NINTH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

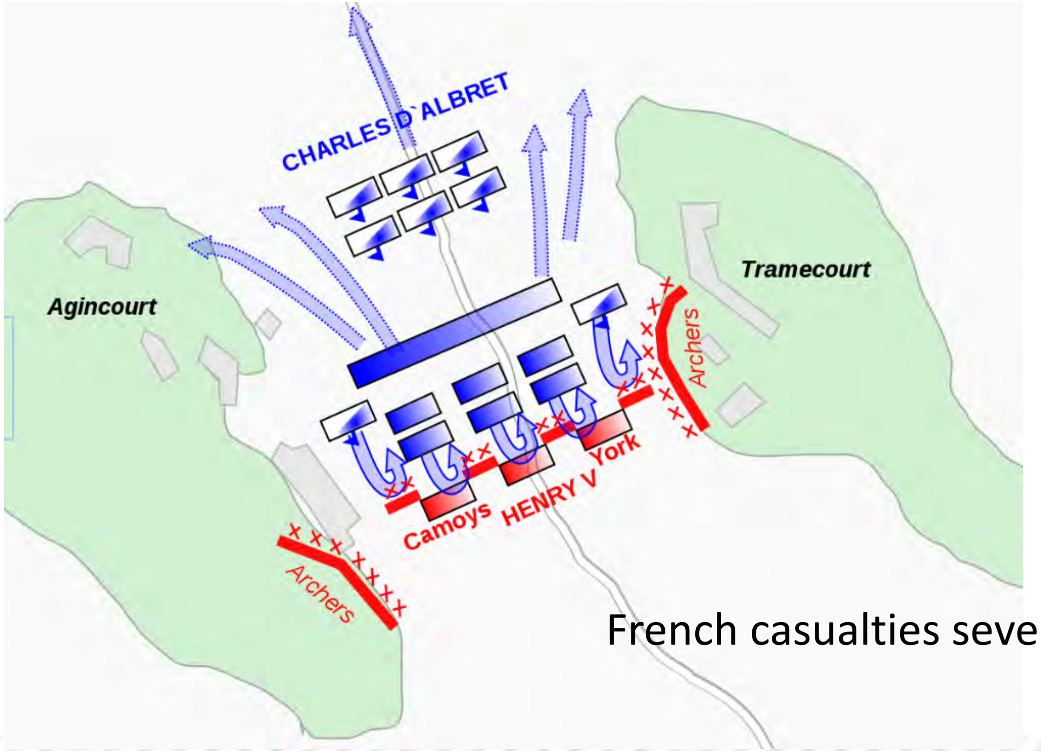
October 28–30, 2019 | Minneapolis Convention Center

cybersecuritysummit.org | #cybersummitmn

Pluck Yew!!!

Battle of Agincourt (Failed Strategy)

- Disjointed French Leaders
- Muddy conditions weighed down French knights
- Longbow – more powerful
- French Armor did not protect



French casualties severe 10,000

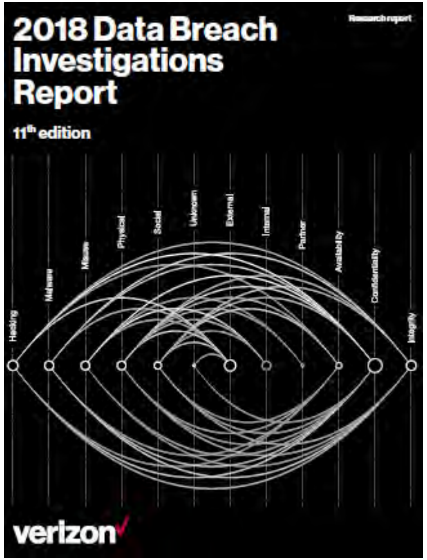
Verizon Data Breach Investigations Report

- In-depth research
- Informative data visualizations
- Just enough Snark

2017 Data Breach Investigations Report

10th Edition

verizon

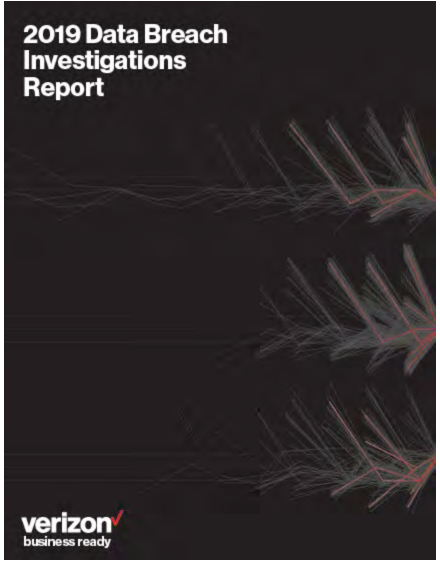


Research report

2018 Data Breach Investigations Report

11th edition

verizon



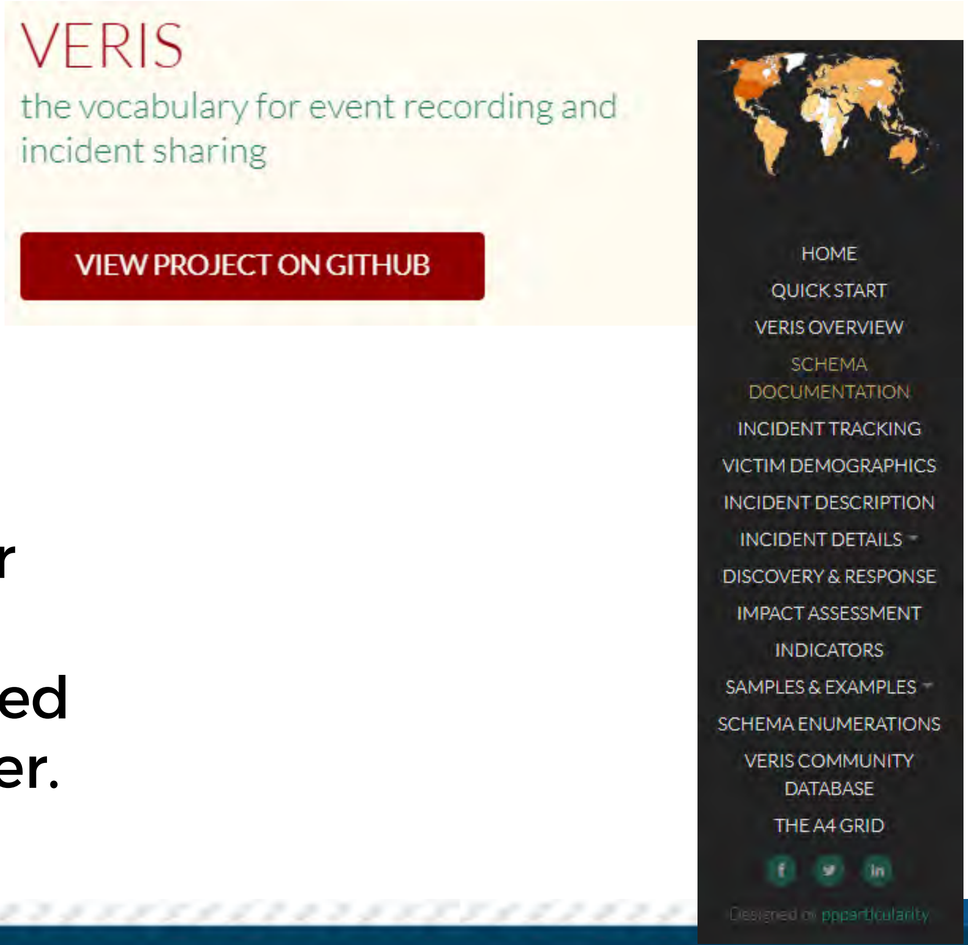
2019 Data Breach Investigations Report

verizon

business ready

VERIS

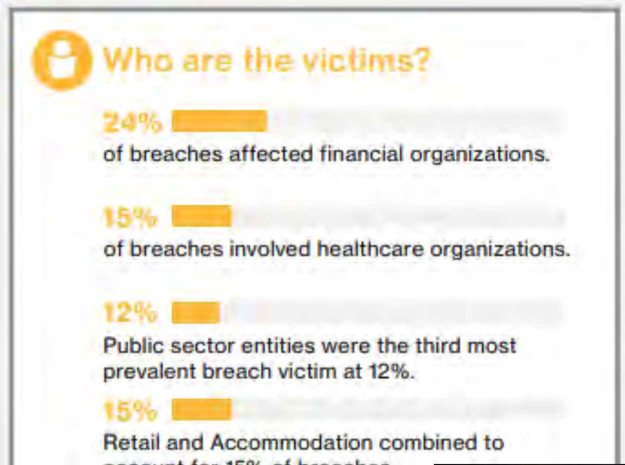
- “Consistent, unequivocal collection of security incident details
  - Common language for describing security incidents in a structured and repeatable manner.
  - Basis for enumeration



VERIS

the vocabulary for event recording and incident sharing

Executive Summary - Victims



Who are the victims?

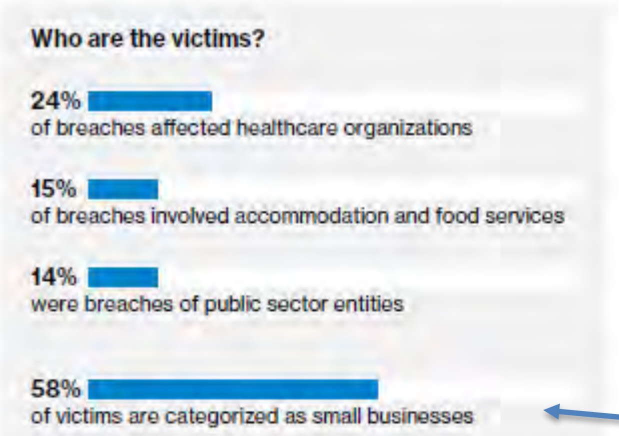
24% of breaches affected financial organizations.

15% of breaches involved healthcare organizations.

12% Public sector entities were the third most prevalent breach victim at 12%.

15% Retail and Accommodation combined to account for 15% of breaches.

2017 Data Breach Investigations Report
10th Edition
verizon



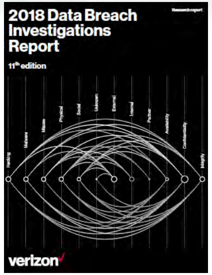
Who are the victims?

24% of breaches affected healthcare organizations

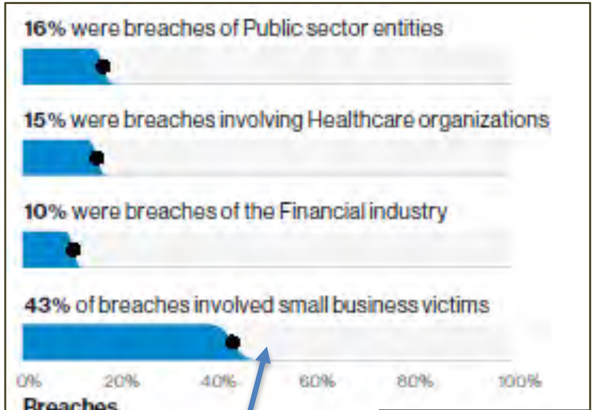
15% of breaches involved accommodation and food services

14% were breaches of public sector entities

58% of victims are categorized as small businesses



2018 Data Breach Investigations Report
11th edition
verizon



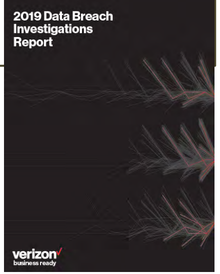
16% were breaches of Public sector entities

15% were breaches involving Healthcare organizations

10% were breaches of the Financial industry

43% of breaches involved small business victims

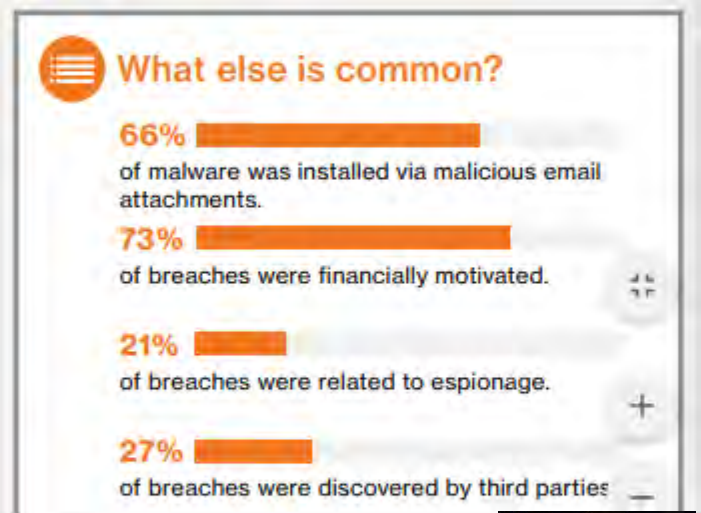
Figure 2. Who are the victims?



2019 Data Breach Investigations Report
verizon
business ready

Small Business

Executive Summary - Commonalities



What else is common?

66% of malware was installed via malicious email attachments.

73% of breaches were financially motivated.

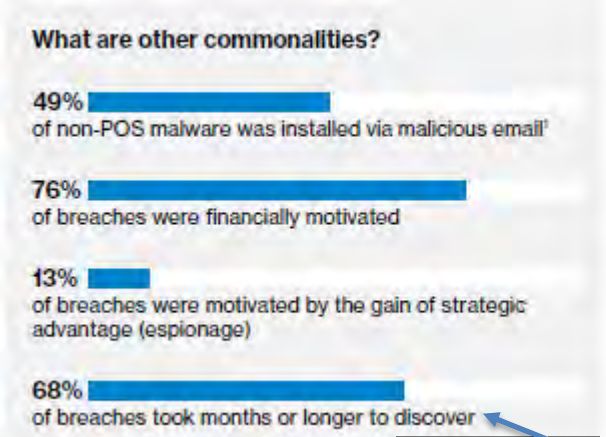
21% of breaches were related to espionage.

27% of breaches were discovered by third parties

2017 Data Breach Investigations Report

10th Edition

verizon



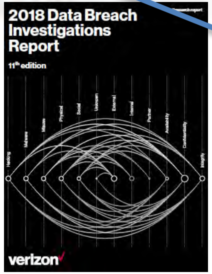
What are other commonalities?

49% of non-POS malware was installed via malicious email¹

76% of breaches were financially motivated

13% of breaches were motivated by the gain of strategic advantage (espionage)

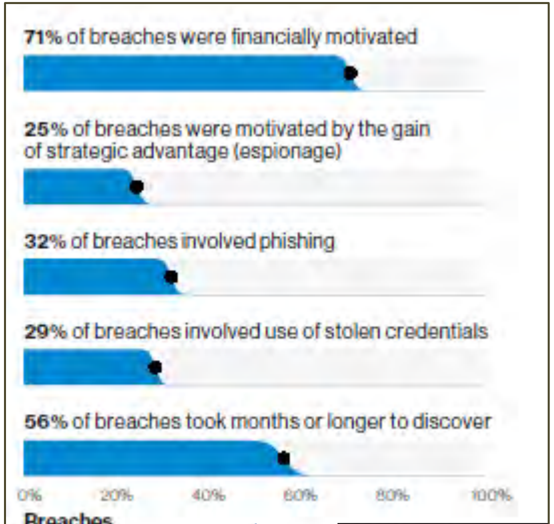
68% of breaches took months or longer to discover



2018 Data Breach Investigations Report

11th edition

verizon



71% of breaches were financially motivated

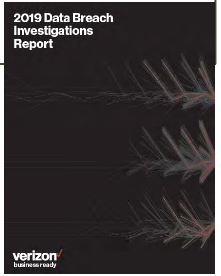
25% of breaches were motivated by the gain of strategic advantage (espionage)

32% of breaches involved phishing

29% of breaches involved use of stolen credentials

56% of breaches took months or longer to discover

Figure 5. What are other commonalities?

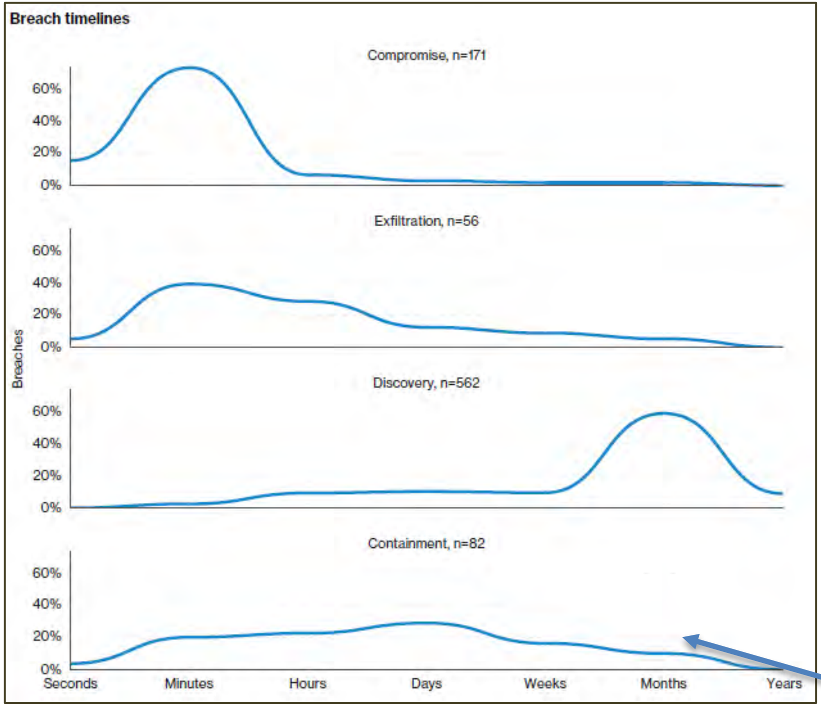


2019 Data Breach Investigations Report

verizon business ready

Detection

Breach Timeline



2018 Data Breach Investigations Report

11th edition

verizon

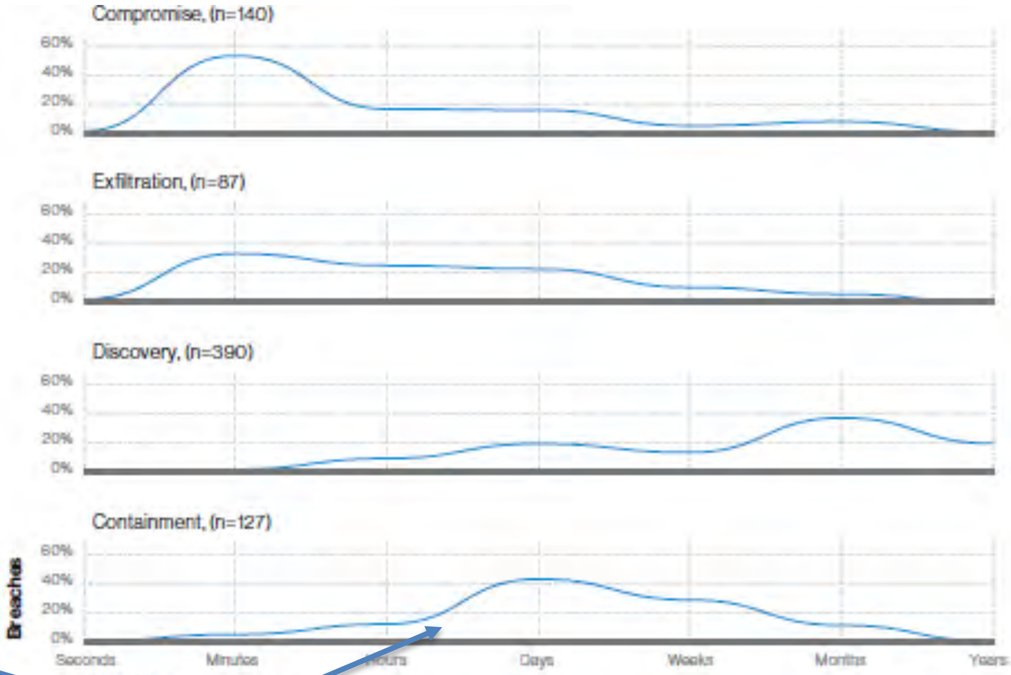


Figure 28. Breach timelines

Detection

2019 Data Breach Investigations Report

verizon

business ready

Incident Classification Patterns

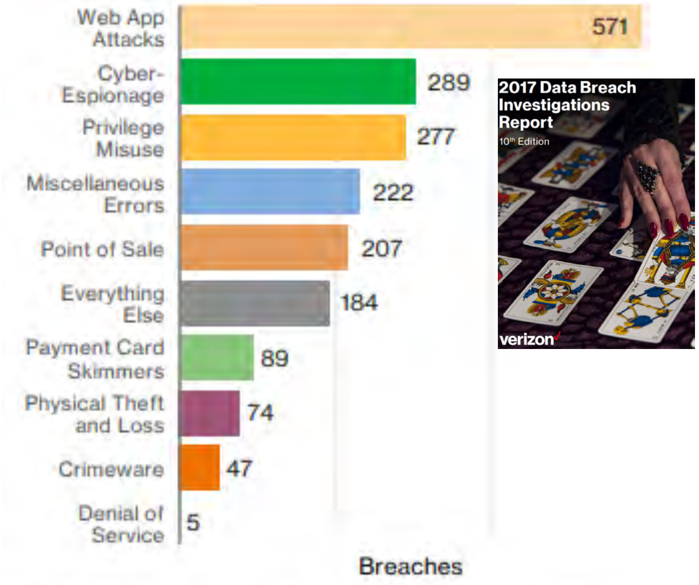


Figure 33: Percentage and count of breaches per pattern (n=1,935)

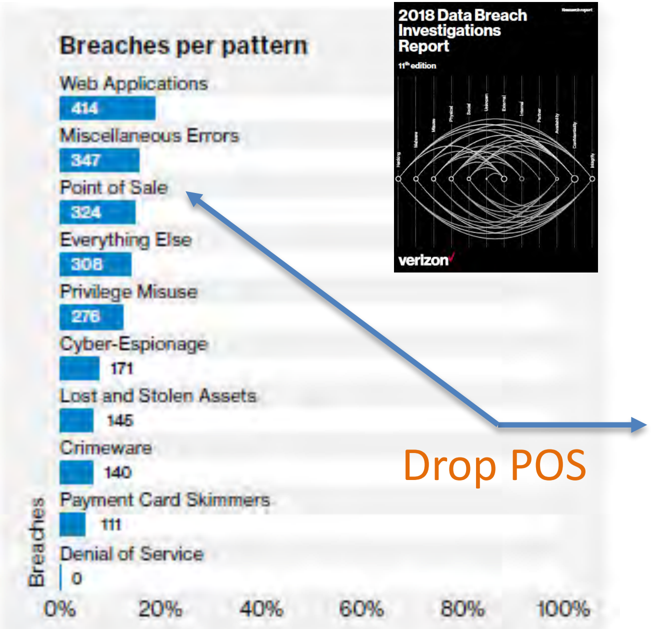


Figure 27. Percentage and count of breaches per pattern (n=2,216)

Drop POS

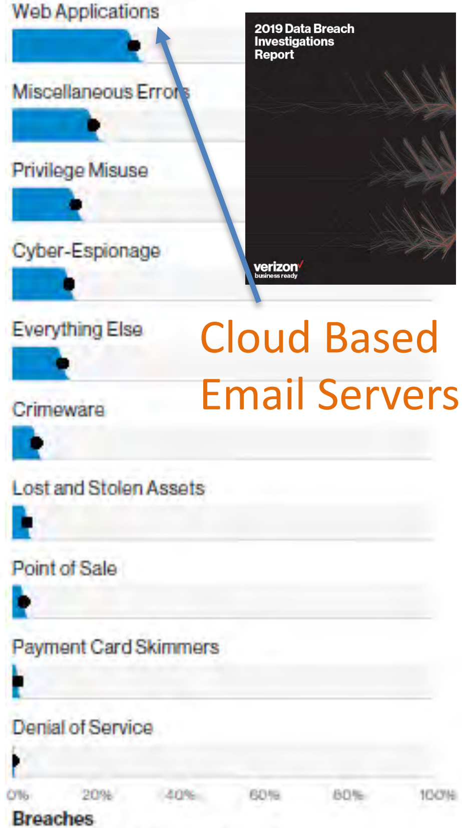


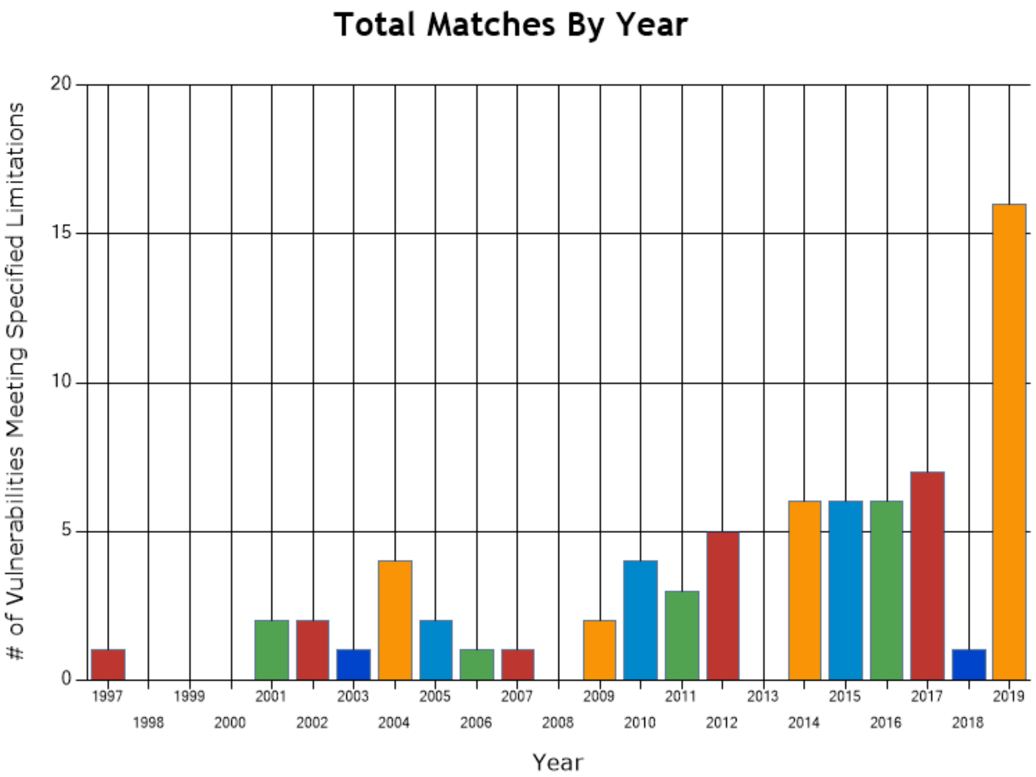
Figure 36. Breaches per pattern (n=2,013)

Cloud Based Email Servers

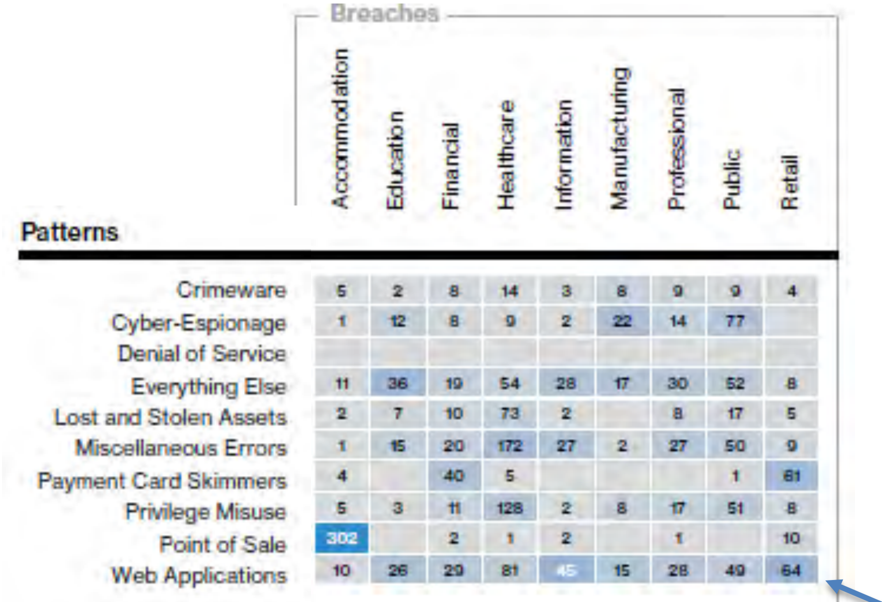
EXIM vulnerabilities

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

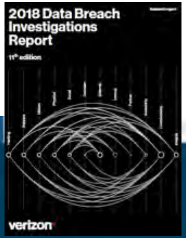


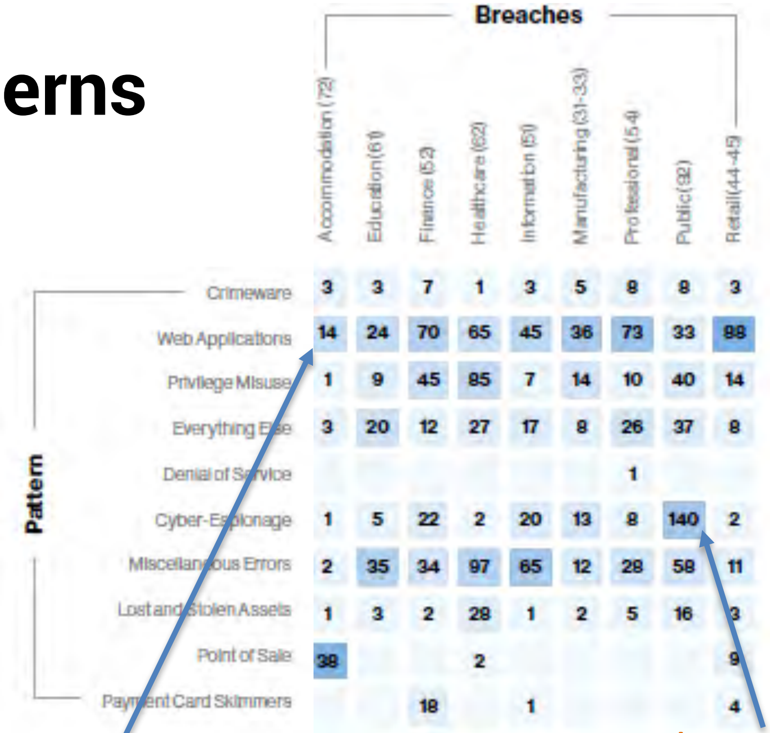
Industry Comparison - Patterns



Breaches

Patterns	Accommodation	Education	Financial	Healthcare	Information	Manufacturing	Professional	Public	Retail
Crimeware	5	2	8	14	3	8	9	9	4
Cyber-Espionage	1	12	8	9	2	22	14	77	
Denial of Service									
Everything Else	11	36	19	54	28	17	30	52	8
Lost and Stolen Assets	2	7	10	73	2		8	17	5
Miscellaneous Errors	1	15	20	172	27	2	27	50	9
Payment Card Skimmers	4		40	5				1	61
Privilege Misuse	5	3	11	128	2	8	17	51	8
Point of Sale	302		2	1	2		1		10
Web Applications	10	26	29	81	45	15	28	49	64



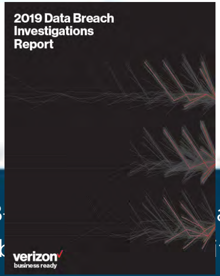


Breaches

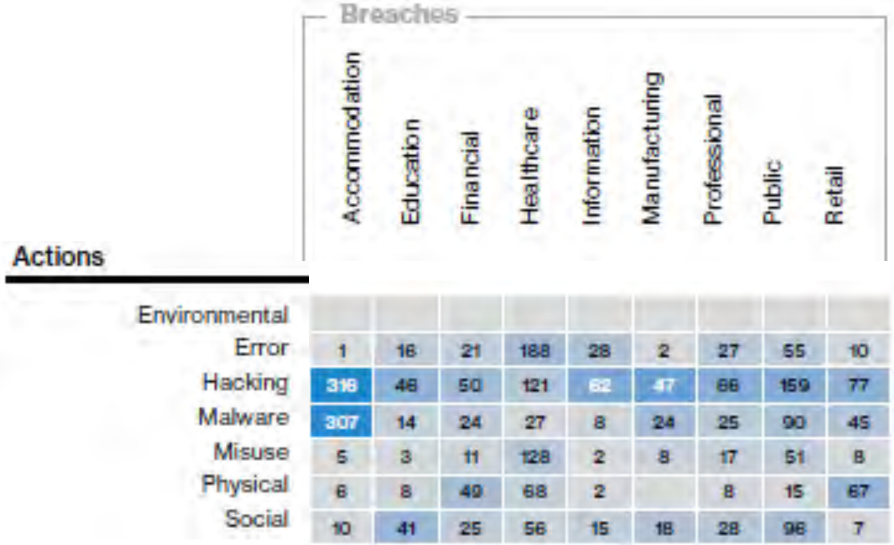
Pattern	Accommodation (72)	Education (61)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Professional (54)	Public (92)	Retail (44-45)
Crimeware	3	3	7	1	3	5	8	8	3
Web Applications	14	24	70	65	45	36	73	33	88
Privilege Misuse	1	9	45	85	7	14	10	40	14
Everything Else	3	20	12	27	17	8	26	37	8
Denial of Service							1		
Cyber-Espionage	1	5	22	2	20	13	8	140	2
Miscellaneous Errors	2	35	34	97	65	12	28	58	11
Lost and Stolen Assets	1	3	2	28	1	2	5	16	3
Point of Sale	38			2					9
Payment Card Skimmers			18		1				4

Web App

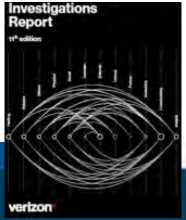
Increase Cyber Espionage

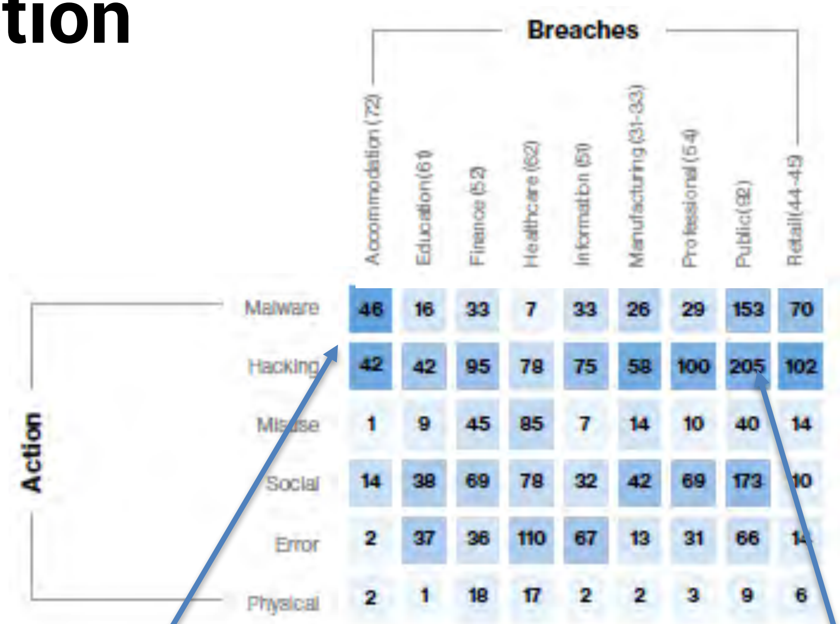


Industry Comparison - Action



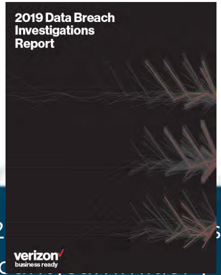
Actions	Accommodation	Education	Financial	Healthcare	Information	Manufacturing	Professional	Public	Retail
Environmental									
Error	1	16	21	188	28	2	27	55	10
Hacking	316	46	50	121	62	47	66	159	77
Malware	307	14	24	27	8	24	25	90	45
Misuse	5	3	11	128	2	8	17	51	8
Physical	6	8	49	68	2		8	15	67
Social	10	41	25	56	15	18	28	96	7





Action	Accommodation (72)	Education (61)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Professional (54)	Public (92)	Retail (44-45)
Malware	46	16	33	7	33	26	29	153	70
Hacking	42	42	95	78	75	58	100	205	102
Misuse	1	9	45	85	7	14	10	40	14
Social	14	38	69	78	32	42	69	173	10
Error	2	37	36	110	67	13	31	66	14
Physical	2	1	18	17	2	2	3	9	6

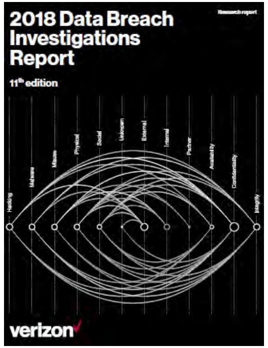
Drop in Accommodation



Increase Public

Mobile

There is evidence that some actors are expanding from traditional user devices and beginning to target mobile



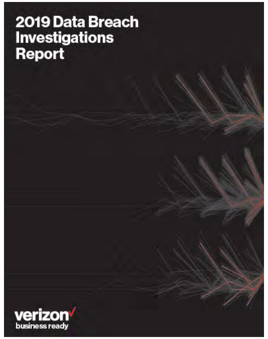
Research report

2018 Data Breach Investigations Report

11th edition

verizon

Research points to users being significantly
more susceptible to social attacks they
receive on mobile devices.



2019 Data Breach Investigations Report

verizon
business ready

Financially-Motivated Social Engineering (FMSE)

- Financial Pretextir
- Phishing Attacks

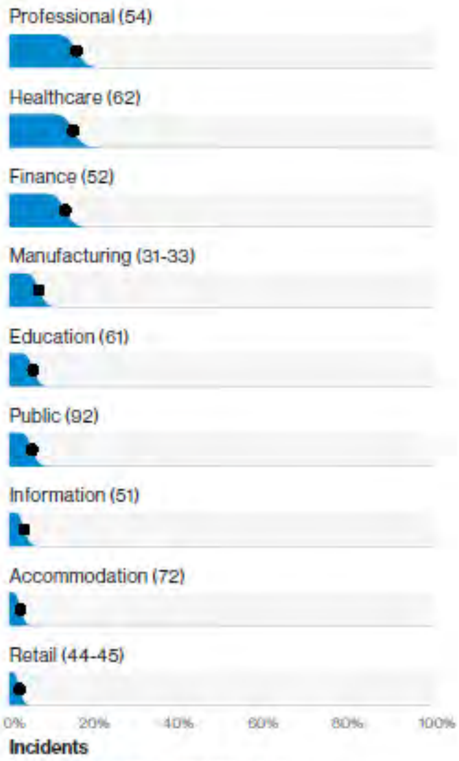


Figure 40. FMSE incidents by industry (n=370)

Is the Phishing Training working

2017 Data Breach Investigations Report

10th Edition

verizon

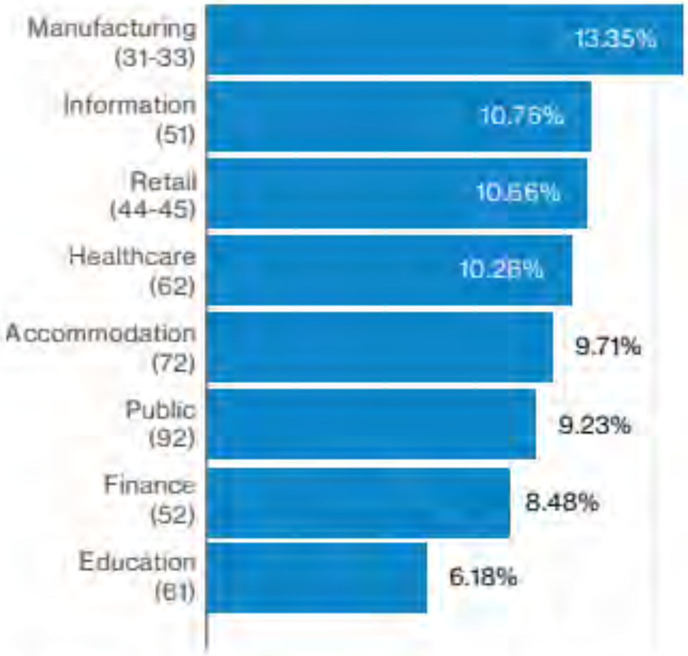


Figure 12: Median click rate per campaign by industry (n=1,58

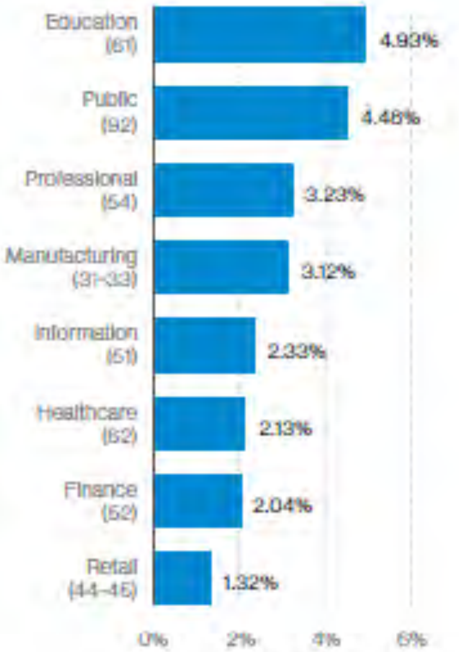
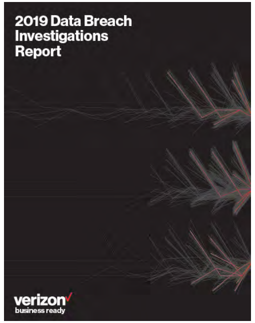


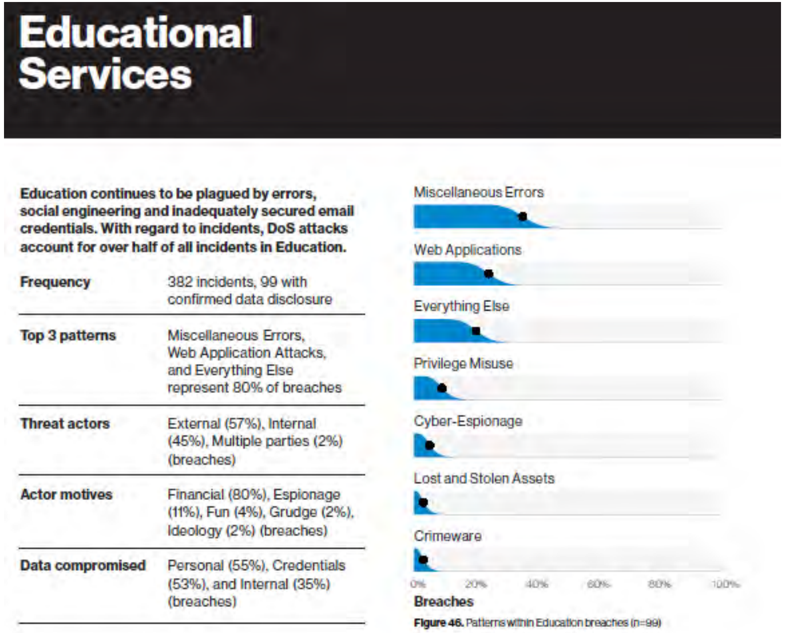
Figure 41. Click rate in phishing tests by industry



2019 Data Breach Investigations Report

verizon business ready

Industry Specific Sections

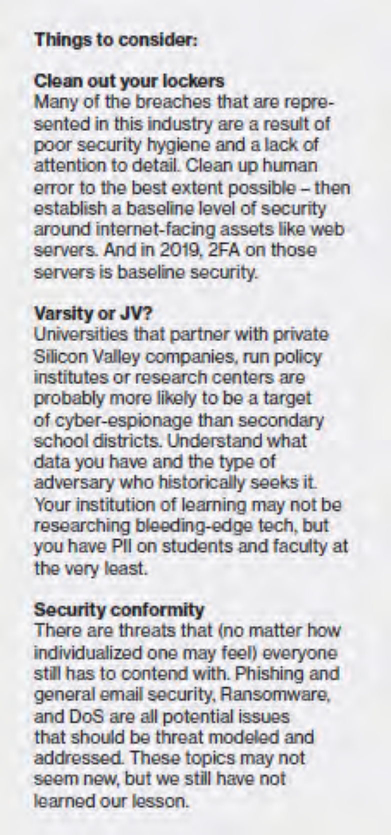


Educational Services

Education continues to be plagued by errors, social engineering and inadequately secured email credentials. With regard to incidents, DoS attacks account for over half of all incidents in Education.

Frequency	382 incidents, 99 with confirmed data disclosure
Top 3 patterns	Miscellaneous Errors, Web Application Attacks, and Everything Else represent 80% of breaches
Threat actors	External (57%), Internal (45%), Multiple parties (2%) (breaches)
Actor motives	Financial (80%), Espionage (11%), Fun (4%), Grudge (2%), Ideology (2%) (breaches)
Data compromised	Personal (55%), Credentials (53%), and Internal (35%) (breaches)

Figure 46. Patterns within Education breaches (n=99)



Things to consider:

Clean out your lockers
Many of the breaches that are represented in this industry are a result of poor security hygiene and a lack of attention to detail. Clean up human error to the best extent possible – then establish a baseline level of security around internet-facing assets like web servers. And in 2019, 2FA on those servers is baseline security.

Varsity or JV?
Universities that partner with private Silicon Valley companies, run policy institutes or research centers are probably more likely to be a target of cyber-espionage than secondary school districts. Understand what data you have and the type of adversary who historically seeks it. Your institution of learning may not be researching bleeding-edge tech, but you have PII on students and faculty at the very least.

Security conformity
There are threats that (no matter how individualized one may feel) everyone still has to contend with. Phishing and general email security, Ransomware, and DoS are all potential issues that should be threat modeled and addressed. These topics may not seem new, but we still have not learned our lesson.

Summary

- Web Attacks
- Cloud Based Email Servers
- Privilege Misuse
- FMSE
- Miscellaneous Errors
- Detection is Still slow
- Phishing may be decreasing