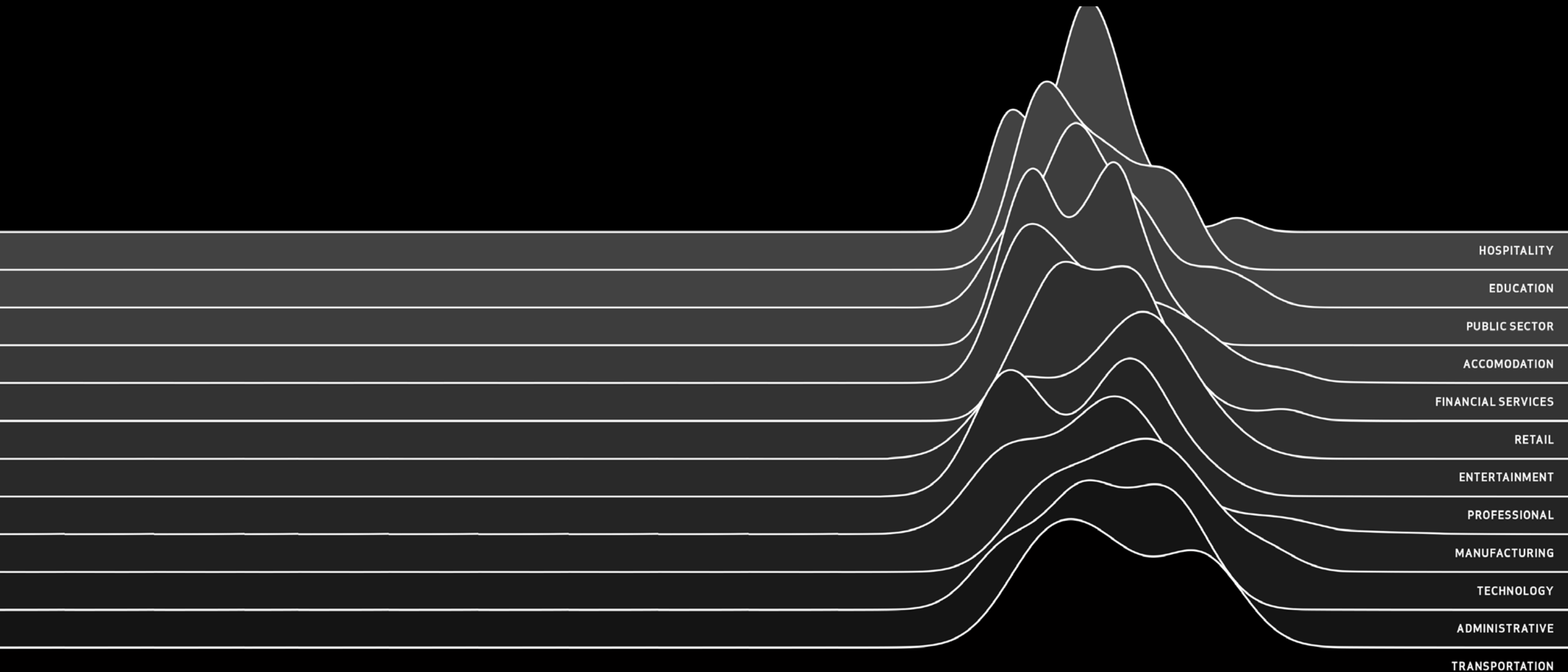


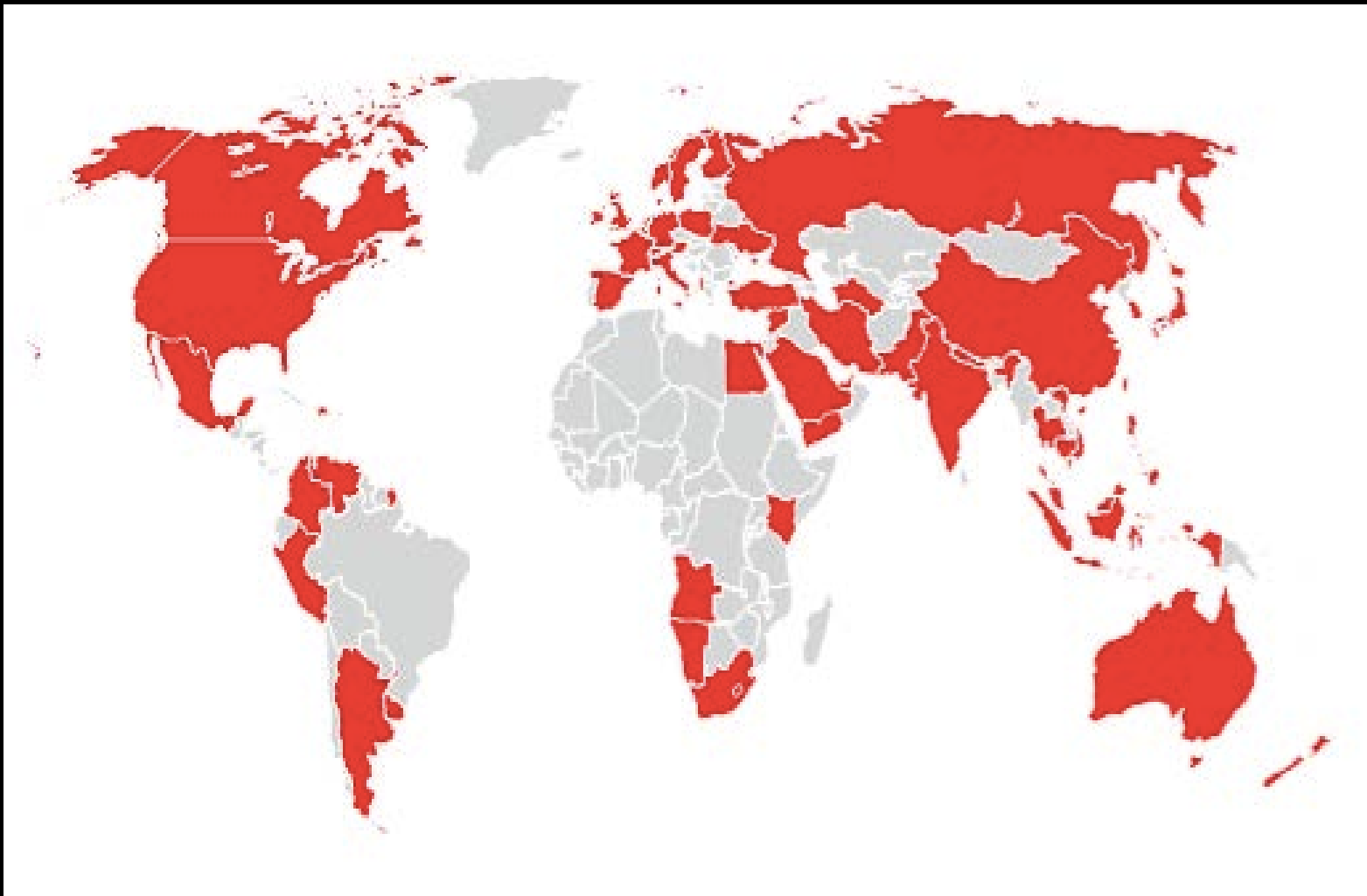


2015 DATA BREACH INVESTIGATIONS REPORT



Suzanne Widup

2015 DBIR



70

CONTRIBUTING ORGANIZATIONS

79,790

SECURITY INCIDENTS

2,122

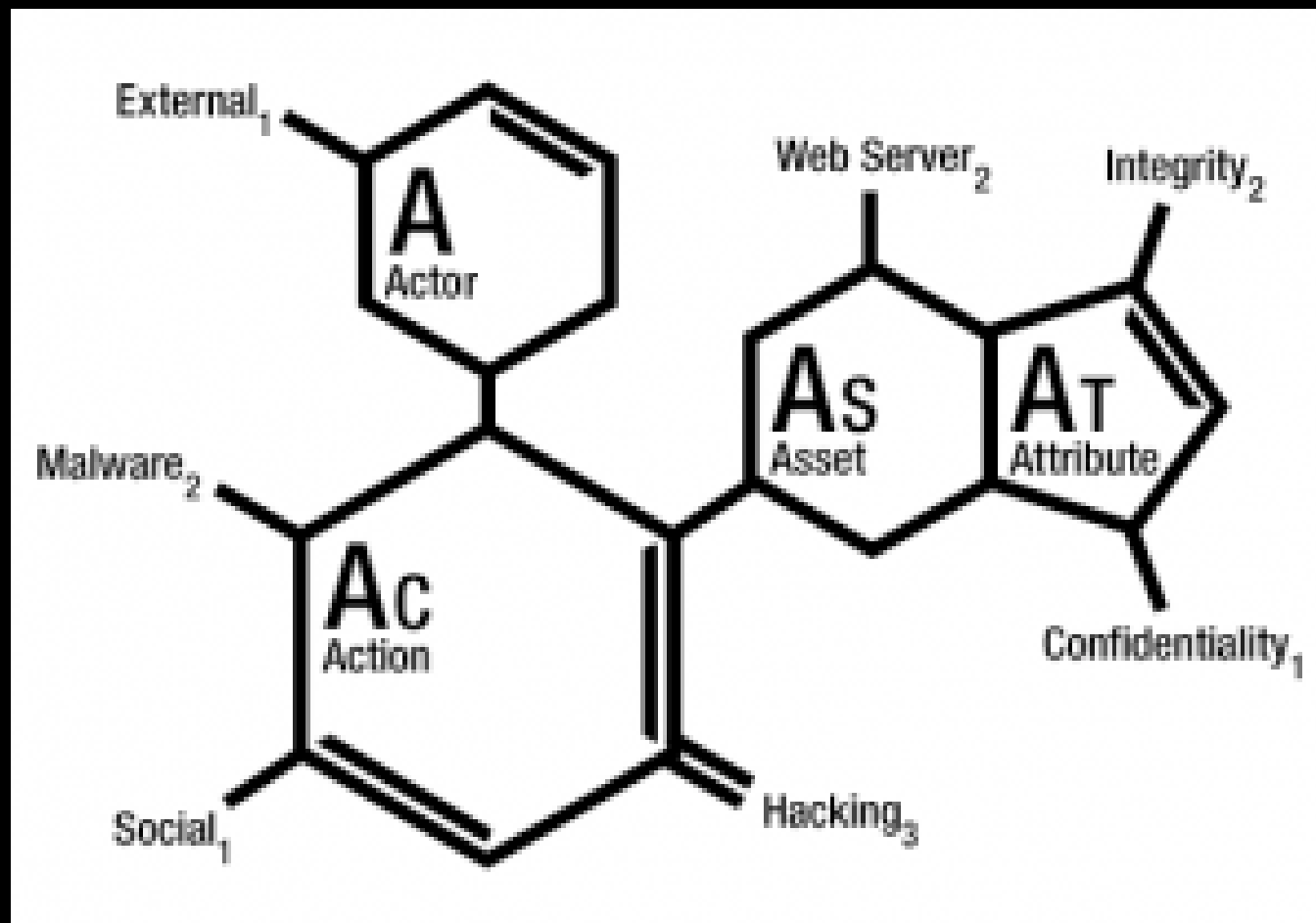
CONFIRMED DATA BREACHES

61

COUNTRIES
REPRESENTED¹

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?

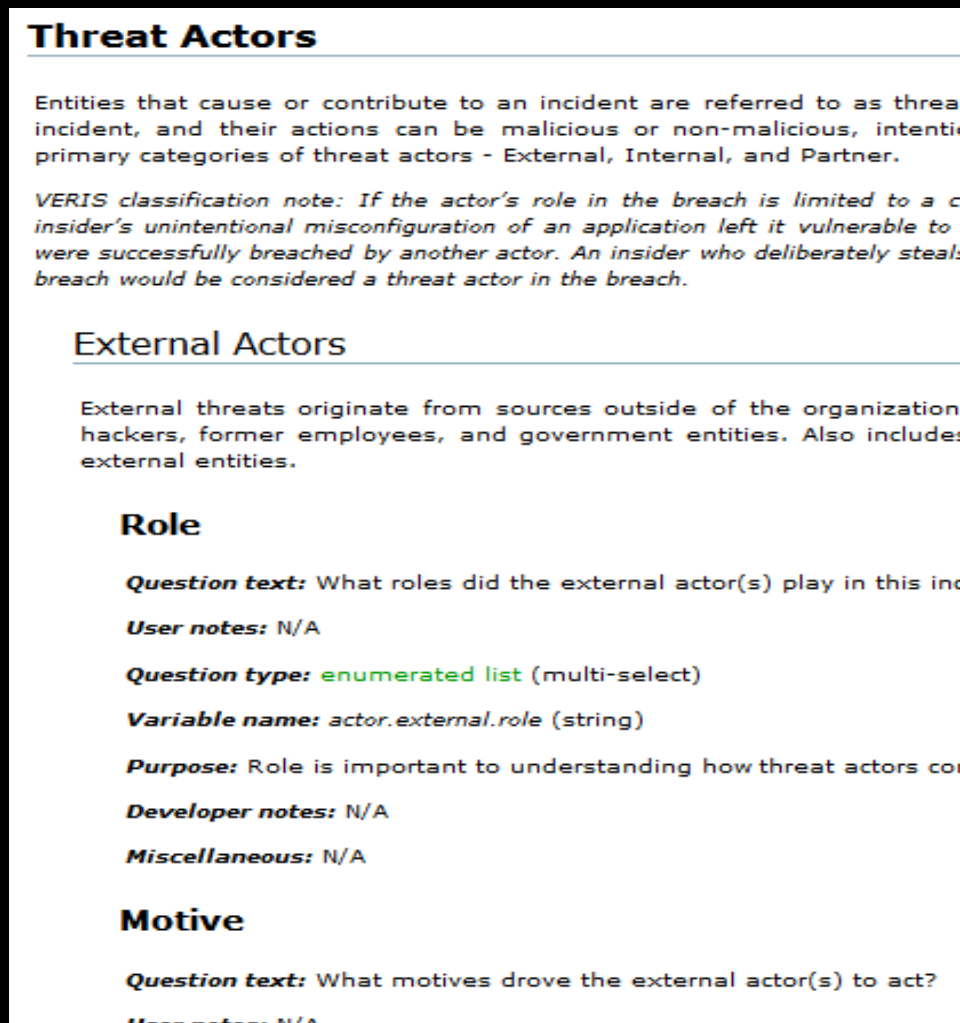
Attribute – How was it affected?

<http://www.veriscommunity.net>

VERIS in Action

VERIS Community Site

- JSON Schema
- All VERIS definitions
- Case examples from popular movies



Threat Actors

Entities that cause or contribute to an incident are referred to as threat actors. Their actions can be malicious or non-malicious, intentional or unintentional. The primary categories of threat actors - External, Internal, and Partner.

VERIS classification note: If the actor's role in the breach is limited to a configuration error or an insider's unintentional misconfiguration of an application left it vulnerable to a breach, the actor would not be considered a threat actor in the breach. An insider who deliberately steals data or causes a breach would be considered a threat actor in the breach.

External Actors

External threats originate from sources outside of the organization, such as hackers, former employees, and government entities. Also includes external entities.

Role

Question text: What roles did the external actor(s) play in this incident?

User notes: N/A

Question type: enumerated list (multi-select)

Variable name: actor.external.role (string)

Purpose: Role is important to understanding how threat actors contribute to an incident.

Developer notes: N/A

Miscellaneous: N/A

Motive

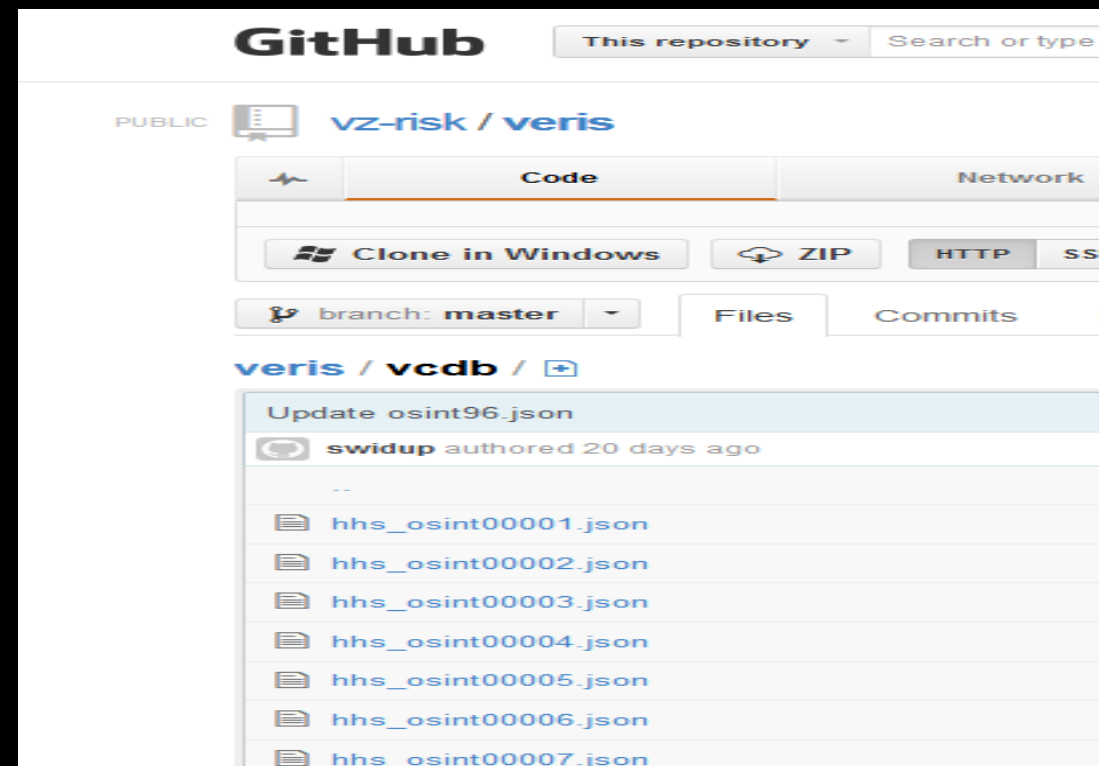
Question text: What motives drove the external actor(s) to act?

User notes: N/A

<http://www.veriscommunity.net>

GitHub Repository

- Over 5,000 publicly disclosed data breaches, and growing
- Coded using VERIS
- Available as JSON files
- Includes URL references to incidents



GitHub This repository Search or type

PUBLIC **vz-risk / veris**

Code Network

Clone in Windows ZIP HTTP SSH

branch: master Files Commits

veris / vcdb /

Update osint96.json

swidup authored 20 days ago

- hhs_osint00001.json
- hhs_osint00002.json
- hhs_osint00003.json
- hhs_osint00004.json
- hhs_osint00005.json
- hhs_osint00006.json
- hhs_osint00007.json

<http://www.vcdb.org>

Publicly Disclosed Data Breaches

VCDB Home Explore Learn About Contact

Exploring the VCDB

Geo

Patterns

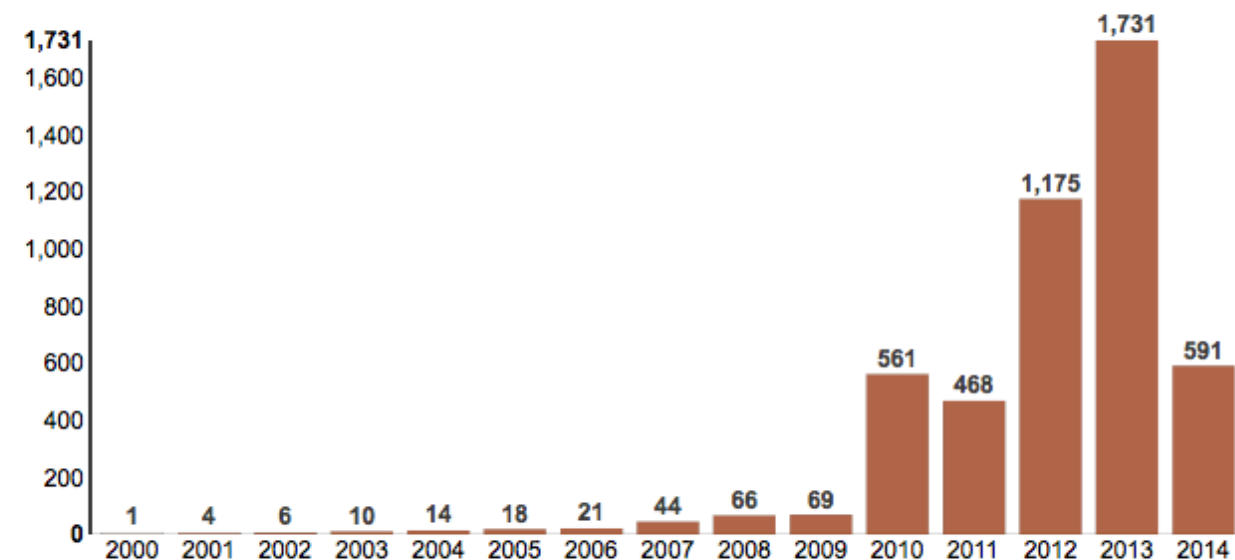
Records Loss Timeline

Welcome to the VCDB Explorer!

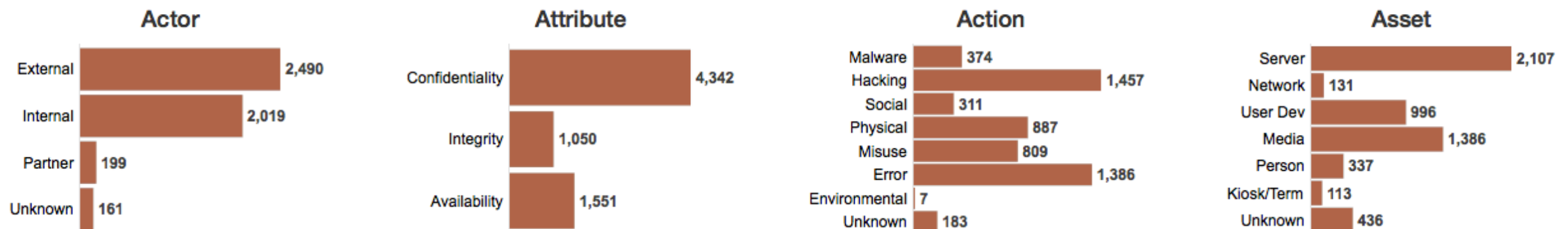
The **Vocabulary for Event Recording and Incident Sharing (VERIS)** is a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner. VERIS is a response to one of the most critical and persistent challenges in the security industry - a lack of quality information. VERIS targets this problem by helping organizations to collect useful incident-related information and to share that information - anonymously and responsibly - with others. The overall goal is to lay a foundation from which we can constructively and cooperatively learn from our experiences to better measure and manage risk. Learn more at <http://www.veriscommunity.net>.

Each tab lets you explore different aspects of the VCDB data set. The visualizations are updated regularly and new ones are always in the works.

Incident Count By Year



Incident Counts by:



<http://vcdb.org/explore.html>

VCDB.org – Be a Security Super hero!

[VCDB](#) [Home](#) [About](#) [Contact](#)

VERIS Community Database

VCDB is a community data initiative to catalog security incidents in the public domain using the VERIS framework. The database contains **raw data** for thousands of security incidents shared under a creative commons license. You can download the latest release, follow the latest changes on github, and even help catalog and code incidents to grow the database.

[Learn more »](#)

Community

Community resources need community members, and this dataset doesn't code itself. Find out how you can contribute incidents to the database.

[Volunteer Now »](#)

Data

Want to go straight to the data? VCDB is hosted on github. You can download the latest release, or clone the repo for advanced users.

[Go to github »](#)

Prefer a visual? [Go to the interactive graphic.](#)

VERIS

The Vocabulary for Event Recording and Incident sharing makes it easy to share anonymized breach data among organizations.

[Learn More »](#)

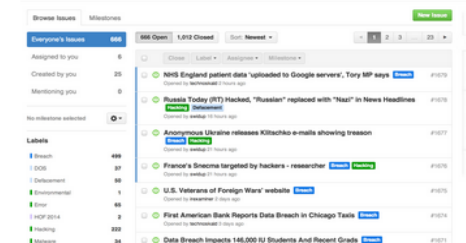
Want to be a security super hero?

Do you enjoy finding new reports of data breach incidents? Would you like to know that you're participating in the world's most awesome project? Have we got a deal for you!

Participate in the VERIS Community Database (VCDB) Project

There are two ways to participate in the VCDB project.

- Find new incidents! Got a headline that says something happened that resulted in a data breach? We want to see it. You can add it to the list of issues to be coded (we use GitHub Issues to track breaches waiting to be coded).
- Finding new breaches not enough for you? You can code them into VERIS format for inclusion into the dataset. Amaze your friends, frustrate your enemies, be the hero you were meant to be!!!



I found an Incident—How do I Add It to the List?

- Identify a publicly disclosed data breach (gotta include the URL).
- Search our repository to make sure it isn't already an existing issue (github.com/vz-risk/VCDB and use the search box at the top). If you find an existing issue, but it doesn't have that reference, add the URL to the body. We like multiple references! You'll need an account at github, but it's free and part of the fun of contributing to an open-source project.
- Create a new issue with the link in the body, the title of the article in the Subject, and if listed, add the organization name that was breached in the subject as well—this makes it easier to do searches.
- Later, rinse, and repeat!

I want to Code All the Things (into VERIS format)!!!

- Send an email to participate@veris.org and tell us you want to help out!
- We send you credentials to the data entry tool.
- You familiarize yourself with VERIS prior to claiming incidents. (veriscommunity.net). Questions can be sent to the same email as above.
- Find an unclaimed issue in GitHub and assign it to yourself.
- Code the incident in the data entry tool and submit.
- Close the issue in GitHub.

Incident Tracking
This section captures some general information about the incident. [More info!](#)

GitHub issue #
101

Confirmed Incident?
☒ Yes - Confirmed
☐ Suspected
☐ Near miss

Incident summary
Something bad happened to someone

Enter the following dates (Yr required) ☐

Year

Month

Day

Incident date

2014

03

01

Public notification date

2014

03

02

Source URL(s) - separate by ;
<http://threatveris.ca>

Multiple copies of this record?
☐ Yes- How many?

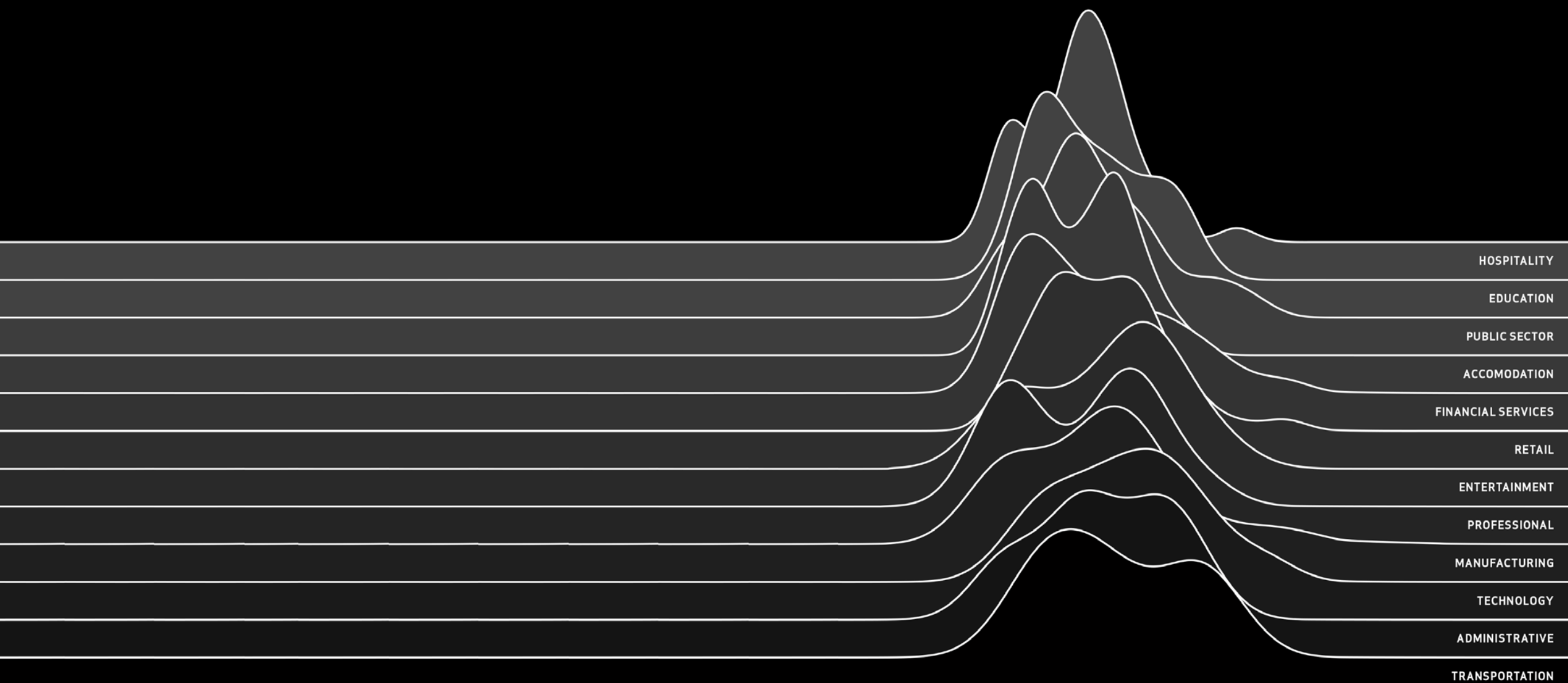
General notes

Victim Organization

We need volunteers to help

- Find data breach articles
- Code articles into VERIS format

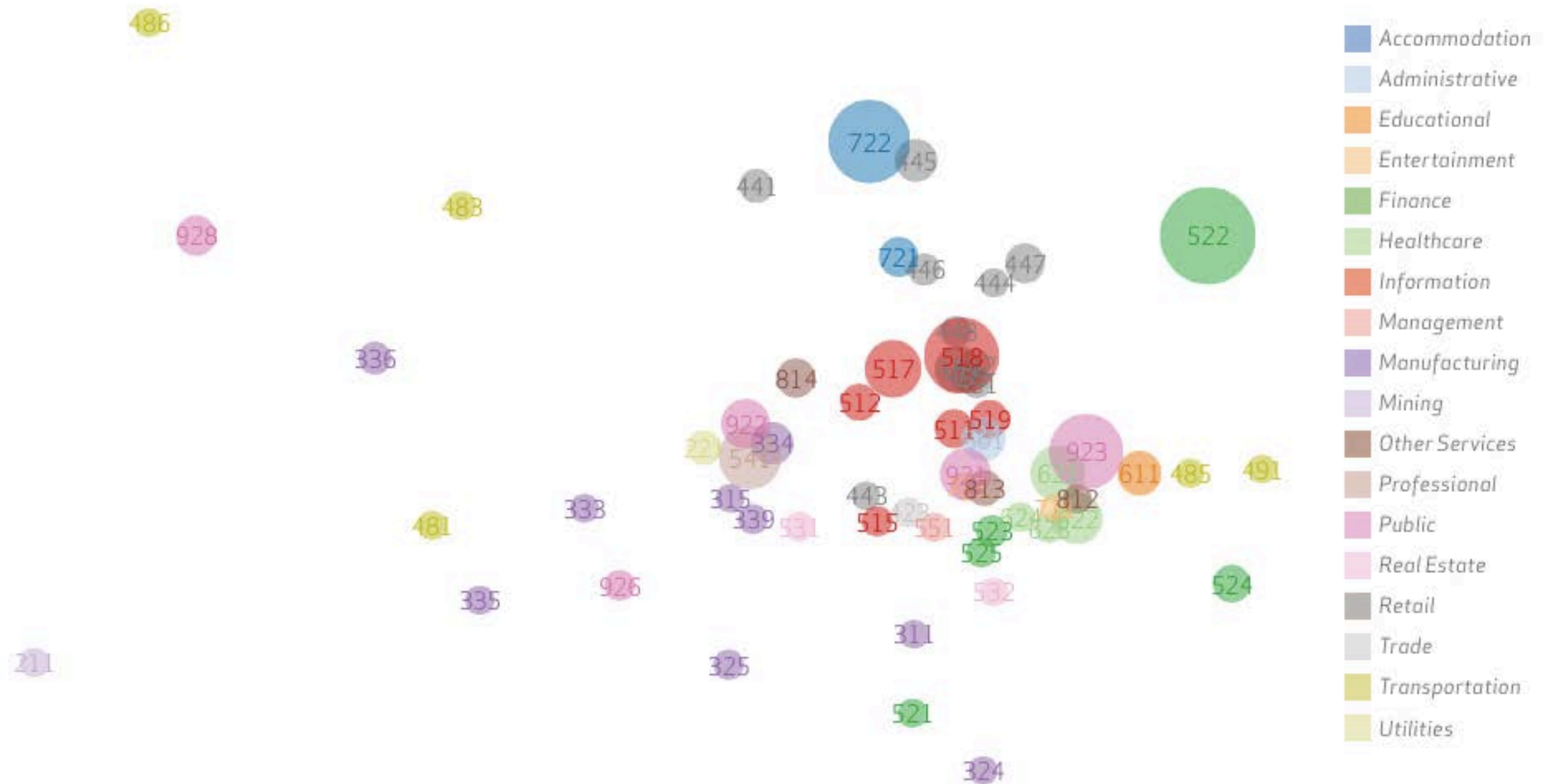
DBIR Overview



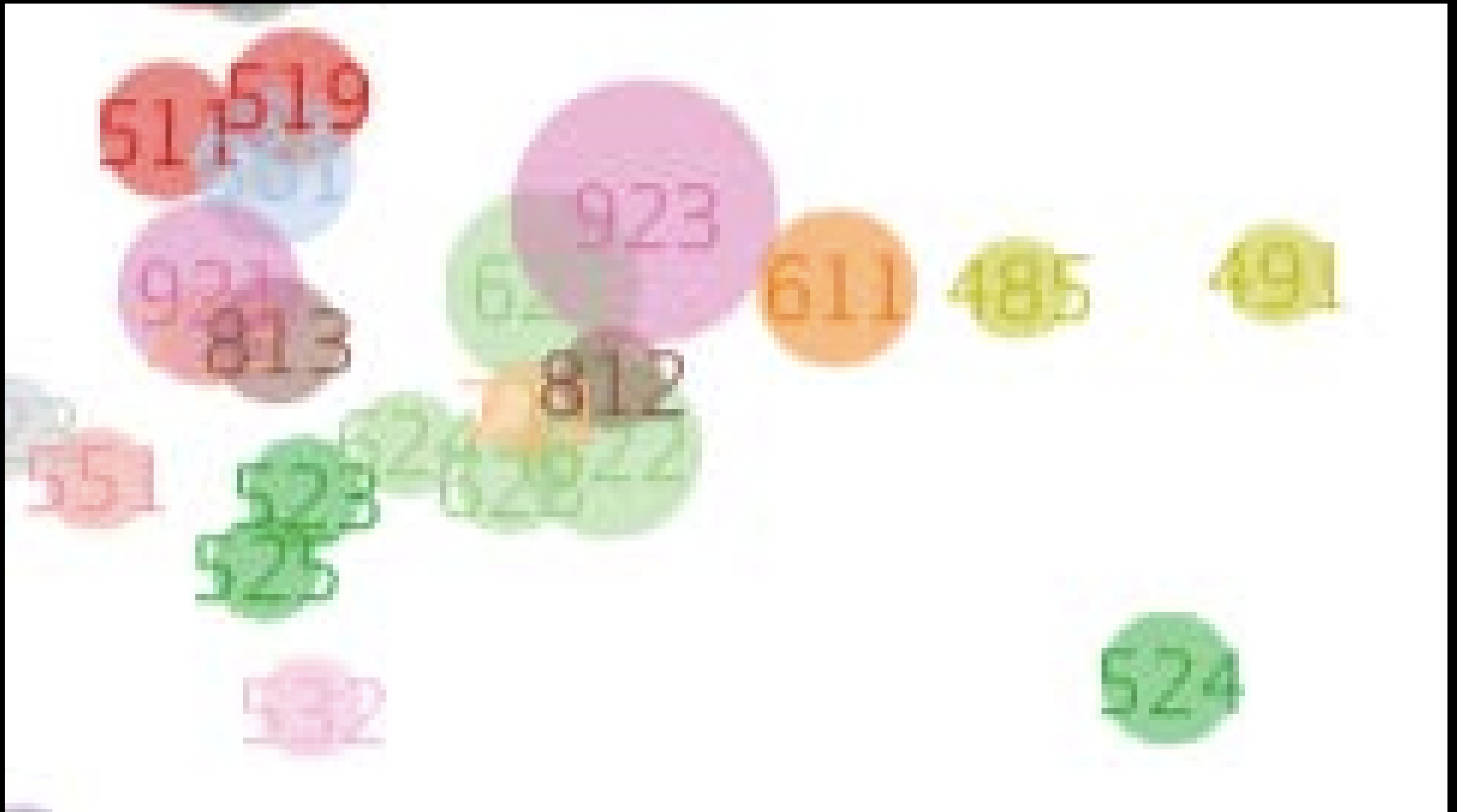
Incidents vs Breaches

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

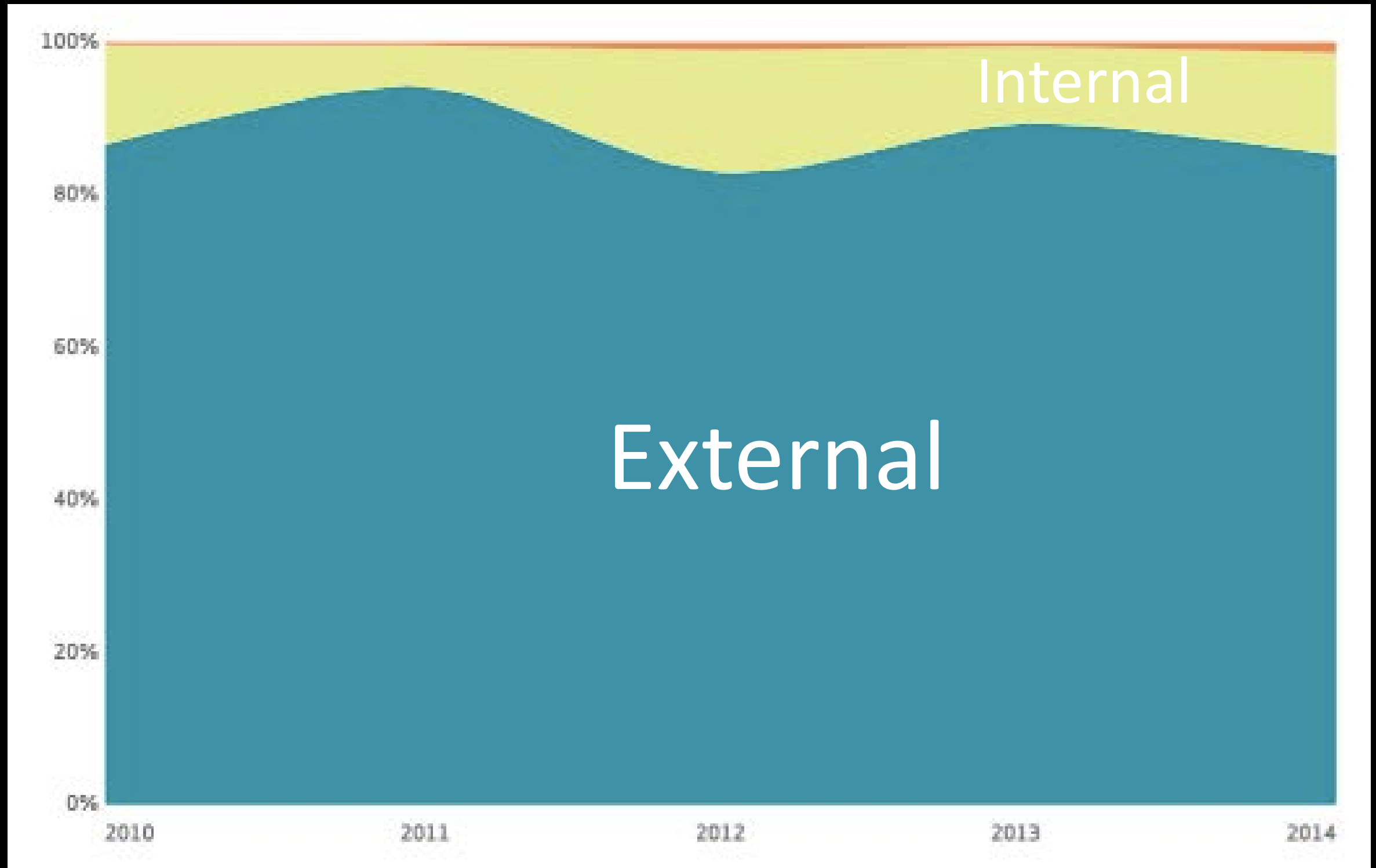
Which industries exhibit similar threat profiles?



Healthcare

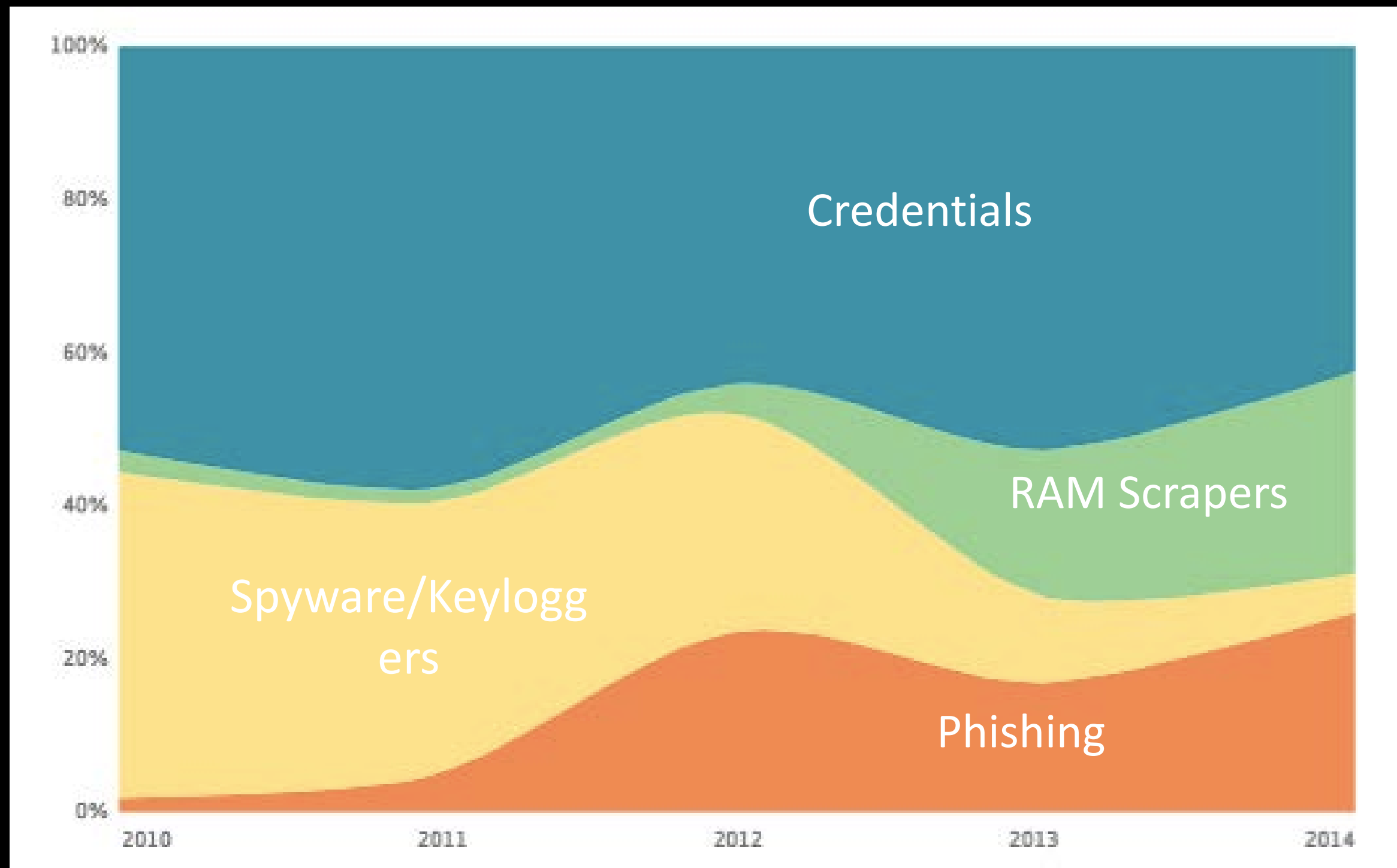


Threat Actors



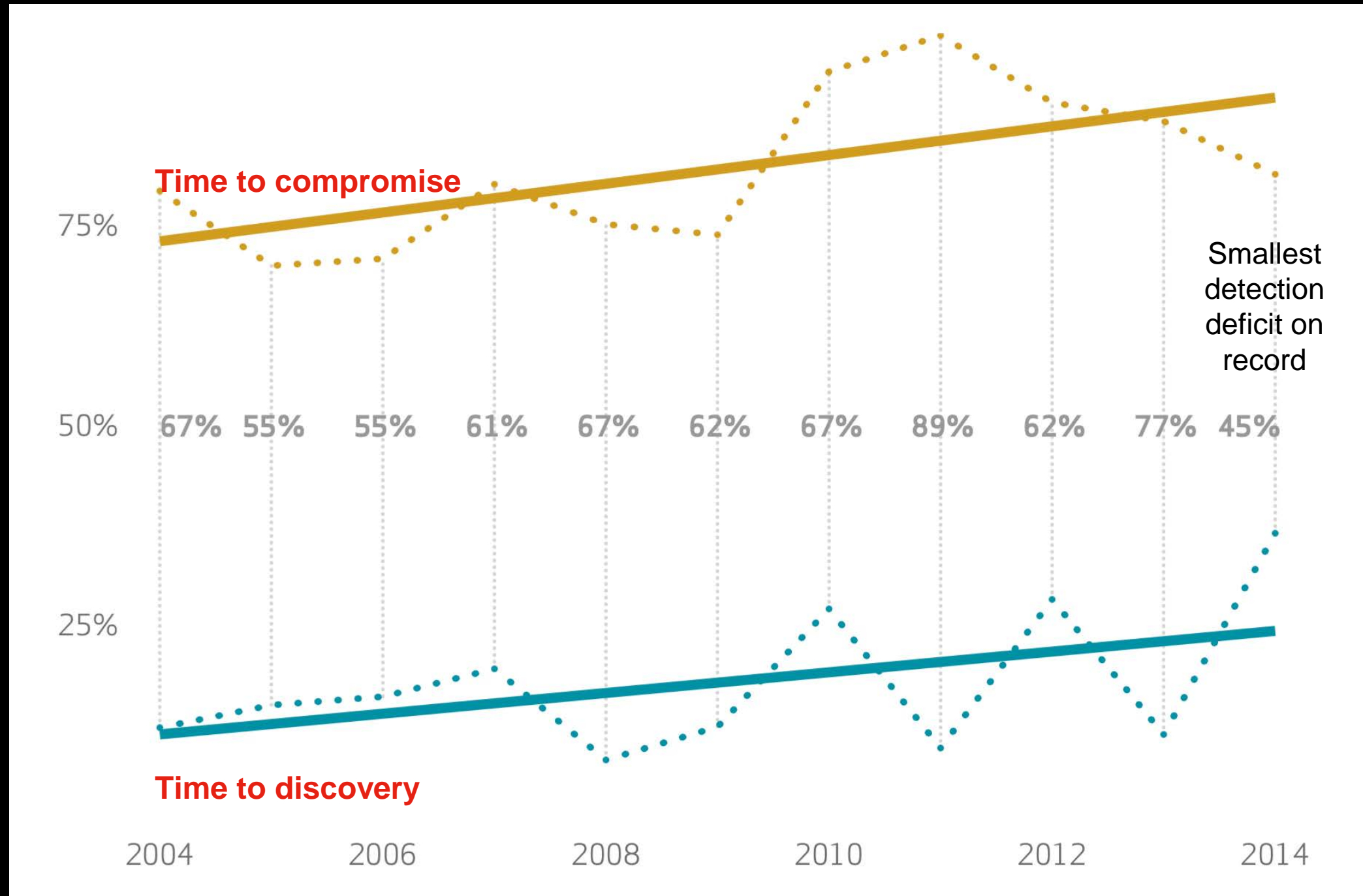
Threat Actions

Significant threat actions over time by percent

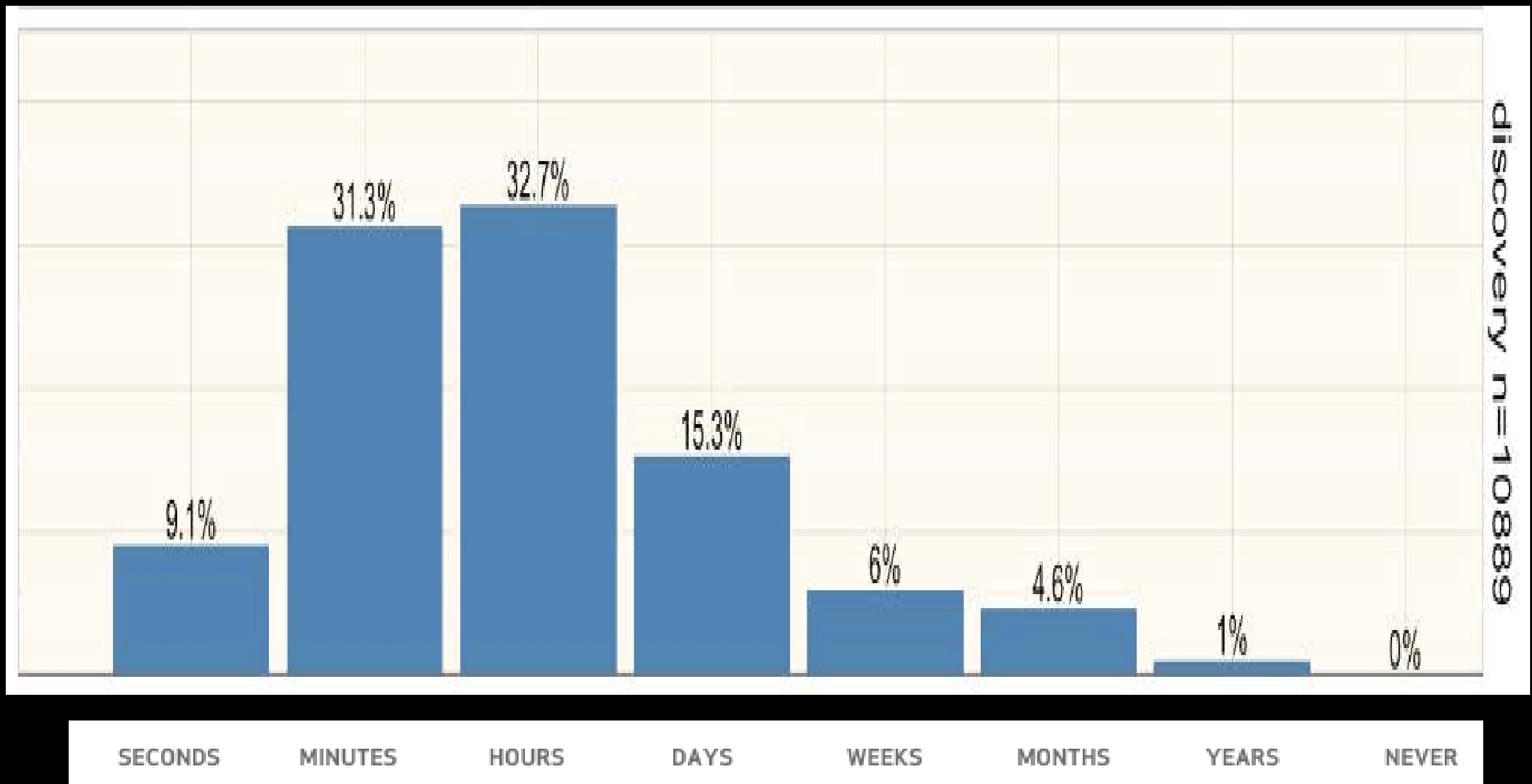


The Detection Deficit

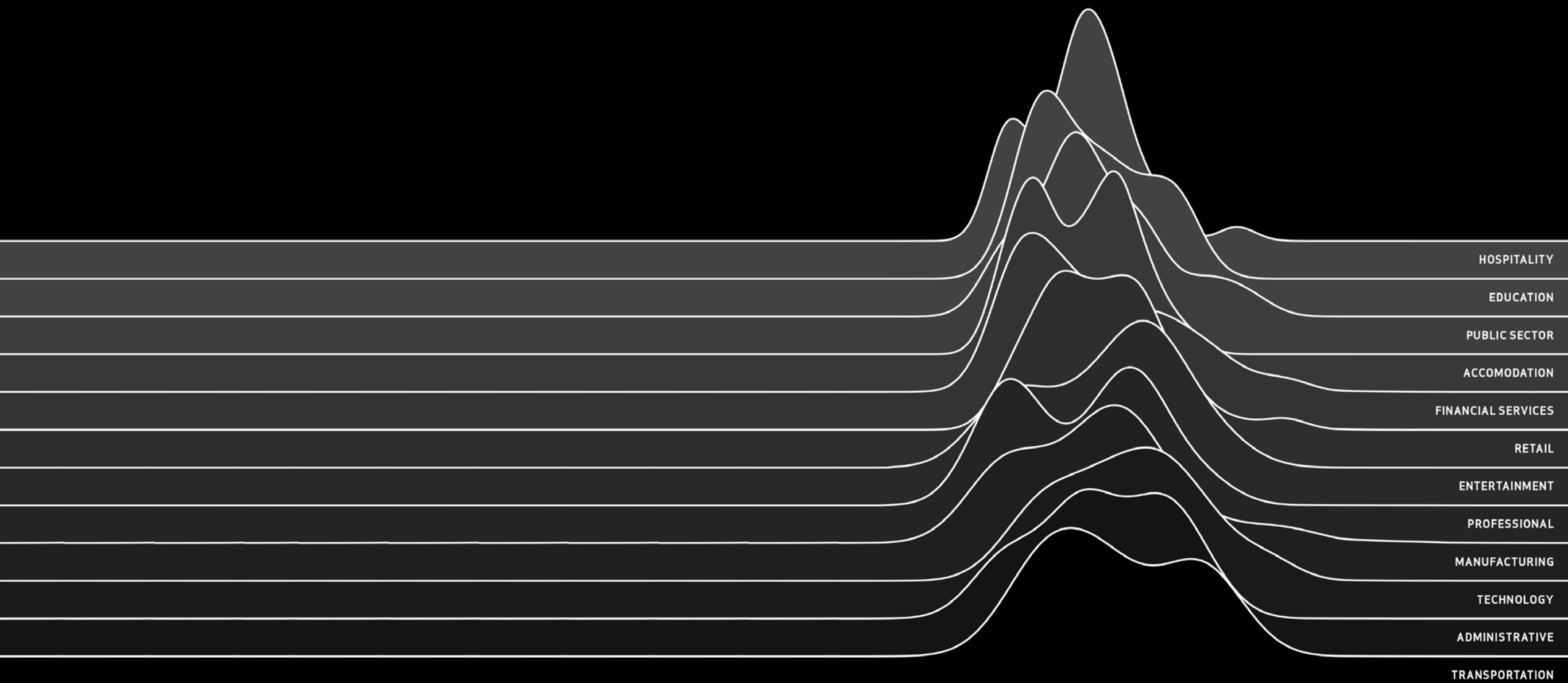
Overall trends are still pretty depressing



Discovery Timeline



Breach Impact



The Impact of Breaches

Groundbreaking Research by Verizon

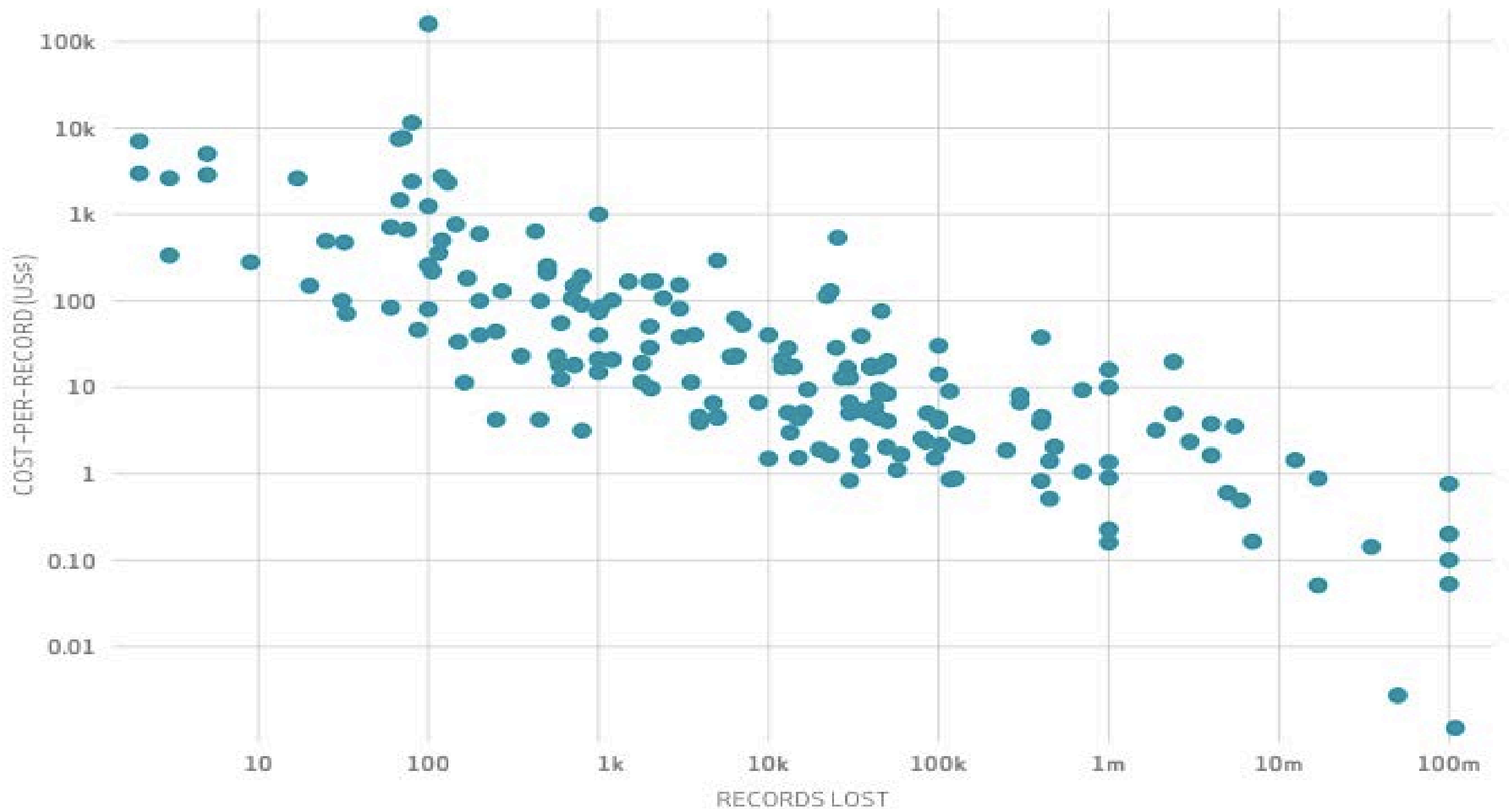
We analyzed real cyber-claims data from nearly 200 incidents and developed a new breach impact estimation model that goes beyond simple cost-per-record average formulas.

The Impact of Breaches

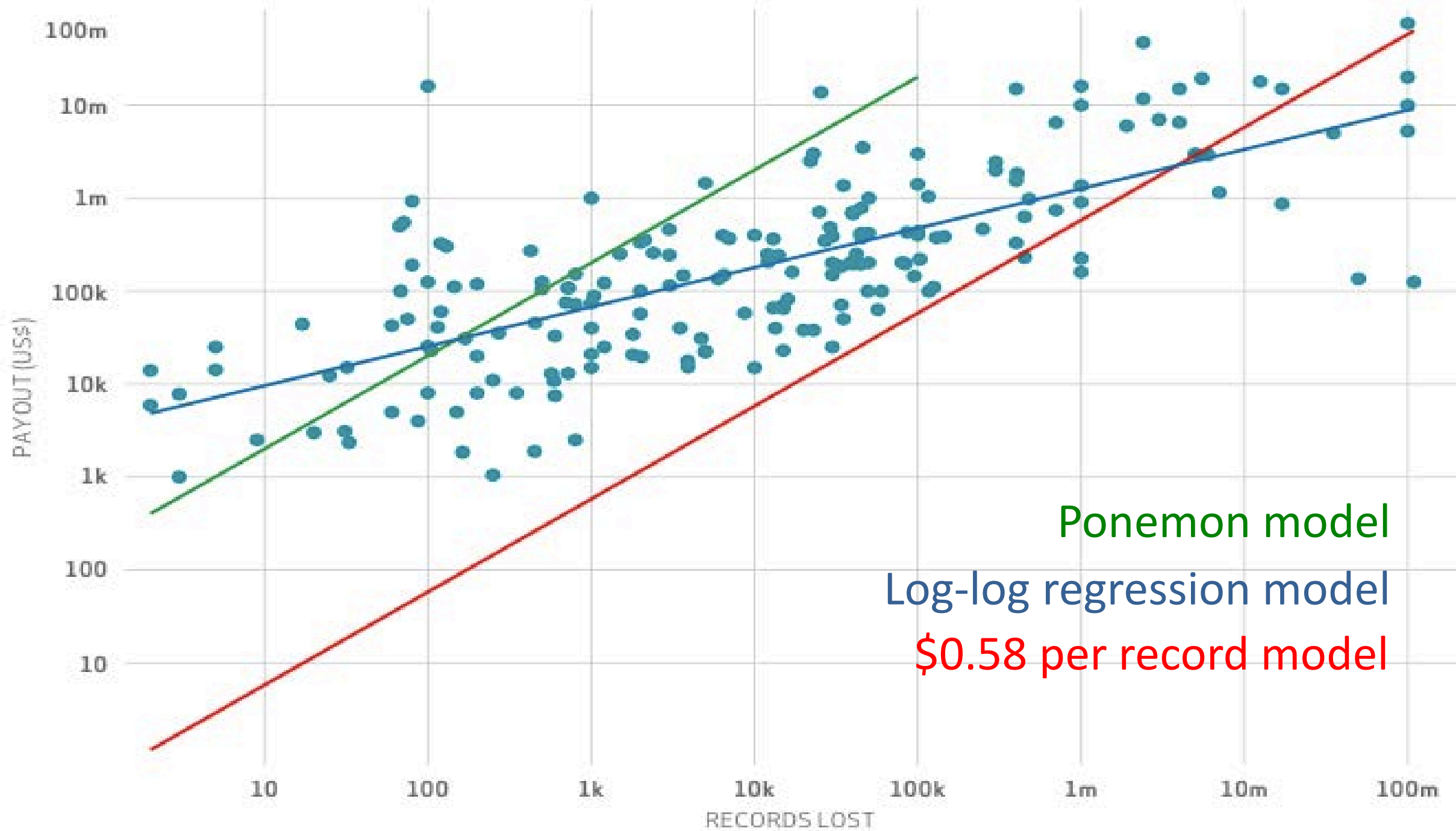
Our model – using only record counts – describes over 50% of the reasons that make up the cost of a breach and we are working on developing the model further with key insurance partners with the goal of publishing an academic paper on it this year.

The Impact of Breaches

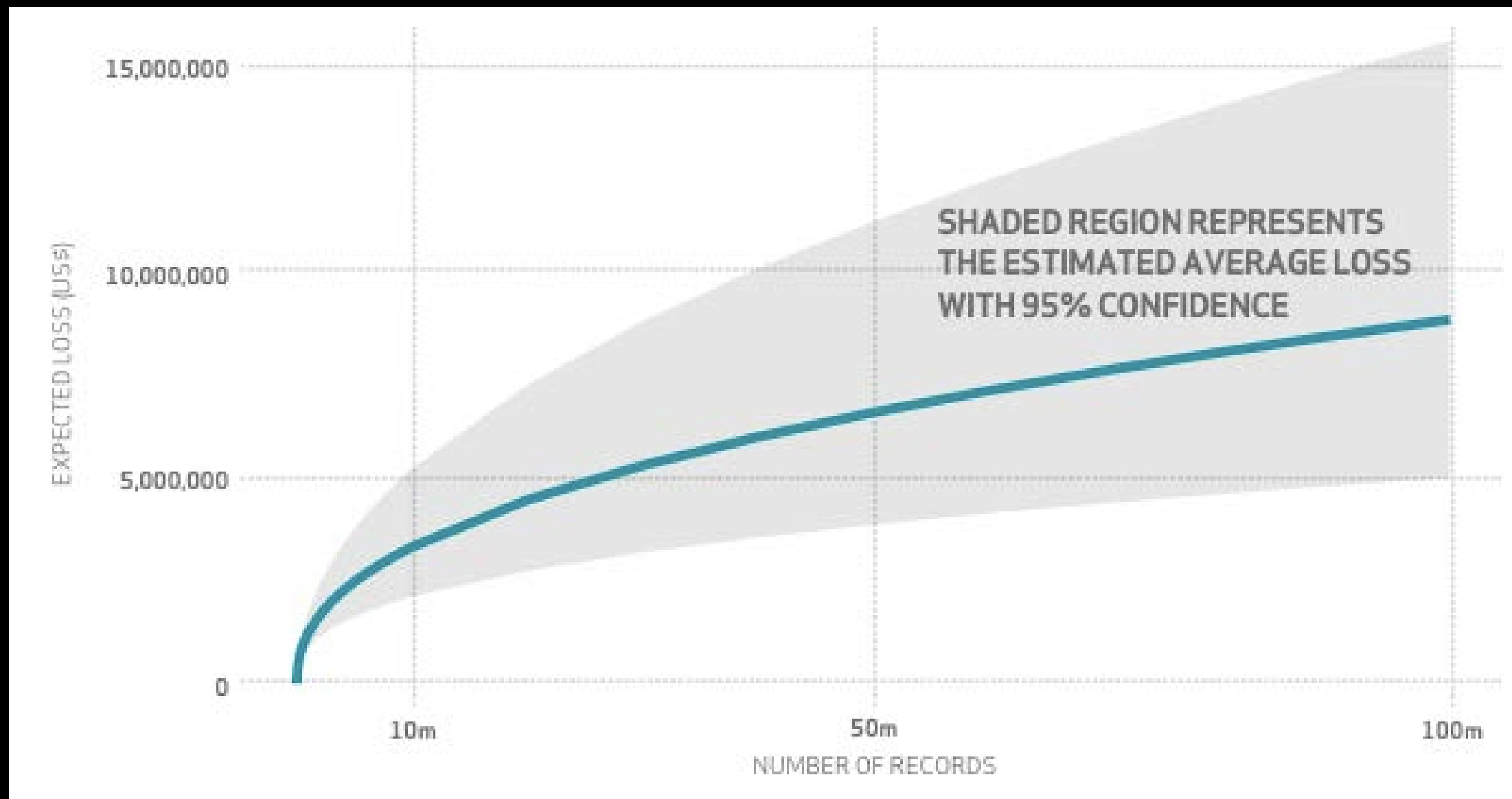
In the beginning, there was record count



The Impact of Breaches



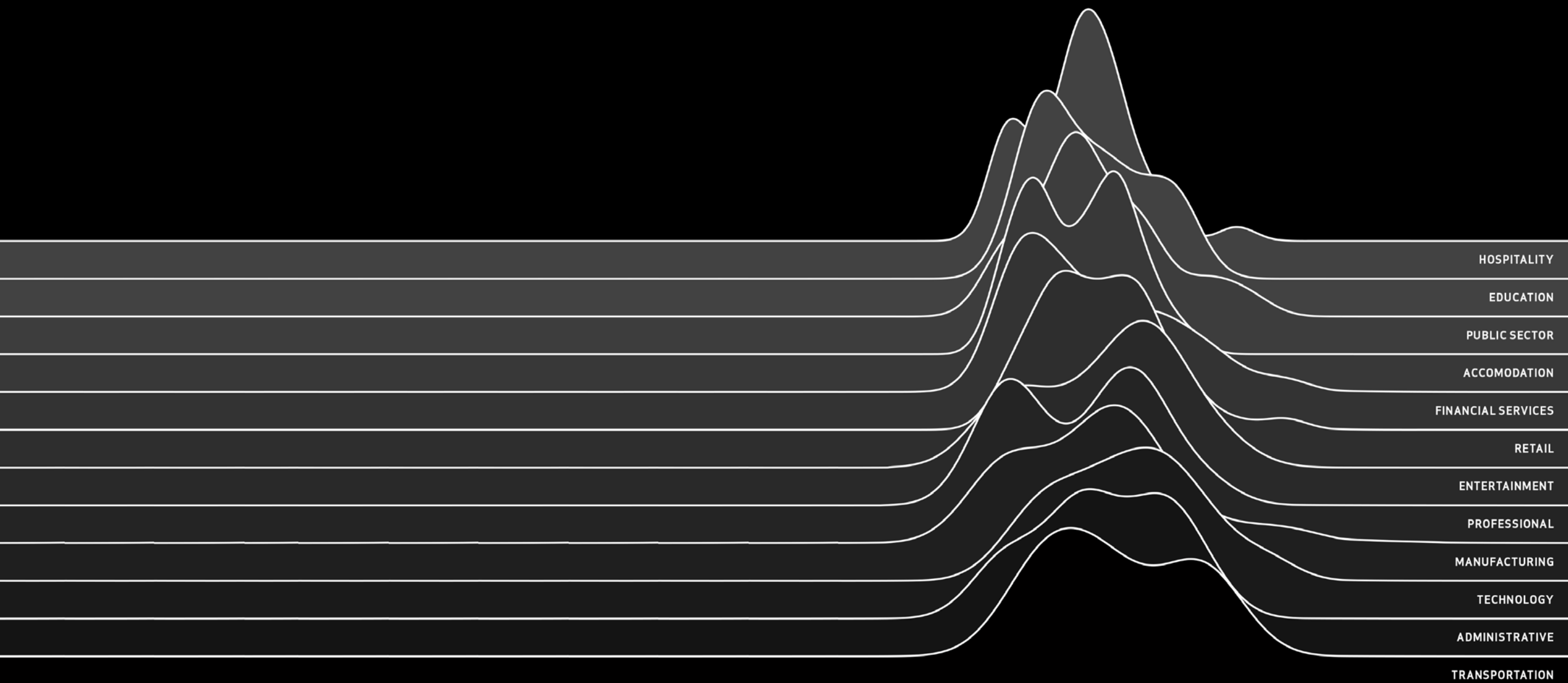
Estimate of Impact



Verizon Breach Impact Model

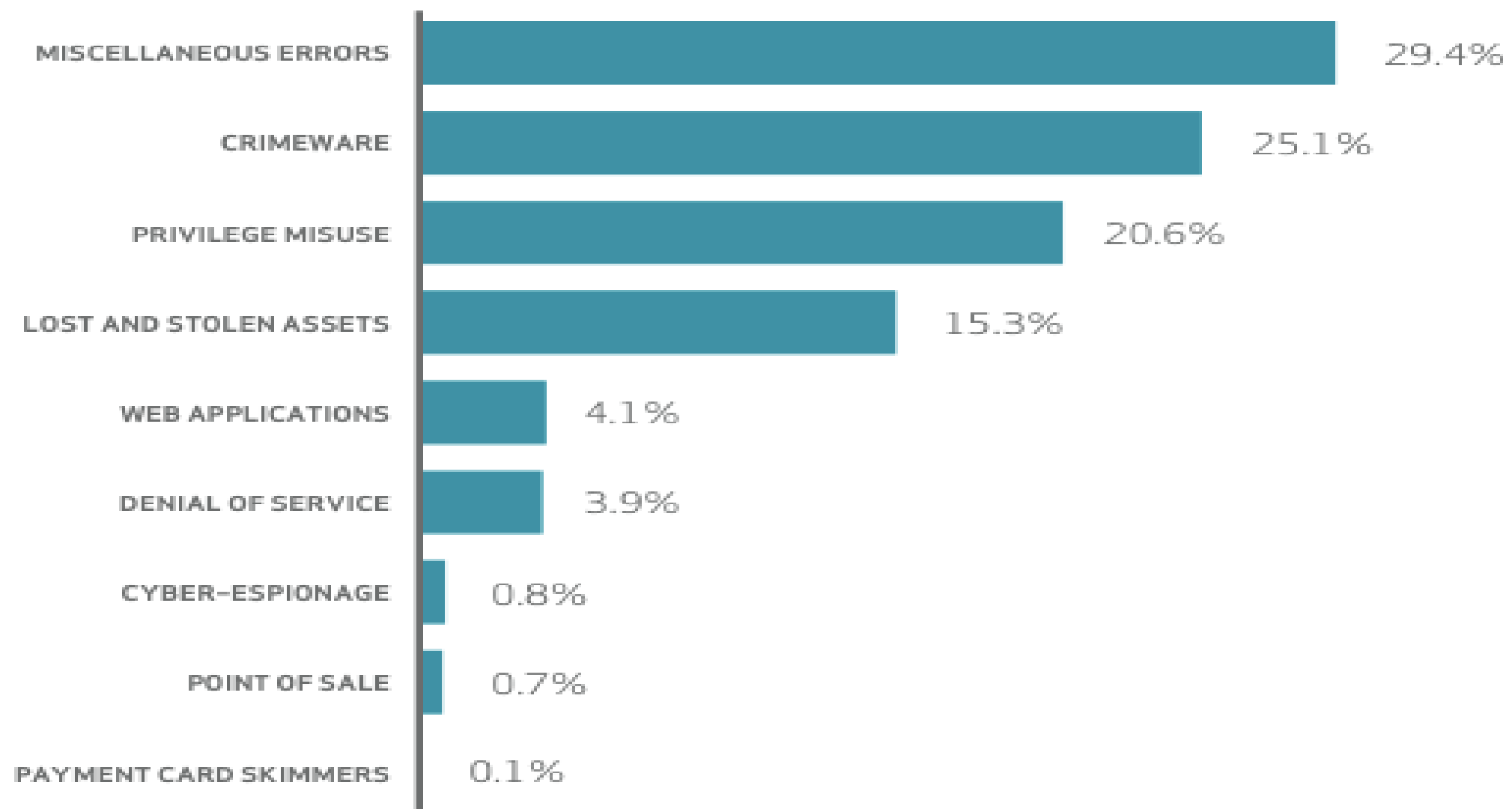
Records	Prediction (lower)	Average (lower)	Expected	Average (upper)	Prediction (upper)
100	\$1,165	\$18,118	\$25,445	\$35,734	\$555,664
1,000	\$3,115	\$52,258	\$67,480	\$87,136	\$1,461,728
10,000	\$8,283	\$143,362	\$178,960	\$223,396	\$3,866,367
100,000	\$21,905	\$366,484	\$474,606	\$614,627	\$10,283,189
1,000,000	\$57,609	\$892,356	\$1,258,669	\$1,775,353	\$27,500,090
10,000,000	\$150,687	\$2,125,897	\$3,338,026	\$5,241,279	\$73,943,954
100,000,000	\$392,043	\$5,016,243	\$8,852,541	\$15,622,747	\$199,895,081

The Incident Patterns



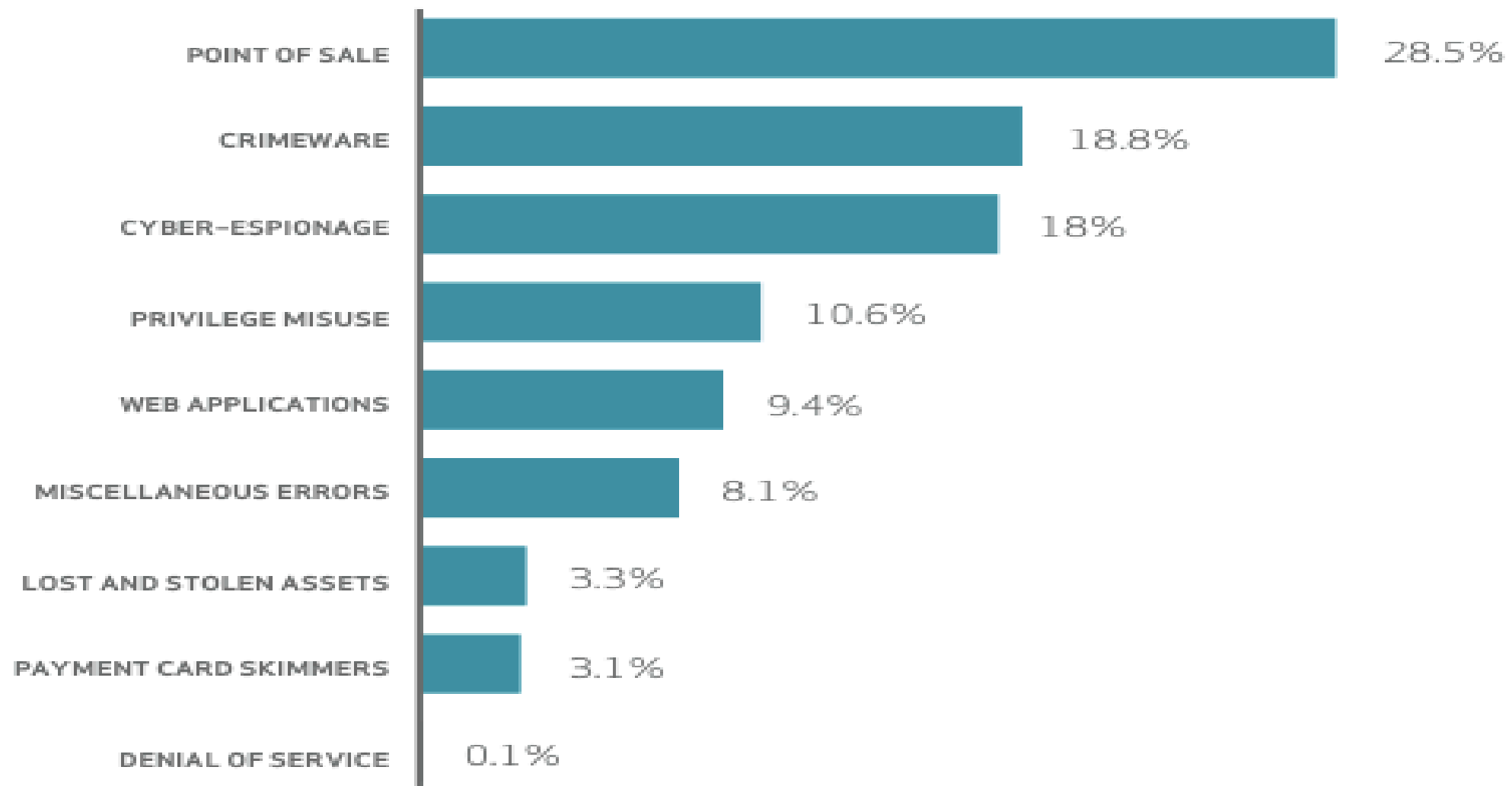
The Nefarious Nine

96% of all incidents could be described with these 9 patterns

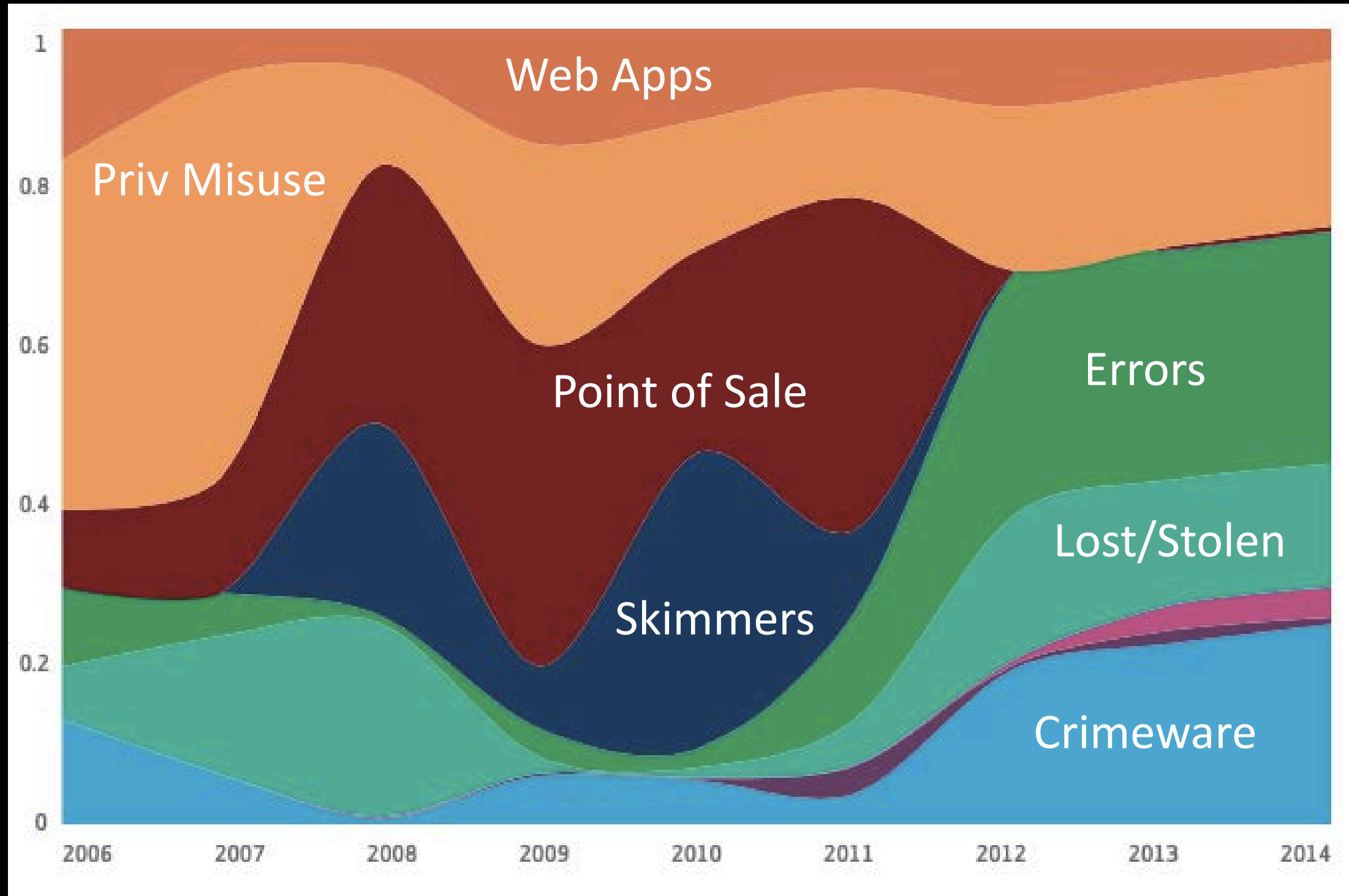


Just the Breaches, Ma'am

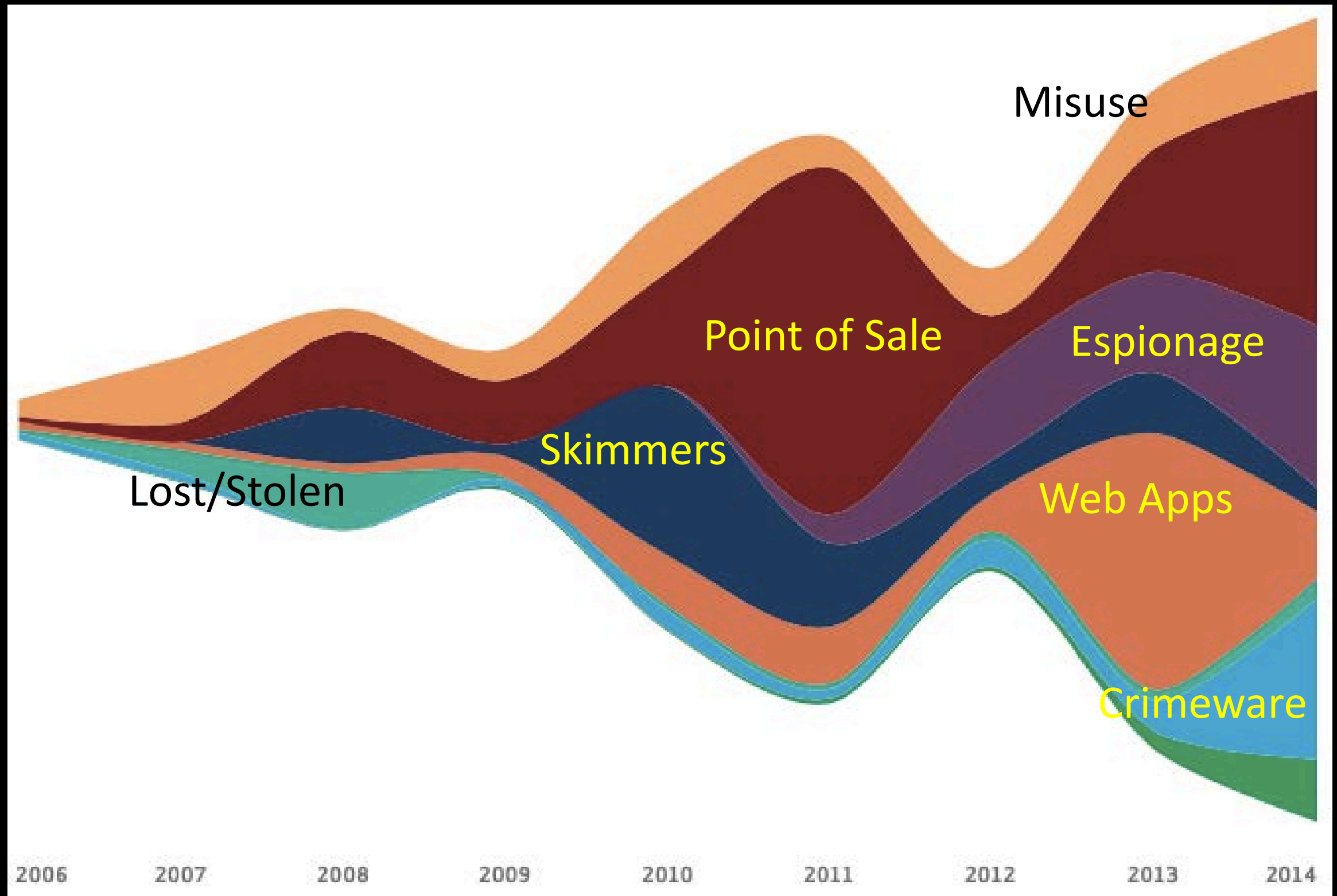
96% of all incidents could be described with these 9 patterns



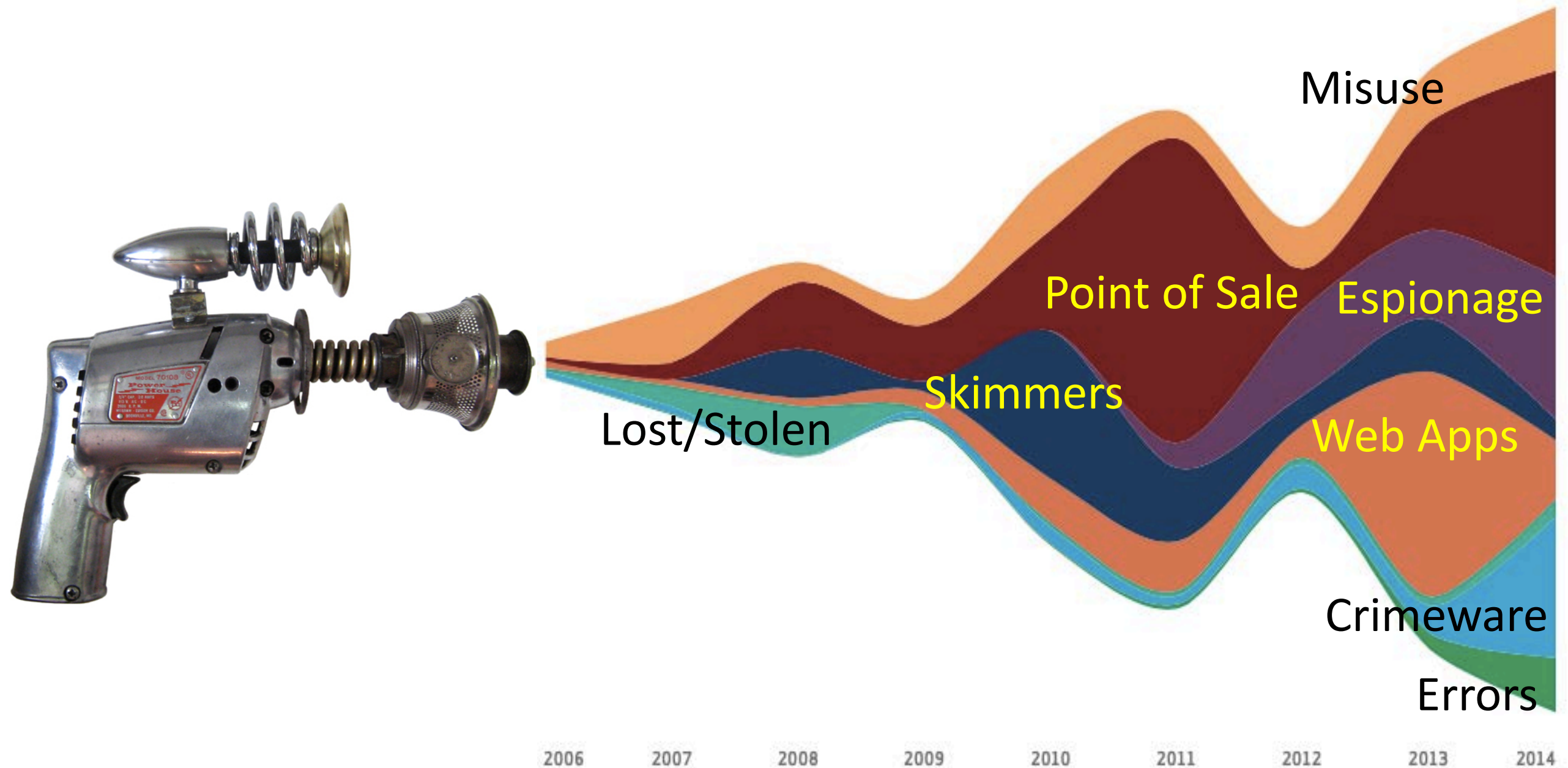
All Incidents (Graphics are Fun)



Just Breaches (Graphics are Really Fun)



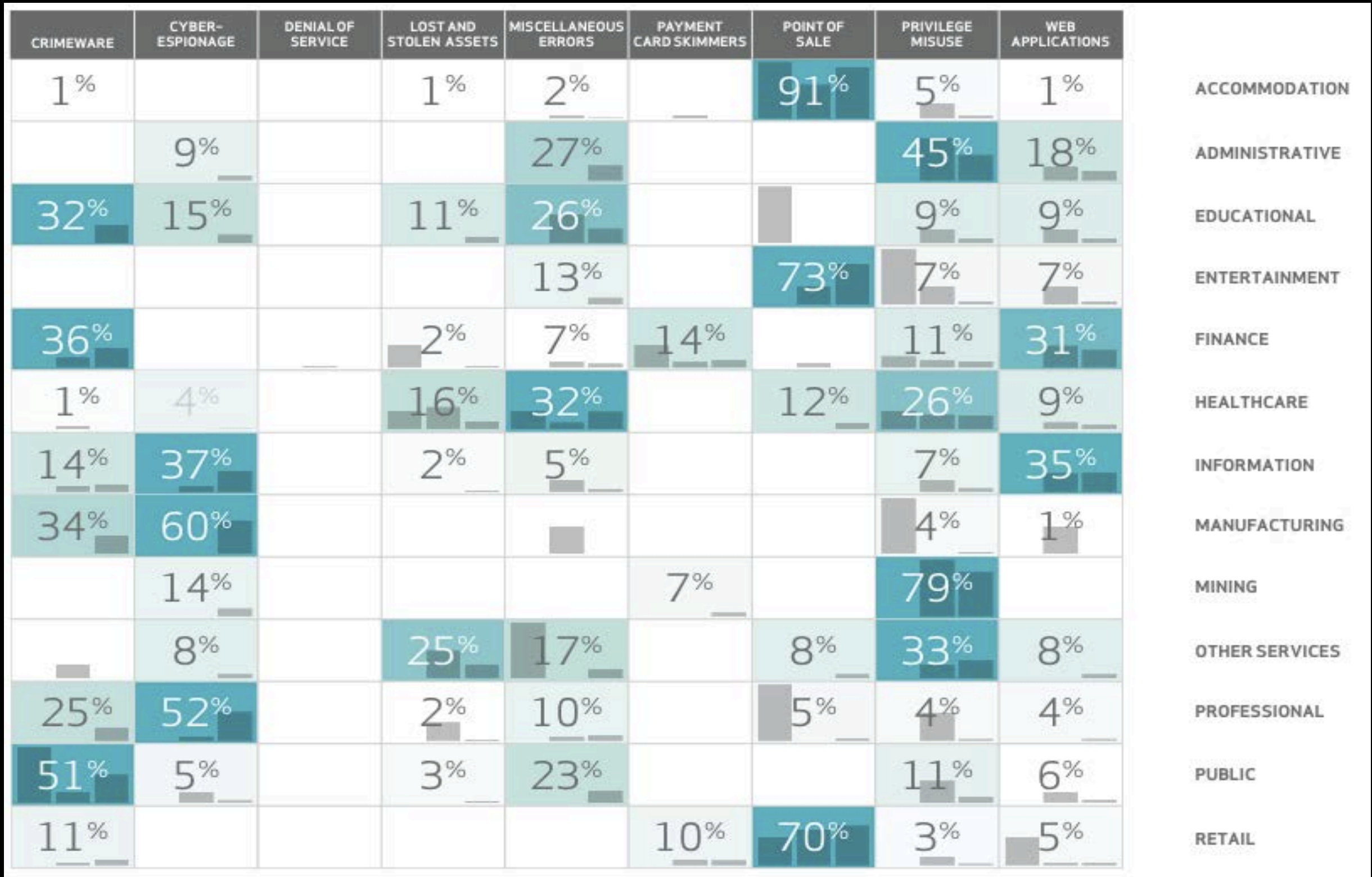
Pew pew pew!!!



Actors and the Nine Patterns



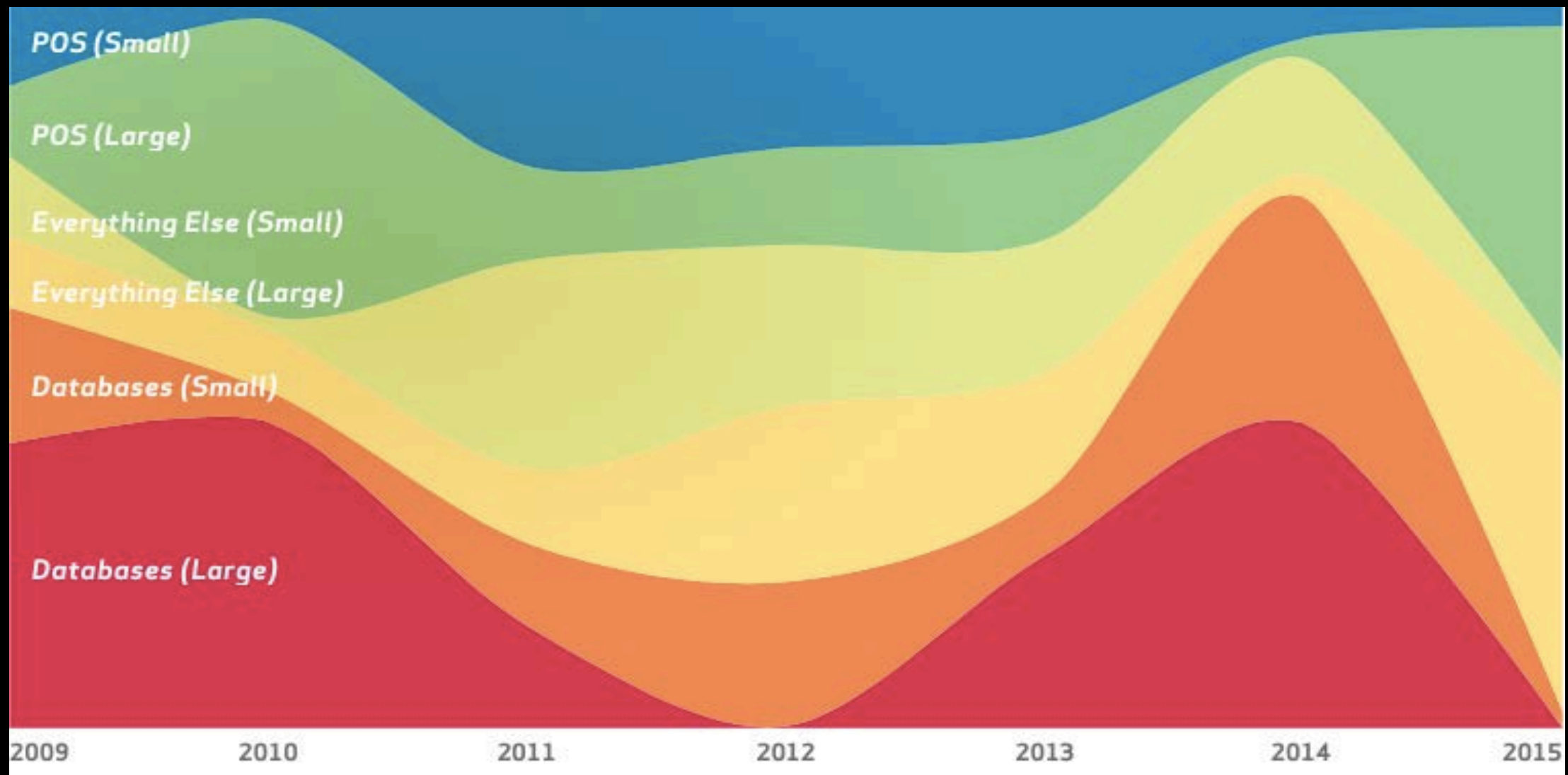
Breaches by Industry



Point of Sale

Industries Most Affected

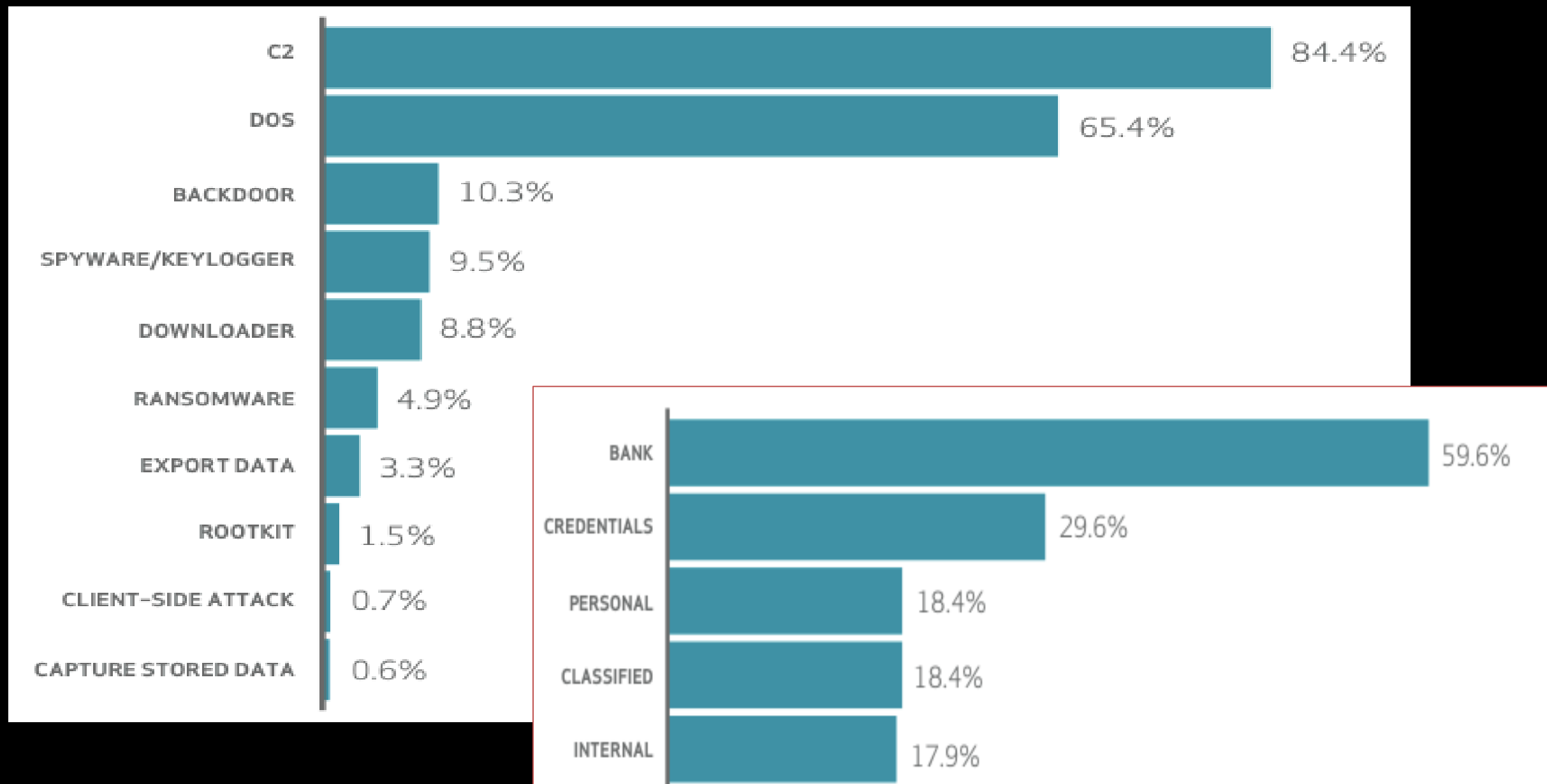
Accommodation, Entertainment, Retail



Crimeware

Industries Most Affected

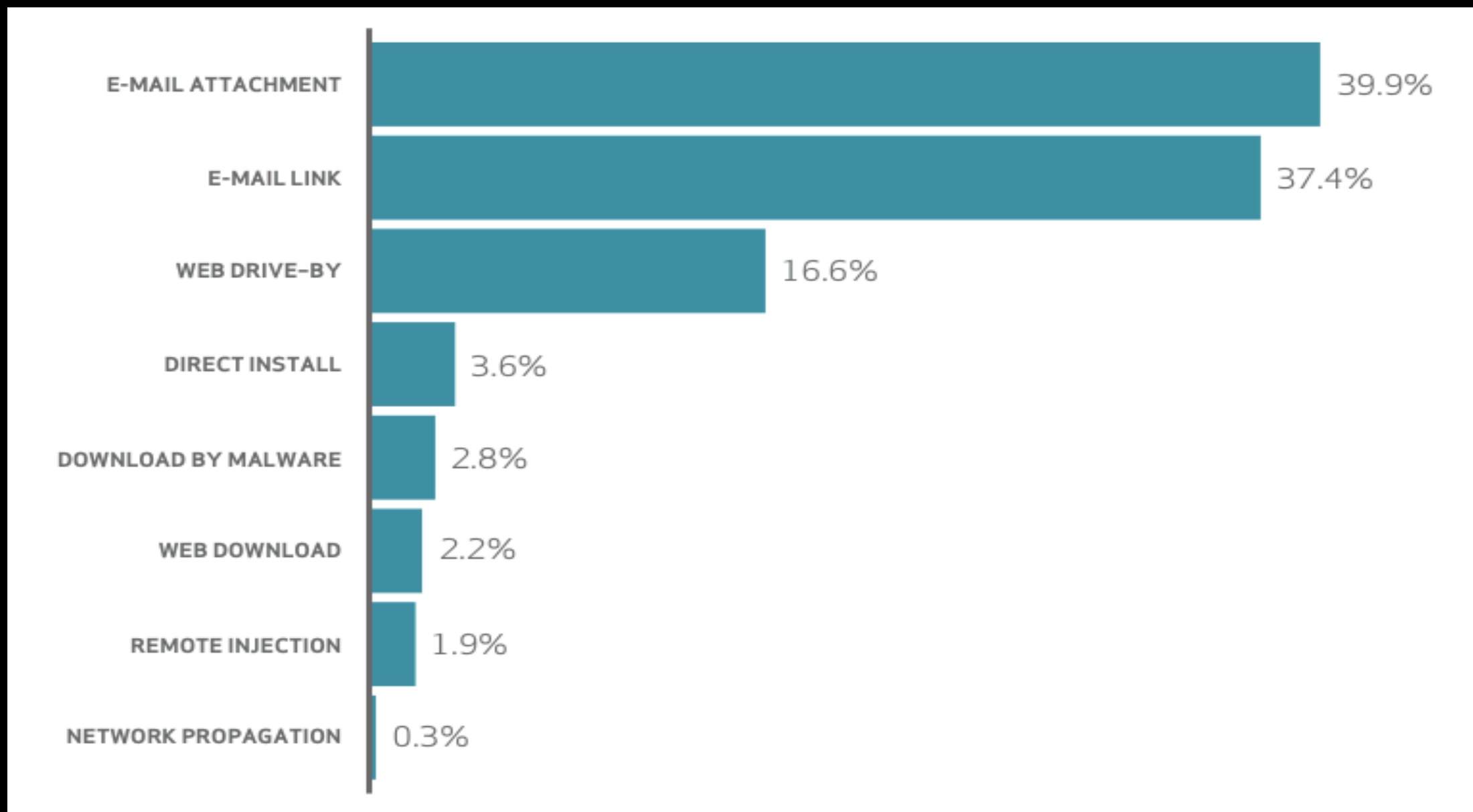
Public, Finance, Mfg, Educational



Cyber-espionage

Industries Most Affected

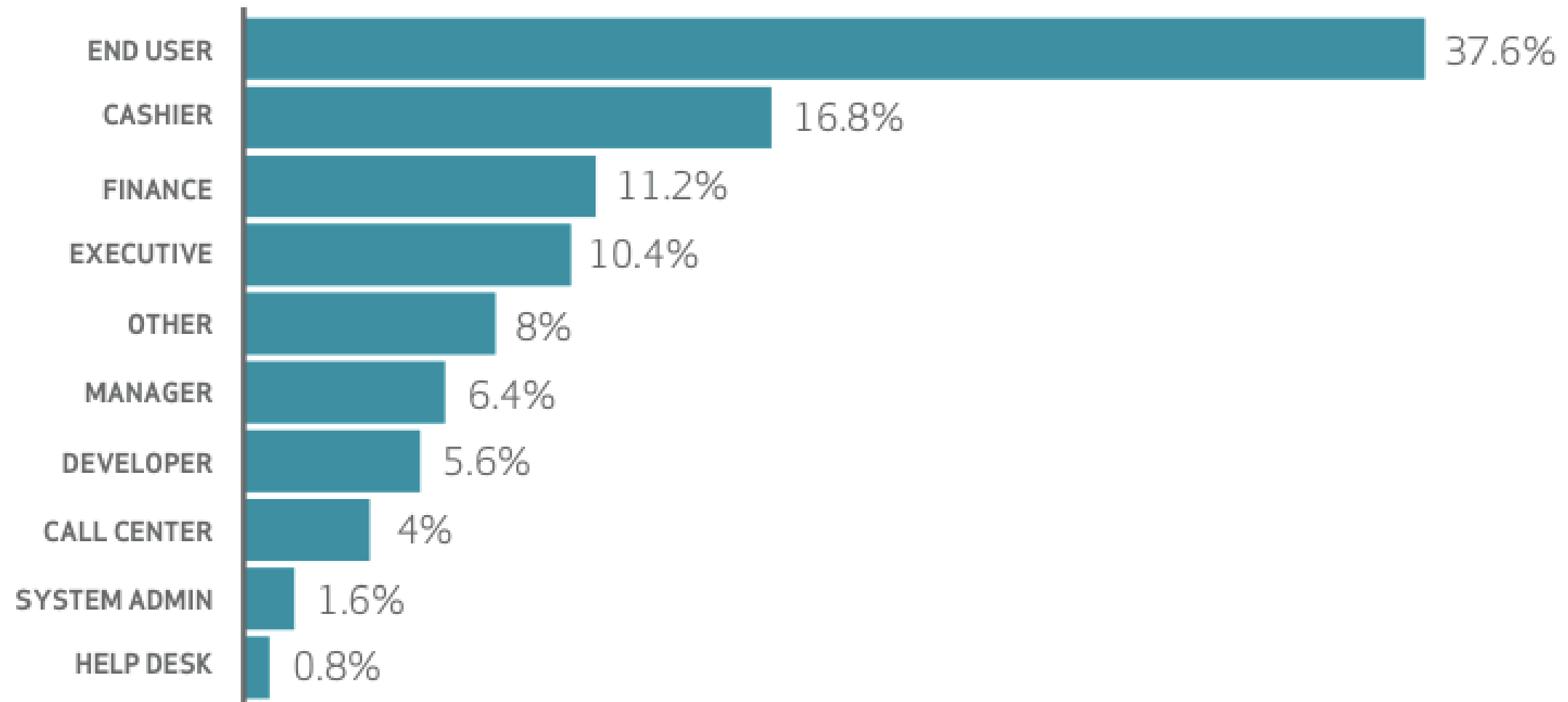
Manufacturing, Public, Professional



Insider and Privilege Misuse

Industries Most Affected

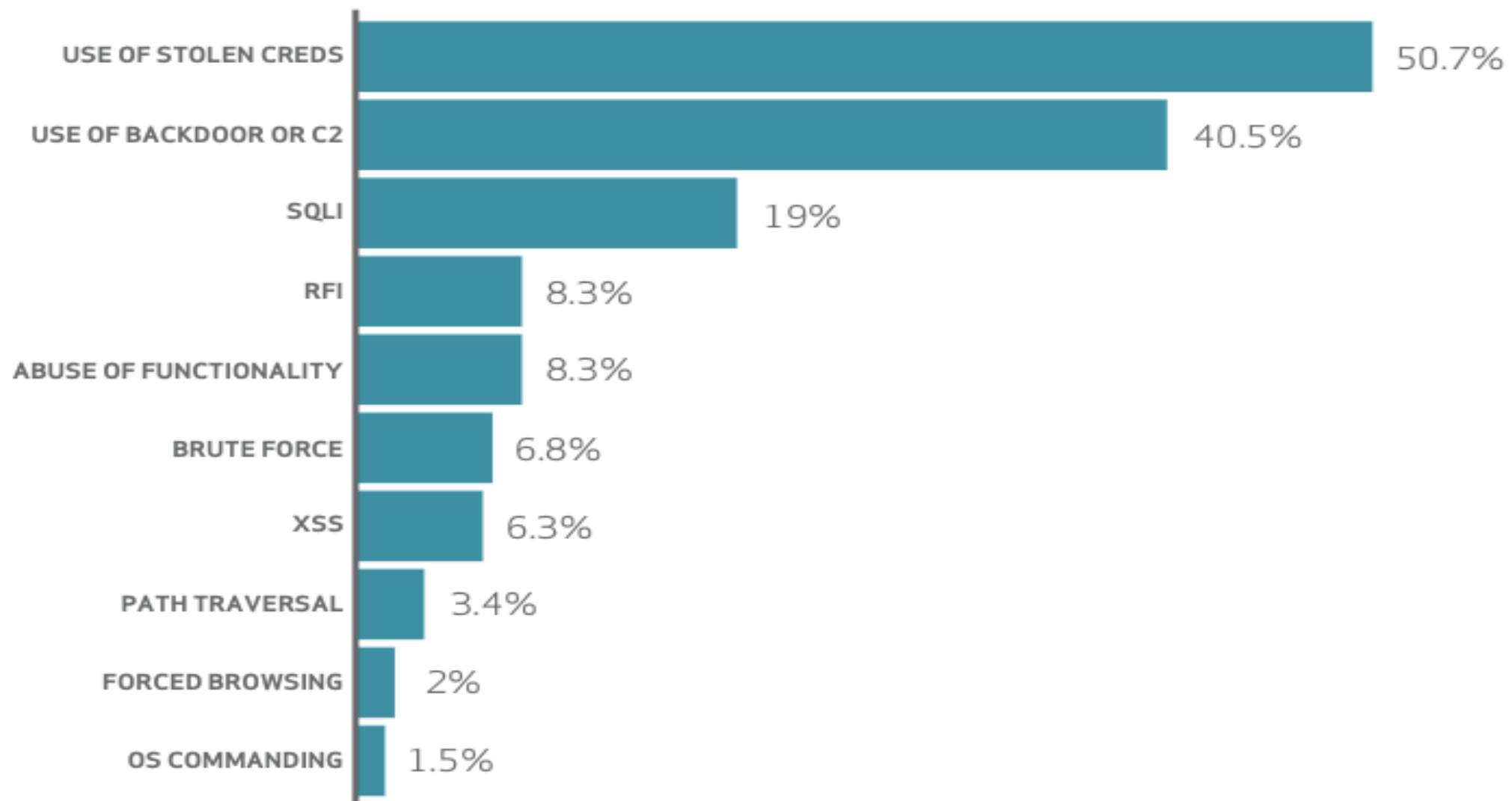
Mining, Administrative, Healthcare, Other Services



Web App Attacks

Industries Most Affected

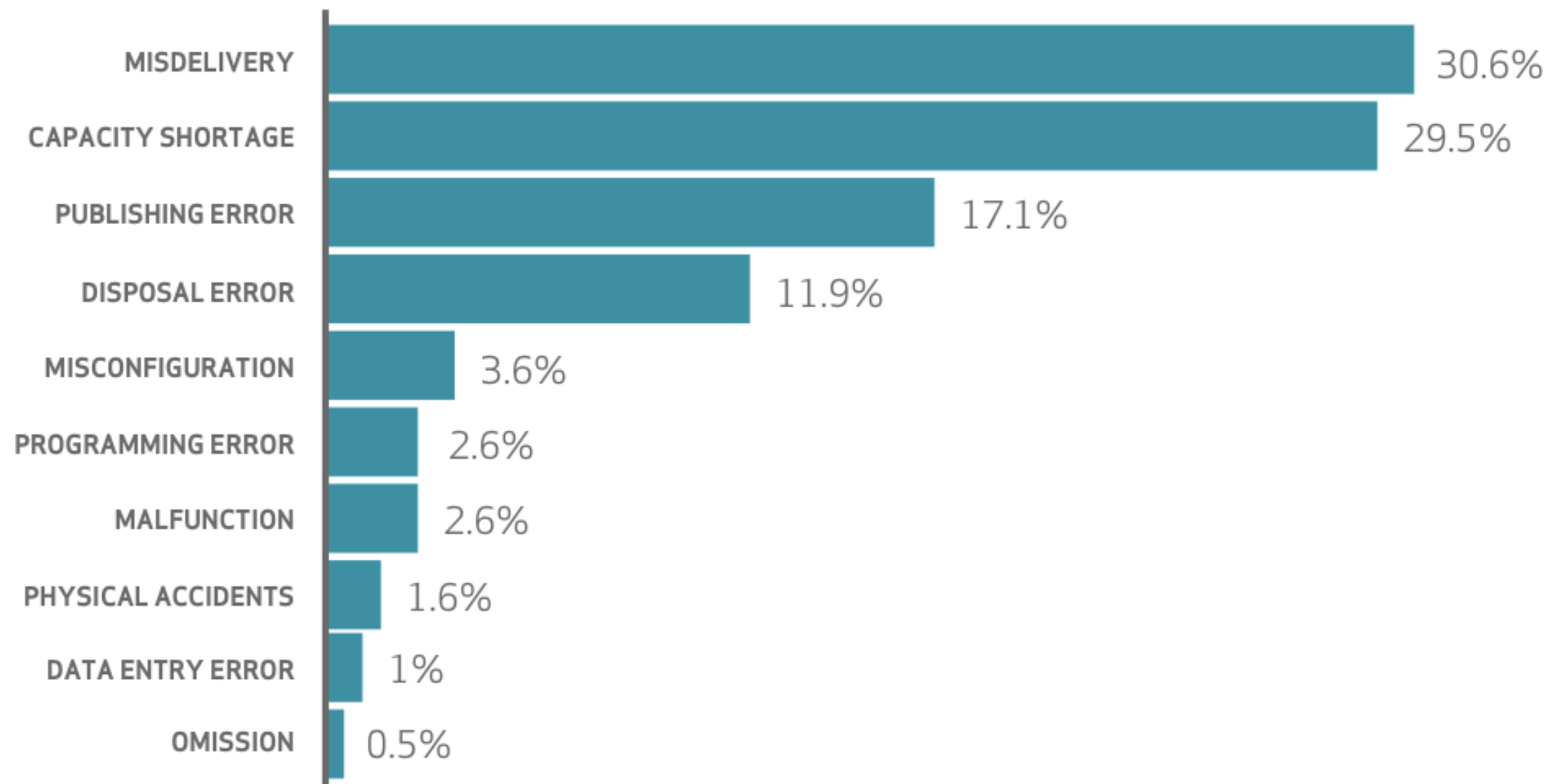
Information, Finance, and Administrative



Miscellaneous Errors

Industries Most Affected

Healthcare, Administrative, Educational



Lost/Stolen Devices

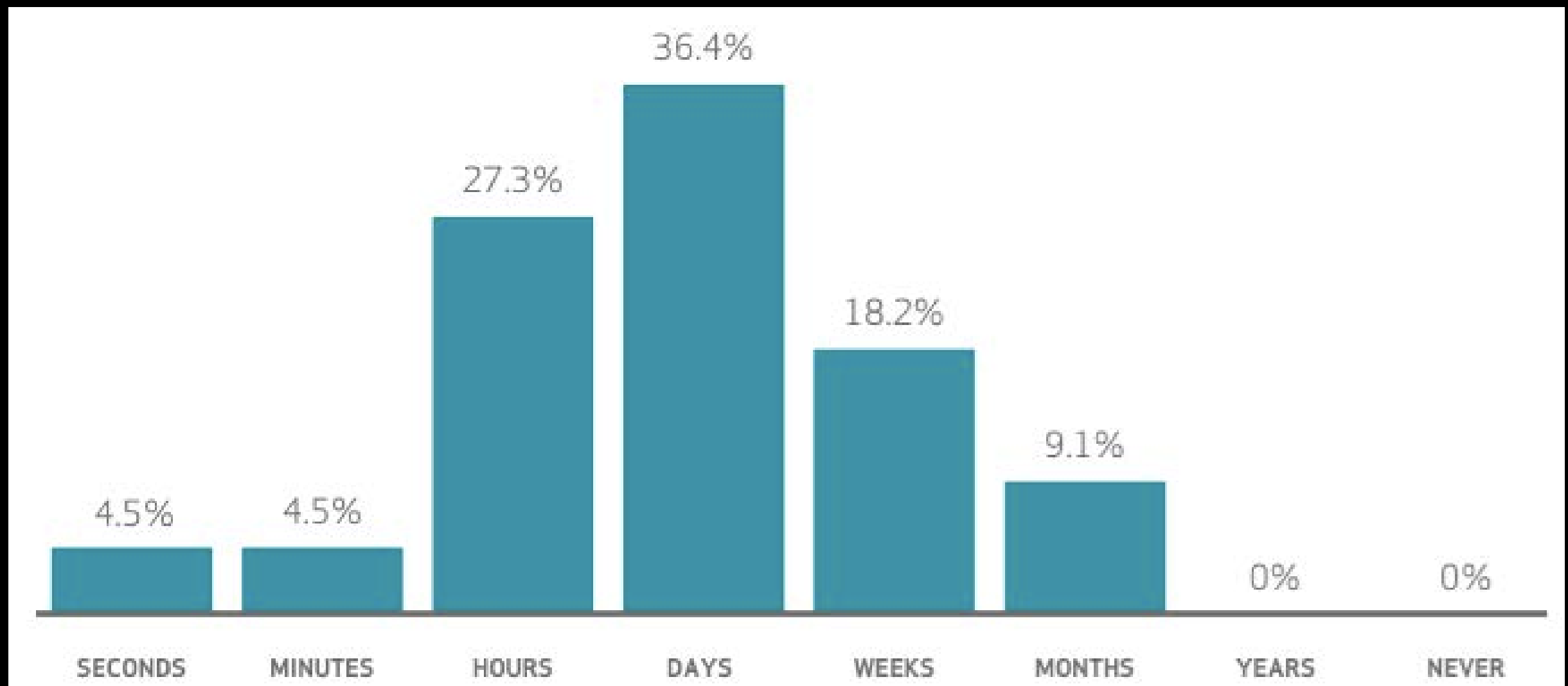
Industries Most Affected

Public Sector, Healthcare and Financial Services

15% of incidents still take days to discover. Ensure your process for reporting lost and stolen devices is easy to follow and incentivize your employees to report these incidents quickly

Payment Card Skimmers

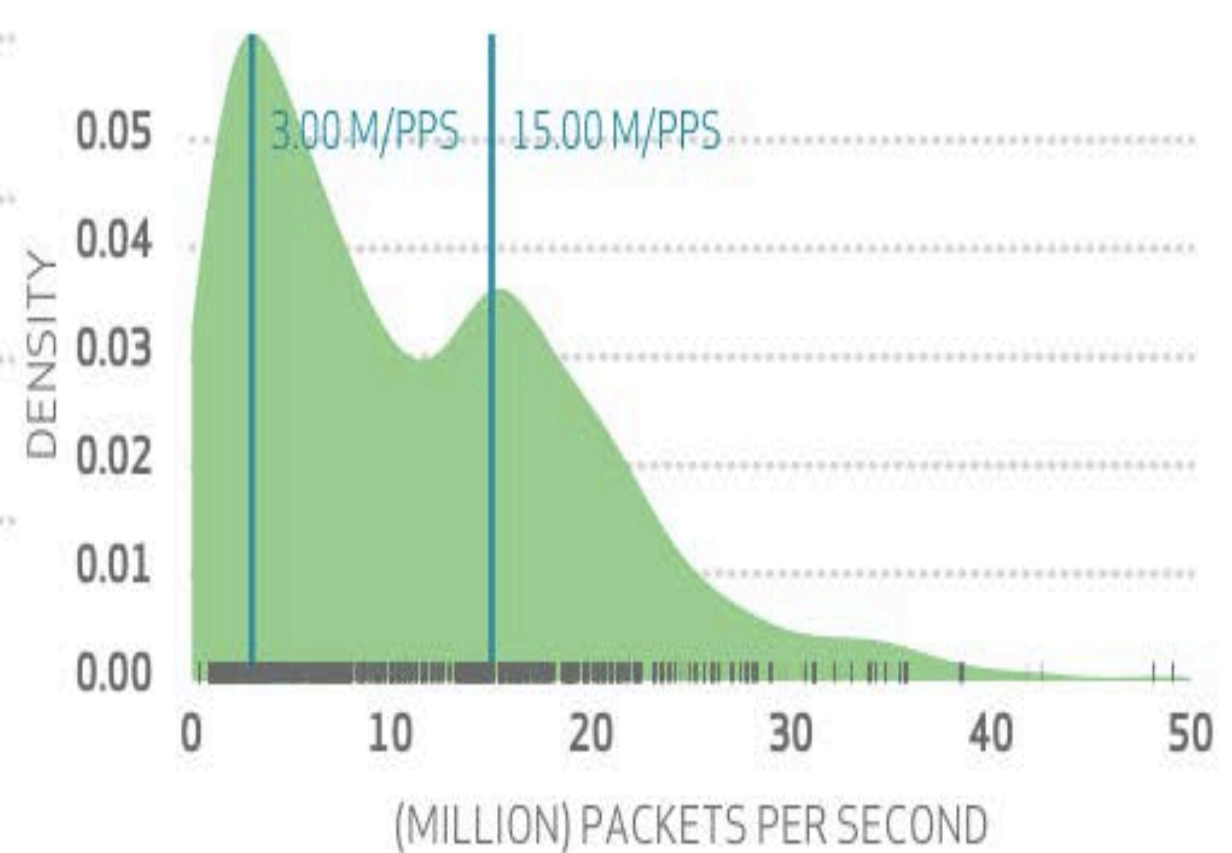
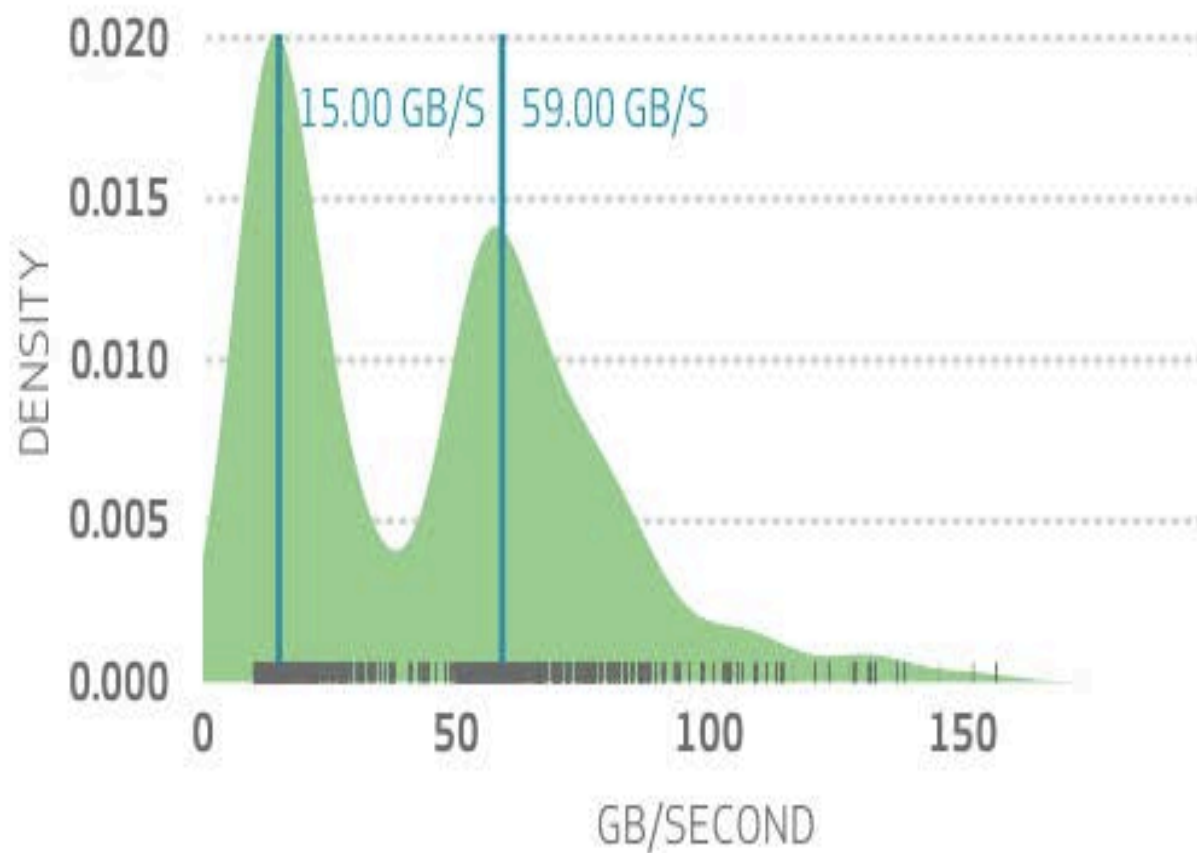
Industries Most Affected
Finance and Retail



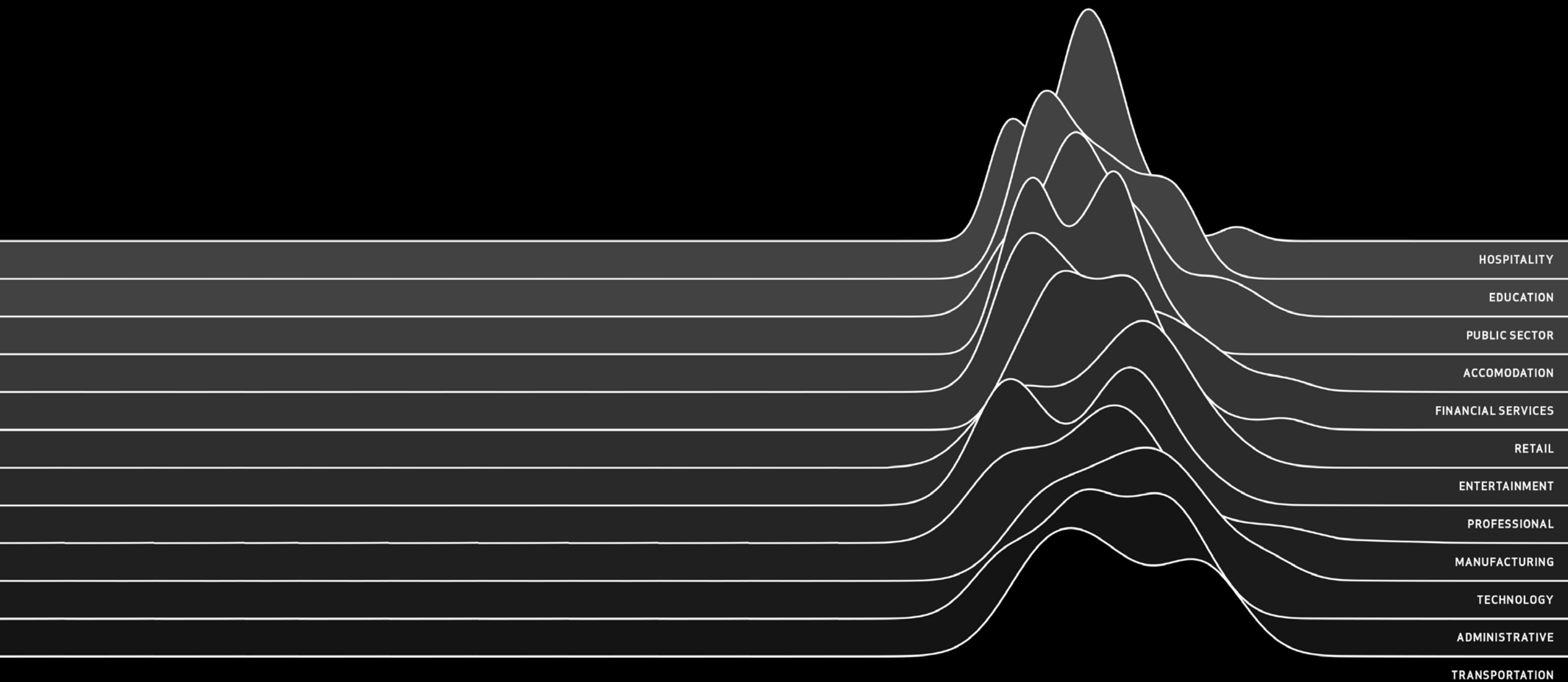
Denial of Service

Industries Most Affected

Public Sector, Retail and Financial Services



Before and Beyond the Breach



Threat Intelligence

(Indicators of Compromise)

Looked at over time, major public threat feeds have **less than 3% overlap across all of them.**

Enterprises either need to use *all* the feeds from *all* the providers (impossible) or implement **intelligent & targeted** application of the feeds.

Threat Intelligence

(Indicators of Compromise)

75% of attacks spread from Victim 0 to Victim 1 within one day (24 hours), meaning we need to close the gap between sharing speed and attack speed



Phishing

150,000 phishing e-mails analyzed from campaigns by two DBIR partners.

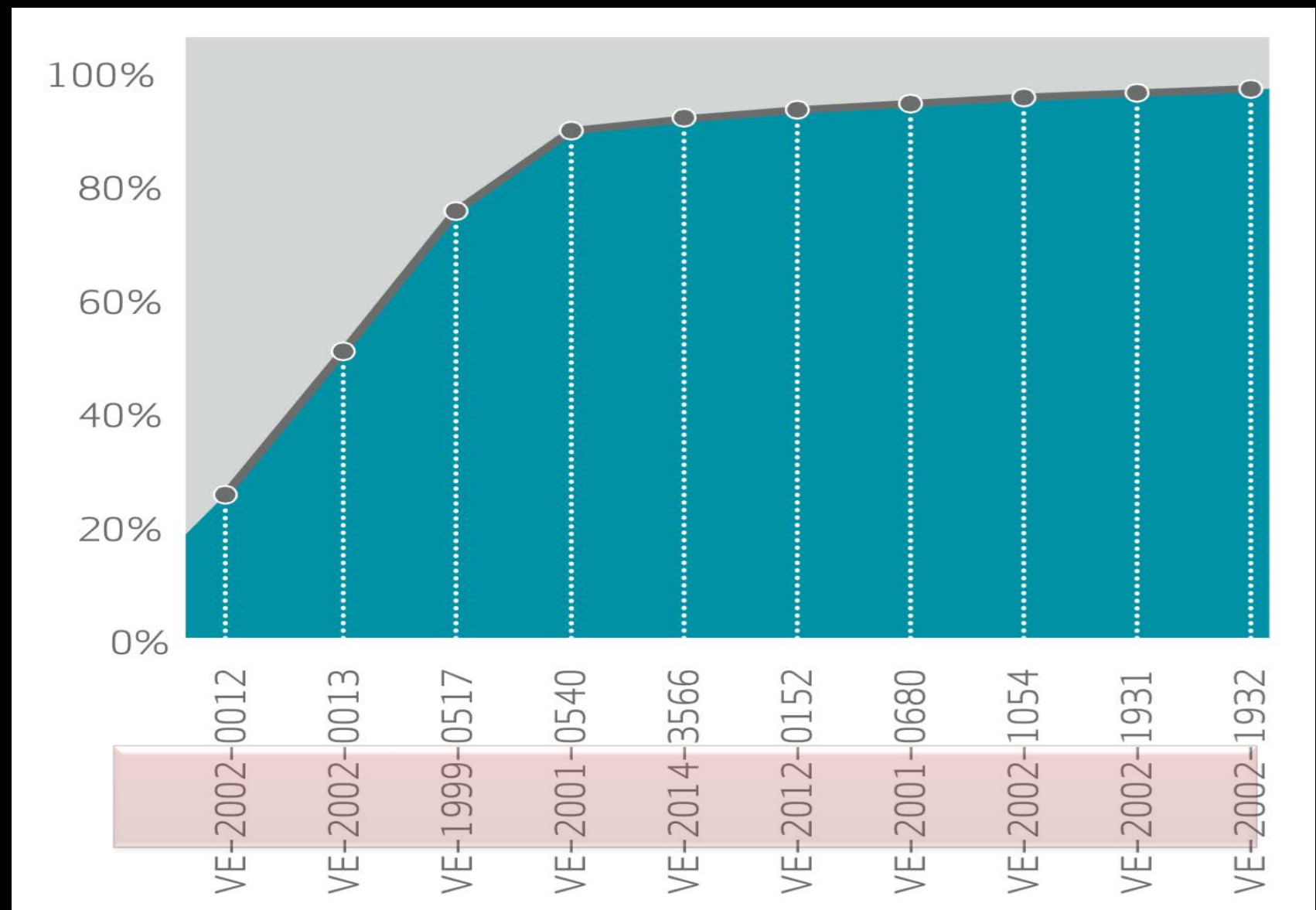
23% of recipients open phishing messages.

11% of recipients click on attachments.

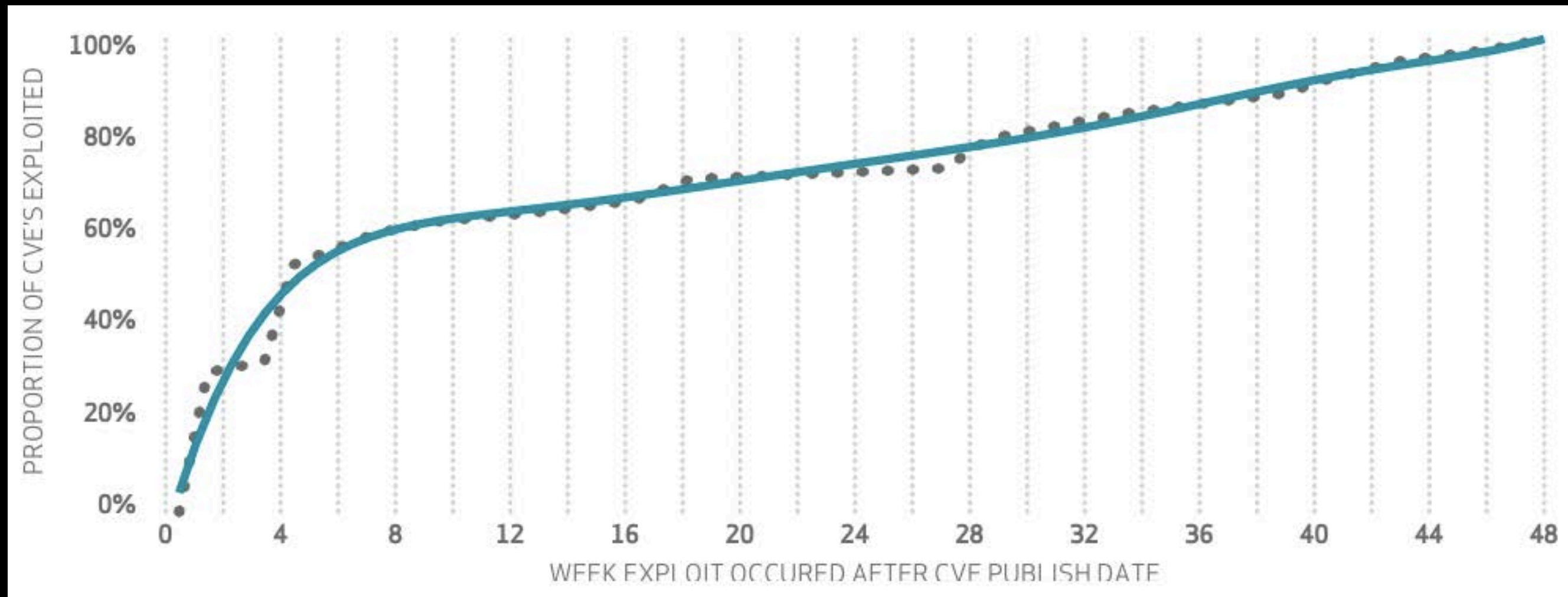
82 seconds from start of campaign to first bite.

All About the Vulns

10 CVEs account for *97%* of the exploits seen in 2014



From Pub to Pwn



Mobile Malware

Verizon Wireless gave us
access to the logs of
malware detections from
tens of millions wireless
devices (phones and
tablets)

Virtually NO iOS (iPhone)
malware detected

(i.e. Android “wins”)

CSC	Description	Percentage	Category
13-7	2FA	24%	Visibility/Attribution
6-1	Patching Web Services	24%	Quick Win
11-5	Verify need for Internet-facing devices	7%	Visibility/Attribution
13-6	Proxy outbound traffic	7%	Visibility/Attribution
6-4	Web application testing	7%	Visibility/Attribution
16-9	User lockout after multiple failed attempts	5%	Quick Win
17-13	Block known file xfer sites	5%	Advanced
5-5	Mail attachment filtering	5%	Quick Win
11-1	Limiting ports and services	2%	Quick Win
13-10	Segregation of Networks	2%	Configuration/Hygiene
16-8	Password complexity	2%	Visibility/Attribution
3-3	Restrict ability to download s/w	2%	Quick Win
5-1	Anti-virus	2%	Quick Win
6-8	Vet security process of vendor	2%	Configuration/Hygiene

Additional Information

- Download DBIR – www.verizonenterprise.com/dbir
- Learn about VERIS - www.veriscommunity.net and <http://github.com/vz-risk/veris>
- Explore the VERIS Community Database: <http://www.vcdb.org>
- Ask a question – DBIR@verizon.com
- Read our blog - <http://www.verizonenterprise.com/security/blog/>
- Follow on Twitter - @vzdbir and hashtag #dbir



2015 DATA BREACH INVESTIGATIONS REPORT

Email: suzanne.widup@verizon.com

Twitter: [@SuzanneWidup](https://twitter.com/SuzanneWidup)

