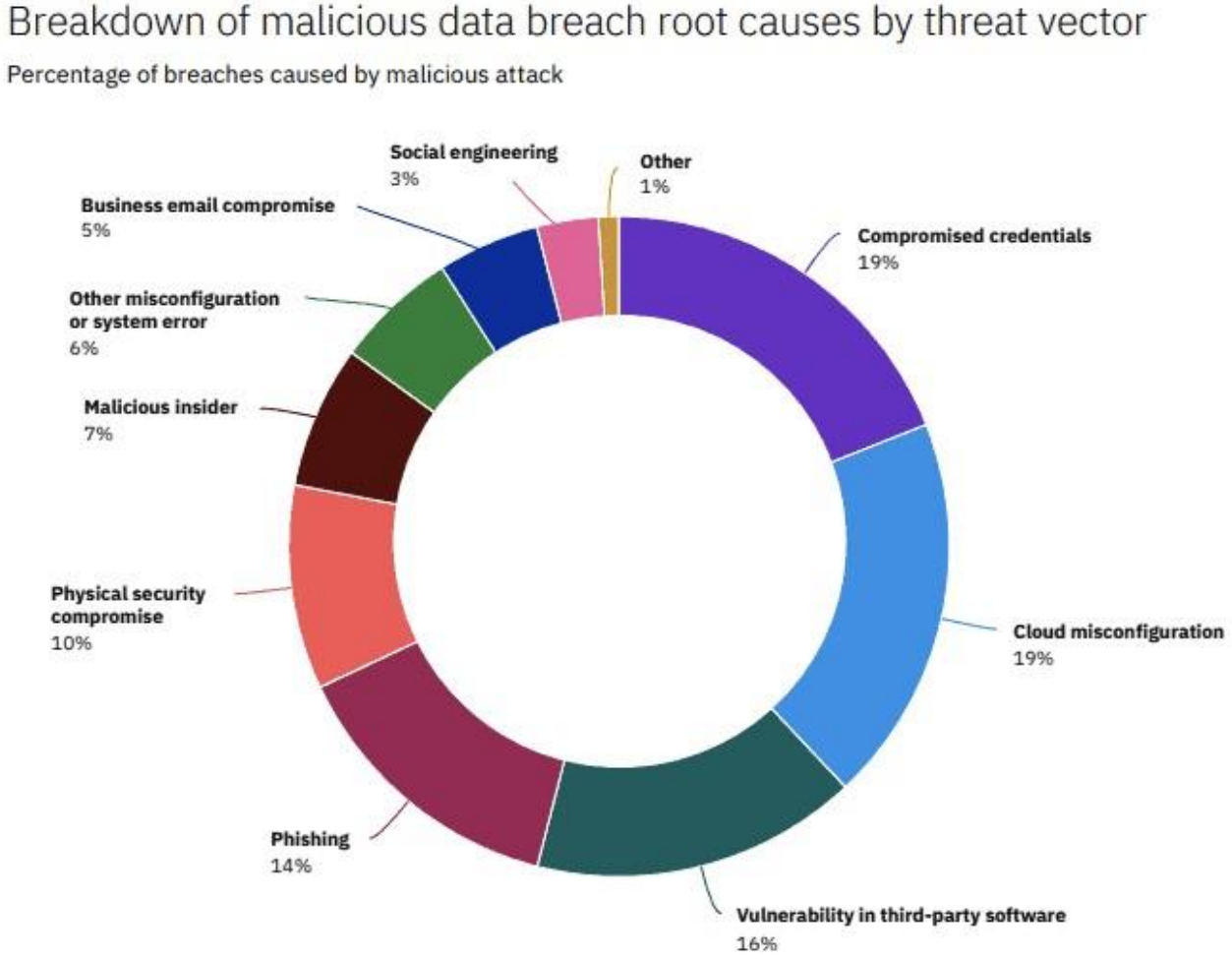
Source IBM Data breach report 2020

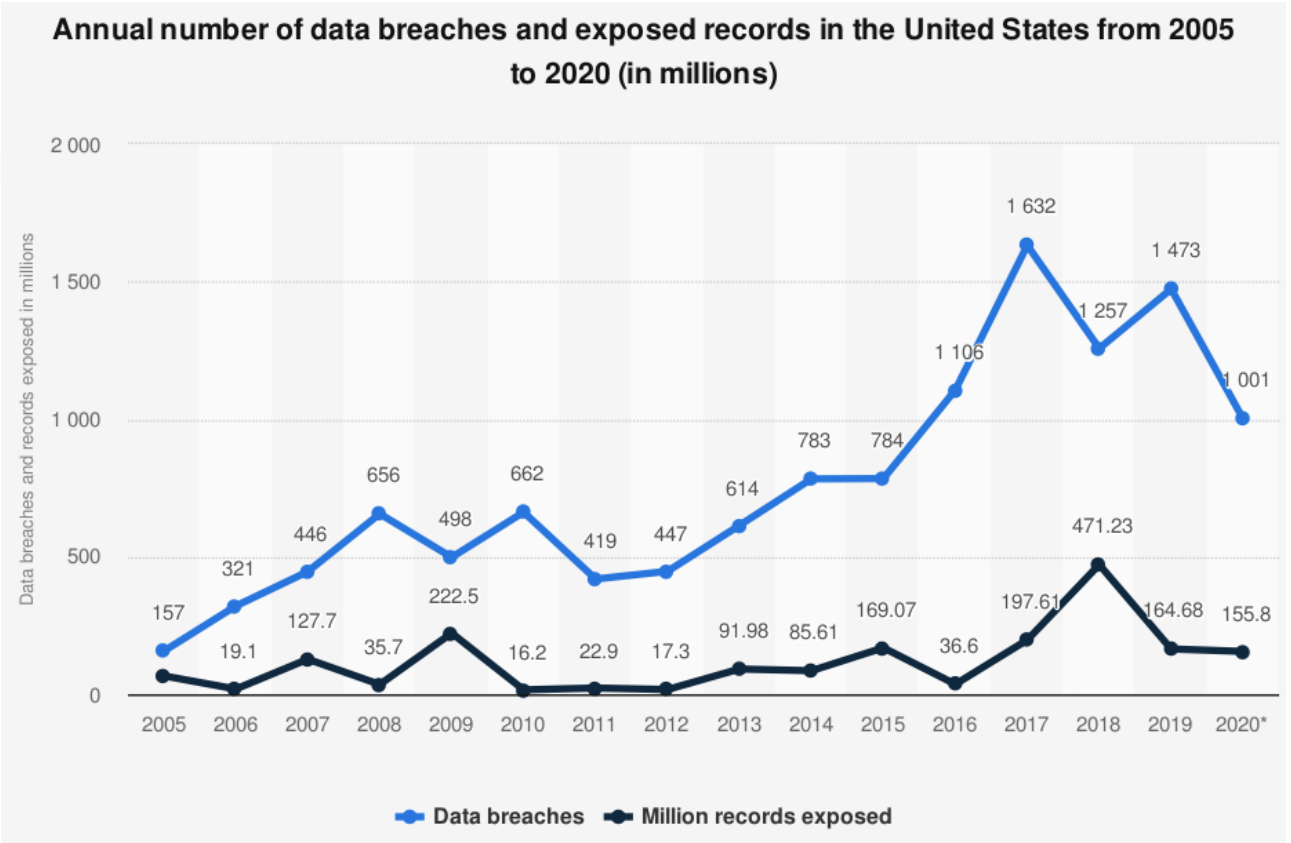
Data Breach Statistics Continued….

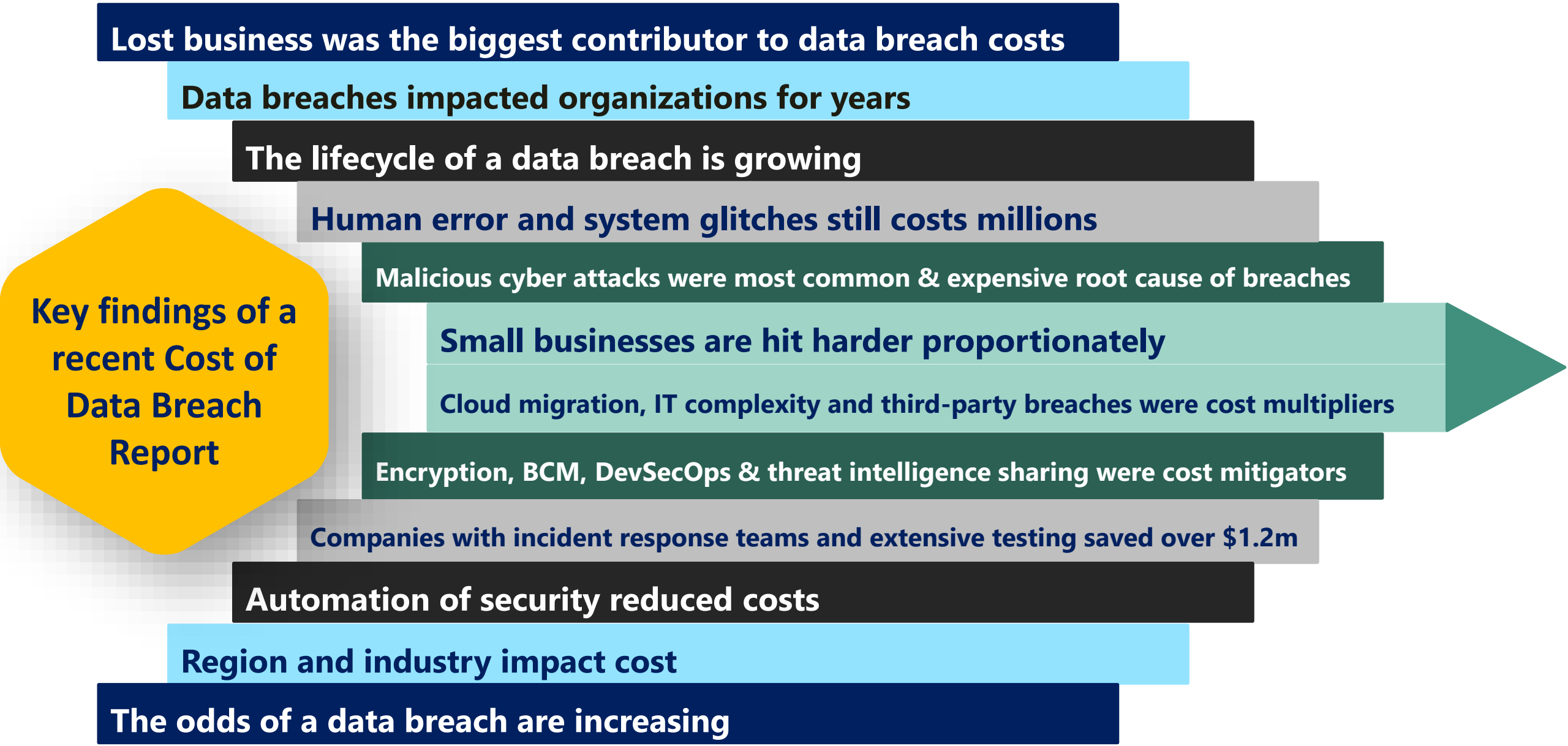




Data Breach types & numbers






Lost business was the biggest contributor to data breach costs
Data breaches impacted organizations for years
The lifecycle of a data breach is growing
Human error and system glitches still costs millions
Malicious cyber attacks were most common & expensive root cause of breaches
Small businesses are hit harder proportionately
Cloud migration, IT complexity and third-party breaches were cost multipliers
Encryption, BCM, DevSecOps & threat intelligence sharing were cost mitigators
Companies with incident response teams and extensive testing saved over $1.2m
Automation of security reduced costs
Region and industry impact cost
The odds of a data breach are increasing
Key findings of a recent Cost of Data Breach Report

Ransomware attacks increase from 2020 to 21

64% increase in Ransomware attacks in last 1 year.

Infra,Travel,BFSI & other Businesses 57% up by 18% over 2020

Infrastructure & Supply chain companies are new targets at 10% or more

Good negotiator can bring down ransom demand by upto 50%

Avg ransom demand $10 Millions.
18% < $10 Millions
30% > $30 Millions

Data Breach Covid19 impact

COVID-19 has impacted every industry and corner of the globe, and cyberspace is no exception. The global pandemic has paved avenues for cybercriminals to target many new victims: the healthcare industry, the unemployed, remote workers and more. Here are a few of the most impactful cybersecurity statistics related to the pandemic.

1. Since the pandemic began, the FBI reported a 300% increase in reported cybercrimes. (IMC Grupo)
2. 27% of COVID-19 cyberattacks on banks/ healthcare orgs. and a 238% rise in cyberattacks on banks in 2020. (Fintech News)
3. Confirmed data breaches in healthcare industry increased by 58% in 2020. (Verizon)
4. 33,000 unemployment applicants were exposed to a data security breach by a Pandemic Unemployment Assistance program in May. (NBC)
5. Americans lost more than $97.39 million to COVID-19 and stimulus check scams. (Atlasvpn)
6. In April 2020, Google blocked 18 million daily malware and phishing emails related to Coronavirus. (Google)
7. 52% of legal and compliance leaders are concerned about third-party cyber risks due to remote work since COVID-19. (Gartner)
8. Remote work has increased the average cost of a data breach by $137,000. (IBM)
9. 47% of employees cited distraction as the reason for falling for a phishing scam while working from home. (Tessian)
10. 81% of cybersecurity professionals have reported their job function changed during the pandemic. (ISC)
11. Half a million Zoom user accounts were compromised and sold on a dark web forum in April 2020. (CPO Magazine)
12. Cloud-based cyber attacks rose 630% between January and April 2020. (Fintech News)
13. Remote workers have caused a security breach in 20% of organizations. (Malwarebytes)

04

Measures & Solutions For Data Breaches

How Data Breaches affect Organizations?

How to prevent Data Breaches?

Always keep Security patches in all software & Hardware up-to-date

Hire CS Teams internal/External Periodical Risk Assessments

Ensure encryption of critical data and keep backups safe.

Regular employee training and awareness programs

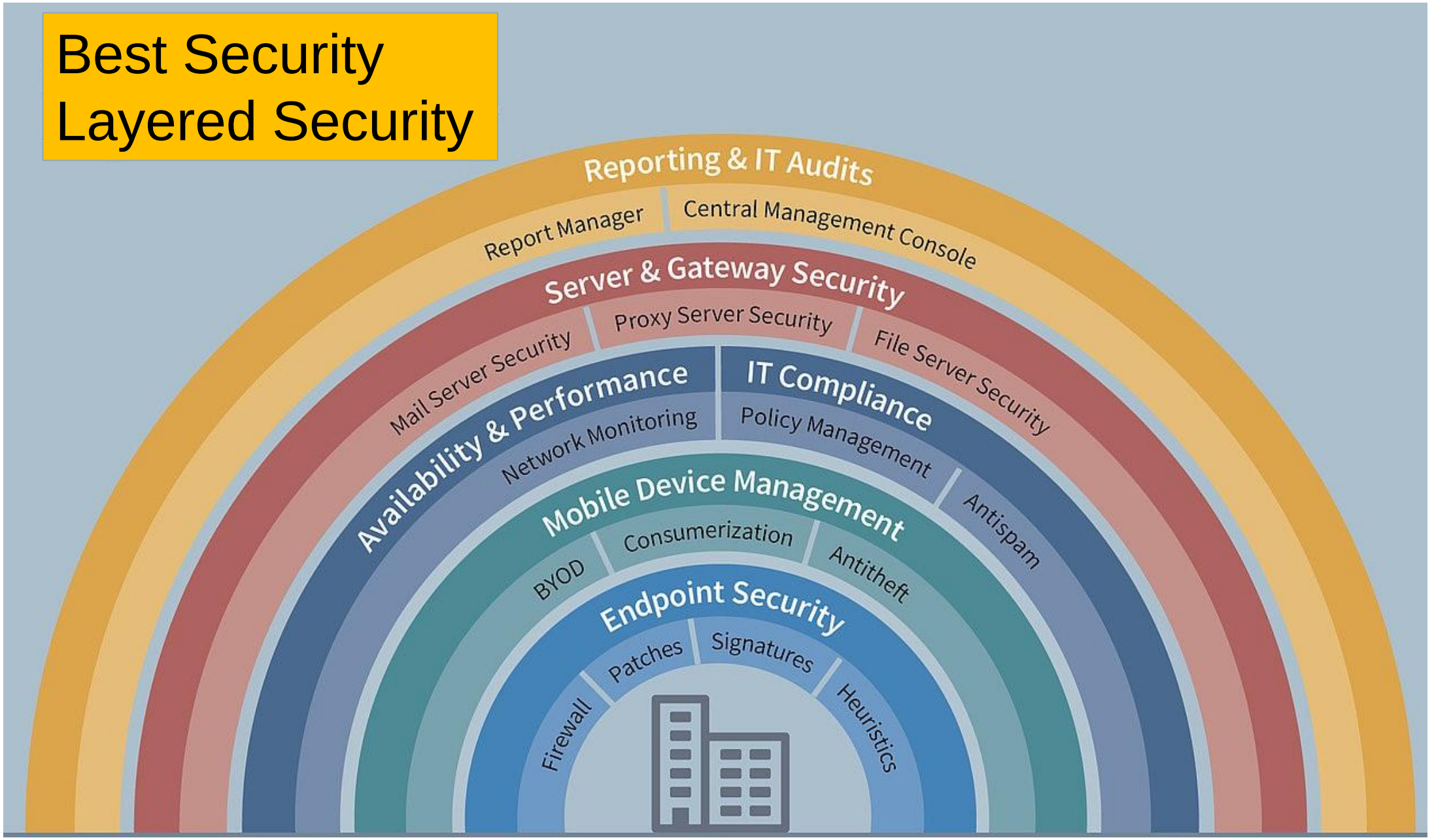
Ensure Vendor/Partners keep high standards of security.

Get 3rd party security audits regularly. Implement improvements.

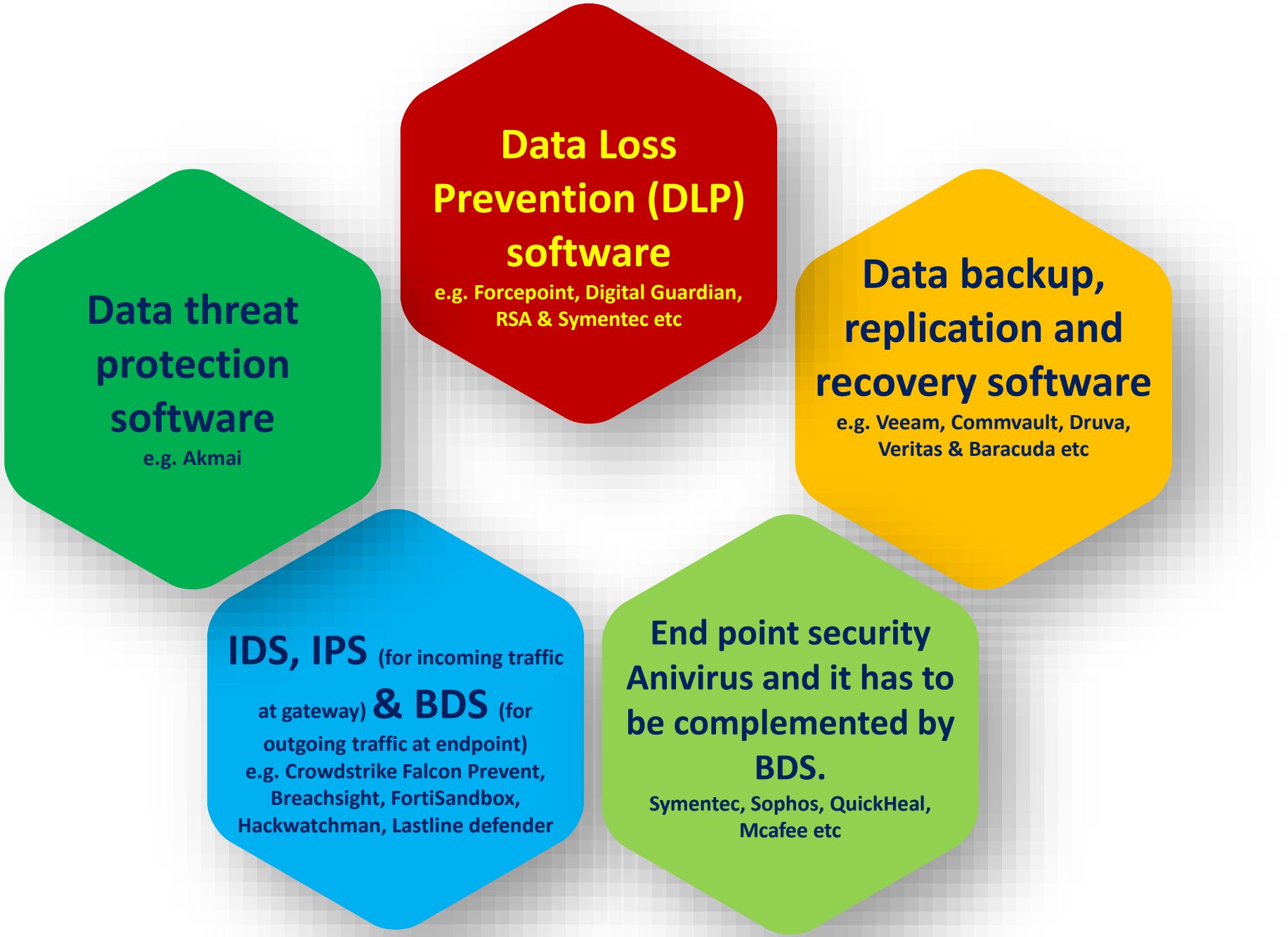
Setting aside a budget for best data protection technology & security.

Keep your IT Asset inventory updated, upgraded & visible

Deploy layered Security



General Data breach protection software



Data breach response plan

1. Create a data breach response Plan
2. Departmental teams to identify , contain & recover from breach
3. Ensure IT resources are allocated to most critical data areas
4. Awareness & mock drills periodically conducted will come handy now.
5. Identify which type of breach has happened?
6. Isolate & Secure all data possible wherever it can be
7. Change all passwords & encryption keys
8. Clear malicious code from all systems
9. Identify the source of breach
10. Alert authorities & legal counsel
11. Protect digital evidence traced
12. Notify data owners about the data breach
13. Activate PR team if needed so
14. Fix vulnerabilities to stop future breaches
15. Correct response plan based current experience, for future breaches

Data Protection Laws Protect you with following properties

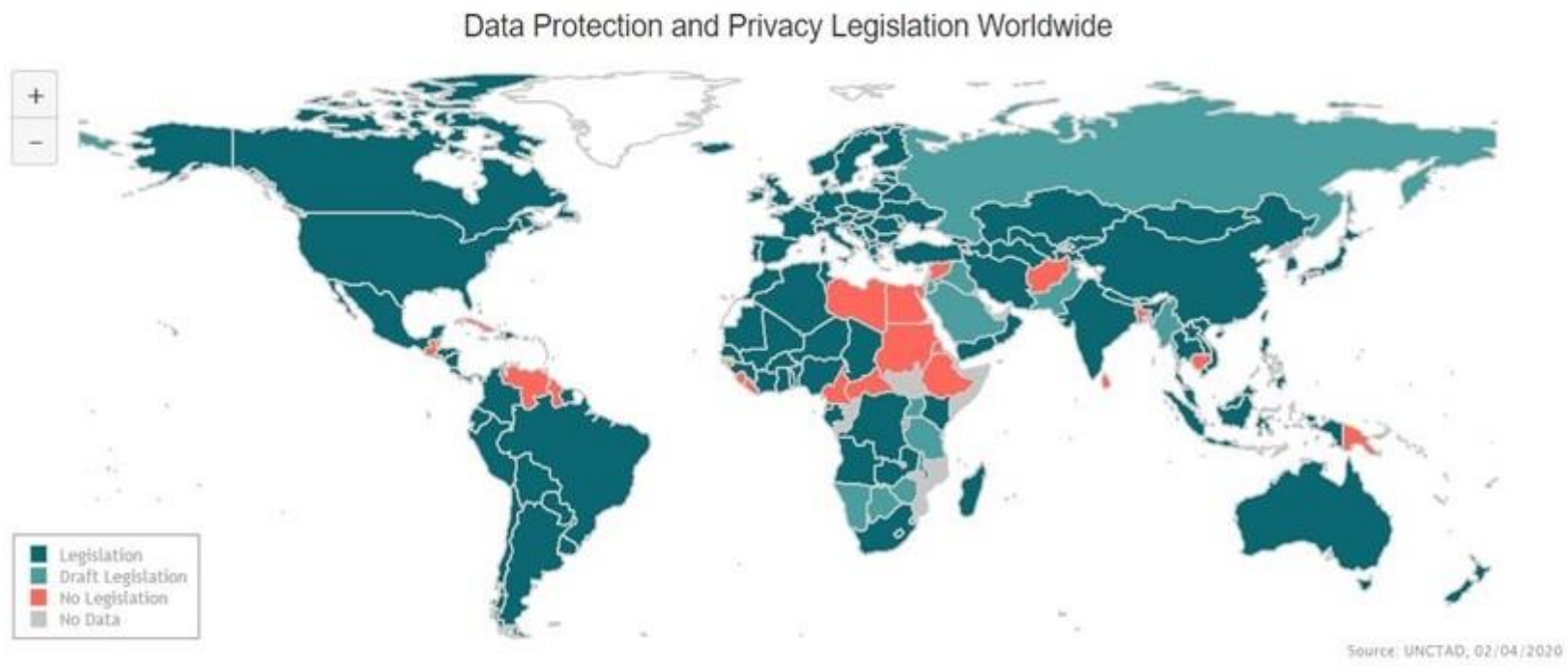
Data Protection Laws - Legal Support

66%	10%	19%	5%
COUNTRIES WITH **LEGISLATION**	COUNTRIES WITH **DRAFT LEGISLATION**	COUNTRIES WITH **NO LEGISLATION**	COUNTRIES WITH **NO DATA**

SELECT A COUNTRY

SELECT A REGION

DOWNLOAD FULL DATA



Major Data Protection Laws across the world

1. **GDPR** effective from May' 2018. Covers European Union but each each many nations have their own DP laws as well.
2. **UK:** has amended GDPR as **UK GDPR** and **DPA 2018**
3. **United State** data privacy laws:
   - California Consumer Privacy Act (CCPA)
   - California Privacy Rights Act (CPRA)
   - Virginia's Consumer Data Protection Act (CDPA)
   - Colorado Privacy Act (CPA)
   - New York SHIELD Act
4. **Brazil's** General Law for the Protection of Personal Data (LGPD)
5. **Philippines:** the Republic Act No.10173 alias Data Privacy Act 2012 is the primary legislation governing data privacy in the country.
6. **Russia:** Federal Law on Personal Data 2006 (Act No. 152 FZ) & Information Technologies and Information Protection Act 2006 (Act No. 149 FZ).
7. **South Africa:** Protection of Personal Information (PoPI) Act 2013
8. **India:** at present governed by Indian IT Act 2000 but Personal Data Protection Bill 2019 on its way

Global Cybersecurity Index (GCI) 2020 by ITU (International Telecommunication Union)

Rank	Country	Rank	Country	Rank	Country	Rank	Country
1	USA	11	Turkey	24	Indonesia	38	North Macedonia
2	UK	12	Australia	25	Vietnam	39	Serbia
2	Saudi Arabia	13	Luxembourg	26	Sweden	40	Azerbaijan
3	Estonia	13	Germany	27	Qatar	41	Cyprus
4	Korea (Rep. of)	14	Portugal	28	Greece	42	Switzerland
4	Singapore	15	Latvia	29	Austria	43	Ghana
4	Spain	16	Netherlands	30	Poland	44	Thailand
5	Russia	17	Norway	31	Kazakhstan	45	Tunisia
5	UAE	17	Mauritius	32	Denmark	46	Ireland
5	Malaysia	18	Brazil	33	China	47	Nigeria
6	Lithuania	19	Belgium	33	Croatia	48	New Zeland
7	Japan	20	Italy	34	Slovakia	49	Malta
8	Canada	21	Oman	35	Hungary	50	Morocco
9	France	22	Finland	36	Israel		
10	India	23	Egypt	37	Tanzania		

The assessment was done on five parameters. These are:

1- Legal measures
2- Technical measures
3- Organizational measures
4- Capacity Development
5- Cooperation

The performance is then aggregated into an overall score.

Results for India in GCI 2020

1- India scored a total of 97.5 points.
2- India secured the fourth position in the Asia Pacific region, underlining its commitment to cybersecurity.
3- India is emerging as a global IT superpower, asserting its digital sovereignty with firm measures to safeguard data privacy and the online rights of citizens.

Questions & Answers

Thank You

Please note that we provide most practical advisory services in the field of Information Technology in medium and large Organizations. Our aim is to share and use our rich experience in establishing high quality secured digital systems in the Organizations to make them advance and highly competitive in today's digital era.

Please connect us at

(91) 9999799664
(91) 9810191565

BizTek Advisors Pvt. Ltd.
sp.arya@biztekadvisors.in