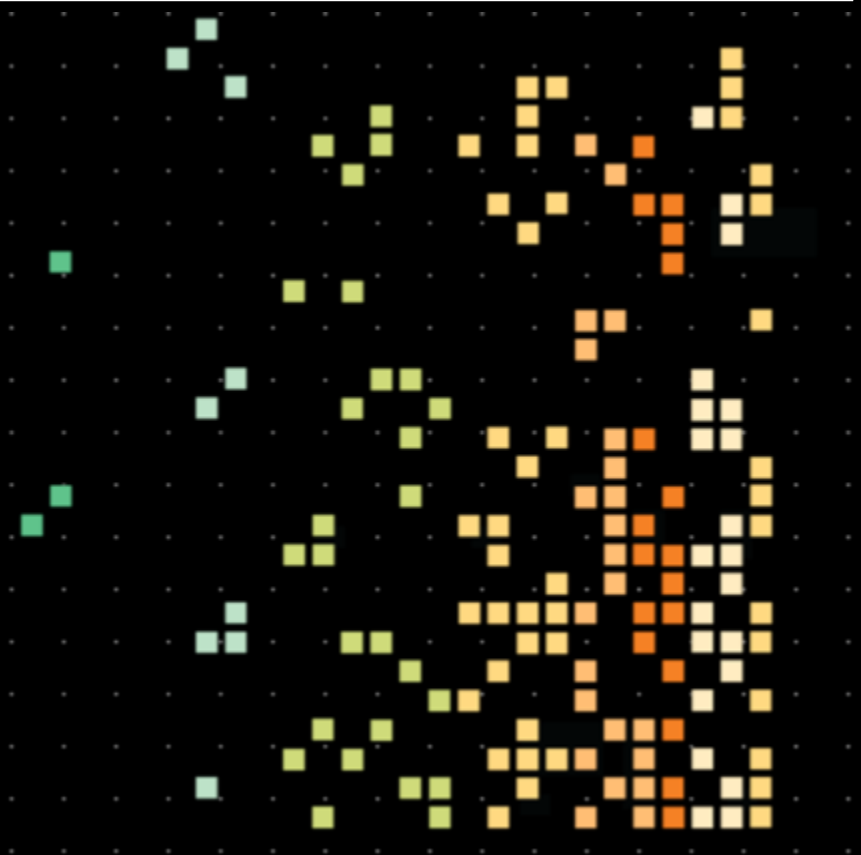
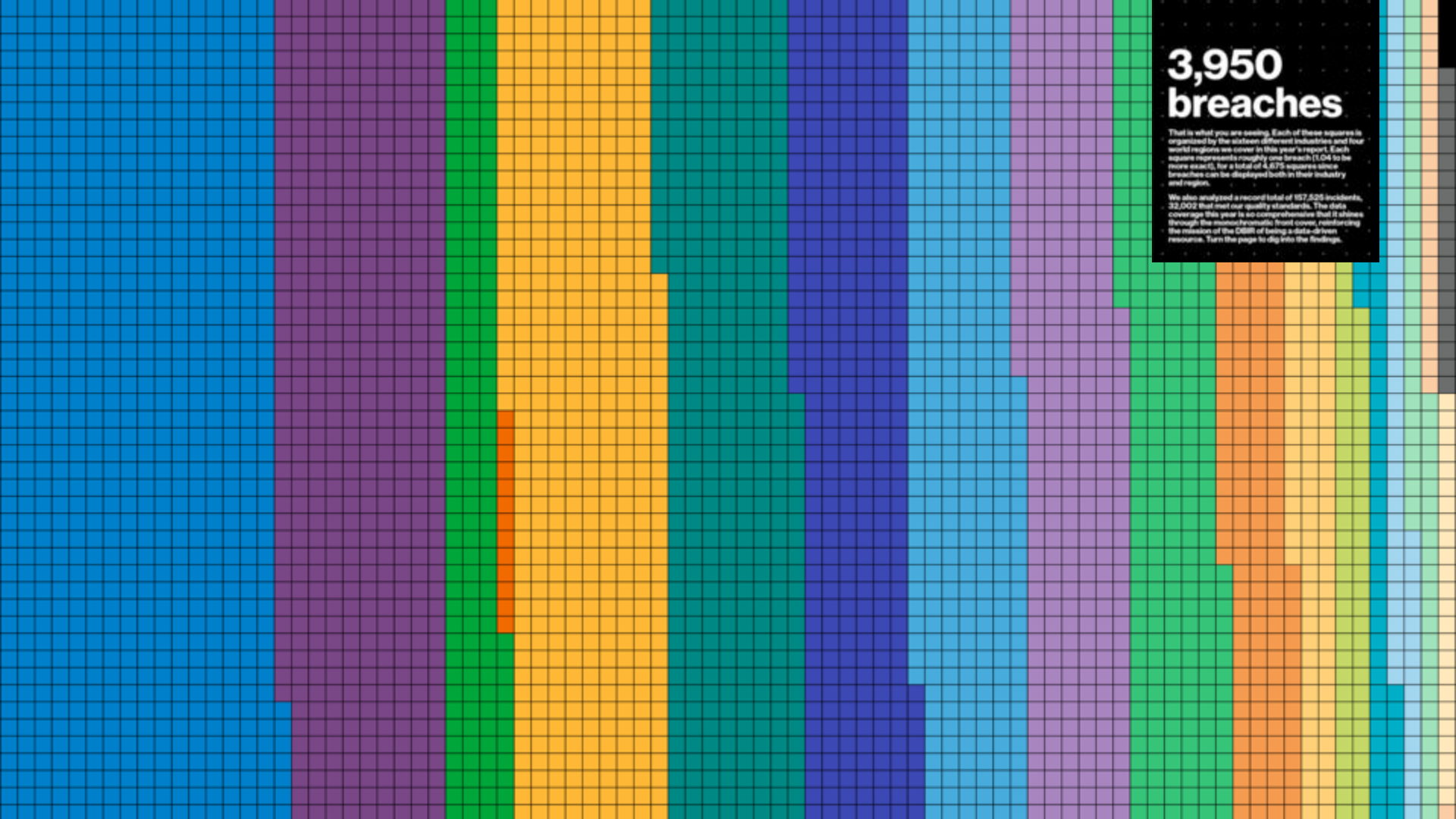
2020 Data Breach Investigations Report



Philippe Langlois
DBIR Author
Philippe.Langlois@Verizon.com

verizon business ready


3,950
breaches
That is what you are seeing. Each of these squares is organized by the sixteen different industries and four world regions we cover in this year's report. Each square represents roughly one breach (1.04 to be more exact), for a total of 4,675 squares since breaches can be displayed both in their industry and region.
We also analyzed a record total of 157,525 incidents, 32,002 that met our quality standards. The data coverage this year is so comprehensive that it shines through the monochromatic frame, reinforcing the mission of the DBIR of being a data-driven resource. Turn the page to dig into the findings.

Proprietary Statement

This document and any attached materials are the sole property of Verizon and are not to be used by you other than to evaluate Verizon's service.

This document and any attached materials are not to be disseminated, distributed or otherwise conveyed throughout your organization to employees without a need for this information or to any third parties without the express written permission of Verizon.

DBIR Authors

What's New - 2020 DBIR in numbers

Figure 6. Select Action varieties over time

13 years

81 countries

81 contributors

32,002 incidents

3,950 data breaches

What's New– Increase in vertical coverage

Industry vertical segments

- Accommodation and Food Services (NAICS 72)
- Arts, Entertainment and Recreation (NAICS 71)
- Construction (NAICS 23)
- Educational Services (NAICS 61)
- Financial and Insurance (NAICS 52)
- Healthcare (NAICS 62)
- Information (NAICS 51)
- Manufacturing (NAICS 31-33)
- Mining, Quarrying, Oil & Gas Extraction + Utilities (NAICS 21 + NAICS 22)
- Other Services (NAICS 81)
- Professional, Scientific, and Technical Services (NAICS 54)
- Public Administration (NAICS 92)
- Real Estate and Rental and Leasing (NAICS 53)
- Retail (NAICS 44-45)
- Transportation and Warehousing (NAICS 48-49)

Regional segments

- Northern America (NA)
- Europe, Middle East and Africa (EMEA)
- Asia Pacific (APAC)
- Latin America and The Caribbean (LAC)

SMB focused segment

- Comparing and contrasting with breaches on large companies

Map of external standards into VERIS

- MITRE ATT&CK Framework
- CIS Critical Security Controls (CSC)

Key Insights - Incidents | Breaches per Pattern

In 2020 report, **85% of security incidents and 78% of confirmed data breaches** continue to fall into the 2014 patterns.

Growth of Phishing-based incidents has been responsible for the growth of the “Everything Else” pattern

Figure 46. Patterns in breaches (n=3,950)

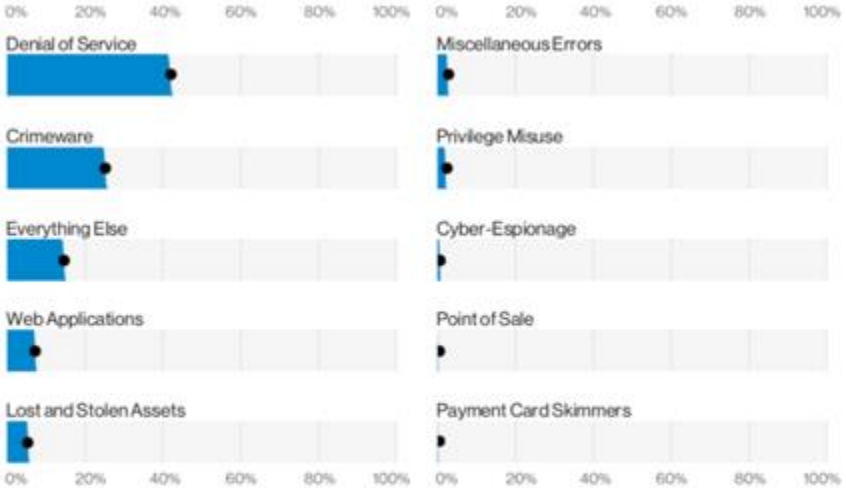


Figure 47. Patterns in incidents (n=32,002)

Key Insights – The times, they aren't a'changing

Credential theft, social attacks (i.e., phishing and business email compromise), and errors cause the majority of breaches (67% or more).

DBIR data continues to show that external actors are—and always have been—more common. In fact, 70% of breaches this year were caused by outsiders.

Espionage gets the headlines but accounts for just 10% of breaches in this year's data. The majority (86% of breaches) continue to be financially motivated. Advanced threats—which also get lots of buzz—represent only 4% of breaches.

Figure 7. Actors over time in breaches

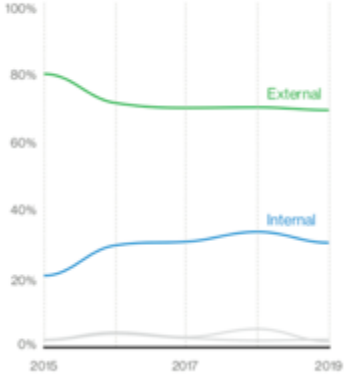
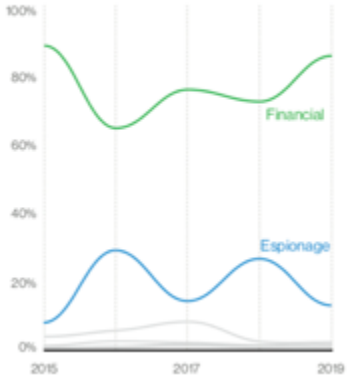


Figure 8. Actor motive over time in breaches



Key Insights – Do as I say, not as I do

This year's DBIR saw a high number of internal error-related breaches (881, versus last year's 424).

This increase is likely due to improved reporting (6x increase on Security Research disclosure from 2019) not insiders making more frequent mistakes.

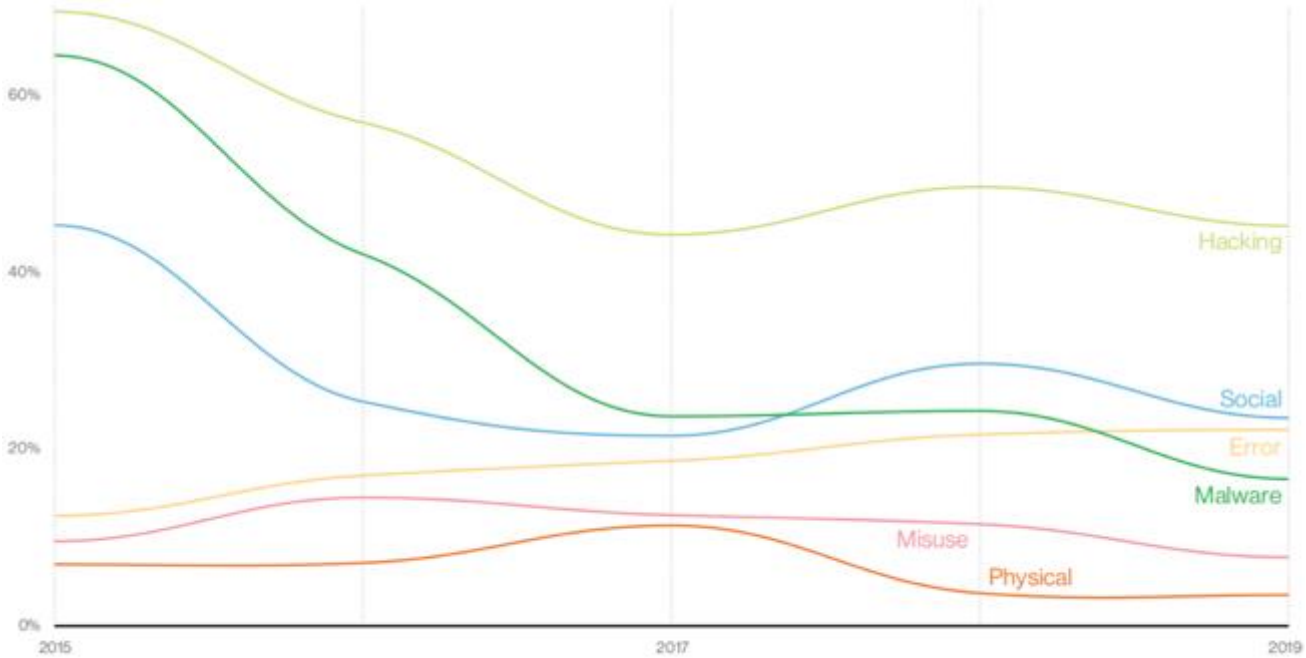


Figure 11. Actions over time in breaches

Key Insights – Up close and personal data

Personal data is getting swiped more often—or those thefts are being reported more often due to disclosure regulations.

Personal data was involved in 58% of breaches, nearly twice the percentage in last year's data. This includes email addresses, names, phone numbers, physical addresses and other types of data that one might find hiding in an email or stored in a misconfigured database.

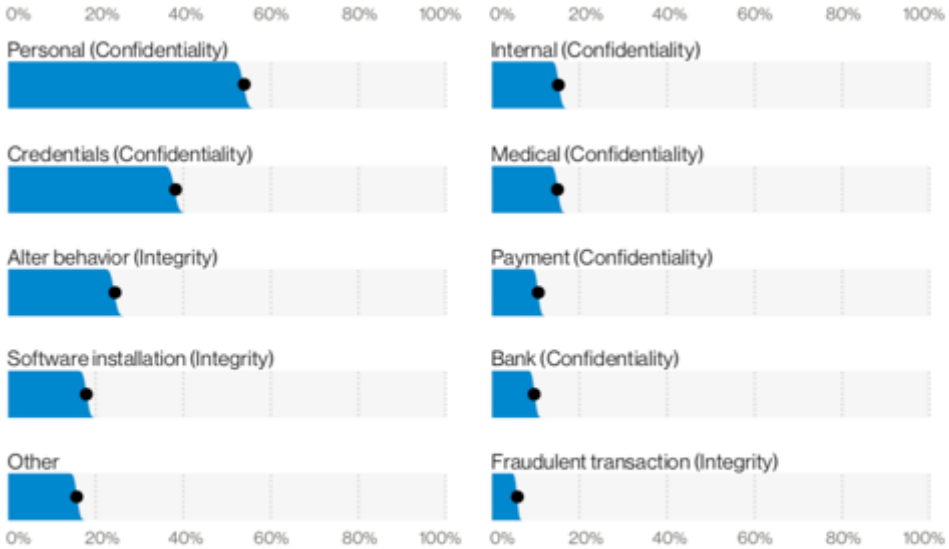


Figure 37. Top compromised Attribute varieties in breaches (n = 3,667)

Key Insights

Ransomware is everywhere.

Ransomware now accounts for 27% of malware incidents, and 18% of organizations blocked at least one piece of ransomware. No organization can afford to ignore it.

Figure 16. Top Malware varieties in breaches (n=506)

Oh, what a tangled web application.

Attacks on web apps were a part of 43% of breaches, more than double the results from last year. As workflows move to cloud services, it makes sense for attackers to follow.

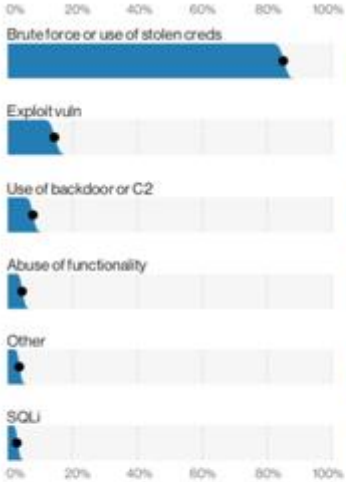


Figure 20. Top Hacking varieties in breaches (n=868)

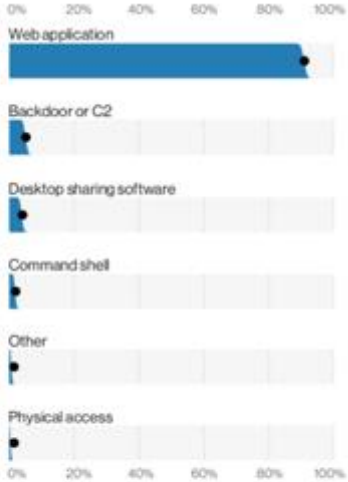


Figure 21. Top Hacking vectors in breaches (n=1,361)

verizon business ready

Key Insights – Good news? In my infosec?

Block party

Security tools are getting better at blocking common malware.

The DBIR data shows that Trojan-type malware peaked at just under 50% of all breaches in 2016 and has since dropped to just 6.5%.

Malware sampling indicates that 45% of malware is either droppers, backdoors or keyloggers. Although this kind of threat is still plentiful, much of it is being blocked successfully.

Patch things up

Less than 5% of breaches involved exploitation of a vulnerability and only 2.5% of security information and event management (SIEM) events involved exploiting a vulnerability.
This finding suggests that most organizations are doing a good job at patching—so keep it up.

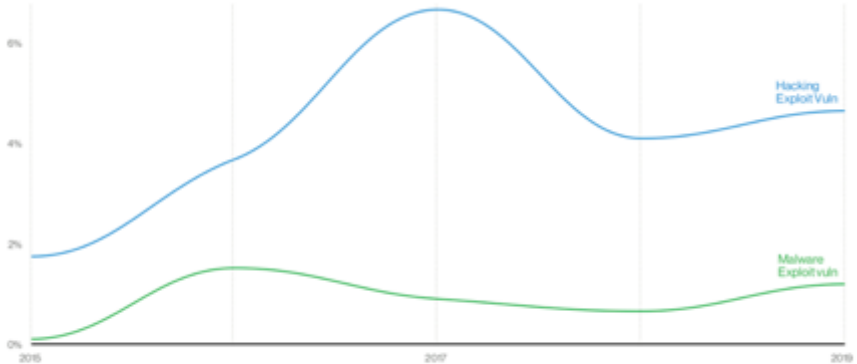
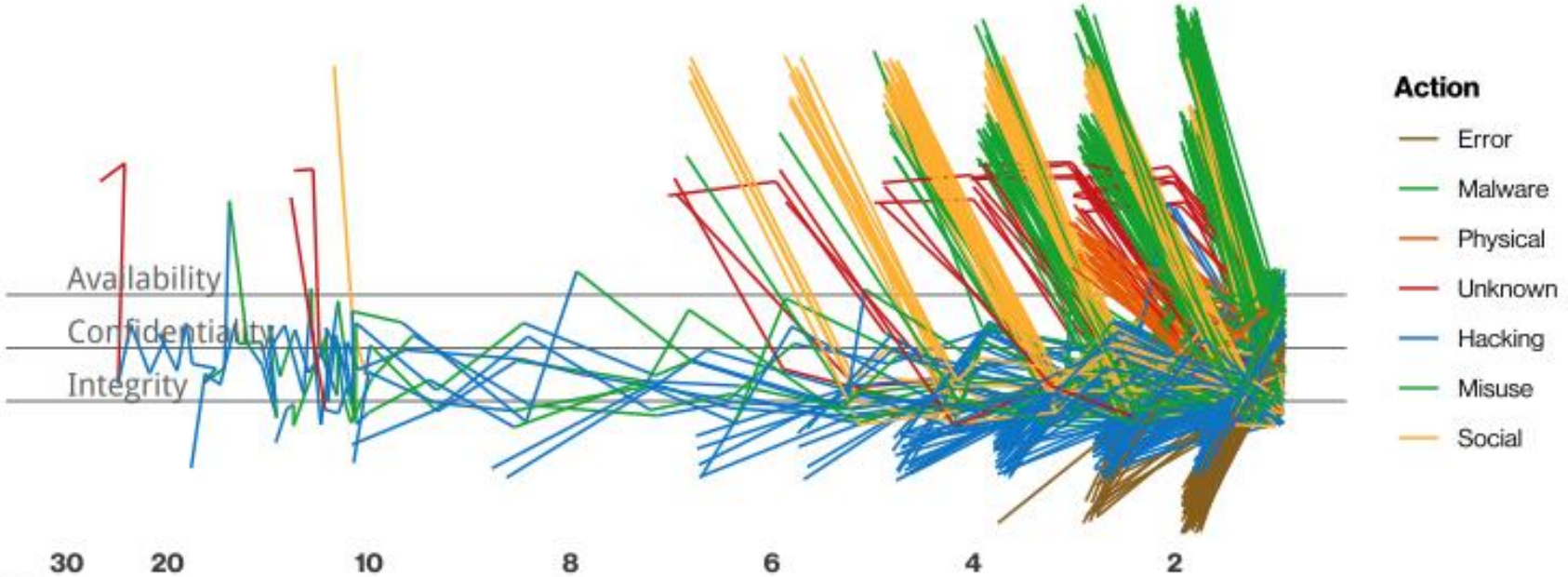


Figure 25. Vulnerability exploitation over time in breaches

Key Insights – Path-based Attacks



4bffaeee. Attack paths in incidents (n = 652. Two breaches, 77 & 391 steps respectively, not shown.)

Key Insights – Path-based Attacks

Most of the successful attacks are short, likely because it is both cheaper and easier for the attacker (or the breach is simply due to a single error) … and more successful.

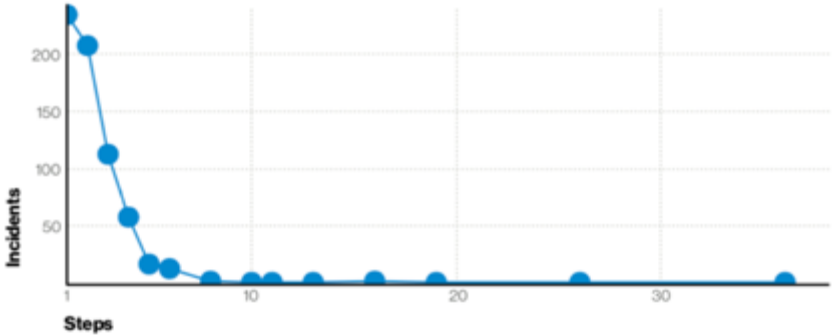


Figure 41. Number of steps per incident, n=654. (Two breaches, 77 & 391 steps respectively, not shown.)

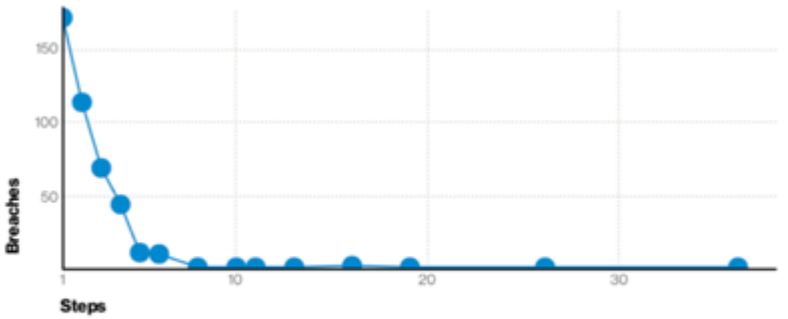
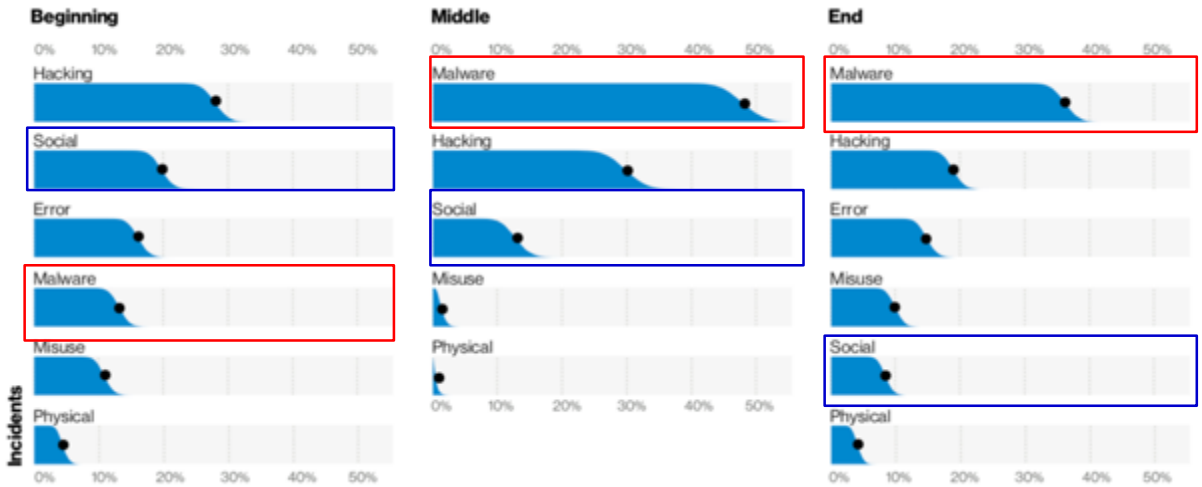


Figure 42. Number of steps per breach, n=429. (Two breaches, 77 & 391 steps respectively, not shown.)

Key Insights – Path-based Attacks

For attack paths, the 'malware' threat action variety usually doesn't begin a breach (it is normally a second or later step on the compromise).

Also, breaches rarely end with a 'social' action, (so if you see a social attack, you can expect more to follow).



Industry vertical segments

- Accommodation and Food Services (NAICS 72)
- Arts, Entertainment and Recreation (NAICS 71)
- Construction (NAICS 23)
- **Educational Services (NAICS 61)**
- **Financial and Insurance (NAICS 52)**
- **Healthcare (NAICS 62)**
- Information (NAICS 51)
- Manufacturing (NAICS 31-33)
- Mining, Quarrying, Oil & Gas Extraction + Utilities (NAICS 21 + NAICS 22)
- Other Services (NAICS 81)
- Professional, Scientific, and Technical Services (NAICS 54)
- **Public Administration (NAICS 92)**
- Real Estate and Rental and Leasing (NAICS 53)
- **Retail (NAICS 44-45)**
- Transportation and Warehousing (NAICS 48-49)

Educational Services

This industry saw phishing attacks in 28% of breaches and hacking via stolen credentials in 23% of breaches. In incident data, Ransomware accounts for approximately 80% of Malware infections in this vertical. Education Services performed poorly in terms of reporting phishing attacks, thus losing critical response time for the victim organizations.

Frequency	819 incidents, 228 with confirmed data disclosure
Top Patterns	Everything Else, Miscellaneous Errors and Web Applications represent 81% of breaches
Threat Actors	External (67%), Internal (33%), Partner (1%), Multiple (1%) (breaches
Actor Motives	Financial (92%), Fun (5%), Convenience (3%), Espionage (3%), Secondary (2%) (breaches)
Data Compromised	Personal (75%), Credentials (30%), Other (23%), Internal (13%) (breaches)
Top Controls	Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12), Secure Configurations (CSC 5, CSC 11)

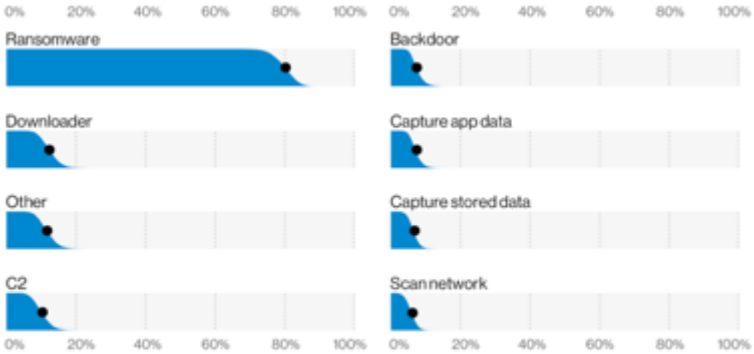


Figure 92. Top Malware varieties in Education Industry incidents (n=129)

Financial and Insurance

The attacks in this sector are perpetrated by external actors who are financially motivated to get easily monetized data (63%), internal financially motivated actors (18%), and internal actors committing errors (9%). Web application attacks that leverage the use of stolen credentials also continue to affect this industry. Breaches caused by internal actors have shifted from malicious actions to benign errors, although both are still damaging.

Frequency	1,509 incidents, 448 with confirmed data disclosure
Top Patterns	Web Applications, Miscellaneous Errors and Everything Else represent 81% of breaches
Threat Actors	External (64%), Internal (35%), Partner (2%), Multiple (1%) (breaches)
Actor Motives	Financial (91%), Espionage (3%), Grudge (3%) (breaches)
Data Compromised	Personal (77%), Other (35%), Credentials (35%), Bank (32%) (breaches)
Top Controls	Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12), Secure Configurations (CSC 5, CSC 11)

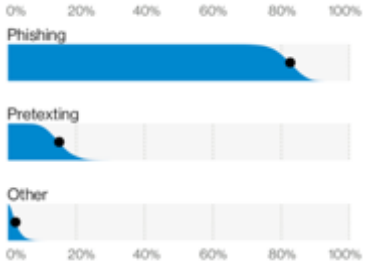


Figure 79. Social variety in Finance and Insurance industry breaches (n=86)

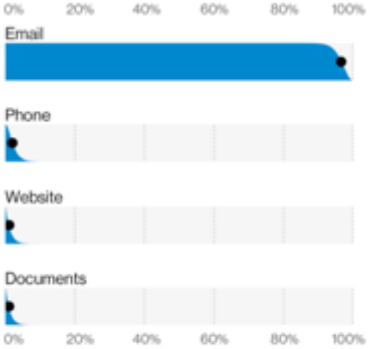


Figure 80. Social vector in Finance and Insurance industry breaches (n=86)

Healthcare

Financially motivated criminal groups continue to target this industry via ransomware attacks. Lost and stolen assets also remain a problem in our incident data set. Basic human error is alive and well in this vertical. Misdelivery grabbed the top spot among error action types, while internal Misuse has decreased.

Frequency	798 incidents, 521 with confirmed data disclosure
Top Patterns	Miscellaneous Errors, Web Applications and Everything Else represent 72% of breaches
Threat Actors	External (51%), Internal (48%), Partner (2%), Multiple (1%) (breaches)
Actor Motives	Financial (88%), Fun (4%), Convenience (3%) (breaches)
Data Compromised	Personal (77%), Medical (67%), Other (18%), Credentials (18%) (breaches)
Top Controls	Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12), Data Protection (CSC 13)

Figure 94. Patterns in Healthcare Industry breaches (n=521)

Public Administration

Ransomware is a large problem for this sector, with financially motivated attackers utilizing it to target a wide array of government entities. Misdelivery and Misconfiguration errors also persist in this sector.

Frequency	6,843 incidents, 346 with confirmed data disclosure
Top Patterns	Miscellaneous Errors, Web Applications and Everything Else represent 73% of breaches
Threat Actors	External (59%), Internal (43%), Multiple (2%), Partner (1%) (breaches)
Actor Motives	Financial (75%), Espionage (19%), Fun (3%) (breaches)
Data Compromised	Personal (51%), Other (34%), Credentials (33%), Internal (14%) (breaches)
Top Controls	Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12), Secure Configurations (CSC 5, CSC 11)

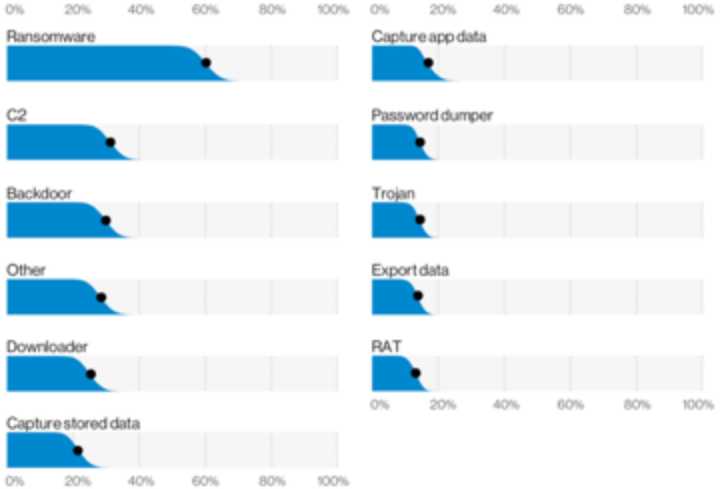


Figure 106. Top Malware variety in Public Administration incidents (n=198)

Retail

Attacks against e-commerce applications are by far the leading cause of breaches in this industry. As organizations continue to move their primary operations to the web, the criminals migrate along with them. Consequently, POS-related breaches, which were for many years the dominant concern for this vertical, continue at the low levels of 2019's DBIR. While Payment is a commonly lost data type, Personal and Credentials also continue to be highly sought after in this sector.

Frequency	287 incidents, 146 with confirmed data disclosure
Top Patterns	Web Applications, Everything Else and Miscellaneous Errors represent 72% of breaches
Threat Actors	External (75%), Internal (25%), Partner (1%), Multiple (1%) (breaches)
Actor Motives	Financial (99%), Espionage (1%) (breaches)
Data Compromised	Personal (49%), Payment (47%), Credentials (27%), Other (25%) (breaches)
Top Controls	Boundary Defense (CSC 12), Secure Configurations (CSC 5, CSC 11), Continuous Vulnerability Management (CSC3)

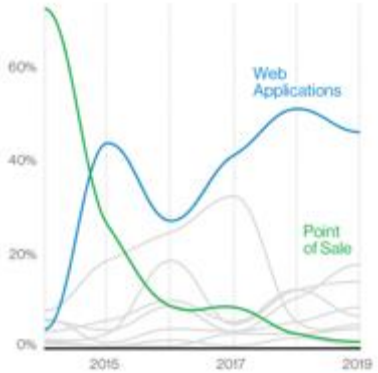


Figure 63. Patterns over time in Retail industry breaches

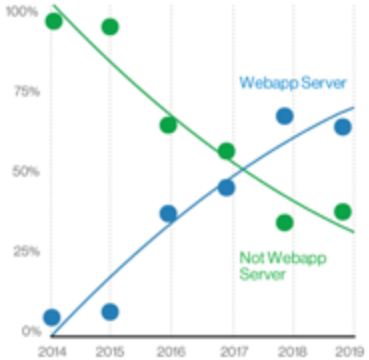


Figure 64. Webapp Server vs. Not Webapp Server assets in Retail Payment Data breaches over time

SMB vs Large Organizations

Summary

While differences between SMBs and large organizations remain, the movement toward the cloud and its myriad web-based tools, along with the continued rise of social attacks has narrowed the dividing line between the two. As SMBs have adjusted their business models, the criminals have adapted their actions in order to keep in step and select the quickest and easiest path to their victims.

	Small (less than 1,000 employees)	Large (more than 1,000 employees)
Frequency	407 incidents, 221 with confirmed data disclosure	8,666 incidents, 576 with confirmed data disclosure
Top Patterns	Web Applications, Everything Else and Miscellaneous Errors represent 70% of breaches	Everything Else, Crimeware and Privilege Misuse represent 70% of breaches
Threat Actors	External (74%), Internal (26%), Partner (1%), Multiple (1%) (breaches)	External (79%), Internal (21%), Partner (1%), Multiple (1%) (breaches)
Actor Motives	Financial (83%), Espionage (8%), Fun (3%), Grudge (3%) (breaches)	Financial (79%), Espionage (14%), Fun (2%), Grudge (2%) (breaches)
Data compromised	Credentials (52%), Personal (30%), Other (20%), Internal (14%), Medical (14%) breaches	Credentials (64%), Other (26%), Personal (19%), Internal (12%) (breaches)

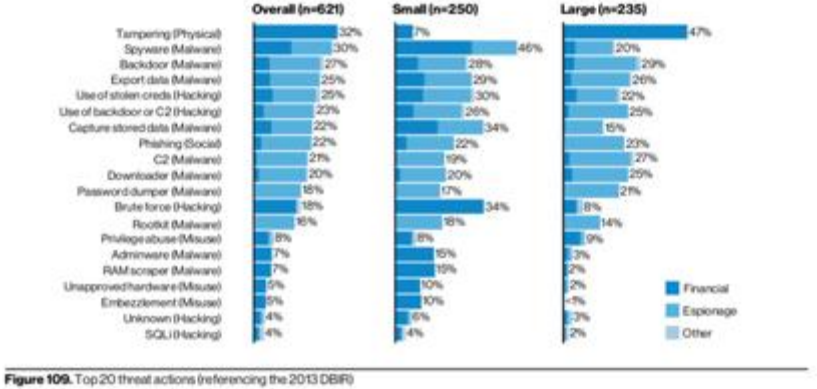


Figure 109. Top 20 threat actions (referencing the 2013 DBIR)

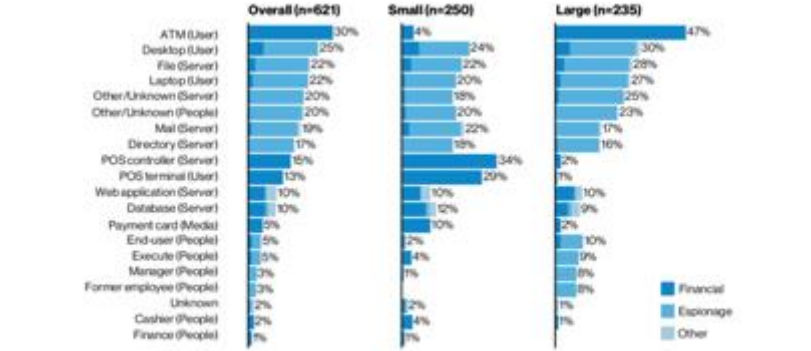


Figure 112. Variety of compromised assets (referencing the 2013 DBIR)

COVID-Update

- Carelessness, limited staffing and rush to adopting new technologies and processes may result in an increase error based breaches
- Phishing and stolen credentials will continue as organizations are moved to SaaS applications
- Ransomware likely to rise as criminals are embracing new techniques and tactics to monetize their access

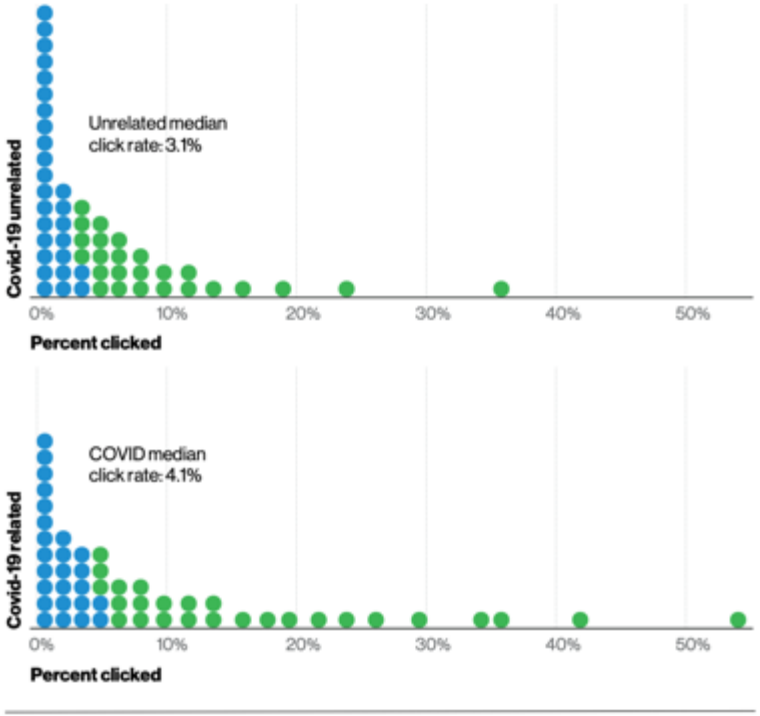


Figure 2. Proportion clicked in simulated phishing tests.
(Each dot represents 2% of organizations.)

What's New – VERIS Common Attack Framework (VCAF)

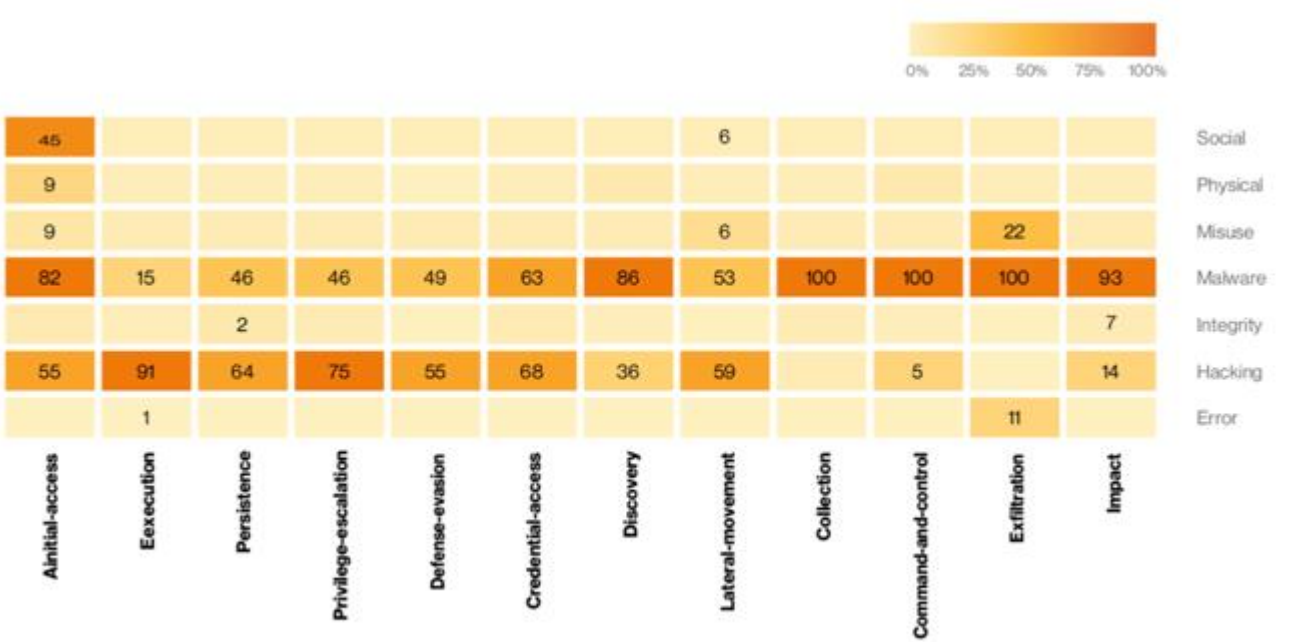


Figure 140. Percentage of MITRE Techniques covered by VERIS

What's New – CIS Control Recommendations

CIS Critical Security Controls

CIS Control 1	Inventory and Control of Hardware Assets
CIS Control 2	Inventory and Control of Software Assets
CIS Control 3	Continuous Vulnerability Management
CIS Control 4	Controlled Use of Administrative Privileges
CIS Control 5	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
CIS Control 6	Maintenance, Monitoring and Analysis of Audit Logs
CIS Control 7	Email and Web Browser Protections
CIS Control 8	Malware Defenses
CIS Control 9	Limitation and Control of Network Ports, Protocol and Services
CIS Control 10	Data Recovery Capabilities
CIS Control 11	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
CIS Control 12	Boundary Defense
CIS Control 13	Data Protection
CIS Control 14	Controlled Access Based on the Need to Know
CIS Control 15	Wireless Access Control
CIS Control 16	Account Monitoring and Control
CIS Control 17	Implement a Security Awareness and Training Program
CIS Control 18	Application Software Security
CIS Control 19	Incident Response and Management
CIS Control 20	Penetration Tests and Red Team Exercises

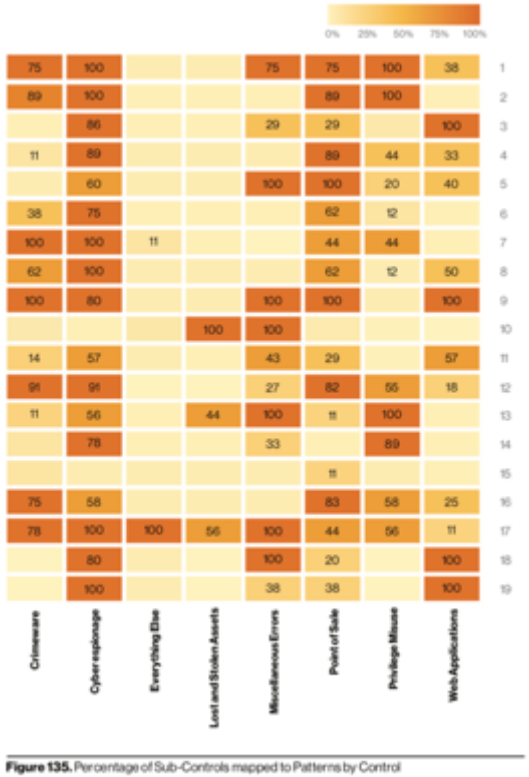


Figure 135. Percentage of Sub-Controls mapped to Patterns by Control

Key Insights – Controls to prioritize

Continuous Vulnerability Management (CSC 3)

A great way of finding and remediating things like code-based vulnerabilities, such as the ones found in web applications that are being exploited and also handy for finding misconfigurations

Secure Configurations (CSC 5, CSC 11)[53]

Ensure and verify that systems are configured with only the services and access needed to achieve their function. That open, world-readable database facing the internet is probably not following these controls.

Email and Web Browser Protection (CSC 7)

Being that browsers and email clients are the main way that users interact with the Wild West that we call the internet, it is critical that you lock these down to give your users a fighting chance.

Limitation and Control of Network Ports, Protocols and Services (CSC 9)

Much like how Control 12 is about knowing your exposures between trust zones, this control is about understanding what services and ports should be exposed on a system and limiting access to them.

Boundary Protection (CSC 12)

Not just firewalls, this Control includes things like network monitoring, proxies and multi-factor authentication, which is why it creeps up into a lot of different actions.

Data Protection (CSC 13)

One of the best ways of limiting the leakage of information is to control access to that sensitive information. Controls in this list include maintaining an inventory of sensitive information, encrypting sensitive data and limiting access to authorized cloud and email providers.

Account Monitoring (CSC 16)

Locking down user accounts across the organization is key to keeping bad guys from using stolen credentials, especially by the use of practices like multi-factor authentication which also shows up here

Implement a Security Awareness and Training Program (CSC 17)

Educate your users, both on malicious attacks and the accidental breaches