ASMGi

Cyber Security

Looking back at 2019 …

Looking ahead at 2020 …

January, 16 2020

2019 - 2020 Cyber Security

Steve Roesing
CEO
ASMGi
sroesing@asmgi.com
http://www.asmgi.com

Frank Yako
CIO, Director Strategic Initiatives
ASMGi
fayko@asmgi.com
http://www.asmgi.com

Ken Makoid
Regional Vice President, Northeast
Flexential
Ken.Makoid@flexential.com
http://www.flexential.com

Agenda

- 2019 Look Back
- 2020 Look Ahead
- Speaker Predictions
- How do we win?
- Announcements

Cyber Security Highlights of 2019

Cost of a Data Breach Report highlights

USD 3.92 million

Average total cost of a data breach

United States

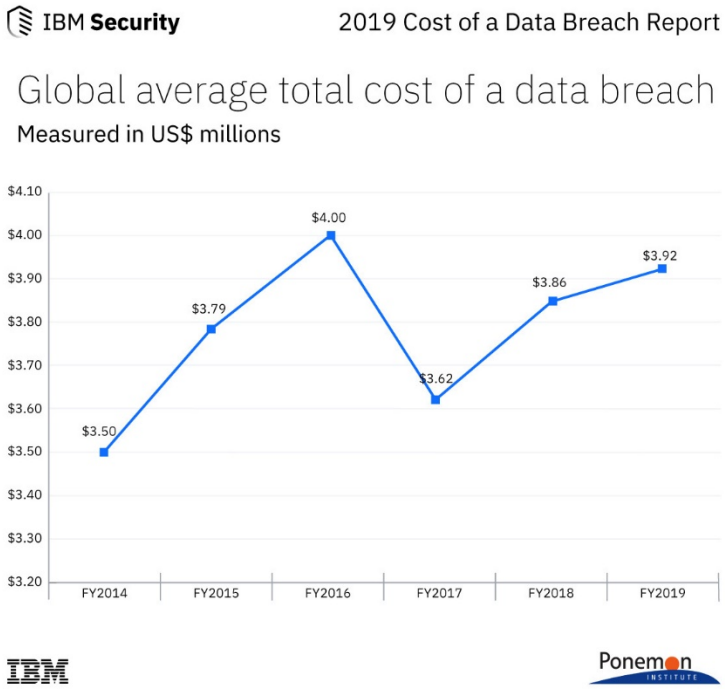
Most expensive country: USD 8.19 million

Healthcare

Most expensive industry: USD 6.45 million

25,575 records

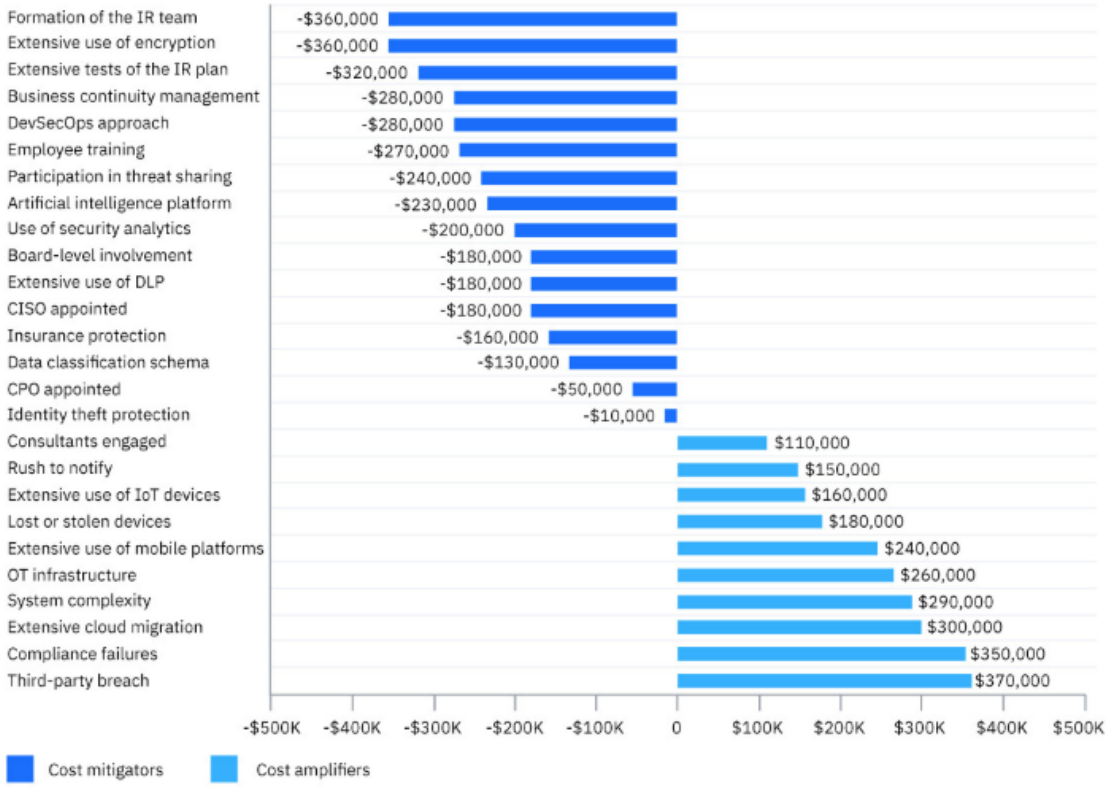
Average size of a data breach



ASMGi

How factors increase or decrease the total cost of a data breach

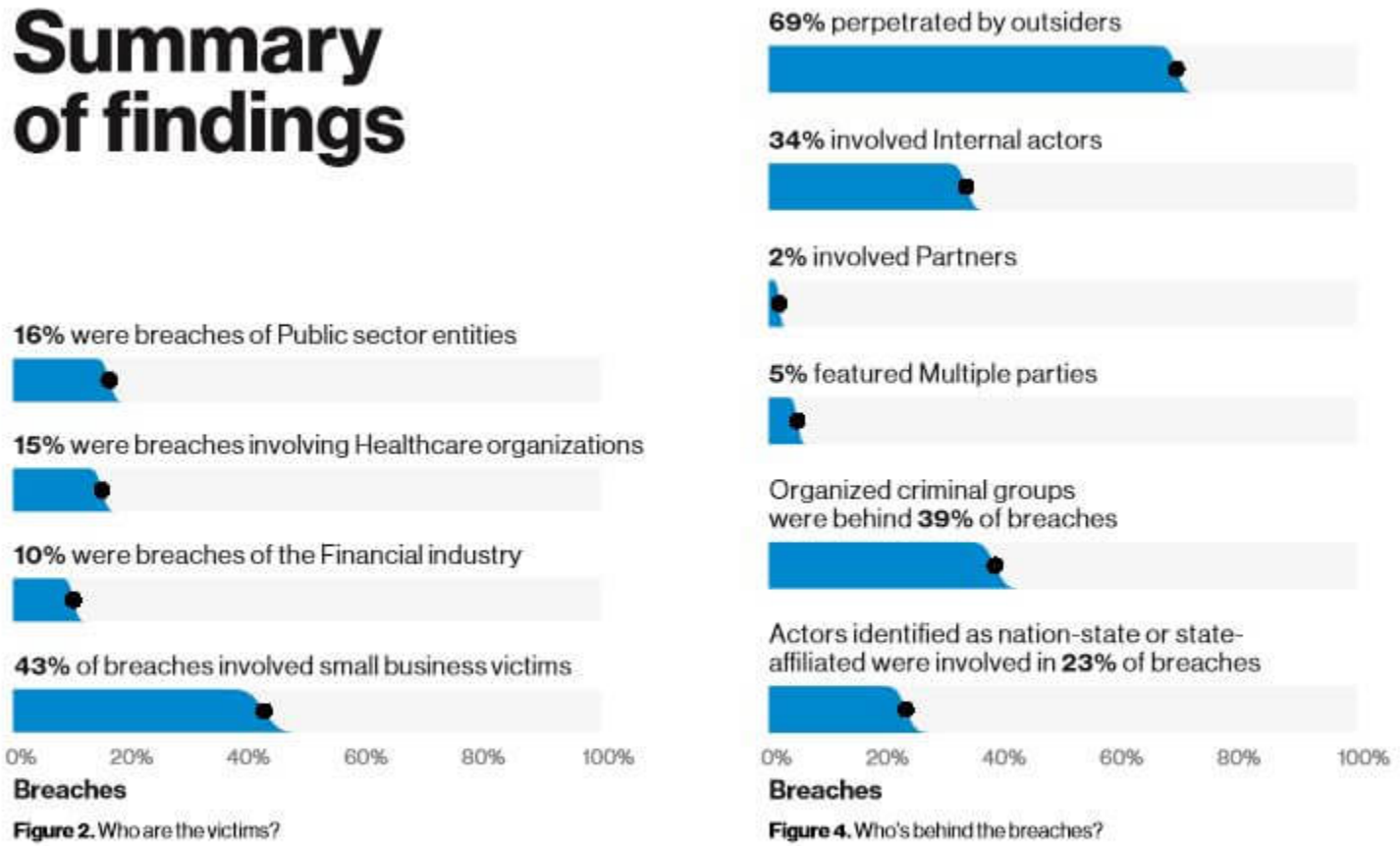
Difference from average total cost of US $3.92 million



IBM

Ponemon INSTITUTE

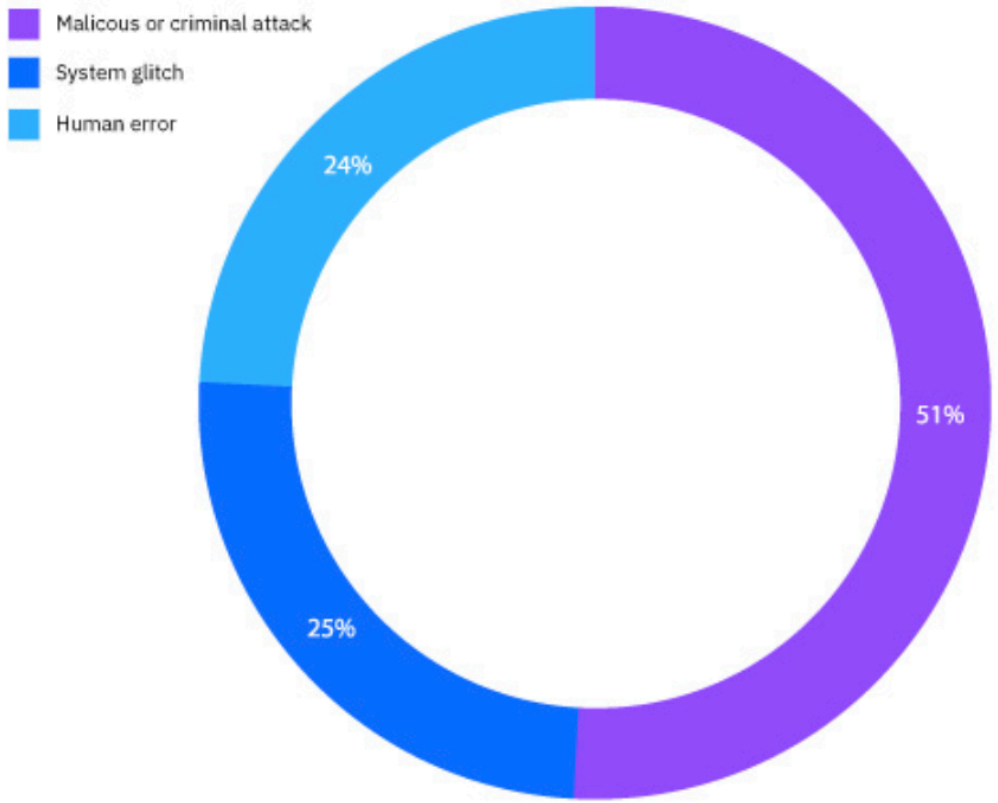
Verizon Data Breach Report 2019



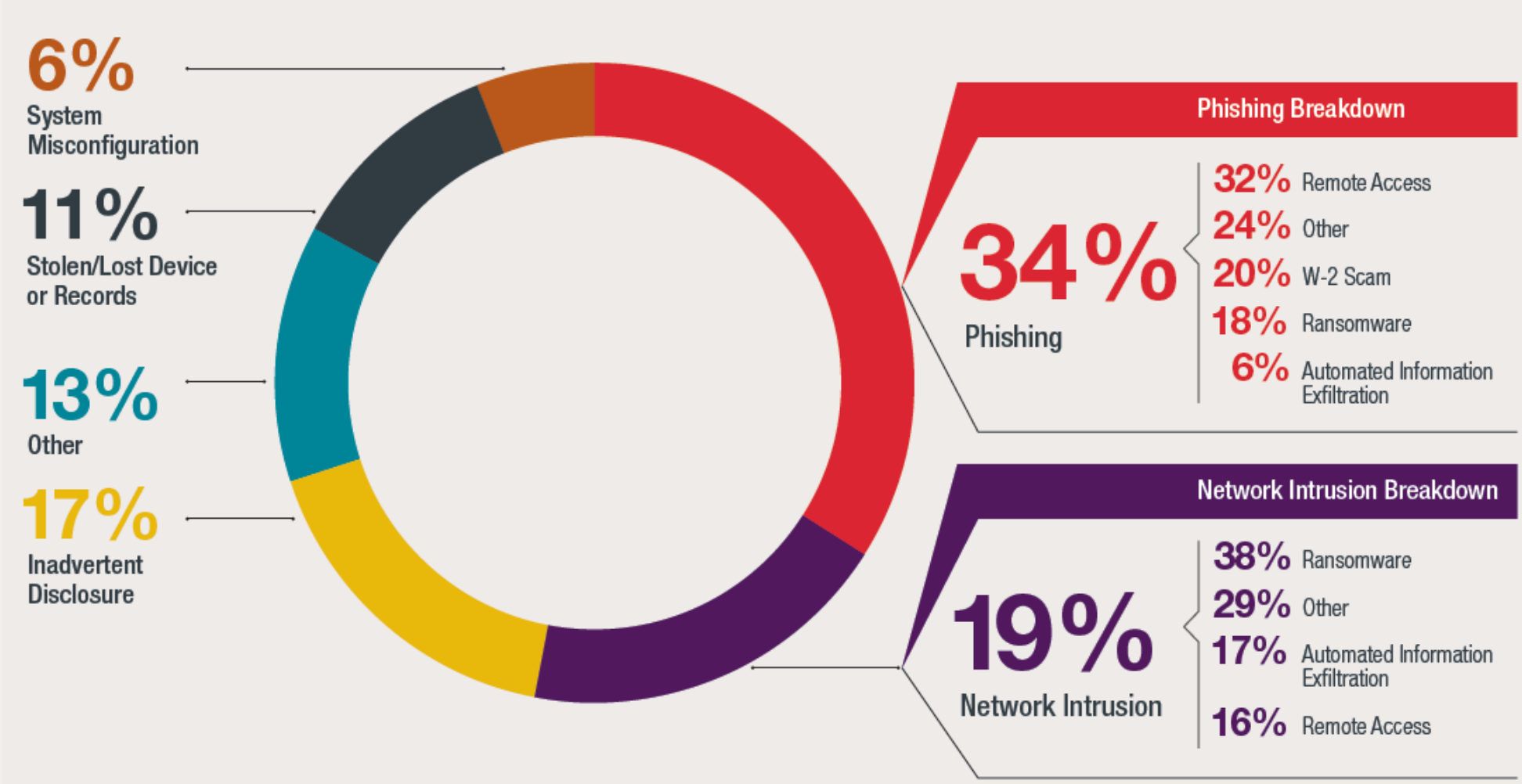
Source: Verizon

Malicious attacks are the leading cause of breaches

Breakdown of data breach root causes

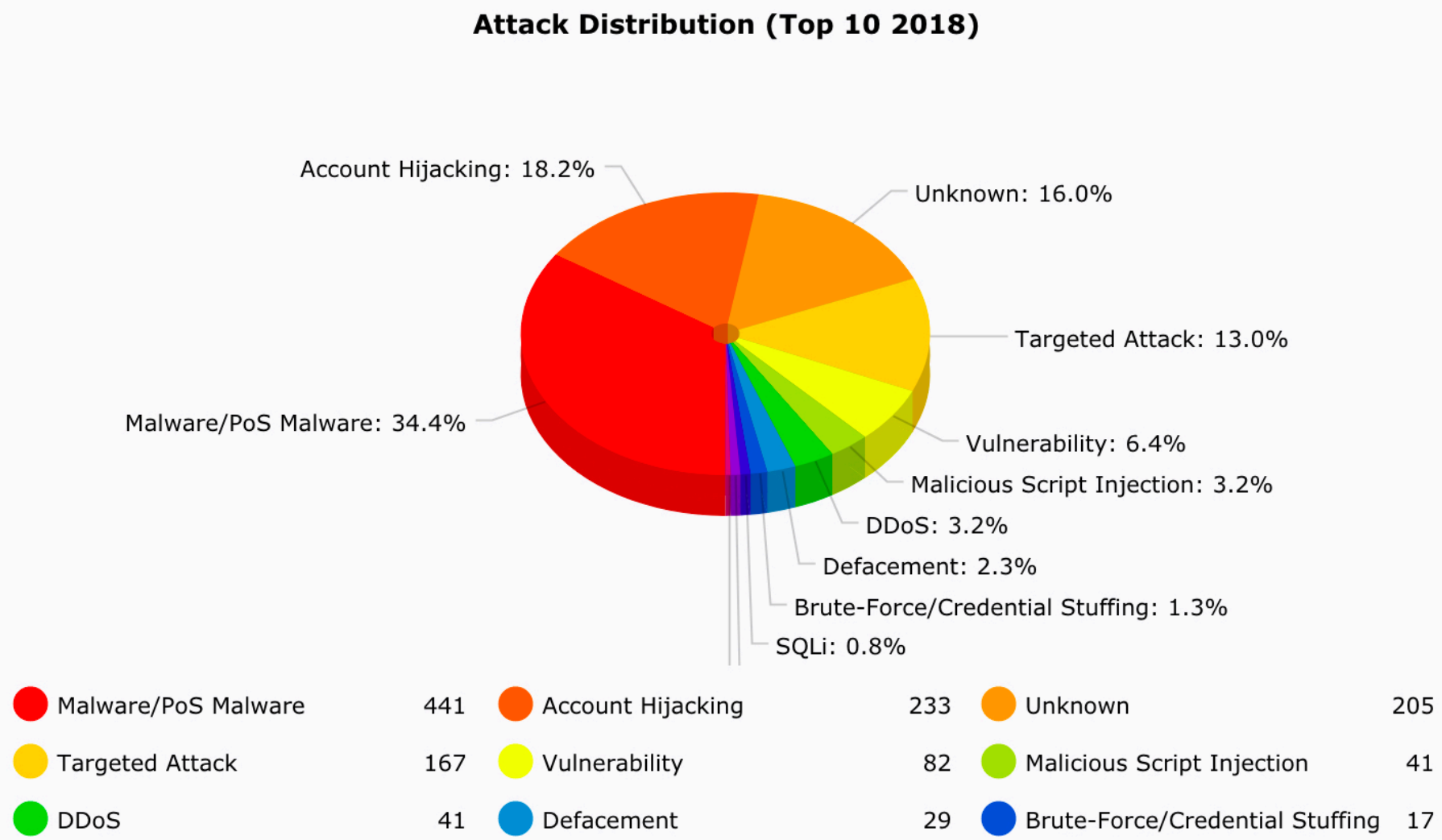


Human Error =


6%
System Misconfiguration
11%
Stolen/Lost Device or Records
13%
Other
17%
Inadvertent Disclosure
Phishing Breakdown
34%
Phishing
32% Remote Access
24% Other
20% W-2 Scam
18% Ransomware
6% Automated Information Exfiltration
Network Intrusion Breakdown
19%
Network Intrusion
38% Ransomware
29% Other
17% Automated Information Exfiltration
16% Remote Access

Top 10 Attacks

ASMGi



Thru Q2 of 2019 <Cyber Risk Analytics>

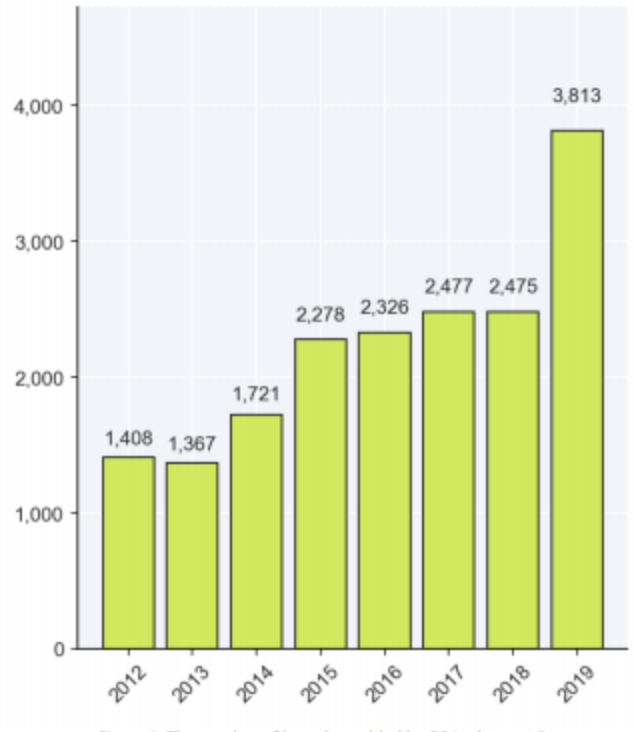


Figure 1: The number of breaches added by Q2 in the past 8 years.

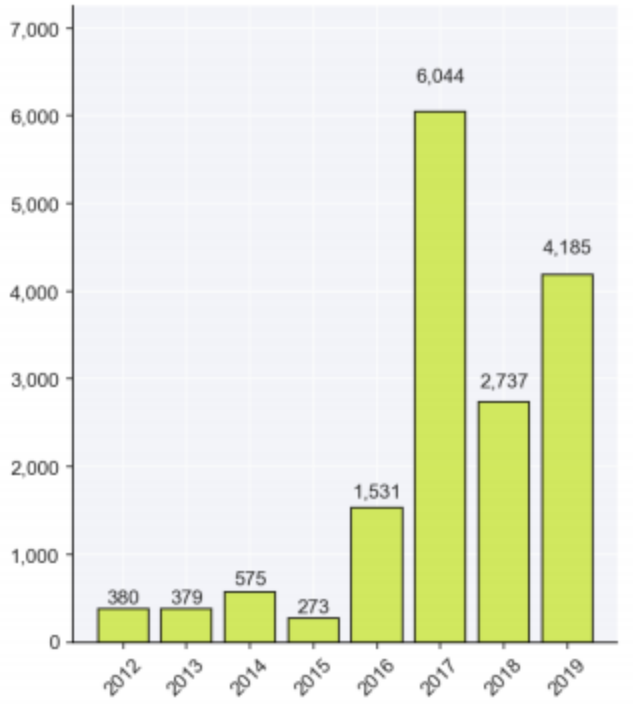


Figure 2: The number of known records exposed (in millions) by Q2 in the past 8 years.

Tactics, Techniques and Procedures evolve over time but the end results have remained consistent. Unauthorized access of systems or services (Hacking) and skimmers and exposure of sensitive data on the Internet (Web) have been the top three breach types since January of 2018. Likewise insider actions, both malicious and accidental, have driven the number of records exposed, with Web and Fraud accounting for over 6.7 billion records exposed over the last 18 months.

Top 10 Breaches in the First Six Months

Organization	Reported	Severity	Records Exposed	Data Type	Breach Type	Inside / Outside	Location
Verifications.io	3/7/19	10	982,864,972	ADD / DOB / EMA / FIN / MISC / NAA / NUM / PWD	Web	Inside- Accident	Estonia
	982,864,972 names, addresses, email addresses, dates of birth, phone numbers, fax numbers, genders, IP addresses, personal mortgage amounts, and FTP server credentials exposed on the Internet due to a misconfigured database						
First American Financial Corporation	5/24/19	10	885,000,000	ADD / EMA / FIN / MISC / NAA / NUM / SSN	Web	Inside- Accident	United States
	Approximately 885,000,000 real estate closing transaction records containing names, Social Security numbers, phone numbers, email and physical addresses, driver's license images, banking details, and mortgage lender names and loan numbers exposed on the Internet due to IDOR flaw						
Cultura Colectiva	4/3/19	10	540,000,000	ACC / MISC	Web	Inside- Accident	Mexico
	Facebook user IDs, account names, comments, and likes exposed on the Internet due to a misconfigured database						
Unknown Organization	5/1/19	9.51893	275,265,298	DOB / EMA / FIN / MISC / NAA / NUM	Web	Inside- Accident	India
	275,265,298 Indian citizens' names, email addresses, genders, dates of birth, phone numbers, education details, and employment details such as salaries, professional skills, and employer history held in publicly indexed MongoDB instance taken by Unistellar hacking group						
Unknown Organization	1/10/19	9.3861	202,730,434	ADD / DOB / EMA / MISC / NAA / NUM	Web	Inside- Accident	China
	202,730,434 job applicant names, addresses, dates of birth, phone numbers, email addresses, marriage statuses, driver's license numbers, professional experiences, and job expectations exposed on the Internet due to a misconfigured database						
Dubsmash, Inc.	2/12/19	9.81036	161,549,210	EMA / MISC / NAA / PWD / USR	Hack	Outside	United States
	161,549,210 users' names, IDs, email addresses, usernames, SHA256-hashed passwords, languages, and countries stolen by hackers and later offered for sale						
Canva	5/24/19	9.74508	139,000,000	EMA / MISC / NAA / NUM / USR	Hack	Outside	Australia
	139,000,000 customer names, usernames, email addresses, bcrypt hashed passwords, and location information stolen by hackers through undisclosed means						
Justdial	4/17/19	9.07918	100,000,000	ADD / DOB / EMA / MISC / NAA / NUM	Web	Inside- Accident	India
	100,000,000 users' names, addresses, email addresses, phone numbers, dates of birth, genders, photos, occupations, and company names exposed online due to a publicly accessible API endpoint						
ApexSMS Inc. dba Mobile Drip	5/9/19	8.68154	80,055,125	ADD / EMA / MISC / NAA / NUM	Web	Inside- Accident	United States
	80,055,125 records containing MD5 hashed email addresses, full names, partial physical addresses, IP addresses, phone numbers, cellular network providers and line types held in a misconfigured database						
Unknown Organization	4/29/19	8.98227	80,000,000	ADD / DOB / FIN / MISC / NAA	Web	Inside- Accident	United States
	80,000,000 names, addresses, ages, dates of birth, genders, incomes, marital statuses, homeowner statuses, and dwelling types exposed on the Internet due to a misconfigured database						

Top 10 Breaches of all Time

Three breaches reported this year have made the list of the ten largest breaches of all time.

Organization	Reported	Severity	Records Exposed	Data Type	Breach Type	Inside / Outside	Location
Altaba, Inc (formerly known as Yahoo)	12/14/16	10	3,000,000,000	DOB / EMA / MISC / NAA / NUM / PWD	Hack	Outside	United States
	3,000,000,000 customer names, email addresses, phone numbers, dates of birth, and MD5 hashed passwords, as well as an unknown number of security questions and answers stolen by hackers using stolen proprietary code						
DU Group dba DU Caller	5/13/17	10	2,000,000,000	ADD / NAA / NUM	Web	Inside	China
	2,000,000,000 user phone numbers, names, and addresses inappropriately made accessible to others through an uncensored public directory						
River City Media, LLC (RCM)	3/3/17	10	1,374,159,612	ADD / EMA / FIN / MISC / NAA	Web	Inside- Accident	United States
	1,374,159,612 names, addresses, IP addresses, and email addresses, as well as an undisclosed number of financial documents, chat logs, and backups exposed by faulty Rsync backup						
NetEase, Inc. dba 163.com	1/25/17	10	1,221,893,767	EMA / PWD	Hack	Outside	China
	1,221,893,767 email addresses and passwords stolen by hackers and sold on the Dark Web by DoubleFlag						
Unknown Organization	1/3/18	10	1,190,000,000	ADD / EMA / MISC / NAA / NUM / SSN	Fraud SE	Unknown	India
	1,190,000,000 names, Aadhaar numbers, addresses, phone numbers, email addresses, postal codes, and photographs of Indian citizens made available to unauthorized users, most likely by former village-level enterprise (VLE) operators selling access to the Aadhaar database						
Verifications.io	3/7/19	10	982,864,972	ADD / DOB / EMA / FIN / MISC / NAA / NUM / PWD	Web	Inside- Accident	Estonia
	982,864,972 names, addresses, email addresses, dates of birth, phone numbers, fax numbers, genders, IP addresses, personal mortgage amounts, and FTP server credentials exposed on the Internet due to a misconfigured database						
First American Financial Corporation	5/24/19	10	885,000,000	ADD / EMA / FIN / MISC / NAA / NUM / SSN	Web	Inside- Accident	United States
	Approximately 885,000,000 real estate closing transaction records containing names, Social Security numbers, phone numbers, email and physical addresses, driver's license images, banking details, and mortgage lender names and loan numbers exposed on the Internet due to IDOR flaw						
Unknown Organization	8/29/17	9.63002	711,000,000	EMA / MISC / PWD	Web	Inside- Accident	Netherlands
	711,000,000 email addresses, passwords, and SMTP credentials exposed on the Internet due to a misconfigured spambot database						
Cultura Colectiva	4/3/19	10	540,000,000	ACC / MISC	Web	Inside- Accident	Mexico
	540,000,000 Facebook user IDs, account names, comments, and likes exposed on the Internet due to a misconfigured database						
Altaba, Inc (formerly known as Yahoo)	9/22/16	10	500,000,000	DOB / EMA / MISC / NAA / NUM / PWD	Hack	Outside	United States
	500,000,000 user names, email addresses, phone numbers, dates of birth, bcrypt hashed passwords and some security questions and associated answers compromised by hackers						

ASMGi

Looking at Historical Breach Data

ASMGi

Historical Breach Data annotated with CIS Controls

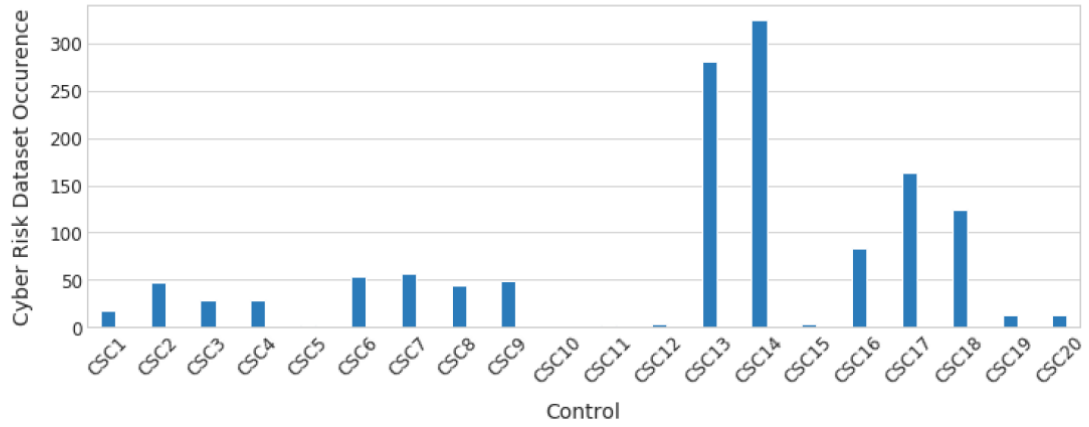


Figure 1: Shows the total number of times a CIS control could have prevented a cyber breach

The 3 most frequently affected controls from our analysis are:

CIS 14—Controlled Access Based on the Need to Know: This covers all the cases when the network was not properly segmented based on application and data sensitivity, e.g. cases when retailer's Point Of Sale (POS) devices were on the same network as regular employee endpoints. It also includes cases when shared folders were not properly protected with access controls and unauthorized people had access to sensitive data such as IP, PII, PHI, PFI, etc. Finally, scenarios such as unencrypted hard drives lost during transport by 3d parties, stolen unencrypted laptops, and disk drives.

CIS 13—Data Protection: This control covers all scenarios related to data stolen from undocumented or misplaced storage locations (laptops, network drives, 3d party cloud providers, etc.), data backups, legacy databases, and applications. Additionally, it includes cases when raw data in the clear text were exfiltrated without detection.

CIS 17—Implement a Security Awareness and Training Program: Covers all cases of fishing and more general cases when the attacker requested an employee to make some action such as making a wire transfer, sending a tax form or other sensitive information. Any unintentional disclosure of sensitive data to the attacker is included as well.

Financial Services Statistics 2019

Frequency

927 incidents, 207 with confirmed data disclosure

Top 3 patterns

Web Applications, Privilege Misuse, and Miscellaneous Errors represent 72% of breaches

---

Threat actors

External (72%), Internal (36%), Multiple parties (10%), Partner (2%) (breaches)

Actor motives

Financial (88%), Espionage (10%) (breaches)

Data compromised

Personal (43%), Credentials (38%), Internal (38%) (breaches)

Verizon Data Breach Report

Financial Services Statistics 2019

ASMGi

Financial and Insurance

Banking Trojan Botnets: 27,000% of Breaches

This threat is so prevalent that the authors chose to exclude it from the report's data to prevent it from eclipsing other insights.

Here's how they described it:

They are "botnets that target organizations' customers, infecting their personally owned devices with malware that captures login details. Those credentials are then used to access banking applications and other sites with authentication."

Nearly 40,000 successful data breaches in financial and insurance companies are attributed to this threat. That's more than 27,000% greater than the remaining 146 confirmed data breaches in this vertical.

So, it's a big problem.

Denial of Service: 56% of Incidents

Setting aside the trojan botnets, DoS attacks caused the majority of remaining security incidents recorded in financial and insurance.

However, not a single DoS was part of a successful data breach. This is true across all industries covered in the report – financial and otherwise.

Cyber Security Predictions for 2020 …

ASMGi

Cyber trends for 2020

Cyber security trend #1: The phishing landscape is changing, though email still ranks as the biggest of those threats

Cyber security trend #2: Increasing use of mobile as an attack vector

Cyber security trend #3: Targeting of local governments and enterprises via ransomware attacks

Cyber security trend #4: Increasing emphasis on data privacy, sovereignty, and compliance

Cyber security trend #5: Increasing investments in cyber security automation

Cyber security trend #6: Increasing use of I0T / OT as an attack vector

Cyber security trend #7: Increasing number and magnitude of breaches

Cyber security trend #8: The growing impact of AI/ML on Cyber

Cyber security trend #9: Emphasis on Quantifying Cyber Risk

Cyber security trend #10: Cyber Insurance will continue to focus more on actual security posture and will become more of a tool in the Cyber Security arsenal.

Speaker Predictions for 2020

Today's expert speaker #1 Cyber Prediction for 2020….

Ken Makoid = ??

Frank Yako = ??

Steve Roesing = ??

How do we win?

ASMGi

Some best practices to prevent breaches

Keep it clean.
Many breaches are a result of poor security hygiene and a lack of attention to detail. Clean up human error where possible, then establish an asset and security baseline around internet-facing assets like web servers and cloud services.

Maintain integrity.
Web application compromises now include code that can capture data entered into web forms. Consider adding file integrity monitoring on payment sites, in addition to patching operating systems and coding payment applications.

Redouble your efforts.
2FA everything. Use strong authentication on customer-facing applications, any remote access and cloud-based email. There are examples of 2FA vulnerabilities, but they don't excuse lack of implementation.

Be wary of inside jobs.
Track insider behavior by monitoring and logging access to sensitive data. Make it clear to staff just how good you are at recognizing fraudulent transactions.

Scrub packets.
Distributed denial of service (DDoS) protection is an essential control for many industries. Guard against nonmalicious interruptions with continuous monitoring and capacity planning for traffic spikes.

Stay socially aware.
Social attacks are effective ways to capture credentials. Monitor email for links and executables. Give your teams ways to report potential phishing or pretexting.

How do we win?

ASMGi

Technology partner integrations

Build a Cyber-Technology Ecosystem

How do we win?

ASMGi

Plan & Practice, Practice, Practice

Educate & Create a Culture of Security

Outsource where you are limited in Resources and/or Capabilities

Have a deliberate, intentional plan for executing cyber control implementations

How many of your data centers look like this …

… Or meet these compliance requirements

ITIL V3 Certified

ITAR

NIST

AICPA SOC — American Institute of Certified Public Accountants Trust Services Principles for security, and availability

SOC 3 — SOC 3 Trust Services Report

PCI DSS COMPLIANT — Level 1 PCI DSS service provider for colocation and cloud

ISO 27001 CERTIFIED by schellman — Information Security Management System standard

HITRUST CSF Certified — HITRUST CSF service provider for colocation and cloud

SSAE 16 CERTIFIED — SOC 1 dual-standard report

HIPAA Health Insurance Portability & Accountability Act — Health Insurance Portability and Accountability Act Security Rule

FLEXENTIAL

A Holistic Approach to Cyber Security

ASMGi

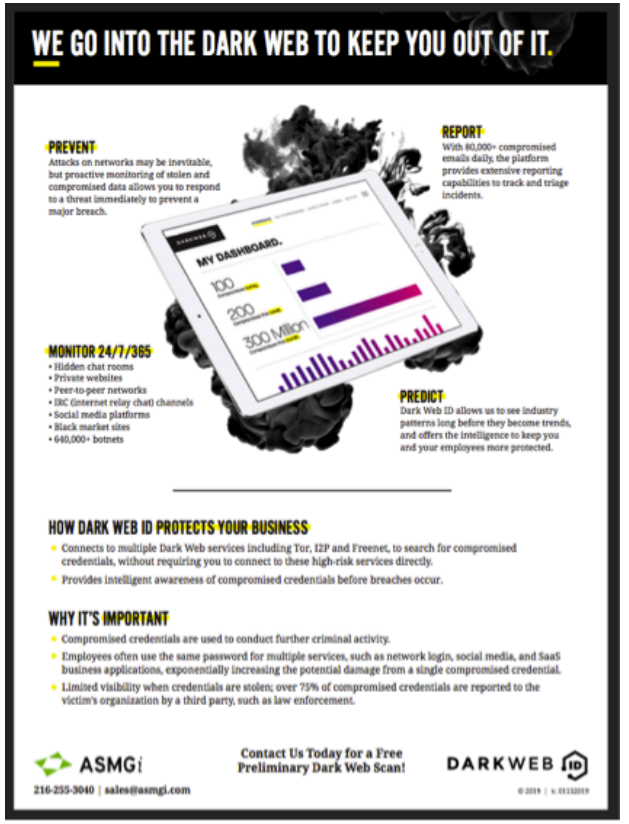
Total Solution = Program + Technology + Operations

Special Webinar Offer …

- … for those attending today's webinar, please call +1 216.255.3040 or email *Steve Roesing or Frank Yako* directly for a **NO COST Dark Web Scan**.

sroesing@asmgi.com *fyako@asmgi.com*

- We will perform a **FREE** Dark Web Scan and review the results with you help you to track and triage compromised credentials.
- When combined with an overall Holistic Cyber Security Program it can help you prevent and predict breaches.



ASMGi

Thank You!

800 Superior Ave E, Ste 1050
Cleveland, OH 44114

Phone: 216.255.3040
Fax: 216.274.9647

Email: info@asmgi.com

www.asmgi.com