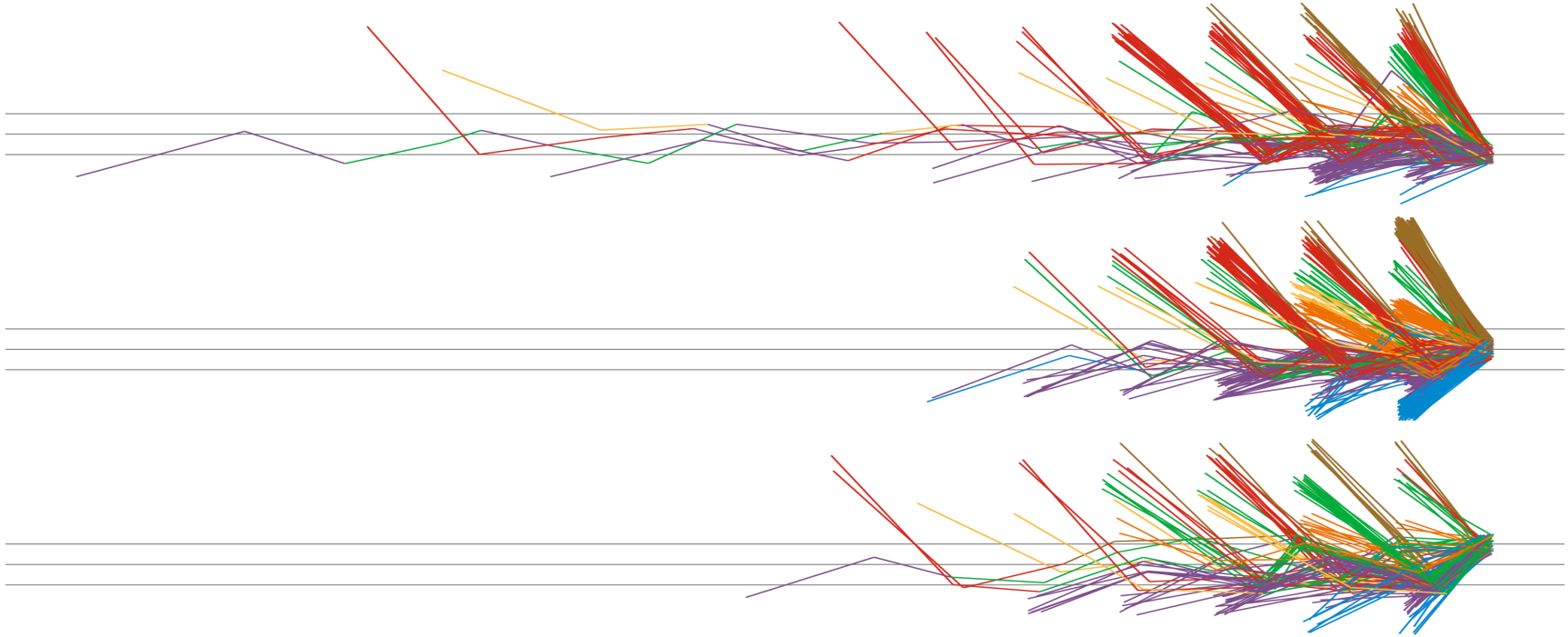
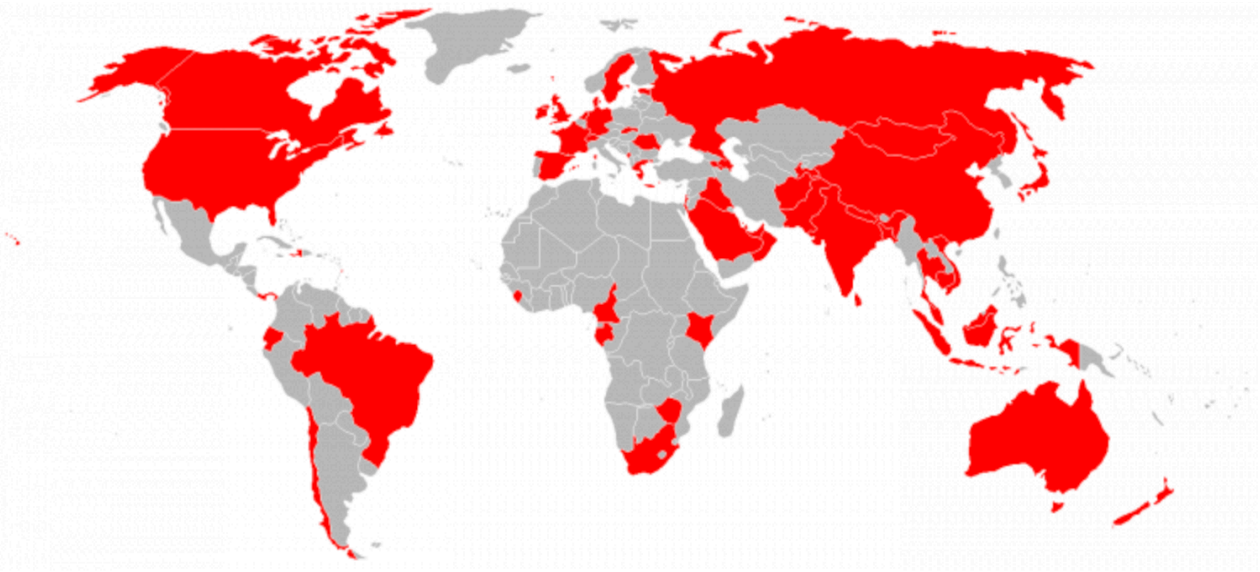


2019 Verizon Data Breach Investigations Report

Suzanne Widup

verizon

Demographics



73

CONTRIBUTING ORGANIZATIONS

41,686

SECURITY INCIDENTS

2,013

CONFIRMED DATA BREACHES

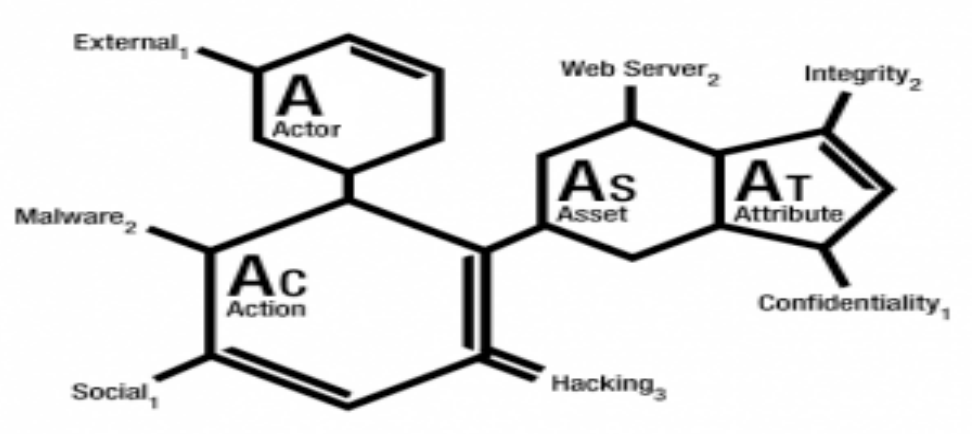
86

COUNTRIES REPRESENTED

verizon

The VERIS Framework

Vocabulary for Event Recording and Incident Sharing (VERIS) is an open framework designed to provide a common language for describing security incidents (or threats) in a structured and repeatable manner.



Actor – Who did it?

Action – How'd they do it?

Asset – What was affected?

Attribute – How was it affected??

http://www.veriscommunity.net

VERIS in Action

MALWARE

Malware is any **mal**icious soft**ware**, script, or code run on a device that alters its state or function without the owner's informed consent. Examples include viruses, worms, spyware, keyloggers, backdoors, etc.

VARIETY

Question Text: What varieties or functions of malware were involved?

User notes: N/A

Question type: enumerated list (multi-select)

Variable name: *action.malware.variety* (string)

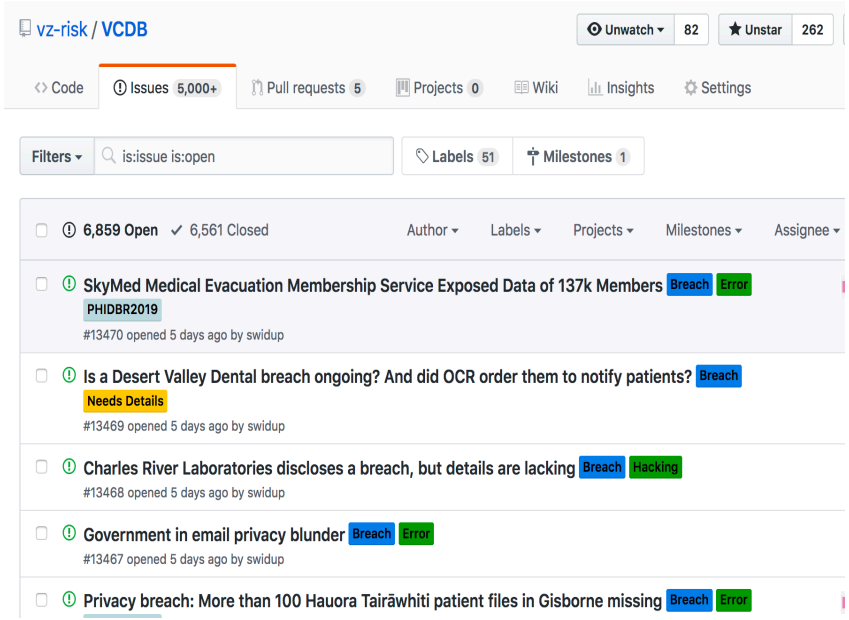
Purpose: In the short term, variety is necessary to adequately describe the incident and its ramifications. In the long term, it gives insight into the evolving nature of malware and how criminals use it.

Developer notes: N/A

Miscellaneous: N/A

VECTOR

Question Text: What were the vectors or paths of infection?



https://github.com/vz-risk/VCDB/issues

DBIR Overview

Incidents vs Breaches

What influences these numbers?

- Regulatory requirements
- Partner visibility
- Breach trends

Incidents:	Total	Small	Large	Unknown	Breaches: Total	Small	Large	Unknown
Accommodation (72)	87	38	9	40	61	34	7	20
Administrative (56)	90	13	23	54	17	6	6	5
Agriculture (11)	4	2	0	2	2	2	0	0
Construction (23)	31	11	13	7	11	7	3	1
Education (61)	382	24	11	347	99	14	8	77
Entertainment (71)	6,299	6	6	6,287	10	2	3	5
Finance (52)	927	50	64	813	207	26	19	162
Healthcare (62)	466	45	40	381	304	29	25	250
Information (51)	1,094	30	37	1,027	155	20	18	117
Management (55)	4	1	3	0	2	1	1	0
Manufacturing (31-33)	352	27	220	105	87	10	22	55
Mining (21)	28	3	6	19	15	2	5	8
Other Services (81)	78	14	5	59	54	6	5	43
Professional (54)	670	54	17	599	157	34	10	113
Public (92)	23,399	30	22,930	439	330	17	83	230
Real Estate (53)	22	9	5	8	14	6	3	5
Retail (44-45)	234	58	31	145	139	46	19	74
Trade (42)	34	5	16	13	16	4	8	4
Transportation (48-49)	112	6	23	83	36	3	9	24
Utilities (22)	23	3	7	13	8	2	0	6
Unknown	7,350	0	3,558	3,792	289	0	109	180
Total	41,686	429	27,024	14,233	2,013	271	363	1,379

Table 2
Number of security incidents by victim industry and organization size

verizon

Threat Actors

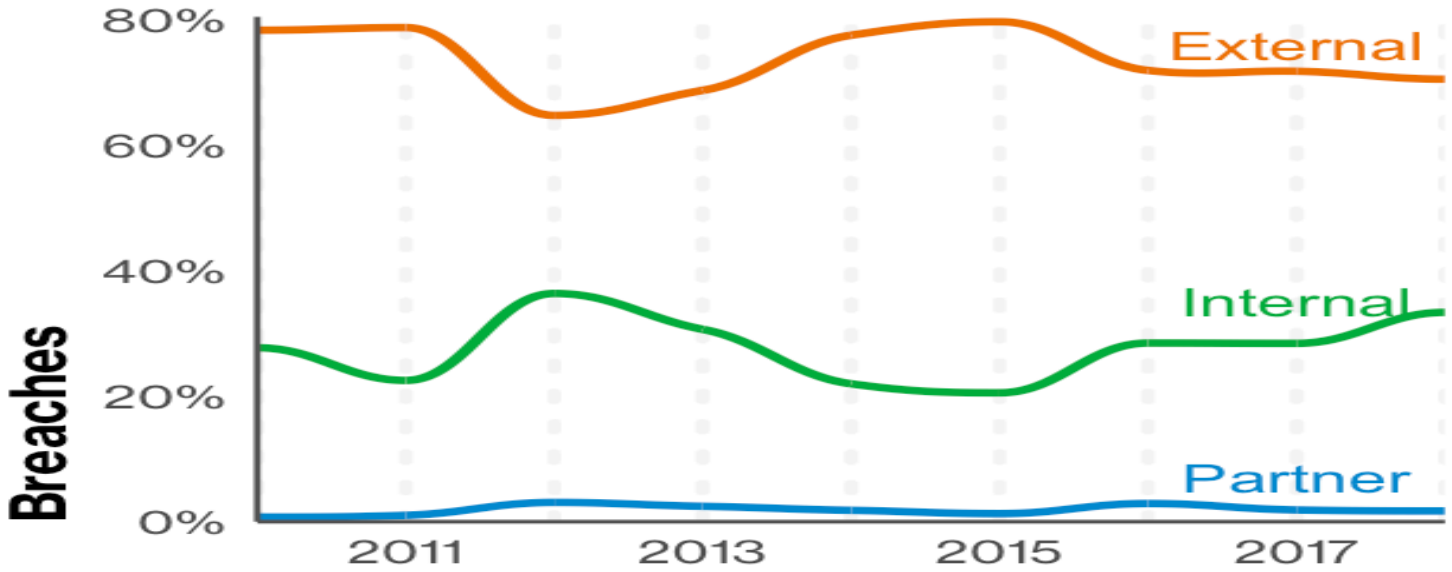


Figure 6. Threat actors in breaches over time

Actor Motives

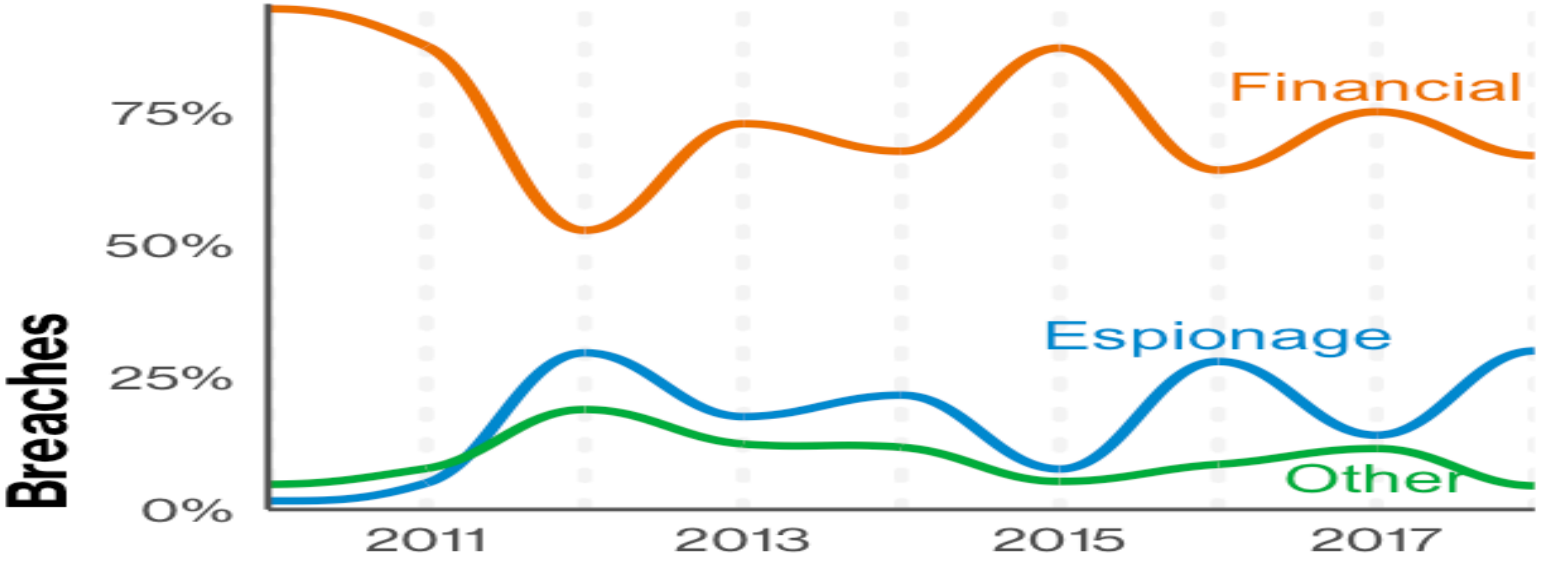


Figure 7. Threat actor motives in breaches over time

Actor Varieties

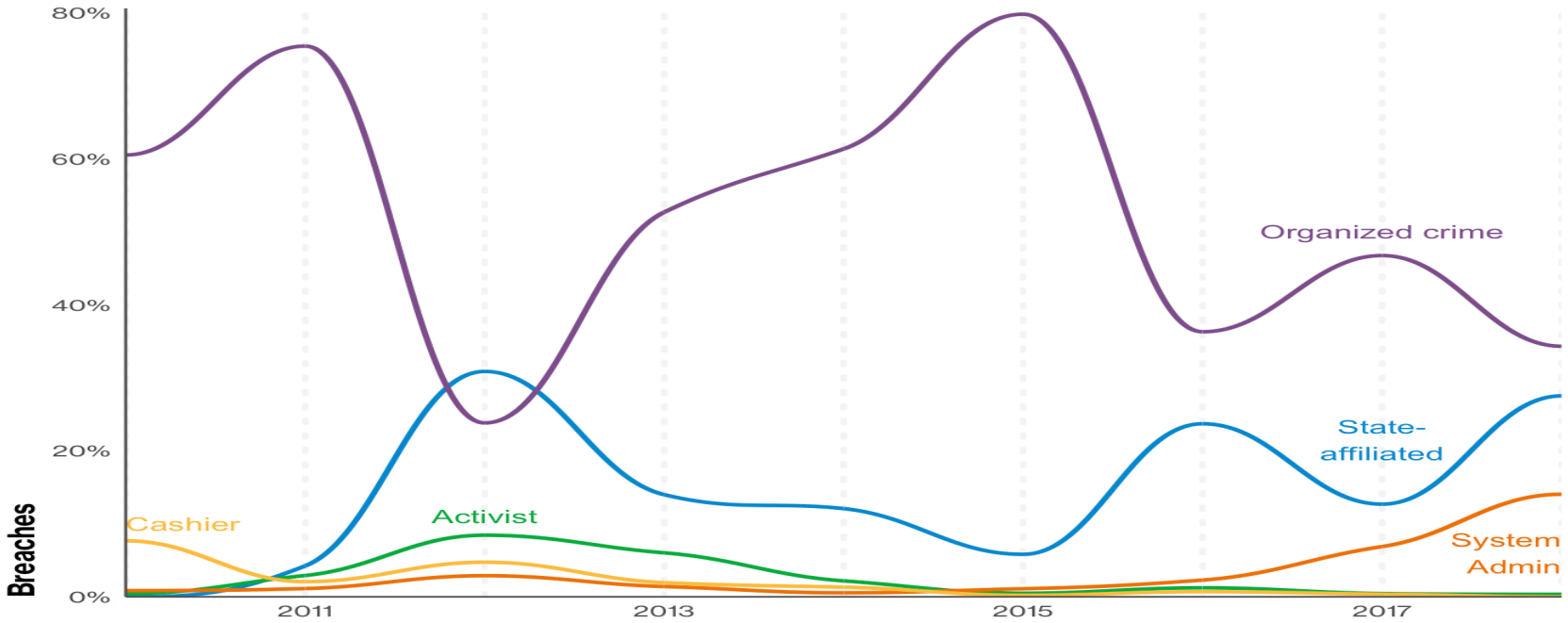


Figure 8. Select threat actors in breaches over time

Discovery Timeline

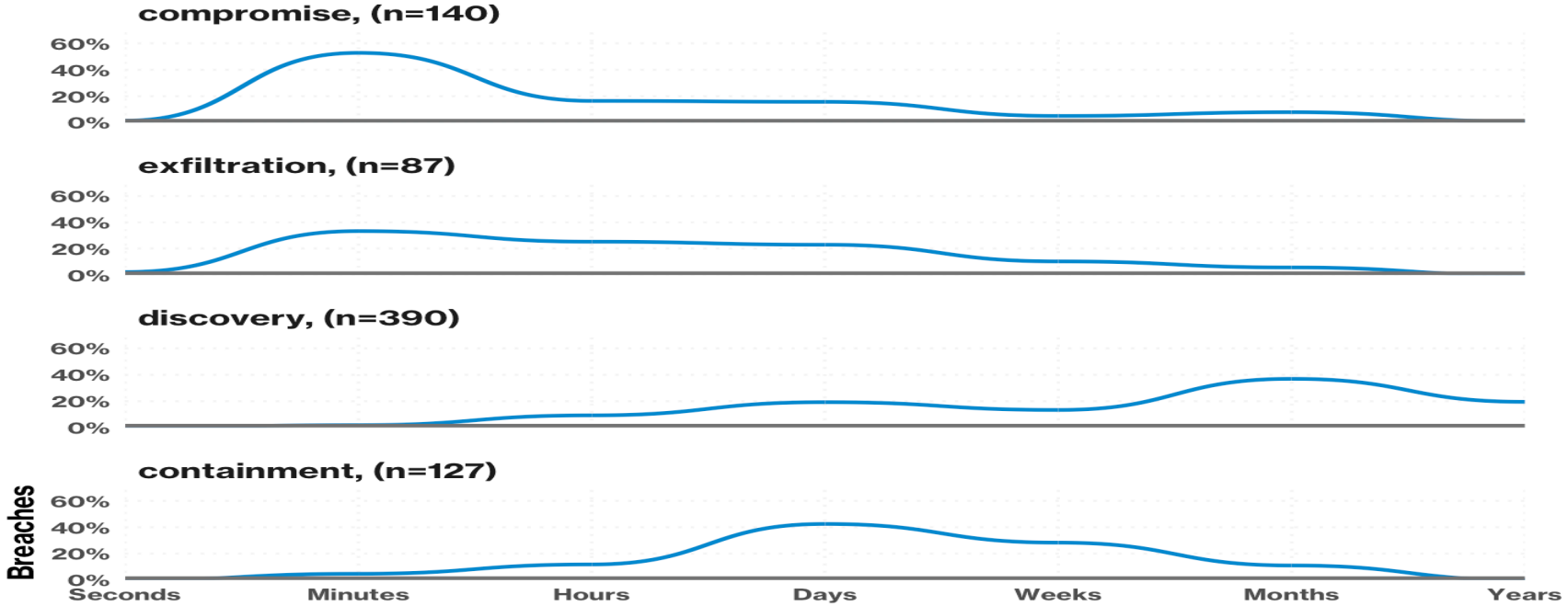
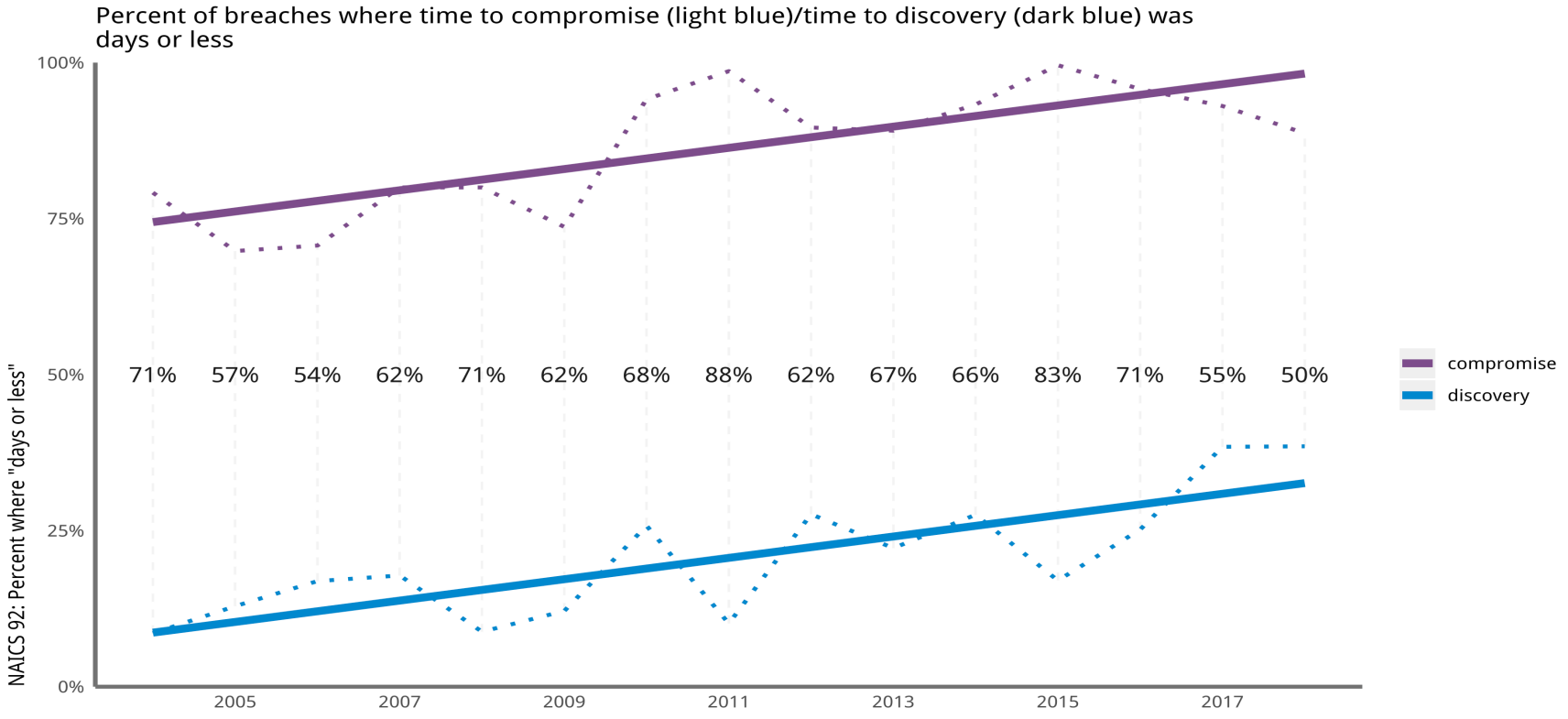
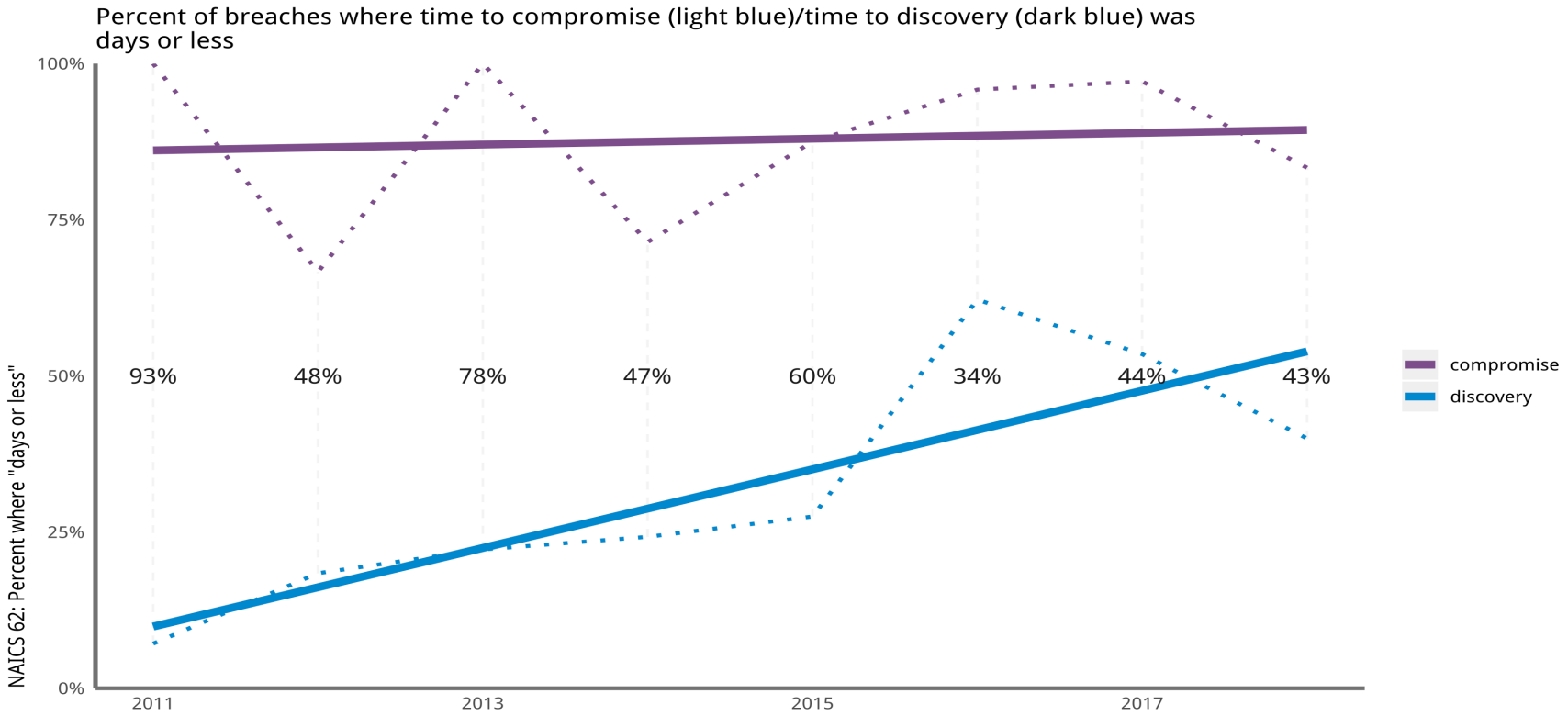


Figure 28. Breach timelines

The Detection Deficit



The Healthcare Detection Deficit (2011-2018)



Industries

The Nefarious Nine Patterns

Figure 35. Incidents per pattern (n=41,686)

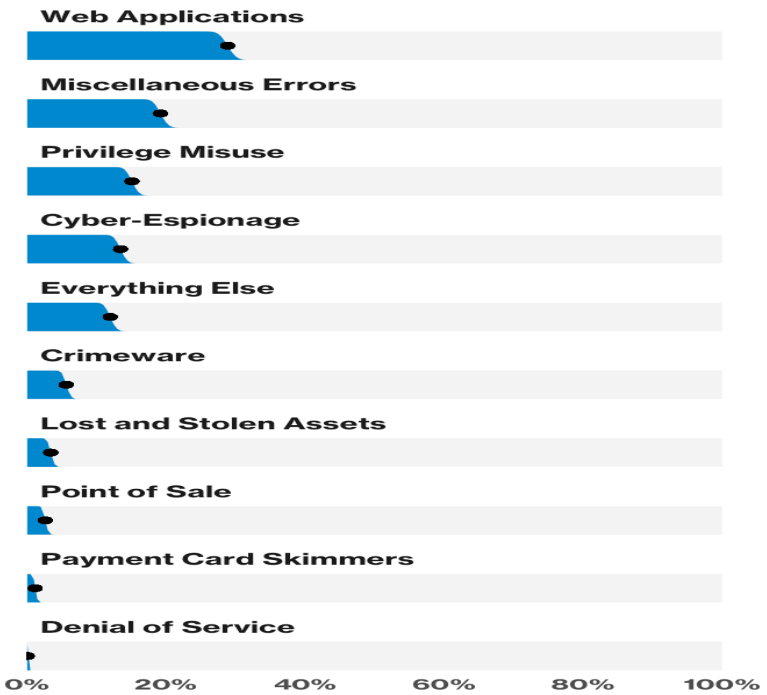
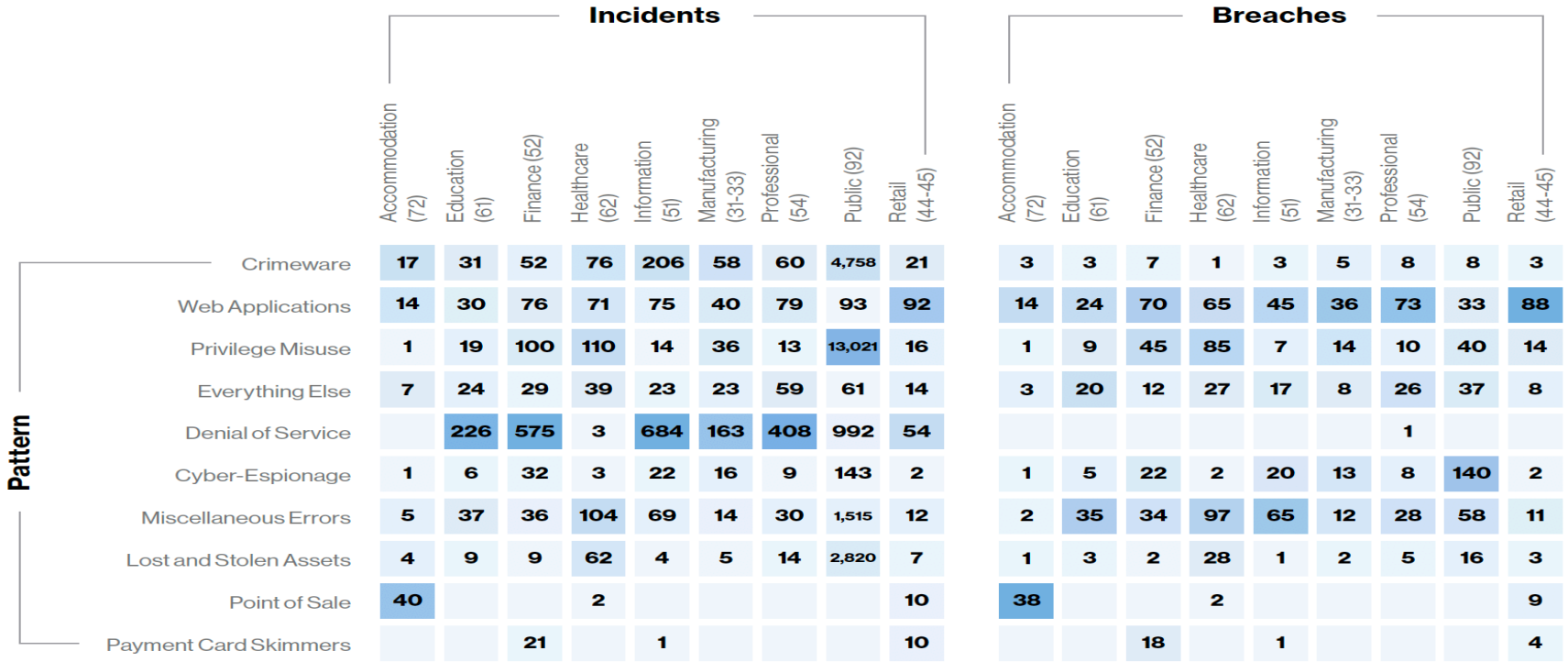


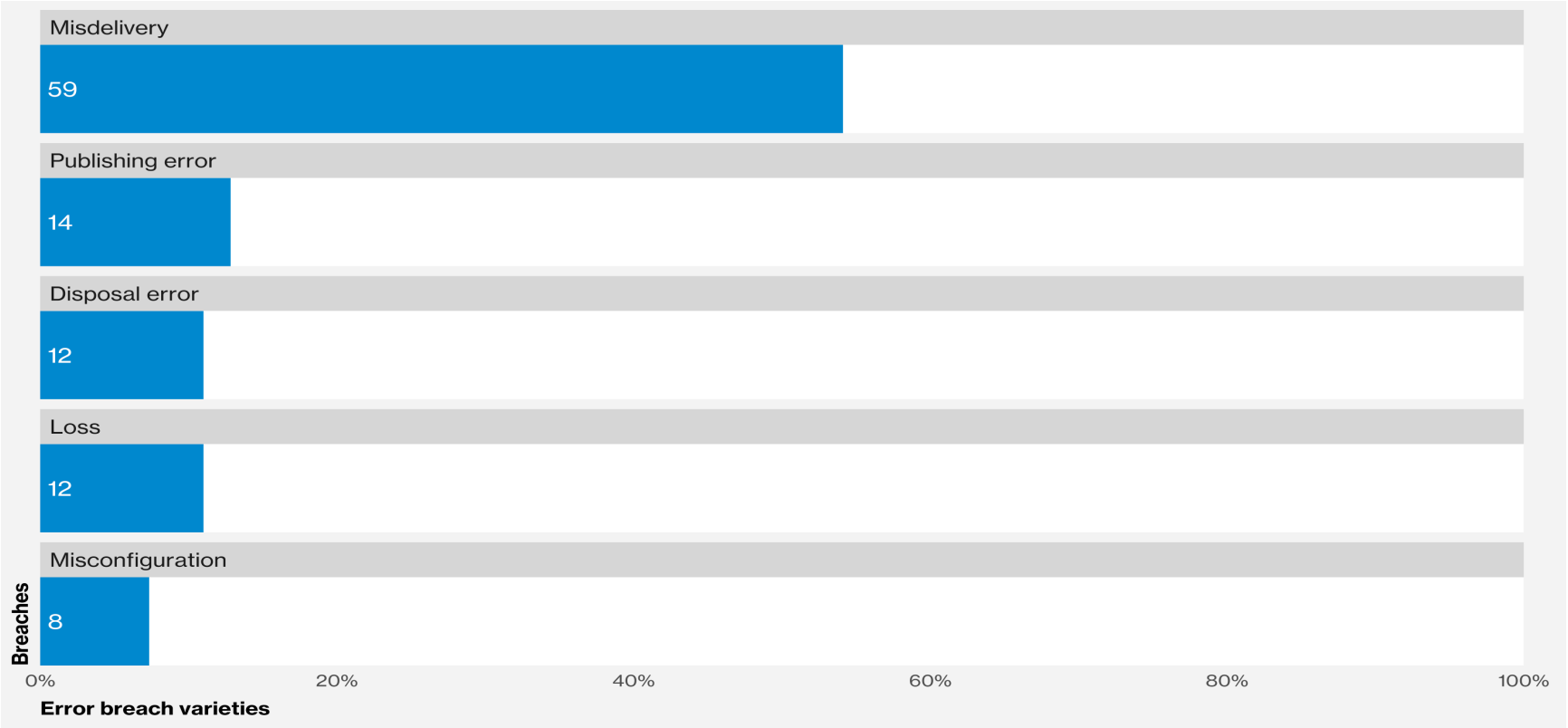
Figure 36. Breaches per pattern (n=2,013)

Industry Comparison

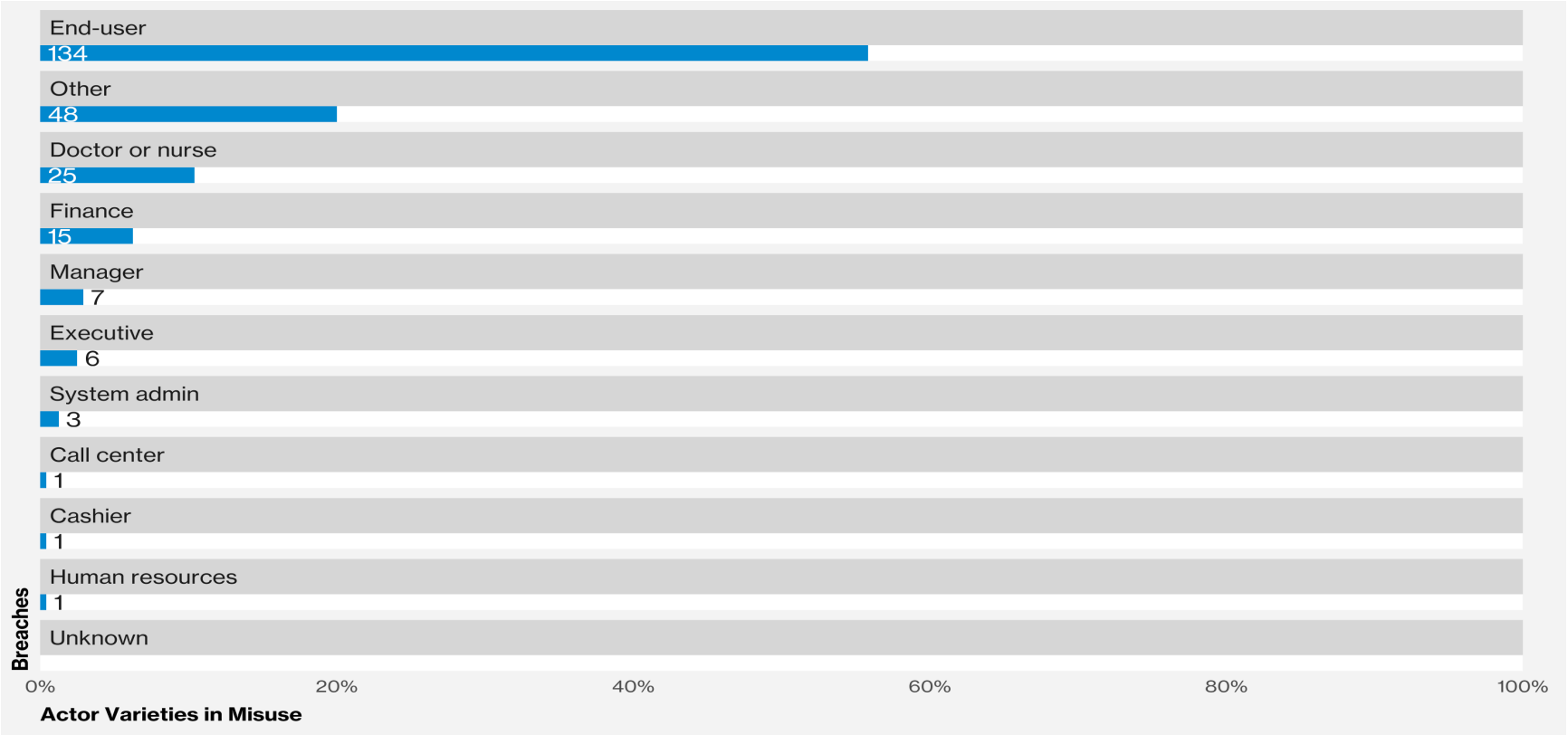


Pattern	Incidents									Breaches								
	Accommodation (72)	Education (61)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Professional (54)	Public (92)	Retail (44-45)	Accommodation (72)	Education (61)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Professional (54)	Public (92)	Retail (44-45)
Crimeware	17	31	52	76	206	58	60	4,758	21	3	3	7	1	3	5	8	8	3
Web Applications	14	30	76	71	75	40	79	93	92	14	24	70	65	45	36	73	33	88
Privilege Misuse	1	19	100	110	14	36	13	13,021	16	1	9	45	85	7	14	10	40	14
Everything Else	7	24	29	39	23	23	59	61	14	3	20	12	27	17	8	26	37	8
Denial of Service		226	575	3	684	163	408	992	54							1		
Cyber-Espionage	1	6	32	3	22	16	9	143	2	1	5	22	2	20	13	8	140	2
Miscellaneous Errors	5	37	36	104	69	14	30	1,515	12	2	35	34	97	65	12	28	58	11
Lost and Stolen Assets	4	9	9	62	4	5	14	2,820	7	1	3	2	28	1	2	5	16	3
Point of Sale	40			2					10	38			2					9
Payment Card Skimmers			21		1				10			18		1				4

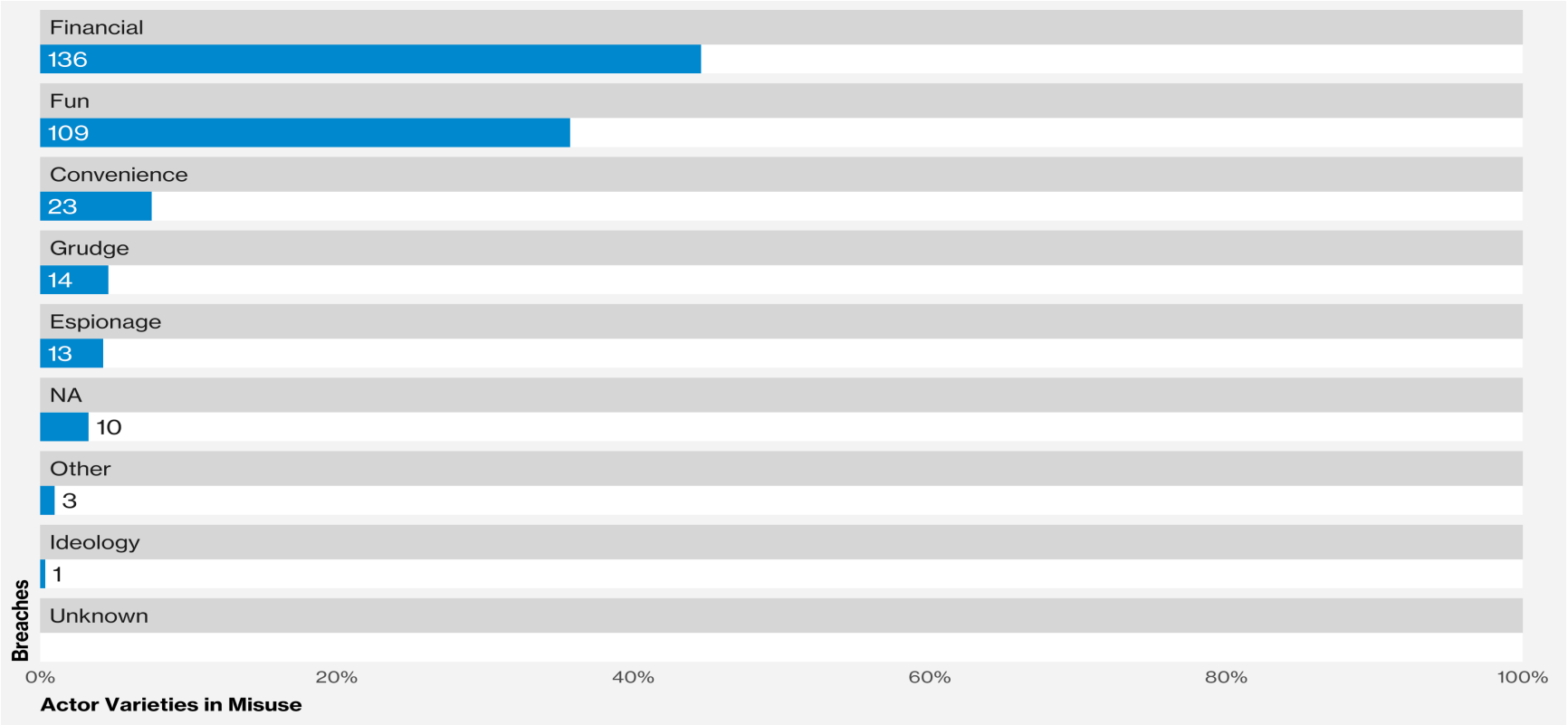
Healthcare Errors



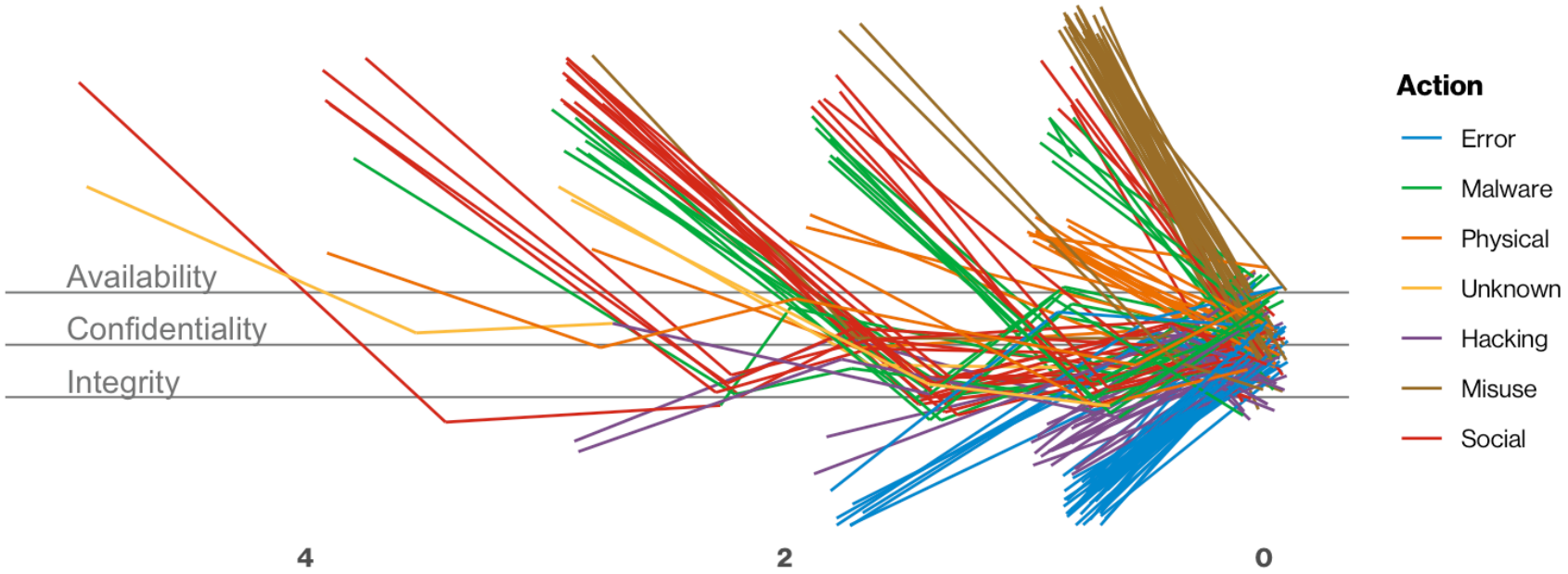
Healthcare Misuse Actor Varieties



Healthcare Misuse Motivations



Healthcare



Attack chains in Healthcare incidents

I Click, Therefore I am

Types of Social Attacks

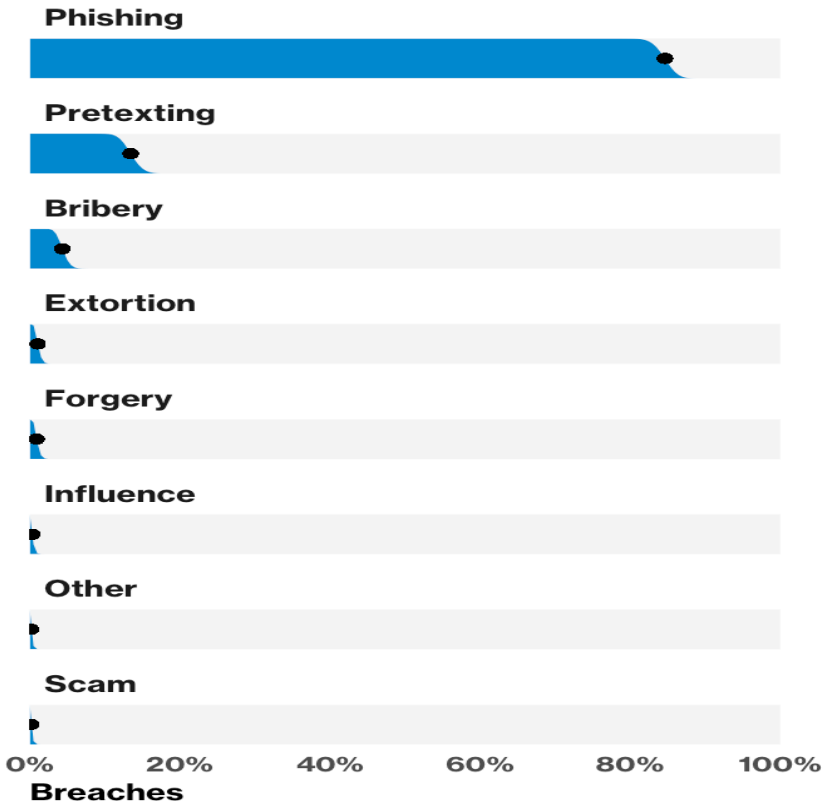


Figure 20. Top social action varieties in breaches (n=670)

verizon

Progress

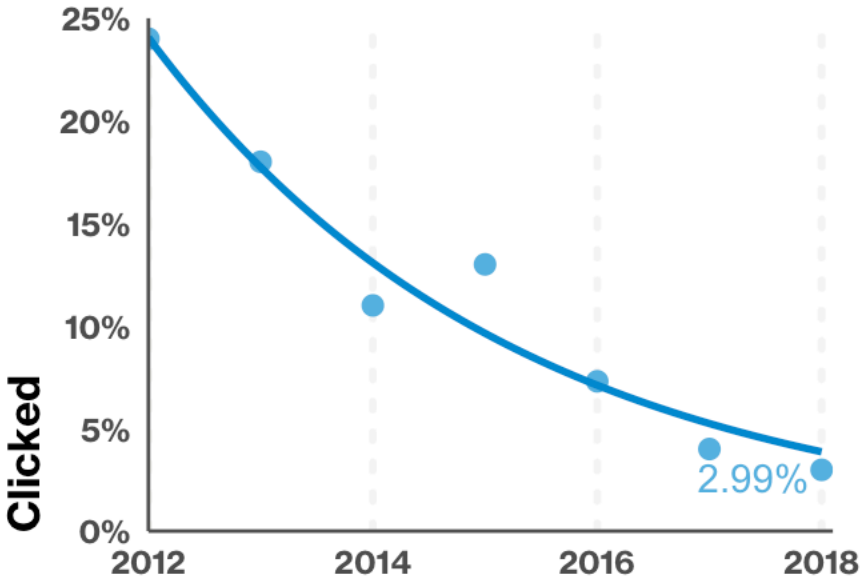


Figure 21. Click rates over time in sanctioned phishing exercises

By Industry

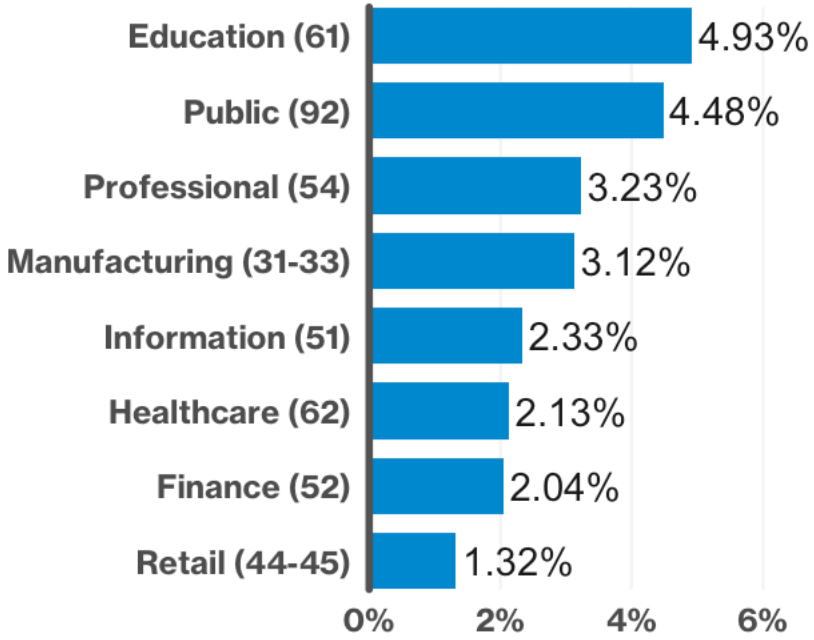


Figure 41. Click rate in phishing tests by industry

Financially-motivated Social Engineering

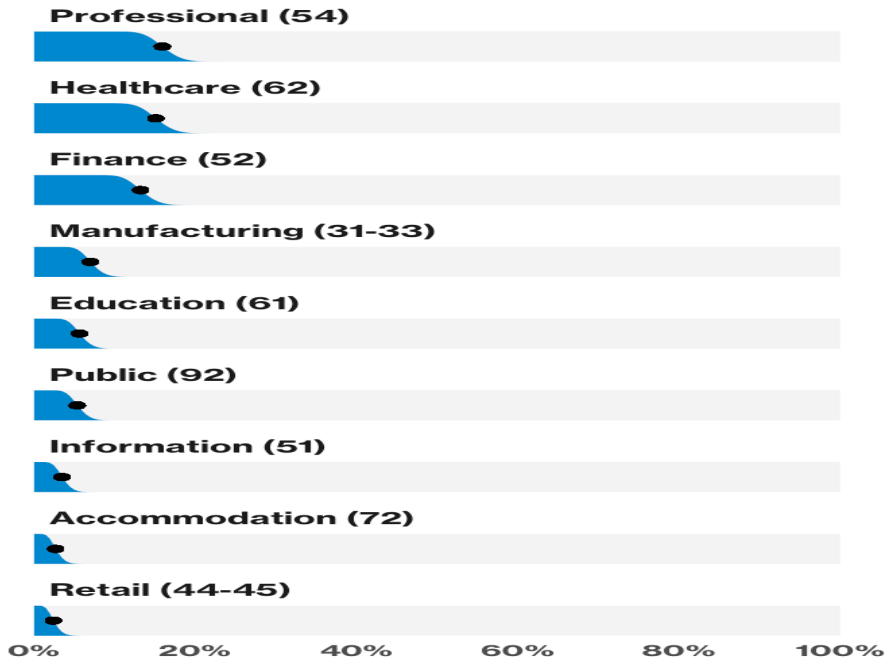


Figure 40. FMSE incidents by industry (n=370)

Malware

Choose the Form of the Destructor

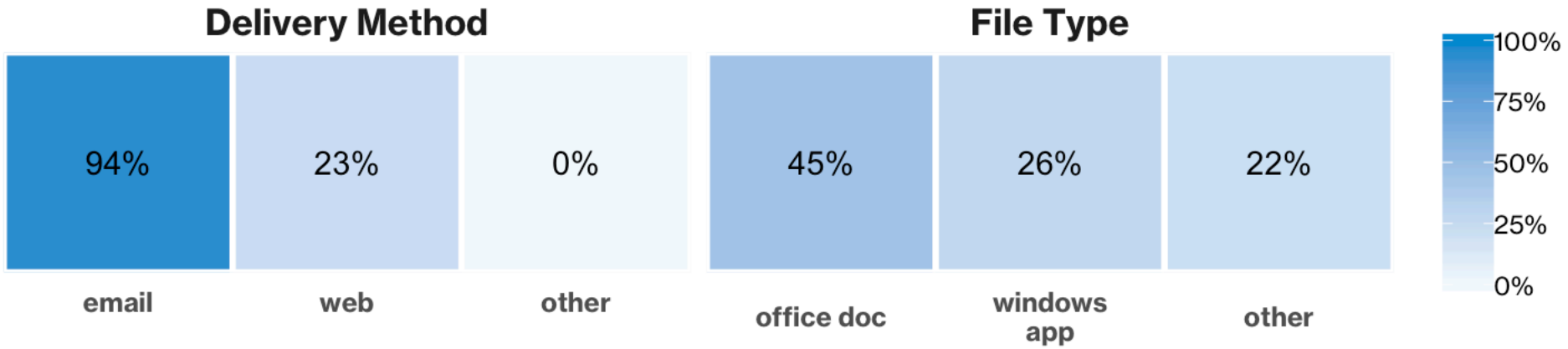


Figure 19. Malware types and delivery methods

Vectors and Varieties

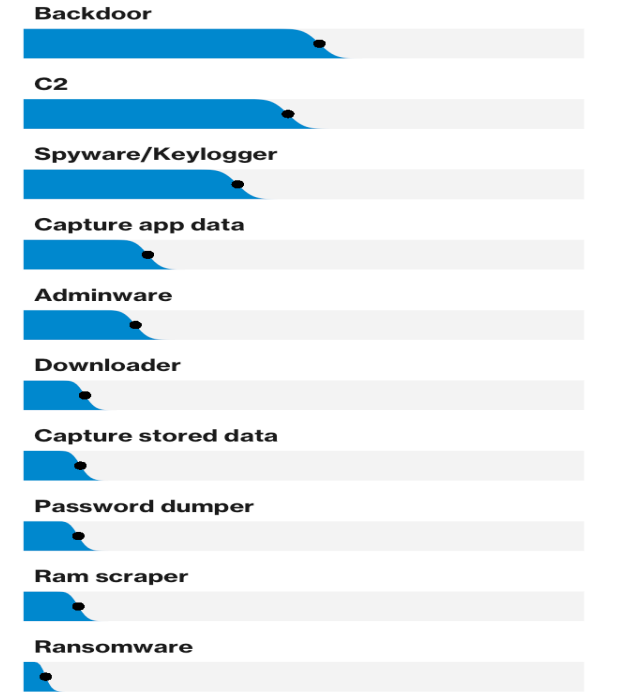


Figure 17. Top malware action varieties in breaches (n=500)

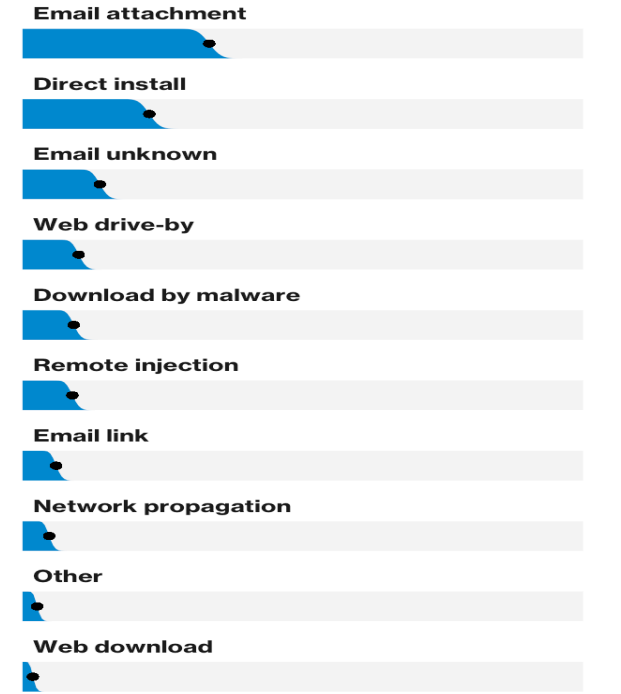


Figure 18. Top malware action vectors in incidents (n=795)

Denial of Service Attacks

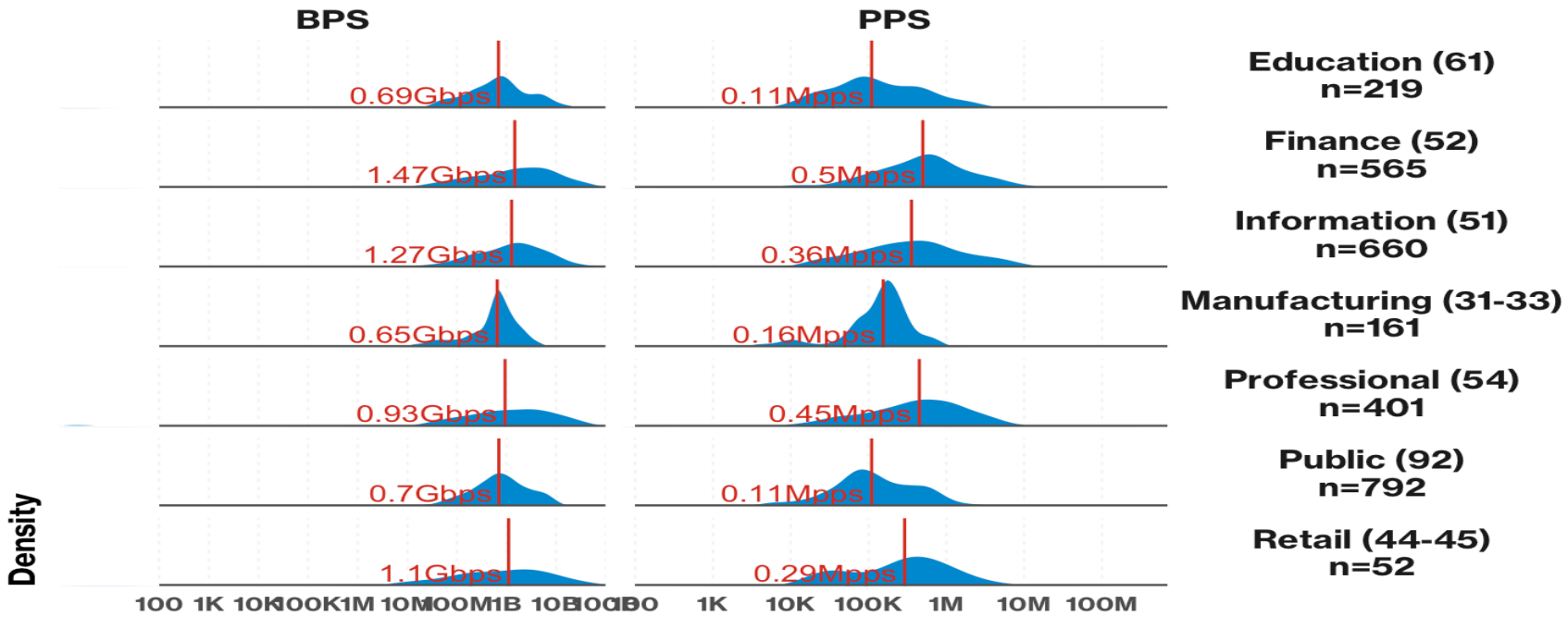


Figure 42. DDoS attack bandwidth and packet counts by industry

Unbroken Chains

Steps to Success

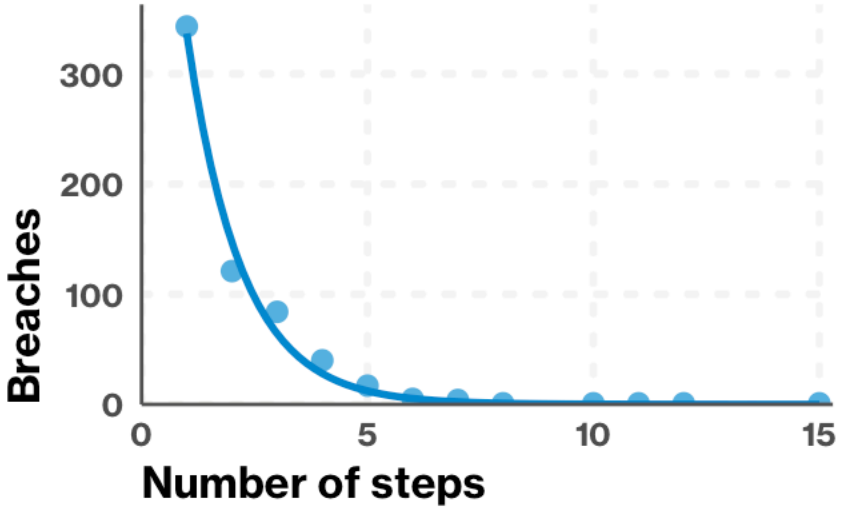


Figure 29. Number of steps per incident (n=1,285) Short attack paths are much more common than long attack paths.

Paths

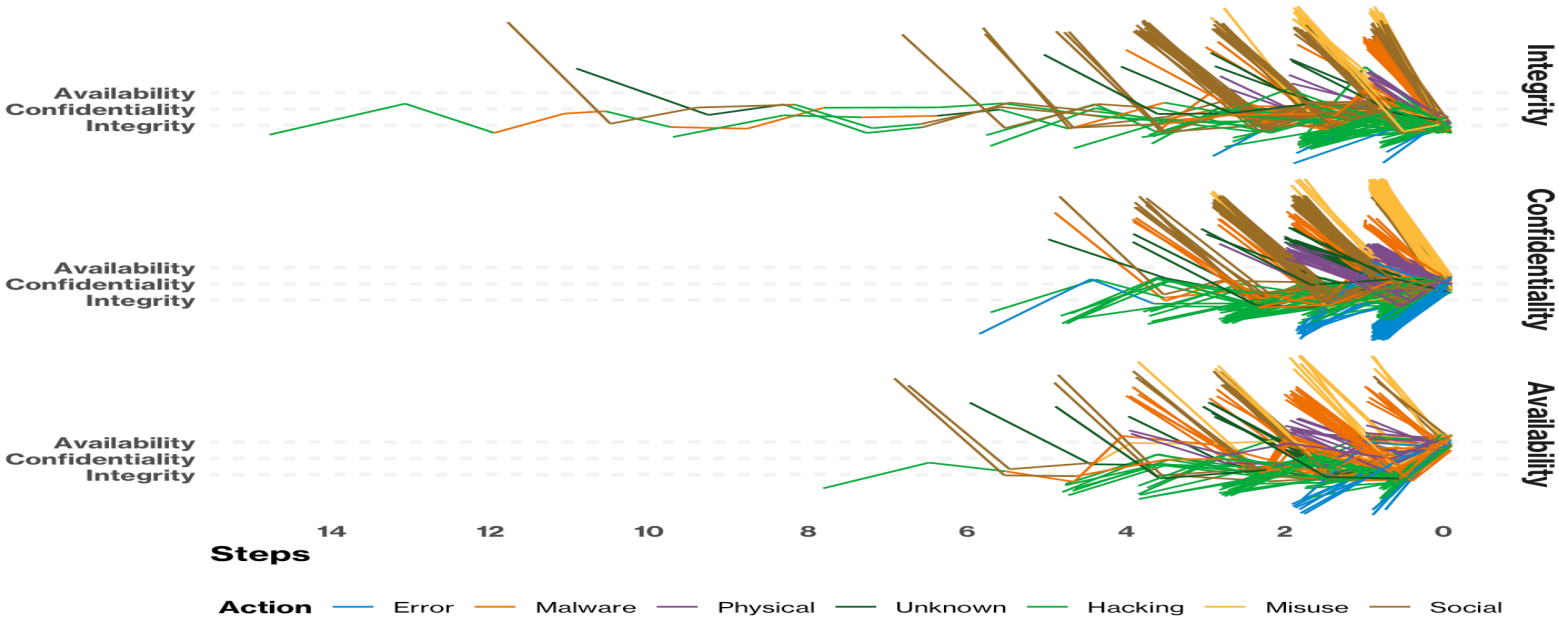


Figure 30. Attack chain by final attribute compromised[12] (n=941)

Beginning, Middle and End

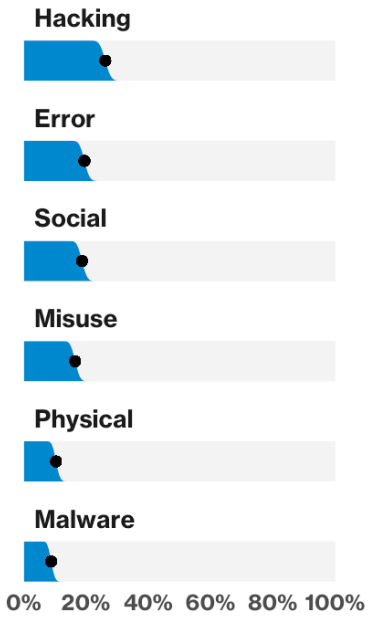


Figure 31. Actions in first step of incidents (n=909)
An additional 32 incidents, (3.40% of all paths), started with an unknown action.

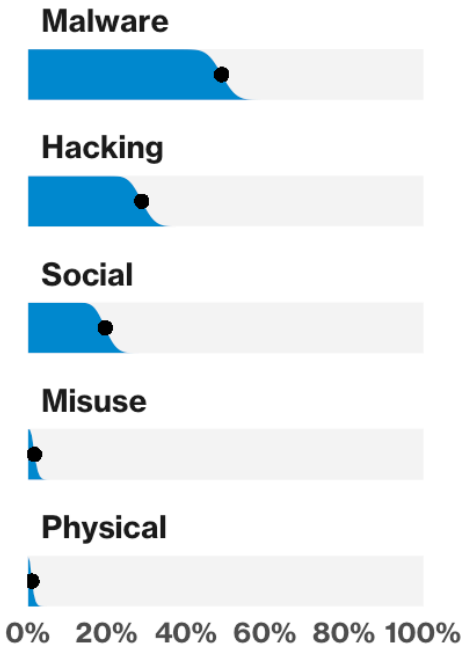


Figure 32. Actions in middle steps of incidents (n=302)

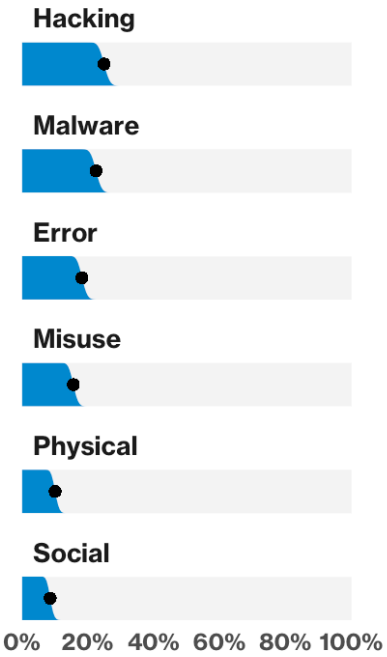


Figure 33. Actions in last step of incidents (n=942)

Simulation

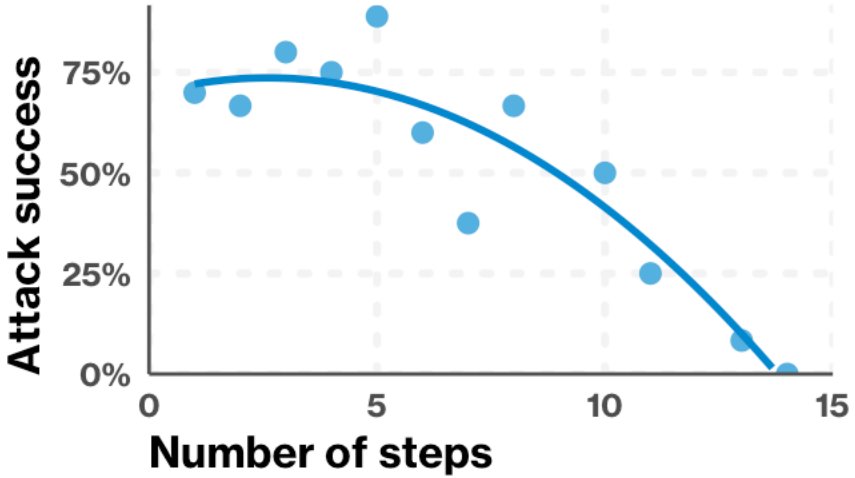


Figure 34. Attack success by chain length in simulated incidents (n=87)

More Information

Download the DBIR	**http://www.verizonenterprise.com/verizon-insights-lab/dbir/**
Grab the DBIR Graphics	**https://github.com/vz-risk/dbir/tree/gh-pages/2019**
Learn about VERIS	**www.veriscommunity.net and http://github.com/vz-risk/veris**
Explore the VERIS Community Database	**http://www.vcdb.org and https://github.com/vz-risk/VCDB/issues**
Ask a Question	**DBIR@verizon.com**
Follow Us	**@vzdbir and hashtag #dbir**

Thank you.

Twitter: @SuzanneWidup

suzanne.widup@verizon.com

and

@VERISDB for data breach feed

verizon