Know your enemy

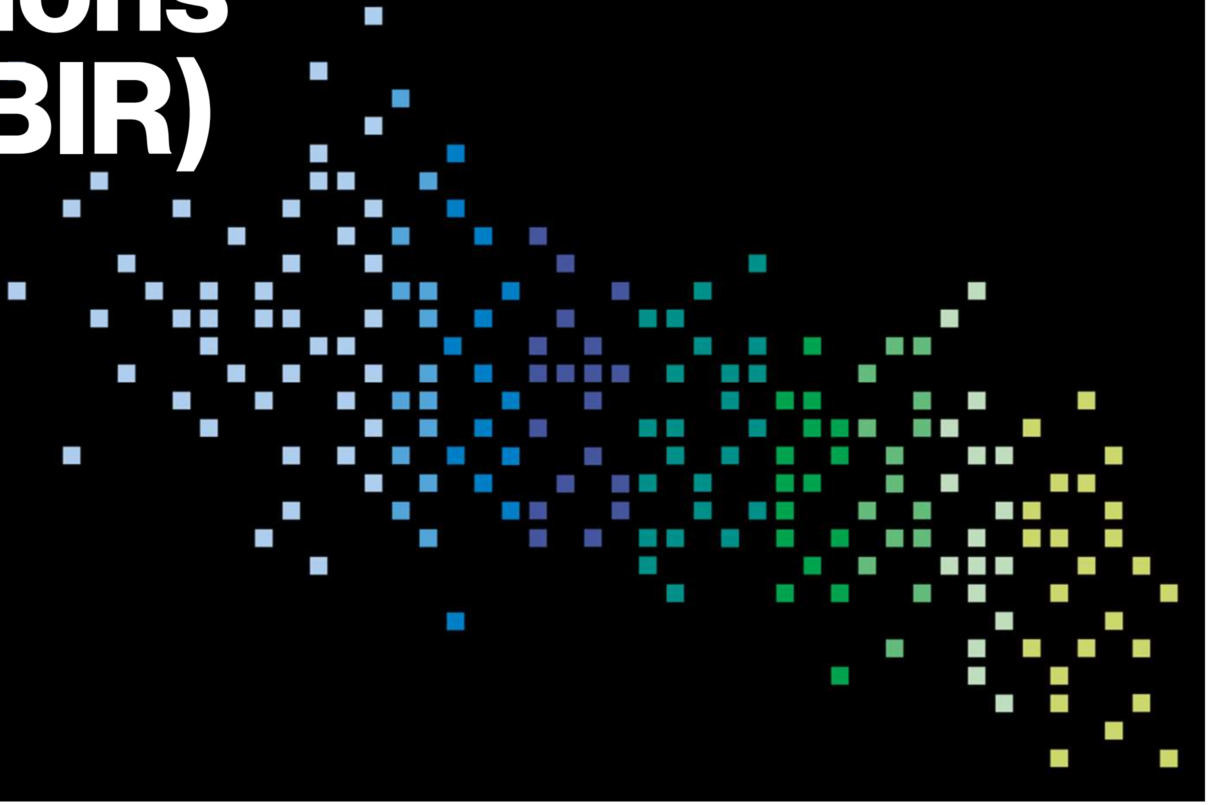
Sun Tzu 544 – 496 BC

“If you know the enemy and know yourself, you need not fear the results of hundred battles.”

.

2020

Data Breach Investigations Report (DBIR)



verizon

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.

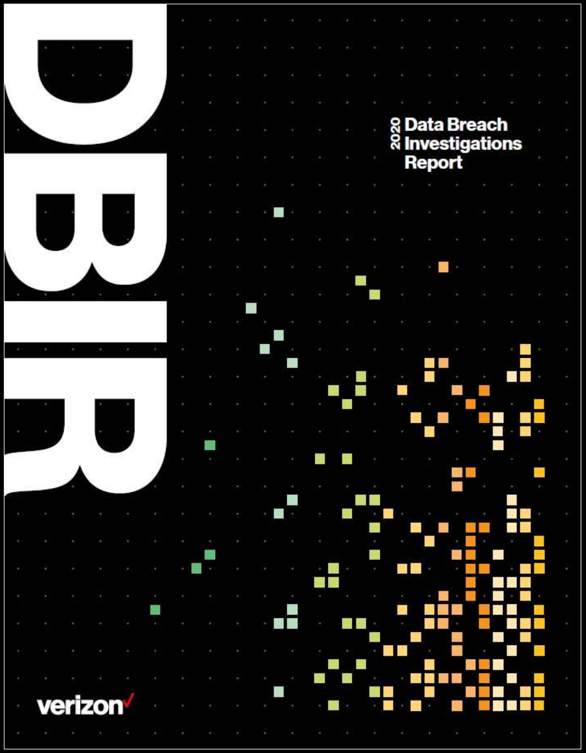
This document and any attached materials are not to be disseminated, distributed or otherwise conveyed throughout your organization to employees without a need for this information or to any third parties without the express written permission of Verizon.

Agenda

1. What’s new?
2. Key insights
3. Industries
4. Regions and size
5. Controls
6. Q&A

What's new?

2020 Data Breach Investigations Report



- 13 years
- 81 countries
- 81 contributors
- 32,002 incidents
- 3,950 data breaches

verizon

Contributing organizations (n=81)

MOSSADAMS
Akamai
CROWDSTRIKE
EMERGENCE
apura
LARES
WatchGuard
SecurityTrails
SHODAN
S21sec
Malicious Streams
CERT-EU
Mishcon de Reya
VICTORIA
BITSIGHT
paloalto networks
RAPID7
CIS Center for Internet Security
Qualys
CyberSecurity MALAYSIA
An agency under MOSTI
GREYNOISE
AFP
CHUBB
zscaler
swisscom
VESTIGE Digital Investigations
SHADOWSERVER
KASPERSKY lab
ICSA labs
edgescan
bit-x-bit
IRISS
TALOS INCIDENT RESPONSE
proofpoint. Security Awareness Training
Elevate Security
PALADION
VMRAY
MWR an F-Secure company
digital shadows_
KnowBe4 Human error. Conquered.
FS-ISAC
ATTACKIQ
VCDB
TETRA DEFENSE
NETSCOUT
SISAP Sistemas Aplicativos
DELL
NASK CERT.PL>_
CIRCL Computer Incident Response Center Luxembourg
HSC
mnemonic
DRAGOS
NetDiligence
wandera
CISA
tripwire
BeyondTrust
MICRO FOCUS
JPCERT CC
Coalition
Carnegie Mellon University Software Engineering Institute
PARAFLARE
Recorded Future
NCCIC
LMG SECURITY
BIT DISCOVERY
Check Point SOFTWARE TECHNOLOGIES LTD
HPI Hasso Plattner Institut
DFDR CONSULTING

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 and 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

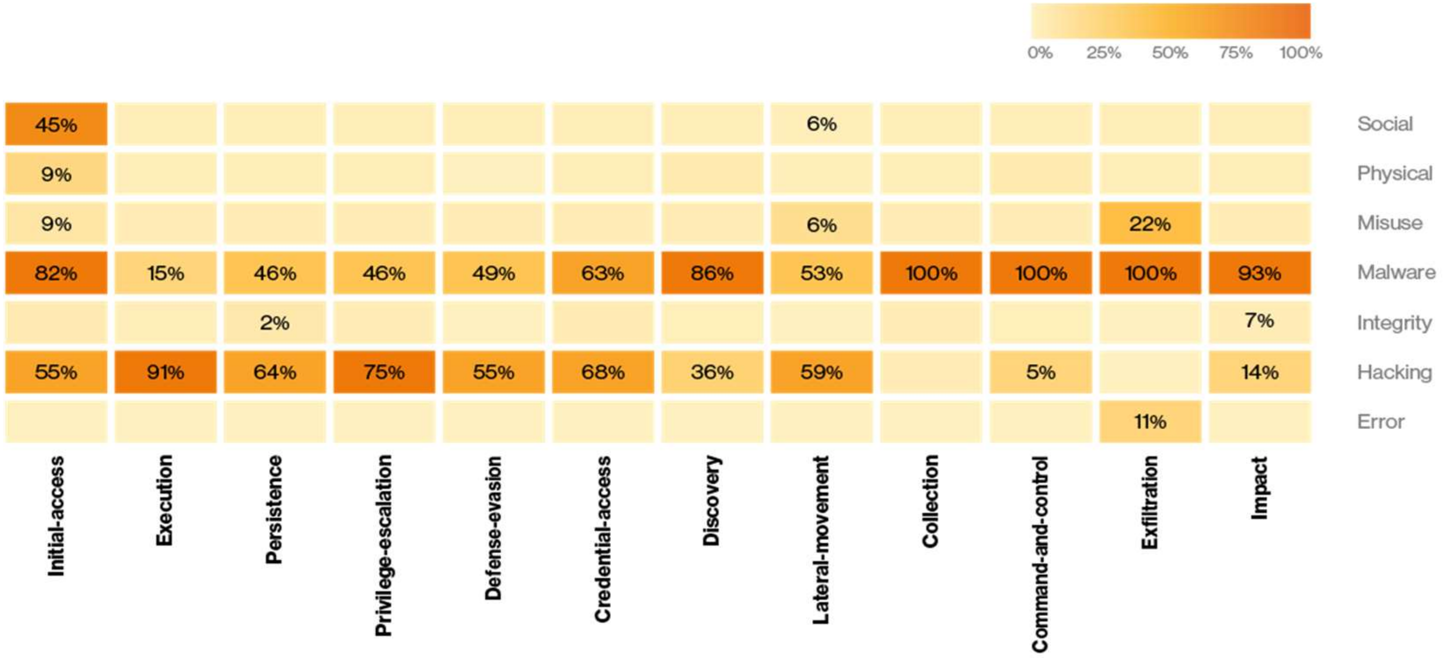
Comparing and contrasting with breaches on large companies

Map of external standards into VERIS

- MITRE ATT&CK® Framework
- Center for Internet Security Critical Security Controls (CIS CSCs)

What's new

VERIS Common Attack Framework (VCAF)



	Initial-access	Execution	Persistence	Privilege-escalation	Defense-evasion	Credential-access	Discovery	Lateral-movement	Collection	Command-and-control	Exfiltration	Impact
Social	45%							6%				
Physical	9%											
Misuse	9%							6%			22%	
Malware	82%	15%	46%	46%	49%	63%	86%	53%	100%	100%	100%	93%
Integrity			2%									7%
Hacking	55%	91%	64%	75%	55%	68%	36%	59%		5%		14%
Error											11%	

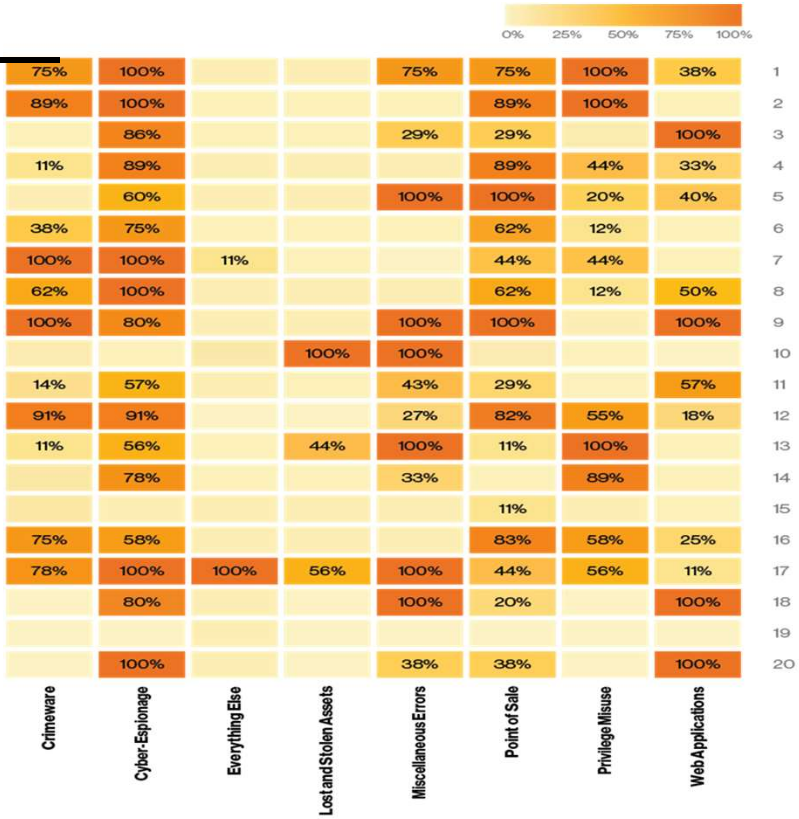
Figure 139. Percentage of MITRE Techniques covered by VERIS

CIS Critical Security Control recommendations

CIS Critical Security Controls (CSCs)

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

Figure 134. Percentage of Safeguards mapped to Patterns by Critical Security Control

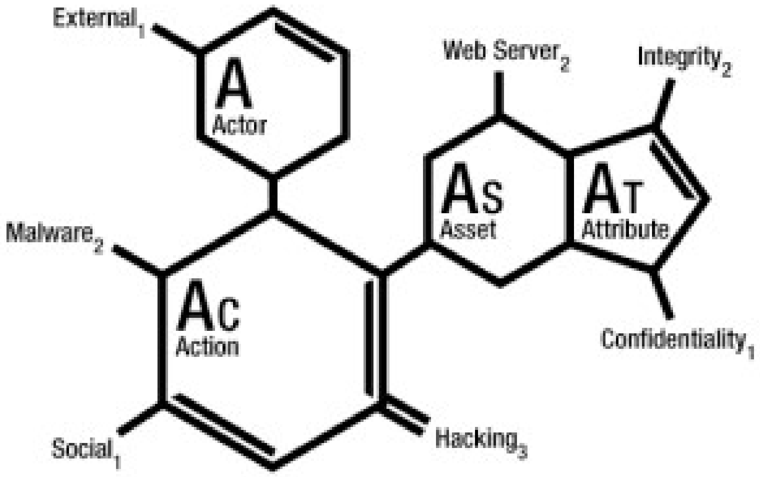


0%
25%
50%
75%
100%

	Crimeware	Cyber-Espionage	Everything Else	Lost and Stolen Assets	Miscellaneous Errors	Point of Sale	Privilege Misuse	Web Applications
1	75%	100%			75%	75%	100%	38%
2	89%	100%				89%	100%	
3		86%			29%	29%		100%
4	11%	89%				89%	44%	33%
5		60%			100%	100%	20%	40%
6	38%	75%				62%	12%	
7	100%	100%	11%			44%	44%	
8	62%	100%				62%	12%	50%
9	100%	80%			100%	100%		100%
10				100%	100%			
11	14%	57%			43%	29%		57%
12	91%	91%			27%	82%	55%	18%
13	11%	56%		44%	100%	11%	100%	
14		78%			33%		89%	
15						11%		
16	75%	58%				83%	58%	25%
17	78%	100%	100%	56%	100%	44%	56%	11%
18		80%			100%	20%		100%
19								
20		100%			38%	38%		100%

Key Terms

The DBIR uses the VERIS framework for data collection and analysis



Actor – Who did it?

Action – How'd they do it?

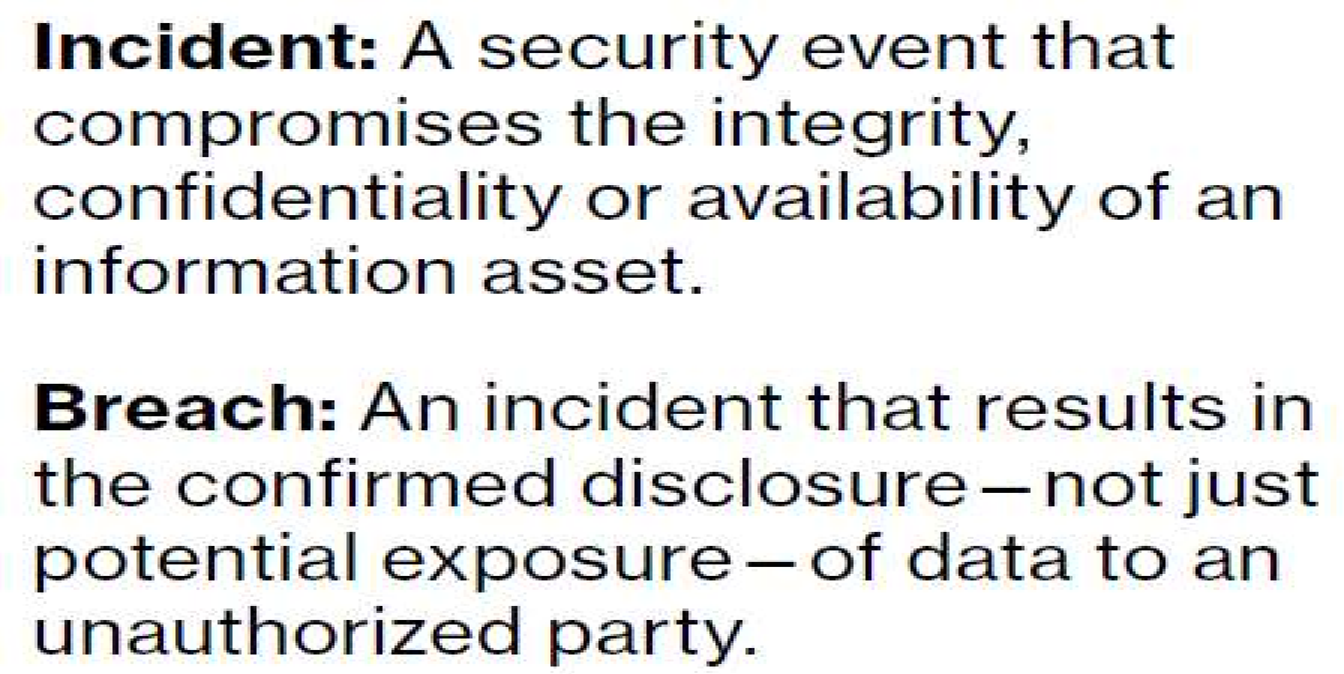
Asset – What was affected?

Attribute – How was it affected?

Documentation, classification examples, enumerations: http://veriscommunity.net/

What's new

Incident vs Breach



Incident: A security event that compromises the integrity, confidentiality or availability of an information asset.

Breach: An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party.

Key insights

Verizon's latest research confirms the extent of the challenge in keeping up.

32,002

security incidents

3,950

confirmed breaches analyzed

67%

More than two-thirds of all breaches come from three attack types: credential theft, errors and social attacks.

27%

Ransomware makes up 27% of malware incidents, and the threat continues to grow.

58%

Personal data is the target in more than half of breaches, almost double from a year ago.

43%

Almost half of breaches involve web application attacks, twice as many as last year.

21%

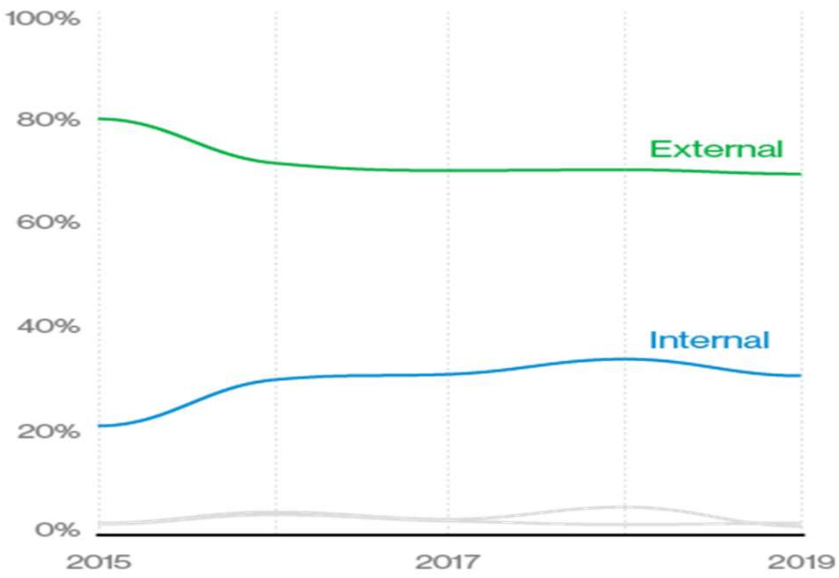
One in five breaches is caused by errors, which represents a doubling of the total number of breaches from last year.

Key insights

Who is behind this?

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

Figure 7. Actors over time in breaches



Who is behind this?

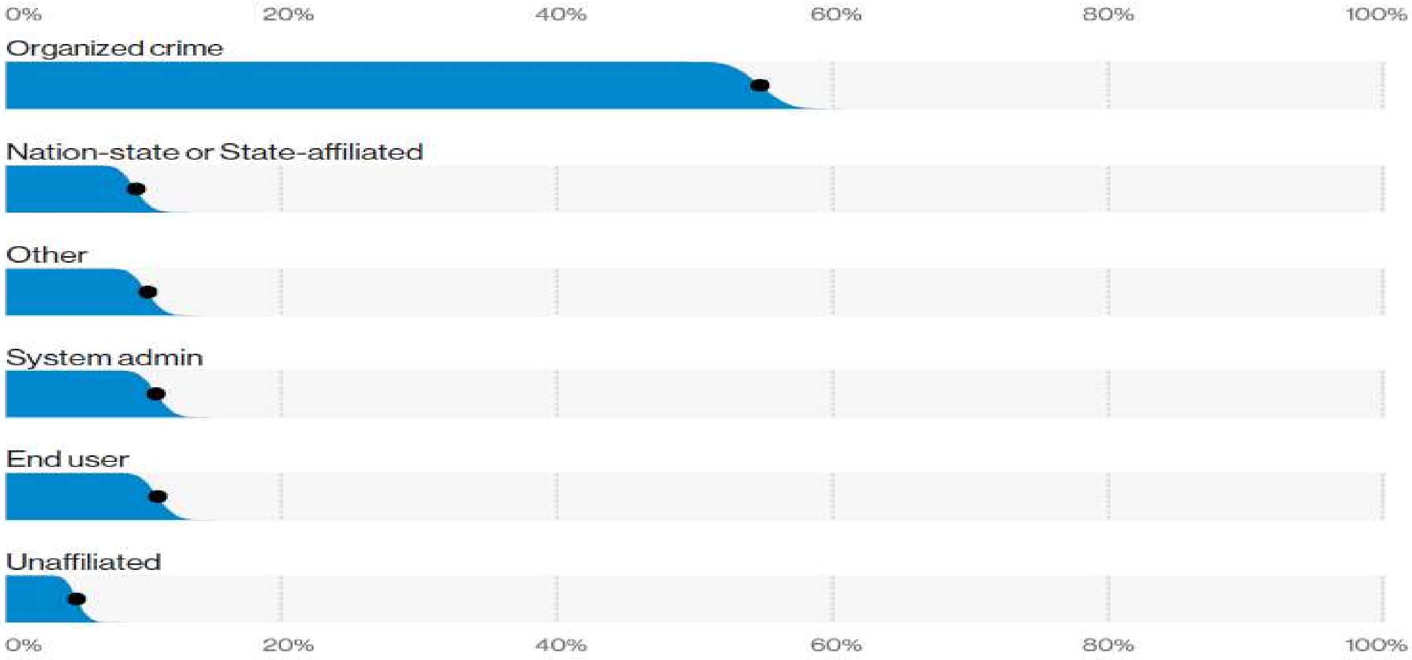


Figure 10. Top Actor varieties in breaches (n = 977)

Key insights

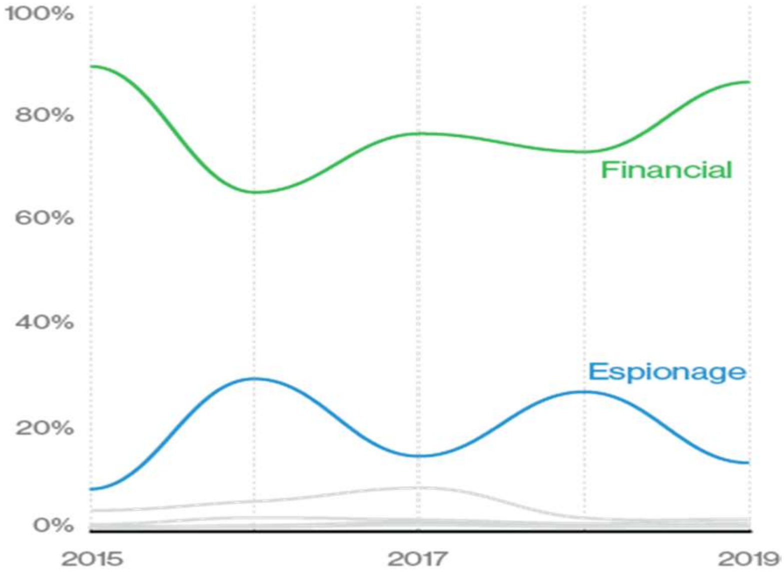
The times, they aren't a'changing.

The majority (86% of breaches) continue to be financially motivated.

Espionage gets the headlines but accounts for just 10% of breaches in this year's data.

Advanced threats—which also get lots of buzz—represent only 4% of breaches.

Figure 8. Actor motives over time in breaches

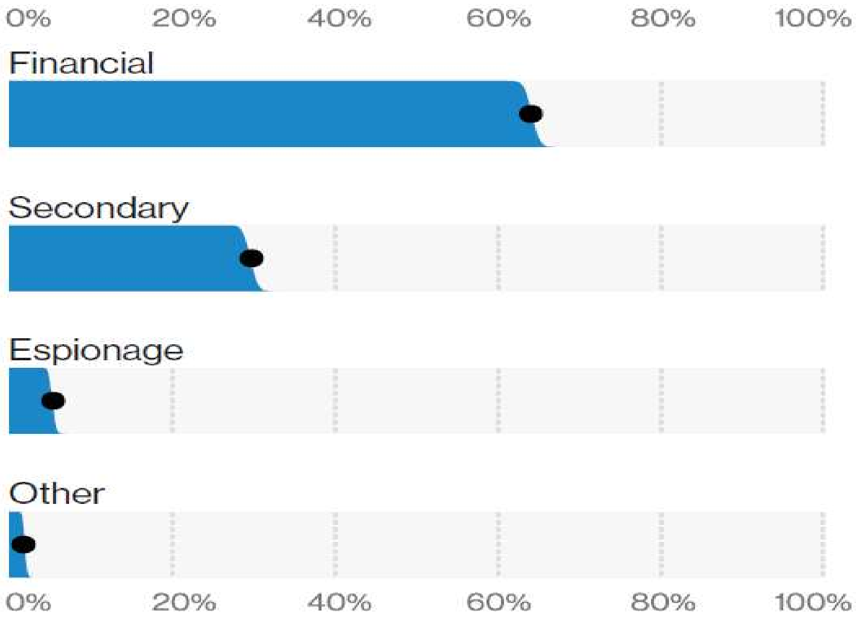


verizon

Verizon proprietary. Unauthorized disclosure, reproduction or other use prohibited.

Top Actor Motives Incidents

Figure 9. Top Actor motives in incidents (n = 3,828)



Key insights

Incidents and breaches per pattern

In the 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.

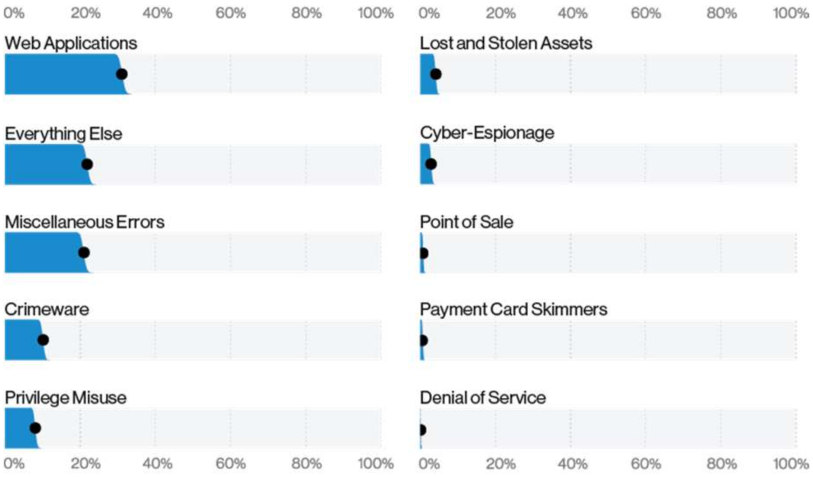


Figure 46. Patterns in breaches (n = 3,950)

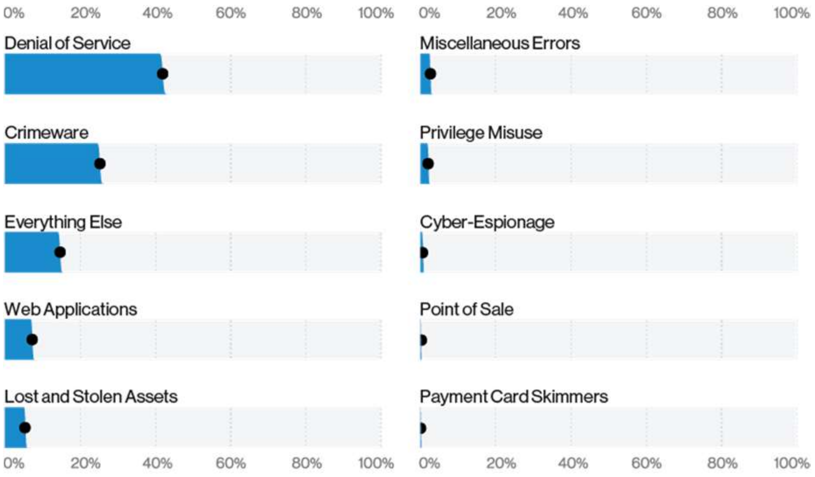


Figure 47. Patterns in incidents (n = 32,002)

Actions

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.

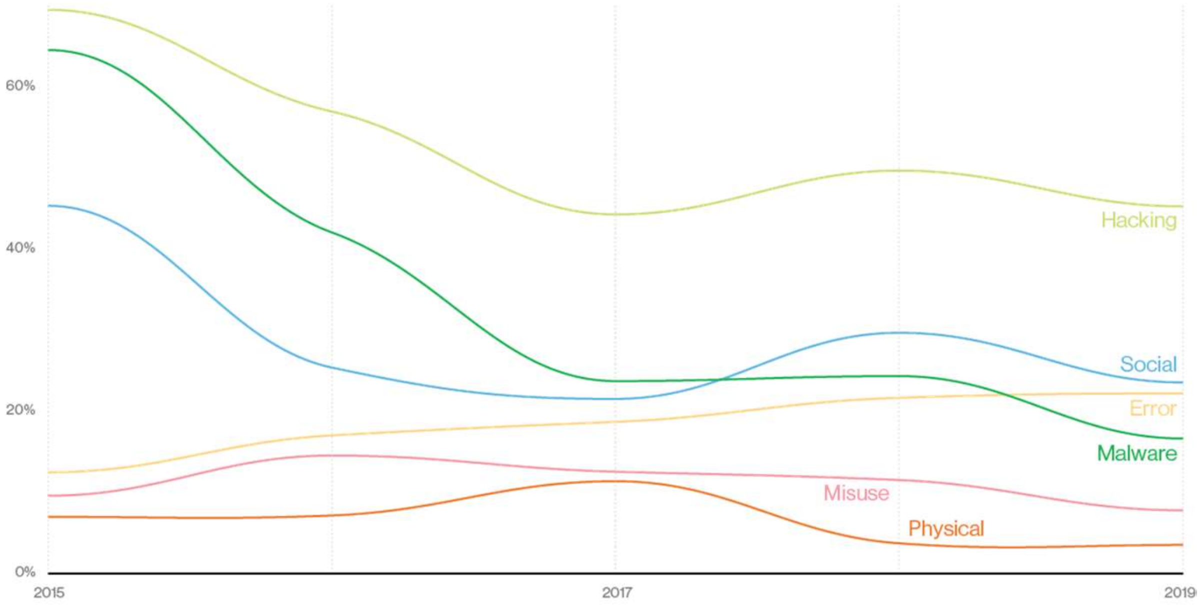


Figure 11. Actions over time in breaches

Ransomware and web application

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.

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

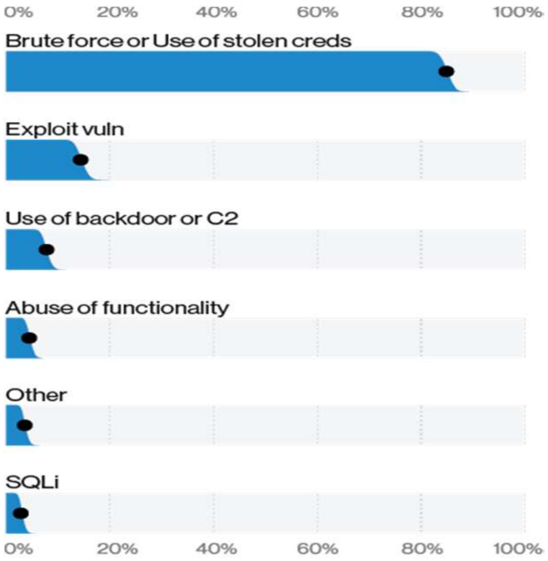


Figure 20. Top Hacking varieties in breaches (n = 868)

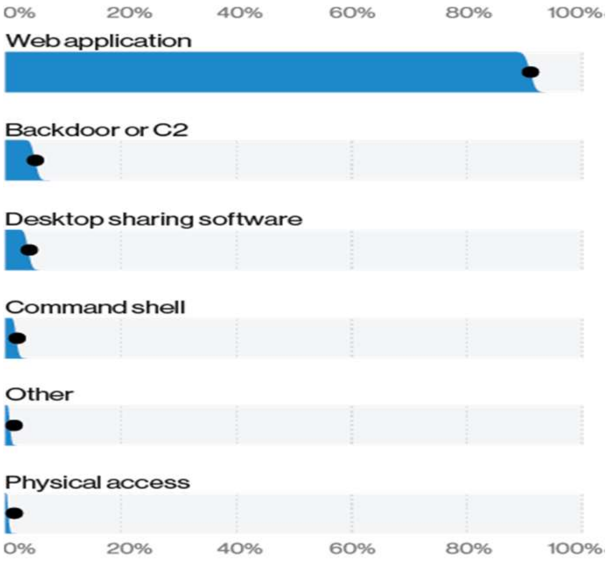


Figure 21. Top Hacking vectors in breaches (n = 1,361)

Key insights

Errors

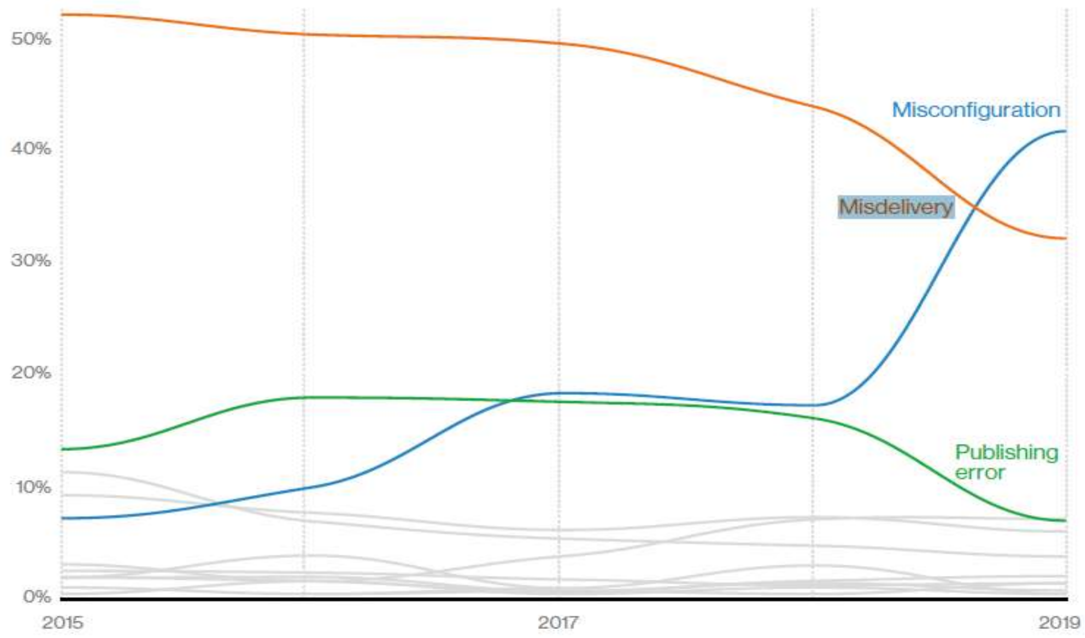


Figure 14. Top Error varieties over time in breaches

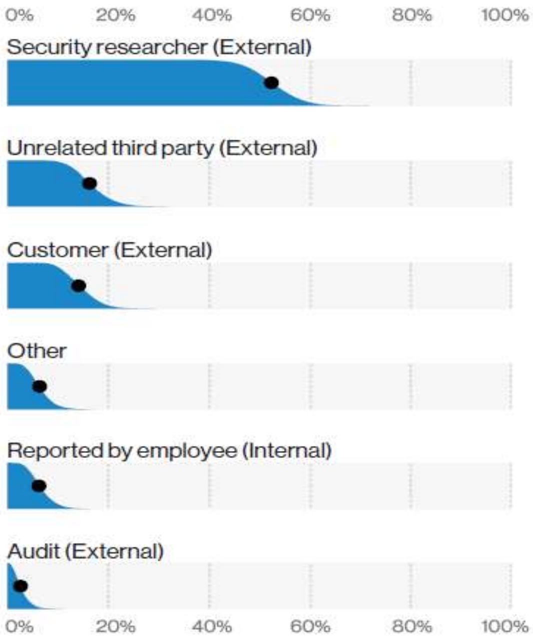


Figure 15. Top discovery methods in Error breaches (n = 95)

Up-close-and-personal data

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.

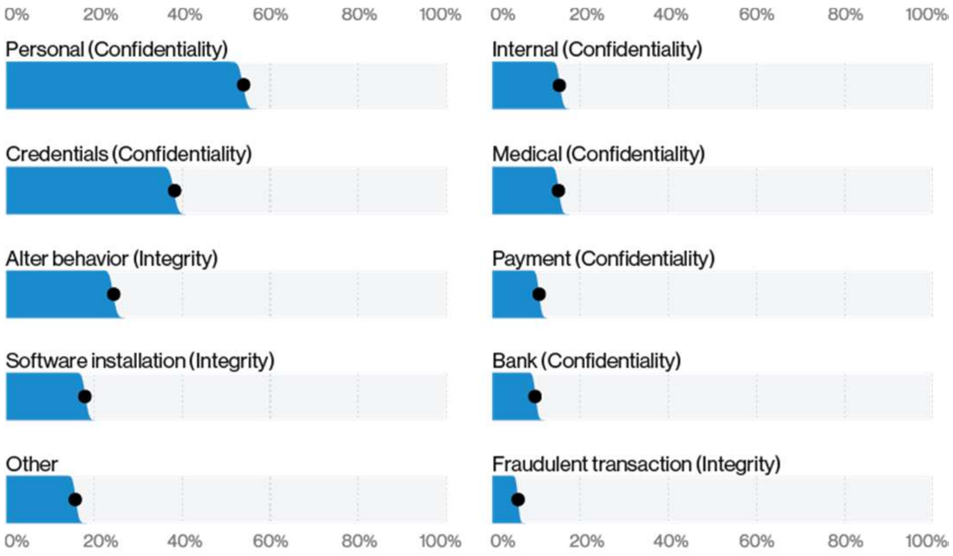


Figure 37. Top compromised Attribute varieties in breaches (n = 3,667)

Poll

For a moment I would like to think like an Hacker. You have a choice to one of the following strategy. Which one will you choose? Select your answers now. Both take a month to complete.

1. Target 1000 firms/individuals with success rate of 10% with 1-5 steps to hack and make financial gains of £1000 for each successful compromise.

2. Target 100 firms/individuals with success rate of 1% with 100 steps and financial gains of £100,000

Unbroken chains and path-based attacks

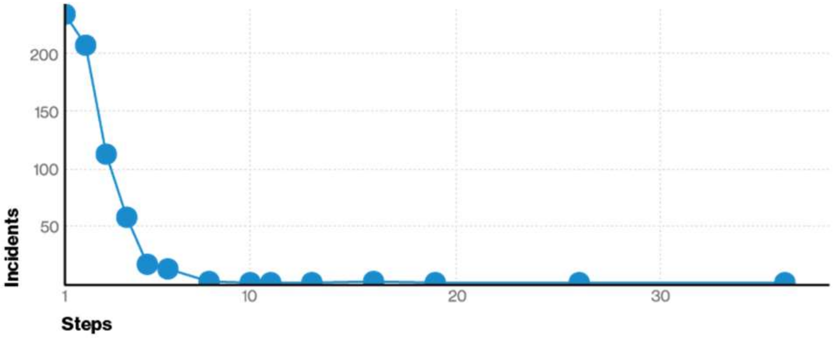


Figure 41. Number of steps per incident
(n = 654. Two breaches, 77 and 391 steps respectively, not shown.)

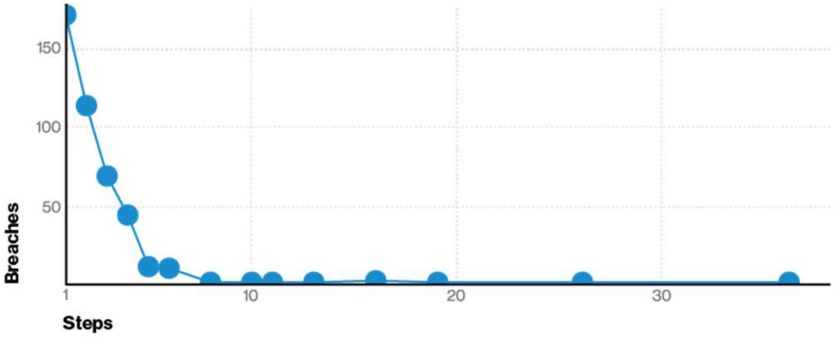
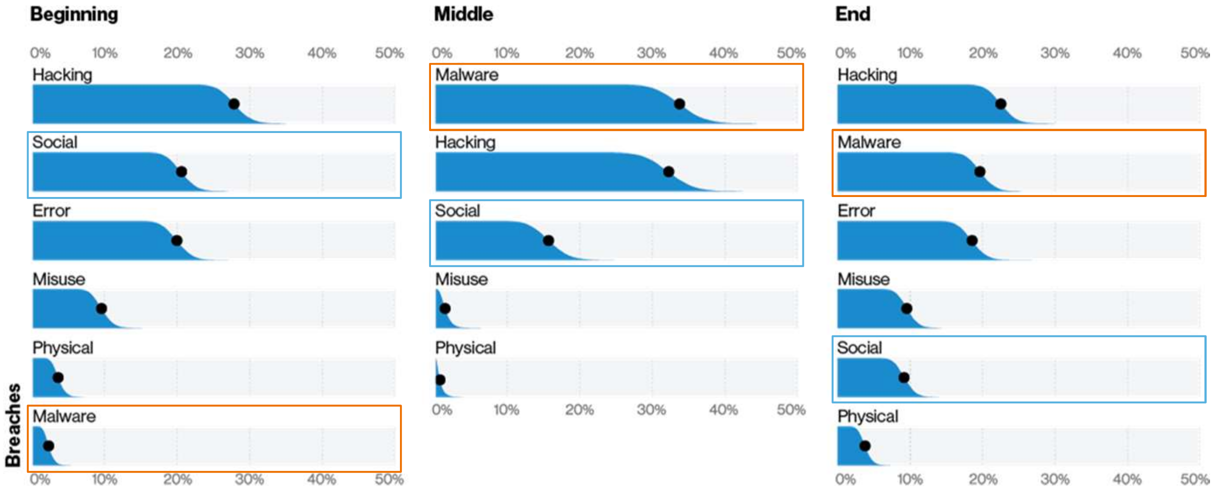


Figure 42. Number of steps per breach
(n = 429. Two breaches, 77 and 391 steps respectively, not shown.)

Unbroken chains and path-based attacks (cont'd)



Key insights

Good news? In my infosec?

.

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.

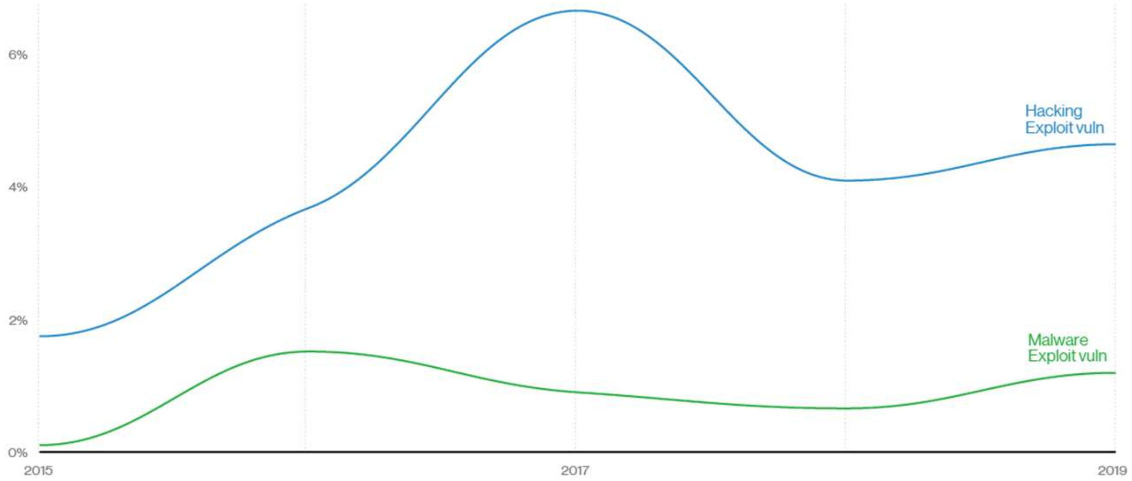


Figure 25. Vulnerability exploitation over time in breaches

Industries

Increase in industry 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 and 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)

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)

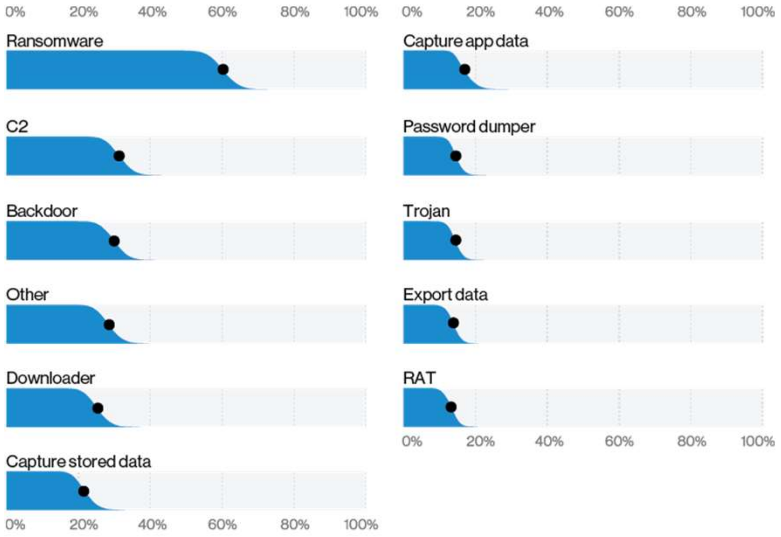


Figure 92. Top Malware varieties in Public Administration incidents (n = 198)

Regions and size

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 and 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
- Center for Internet Security Critical Security Controls (CSC)

SMB vs large organizations

While differences between small and medium-sized businesses (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)

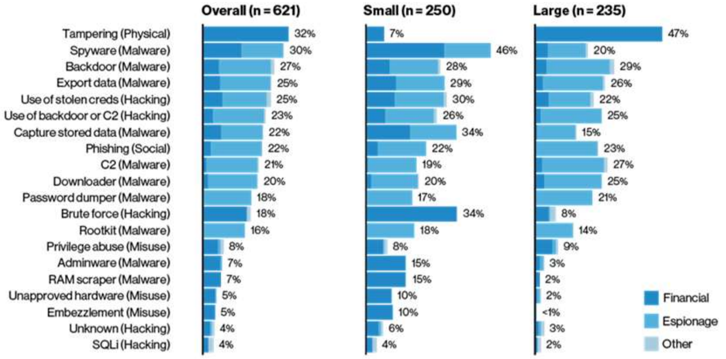


Figure 109. Top 20 threat actions (referencing the 2013 DBIR)

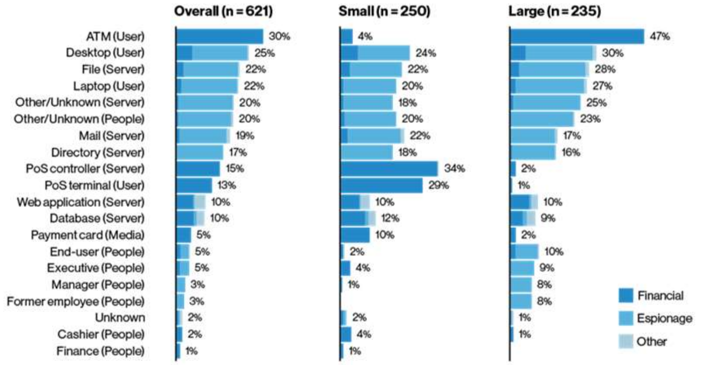
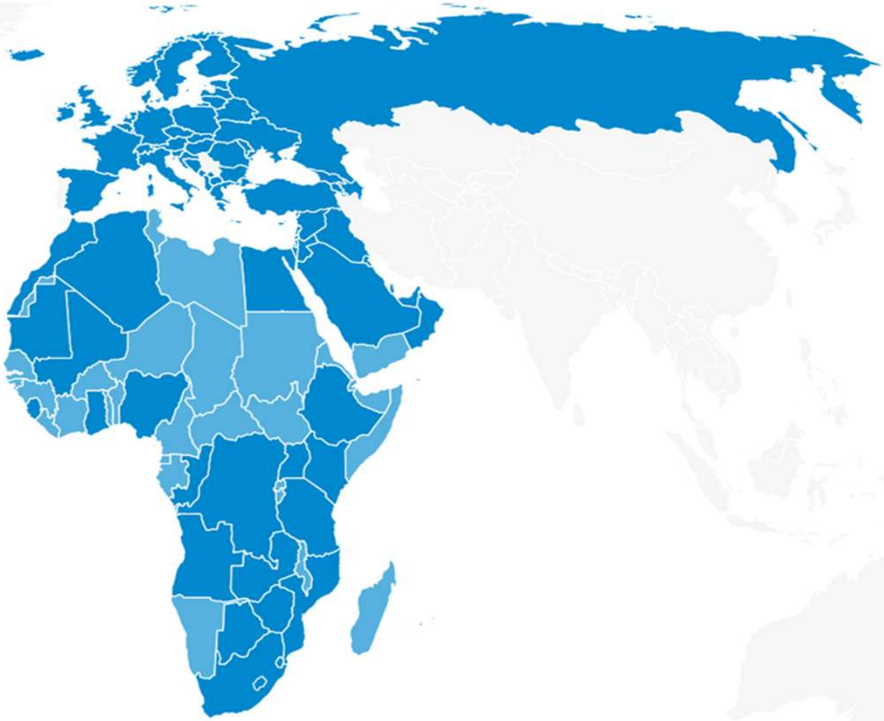


Figure 112. Varieties of compromised assets (referencing the 2013 DBIR)

Europe, Middle East and Africa (EMEA)

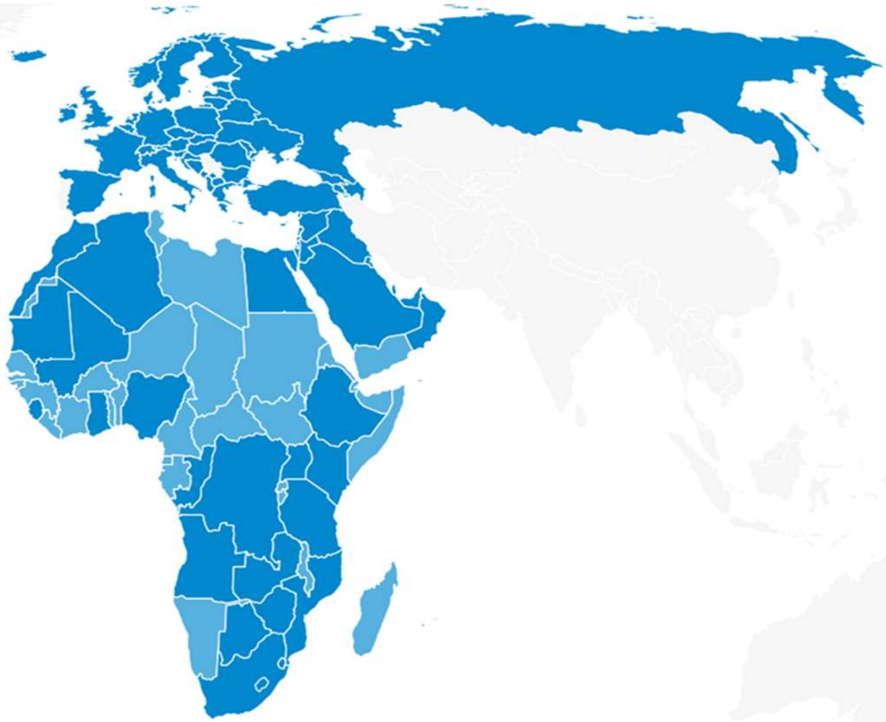
Attackers are targeting web applications in EMEA with a combination of hacking techniques that leverage either stolen credentials or known vulnerabilities. Cyber-Espionage attacks leveraging these tactics were common in this region. Denial of Service attacks continue to cause availability impacts on infrastructure as well.

Frequency	4,209 incidents, 185 with confirmed data disclosure
Top Patterns	Web Applications, Everything Else and Cyber-Espionage represent 78% of data breaches in EMEA.
Threat Actors	External (87%), Internal (13%), Partner (2%), Multiple (1%) (breaches)
Actor Motives	Financial (70%), Espionage (22%), Ideology (3%), Fun (3%), Grudge (3%), Convenience (1%) (breaches)
Data Compromised	Credentials (56%), Internal (44%), Other (28%), Personal (20%) (breaches)



Europe, Middle East and Africa (EMEA)

- Attackers are targeting web applications in EMEA with a combination of hacking techniques that leverage either stolen credentials or known vulnerabilities resulting in over 40% of the breaches
- Fourteen percent of the breaches in the EMEA region were associated with Cyber-Espionage, which is a higher rate than the overall data at 3% of breaches
- Denial of Service attacks continue to cause availability impacts on infrastructure as well making up over 90% of the incidents



Controls

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.

Email and Web Browser Protection (CSC 7)

Since 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.

Boundary Defense (CSC 12)

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

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 multifactor authentication, which also shows up here.

Secure Configuration (CSC 5, CSC 11)

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.

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.

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.

Implement a Security Awareness and Training Program (CSC 17)

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

Questions?

verizon✓

Verizon proprietary. Unauthorized disclosure, reproduction or other use prohibited.

DBIR Resources

VERIZON DBIR 2020
https://enterprise.verizon.com/resources/reports/dbir/

VERIZON DBIR ARCHIVE
https://enterprise.verizon.com/resources/reports/dbir/

FREE SECURITY ASSESSMENT SIGNUP
https://enterprise.verizon.com/products/security/cyber-risk-monitoring/security-assessment-tool/security-assessment-signup/

Contact Information

Deepinder Chhabra (Deep)

Head of Security Assurance Consulting(UK&I)

Verizon Business Group

- Security Leadership
- GRC, PCI & GDPR
- Cyber/Info. Security
- Security Assurance

Contact Information

Email - Dchhabra@isaca-london.org

LinkedIn - https://www.linkedin.com/in/deepinder-singh-0656122/

Areas of Expertise

Expert Knowledge

- Securiy Leadership
- Governane of IT & Cyber
- Cyber Security Managementt
- Risk Management
- Information Secruity Audit

Vertical experience

- Defense
- Public Sector
- Financial Sector
- Telecommunication
- Manufacturing
- Consulting
- Retail
- Service

Thank you.