

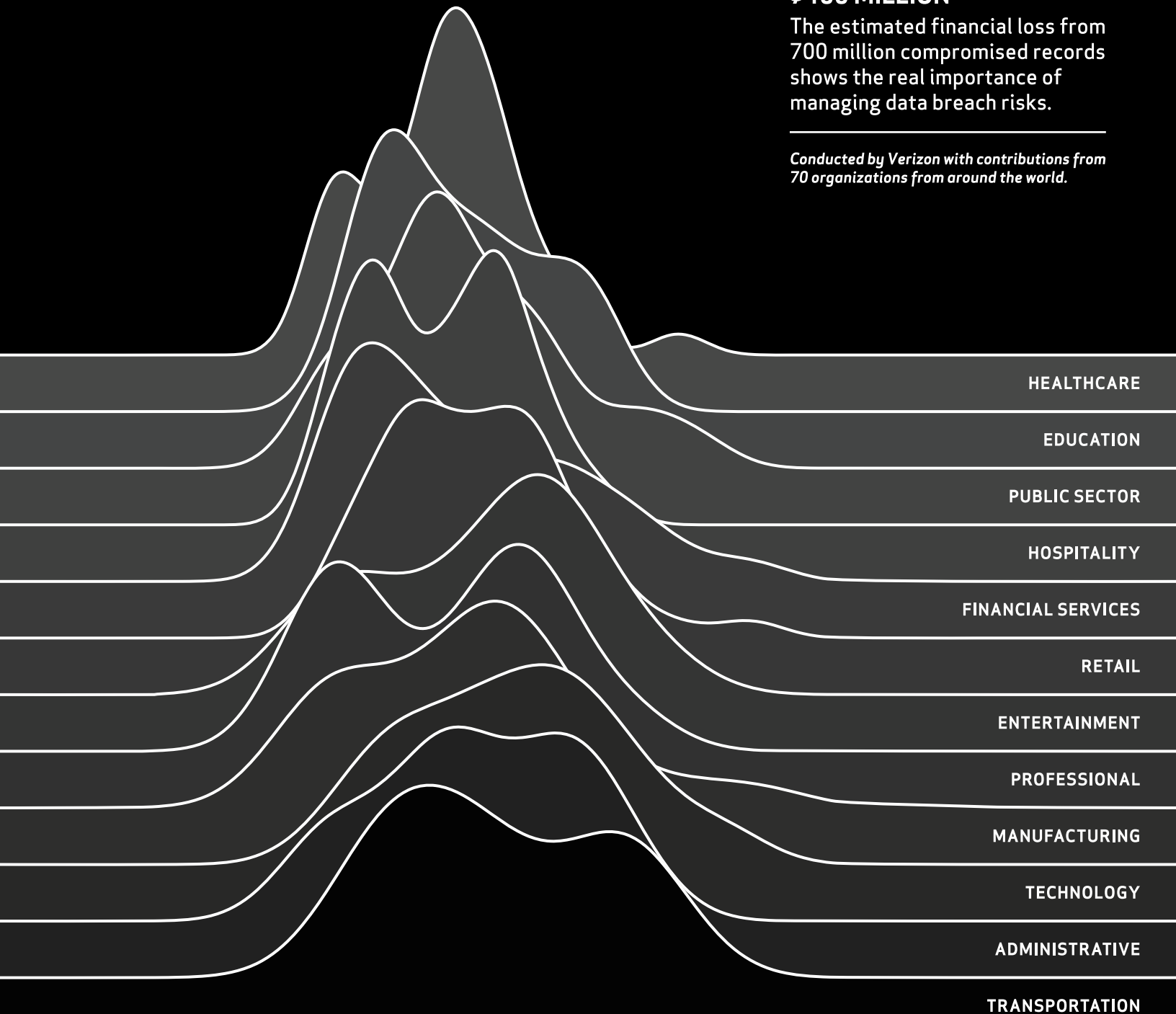


2015 DATA BREACH INVESTIGATIONS REPORT

\$400 MILLION

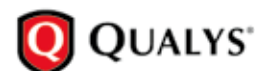
The estimated financial loss from 700 million compromised records shows the real importance of managing data breach risks.

Conducted by Verizon with contributions from 70 organizations from around the world.



2015 DBIR Contributors

(See Appendix C for a detailed list.)





CONTENTS

- Introduction..... 1
- Victim Demographics..... 2
- Breach Trends: Looking Back Before Diving Ahead..... 4
- Before and Beyond the Breach..... 7
- Indicators of Compromise: “Sharing Is Cyber-Caring” 8
- Phishing: “Attn: Sir/Madam”.....12
- Vulnerabilities: “Do We Need Those Stinking Patches?”15
- Mobile: “I Got 99 Problems and Mobile Malware Isn’t Even 1% of Them”18
- Malware: “Volume, Velocity, and Variation”21
- Industry Profiles: “Raising the Stakes With Some Takes on NAICS”24
- Impact: “In the Beginning, There Was Record Count” 27
- Incident Classification Patterns31
 - Point-of-Sale Intrusions 35
 - Payment Card Skimmers 37
 - Crimeware..... 39
 - Web App Attacks41
 - Denial-of-Service Attacks.....43
 - Physical Theft/Loss45
 - Insider Misuse..... 46
 - Miscellaneous Errors.....49
 - Cyber-Espionage 52
- Wrap-Up 55
- Appendix A: Year in Review 57
- Appendix B: Methodology59
- Appendix C: Contributing Organizations61
- Appendix D: The Internet of Things 62

**QUESTIONS?
COMMENTS?
BRILLIANT IDEAS?**

We want to hear them. Drop us a line at dbir@verizon.com, find us on [LinkedIn](#), or tweet [@VZdbir](#) with the hashtag [#dbir](#).

Figure 2 provides the specs for both victim industries⁵ and size ranges. Don't give much credence to the huge number for the Public sector; we have many government CSIRTs participating in this report, and they handle a high volume of incidents (many of which fall under regulatory reporting requirements). The four columns on the right filter out the noise of these incidents—many of which are rather mundane—by including only confirmed data breaches.

The top three industries affected are the same as previous years: Public, Information, and Financial Services.

The industries most affected look remarkably similar to prior years, and the top three are exactly the same: Public, Information, and Financial Services. Our overall take from these results remains consistent as well: No industry is immune to security failures. Don't let a "that won't happen to me because I'm too X" attitude catch you napping. Other than that, we'll refrain from further commentary on these demographics and simply encourage you to look them over to decide how relevant they are to your organization and whether they change the way you read/use this report.

INCIDENTS VS. BREACHES
 This report uses the following definitions:
Security incident: Any event that compromises the confidentiality, integrity, or availability of an information asset.
Data breach: An incident that resulted in confirmed disclosure (not just exposure) to an unauthorized party. We use this term interchangeably with "data compromise" and "data breach" in this report.

INDUSTRY	NUMBER OF SECURITY INCIDENTS				CONFIRMED DATA LOSS			
	TOTAL	SMALL	LARGE	UNKNOWN	TOTAL	SMALL	LARGE	UNKNOWN
Accommodation (72)	368	181	90	97	223	180	10	33
Administrative (56)	205	11	13	181	27	6	4	17
Agriculture (11)	2	0	0	2	2	0	0	2
Construction (23)	3	1	2	0	2	1	1	0
Educational (61)	165	18	17	130	65	11	10	44
Entertainment (71)	27	17	0	10	23	16	0	7
Financial Services(52)	642	44	177	421	277	33	136	108
Healthcare (62)	234	51	38	145	141	31	25	85
Information (51)	1,496	36	34	1,426	95	13	17	65
Management (55)	4	0	2	2	1	0	0	1
Manufacturing (31-33)	525	18	43	464	235	11	10	214
Mining (21)	22	1	12	9	17	0	11	6
Other Services (81)	263	12	2	249	28	8	2	18
Professional (54)	347	27	11	309	146	14	6	126
Public (92)	50,315	19	49,596	700	303	6	241	56
Real Estate (53)	14	2	1	11	10	1	1	8
Retail (44-45)	523	99	30	394	164	95	21	48
Trade (42)	14	10	1	3	6	4	0	2
Transportation (48-49)	44	2	9	33	22	2	6	14
Utilities (22)	73	1	2	70	10	0	0	10
Unknown	24,504	144	1	24,359	325	141	1	183
TOTAL	79,790	694	50,081	29,015	2,122	573	502	1,047

Figure 2.
 Security incidents by victim industry and organization size

⁵ We use the North American Industry Classification System (NAICS) for coding victim industry. www.census.gov/eos/www/naics

BREACH TRENDS

Looking Back Before Diving Ahead

This is an annual report, and as such, it traditionally focuses on interesting developments over the previous year. Some aspects of the threat space change that quickly, but others undulate and evolve over a longer period of time. We don't want to lose sight of either the forest or the trees, so before delving into updates on each incident pattern, let's take a look at some of the longer-term trends and high-level findings from this year's data.

THREAT ACTORS

Though the number of breaches per threat actor changes rather dramatically each year as we add new partners and more data, the overall proportion attributed to external, internal, and partner actors stays roughly the same. The stream plot for Figure 3 demonstrates this well and shows that overall trends in the threat actors haven't shifted much over the last five years.

Threat Actors: Virtually no change in overall proportion attributed to external, internal, and partner actors.

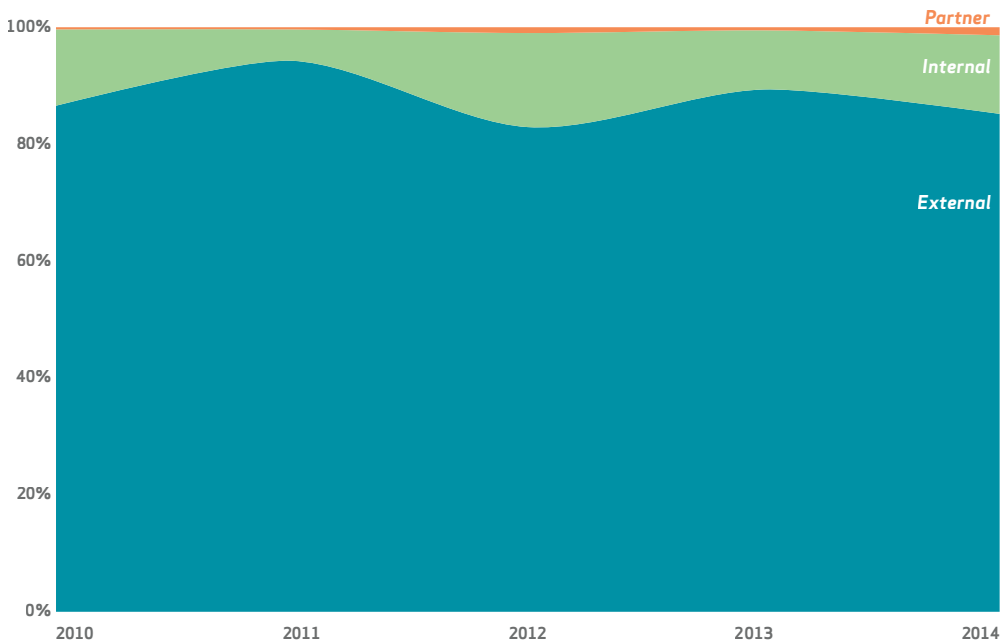


Figure 3.

Actor categories over time by percent of actors