Q3 2022 Data Breach Analysis: Compromises & Victims Up from Q2 – Record High Year Unlikely

Key Takeaways

- Data compromises in the third quarter (Q3) of 2022 increased by 15 percent over Q2 but continued to track behind the record pace of 2021.
- The number of victims jumped dramatically in Q3 – a staggering 210 percent over Q2 2022.
- Supply Chain Attacks made a comeback in Q3 as the number of impacted entities increased 250 percent from H1 2022.
- Cyberattacks made up 88 percent of data breaches in Q3 as Phishing Attacks remained the primary attack vector for the 15th consecutive Quarter.
- More than 45 percent of data breach notices related to cyberattacks did not contain information about the attack that could assist other businesses or individuals take actions to prevent or recover from a similar attack.

Summary

- The number of data compromises reported in Q3 2022 increased to 474 from 413 in Q2 and 403 in Q1 for a year-to-date (YTD) total of 1,291.
- More than 105M victims were impacted by data compromises in Q3 compared to 61M victims in the first half of the year, representing 55 percent of the year's total number of victims.
- Cyberattacks (419) remained the primary source of data compromises, followed by System & Human Errors (39), Physical Attacks (11) and Unknown (5).
- More than 1,280 entities were impacted by 48 Supply Chain/Third-Party attacks in Q3 compared to 367 organizations affected by 44 attacks in the first six months of 2022.
- Phishing remains the attack vector of choice, with 124 attacks in Q3, up from 107 in Q2 and 110 in Q1 2022. Ransomware attacks rebounded slightly in the Quarter – 69 attacks in Q3 compared to 55 in Q2 - while Malware-based attacks dropped to the lowest number in 3.75 years – 13 attacks.
- The number of data breach notices with no information about the root cause of the compromise increased for the fourth consecutive Quarter to 199 of the 419 breaches reported in Q3.

Discussion

- With three months left in 2022, the YTD number of publicly-reported data compromises - 1,291 - is only 69 percent of the year-end total in 2021. Absent a dramatic increase in data compromises in Q4 2022, it is unlikely the total number of data breaches will set a record this year. The total number of data compromises will likely surpass the penultimate record from 2017 of 1,506 compromises.
- Despite a triple-digit increase in victims during Q3, the number of data compromise victims is likely to show a year-over-year (YoY) decline for the fourth year in a row. However, the number of victims impacted by a compromise can increase significantly with only a handful of breaches. For example, two Q3 breaches - an AT&T-related breach (23M victims) and one at Neopets (69M victims) - account for more than half of the YTD victim count.

- The number of cyberattack-related data breach notices where there is no information available about the root cause of an attack continues to grow, along with concerns that this trend will move into 2023. From Q1 2019 through Q3 2021, the ITRC logged only 16 data breach notices where there was no information about the cause of a cyberattack. From Q4 2021 through Q3 2022, the number of notices with no specific attack vector has grown to 617, 37 percent of all cyberattack-related data breaches reported in the period. Businesses and individuals are at increased risk of a cybercrime when important information is not included in data breach notices.
- While Physical Attacks and System & Human Errors still exist, Cyberattacks have been the root cause of the vast majority of data compromises for the past 3.75 years. Within that category, Phishing is, by far, the most common attack vector. Despite a decline in ransomware attacks earlier in the year, ransomware has rebounded slightly. Non-Russian affiliated groups have emerged, and cryptocurrency markets were less volatile in the Quarter.
- Malware attacks are increasingly rare as the number of related attacks has dropped steadily from a recent high of 39 attacks in Q2 2021 to 13 in Q3 2022. That compares to 15 data breaches associated with personal information inadvertently being exposed in correspondence in the most recent Quarter.

Q3 2022 Data Compromise Details

Number of Q3 Compromises

- **Total Data Compromises**: 474 compromises; 105,780,986 victims
- **Data Breaches**: 466 data breaches; 82,966,797 victims
- **Data Exposures**: 3 data exposures; 2,403 victims
- **Data Leaks**: N/A
- **Unknown**: 5 unknown; 22,811,786 victims

Attack Vectors Q3 2022

- **Cyberattacks**: 419 breaches; 82,822,161 victims
  - 124 Phishing/smishing/BEC
  - 69 Ransomware
  - 13 Malware
  - 8 Credential Stuffing
  - 3 Other
  - 2 Zero Day Attack
  - 1 Non-secured Cloud Environment
  - 199 N/A – not specified

- **System & Human Errors:** 39 breaches/exposures; 131,724 victims
  - 15 Correspondence (email/letter)
  - 7 Misconfigured firewalls
  - 5 Other
  - 3 Failure to configure cloud security
  - 3 Lost device or document
  - 6 N/A – not specified
- **Physical Attacks:** 11 breaches; 15,315 victims
  - 3 Device Theft
  - 2 Other
  - 2 Document Theft
  - 2 Skimming Device
  - 1 Improper Disposal
  - 1 N/A
- **Supply Chain Attacks** (*included in the attack vectors above*)
  - 1,286 entities were impacted by 49 third-party/supply chain attacks, including two (2) attacks that were reported in 2020; 5,160,413 individuals were impacted in Q3
    - 1,281 entities affected 3,744,905 individuals impacted by cyberattacks
    - Five (5) entities affected; 1,415,508 victims impacted by system & human errors
  - Noteworthy supply chain attacks include:
    - **Professional Finance Company (2022):** As of 10/3/2022, the ITRC has recorded 618 entities w/ 1,918,941 victims impacted.
    - **Illuminate Education (2022):** As of 10/3/2022, the ITRC has recorded 611 entities w/ 2,108,045 victims impacted. **Note: The ITRC is entering districts as information is reported. The total number of victims per district has not been disclosed.*
    - **Shields Health Care Group, Inc. (2022):** As of 10/3/2022, the ITRC has recorded 56 entities w/ 1,804,069 victims impacted.
    - **OneTouchPoint, Inc. (2022):** As of 10/3/2022, the ITRC has recorded 42 entities w/ 2,651,396 victims impacted.
    - **Eye Care Leaders (2022):** As of 10/3/2022, the ITRC has recorded 36 entities w/ 3,357,880 victims impacted.
    - **Horizon Actuarial Services, LLC (2022):** As of 10/3/2022, the ITRC has recorded three (3) entities w/ 2,292,080 victims impacted.
    - **Nelnet Servicing, LLC (2022):** As of 10/3/2022, the ITRC has recorded two (2) entities w/ 2,501,324 victims impacted.

Charts

Compromise & Victim: Totals		
Year	Compromises	Victims
2022 YTD	**1,291**	**166,782,123**
2021	1,862	298,197,505
2020	1,108	310,218,744
2019	1,279	883,558,186
2018	1,175	2,227,849,622
2017	1,506	1,825,413,935
2016	1,088	2,541,092,072

Compromises & Victims: Quarter-to-Quarter		
Year & Quarter	Compromises	Victims
2022 Q3 (JUL-SEP)	**474**	**105,780,986**
2022 Q2 (APR-JUN)	413	34,239,785
2022 Q1 (JAN-MAR)	404	26,761,352
2021 Q4 (OCT-DEC)	566	35,388,356
2021 Q3 (JUL-SEP)	445	166,233,442
2021 Q2 (APR-JUN)	497	55,321,228
2021 Q1 (JAN-MAR)	354	41,254,479
2020 Q4 (OCT-DEC)	326	16,683,032
2020 Q3 (JUL-SEP)	248	60,952,924
2020 Q2 (APR-JUN)	295	100,918,230
2020 Q1 (JAN-MAR)	239	131,664,558

Compromises by Sector								
Year								
	Q3 2022		YTD 2022		FY 2021		FY 2020	
	Compromises	Victims	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	24	483,412	65	888,905	125	1,687,192	42	974,054
Financial Services	67	3,115,672	194	25,498,818	279	19,978,108	138	2,687,084
Government	19	82,510	52	893,039	66	3,244,455	47	1,100,526
Healthcare	94	2,163,551	255	14,605,207	330	30,853,767	306	9,700,238
Hospitality	10	69,026,205	21	69,103,966	33	238,445	17	22,365,384
Manufacturing & Utilities	64	23,018,654	179	23,506,593	222	49,782,583	70	2,896,627
Military	-	-	-	-	-	-	-	-
Non-Profit/NGO	16	40,875	51	711,574	86	2,339,646	31	37,528
Professional Services	68	1,558,274	163	4,904,796	184	22,729,391	144	73,012,145
Retail	20	288,774	50	614,219	102	7,212,912	53	10,710,681
Technology	21	2,816,199	52	18,403,626	79	44,684,180	67	142,134,883
Transportation	6	2,516,097	25	3,361,030	44	569,684	21	1,208,292
Other	65	670,763	184	4,290,350	308	79,644,478	172	43,391,302
Unknown	-	-	-	-	4	35,232,664	-	-
TOTALS:	474	105,780,986	1,291	166,782,123	1,862	298,197,505	1,108	310,218,744

Notices with Victim Count vs Notices without Victim Count			
Year & Quarter	Compromises	Notices with Victim Count	%
2022 Q3 (JUL-SEP)	**474**	**264**	**56%**
2022 Q2 (APR-JUN)	413	246	60%
2022 Q1 (JAN-MAR)	404	264	65%
2021 Q4 (OCT-DEC)	566	288	51%
2021 Q3 (JUL-SEP)	445	292	66%
2021 Q2 (APR-JUN)	497	299	60%

Compromises by Attack Vector				
	Q3 2022	YTD 2022	FY 2021	FY 2020
Cyberattacks	**419**	**1,154**	**1,613**	**878**
Phishing/smishing/BEC	124	343	537	383
Ransomware	69	194	352	158
Malware	13	60	141	104
Non-secured Cloud Environment	1	6	24	50
Credential Stuffing	8	14	14	17
Unpatched software flaw	-	-	4	3
Zero Day Attack	2	3	4	1
Other	3	19	426	162
NA – not specified	199	515	111	-
System & Human Errors	**39**	**100**	**179**	**152**
Failure to configure cloud security	3	13	54	57
Correspondence (email/letter)	15	36	66	55
Misconfigured firewall	7	22	13	4
Lost device or document	3	4	12	5
Other	5	11	34	31
NA – not specified	6	14	-	-
Physical Attacks	**11**	**27**	**51**	**78**
Document Theft	2	5	9	15
Device Theft	3	12	17	30
Improper Disposal	1	4	5	11
Skimming Device	2	3	1	5
Other	2	2	19	17
NA – not specified	1	1	-	-
Unknown	**5**	**10**	**12**	**n/a**

METHODOLOGY NOTES: For purposes of quarterly and annual reporting, the ITRC aggregates data events based on the date the breach, exposure, or leak was entered into the database rather than the date the event occurred. This avoids the confusion and data conflicts associated with the need to routinely update previous reports and compromise totals. The date of the original compromise, if known, and the date of the event report are noted in the ITRC's *notified* data compromise tracking database.

The number of victims linked to individual compromises are updated as needed and can be accessed in the ITRC's *notified* breach tracking solution.

The ITRC reports Third-Party/Supply Chain Attacks as a single attack against the company that lost control of the information. The total number of individuals impacted by third-party incidents is based on notices sent by the multiple organizations impacted by the single data compromise.

Unless otherwise noted, all data reported here was entered into the ITRC *notified* database between July 1, 2022, through September 30, 2022.