



September Announcements

- ▶ The GoCyber Collective website is live. You can download past presentations from the Blog page.
 - ▶ [GoCyber Collective](#)
- ▶ Signal App
 - ▶ GoCyber Collective will be using Signal to distribute real-time threat intelligence.



Special Interest Groups

- ▶ Special Interest Groups (SIGs)
 - ▶ Defense Industrial Base – Led by Dr. Thomas Autry
 - ▶ Local Government – Led by Darren Davey
 - ▶ Public Safety – Led by Gary Estes
- ▶ October SIG Session Open to All
 - ▶ Northrop Grumman Joint Surveillance Journey, discussing DoD assessment and third-party preparation for new regulations.

October Speaker

- ▶ October 18th Jeff DeRamus, Director of Technology with Shook Construction joins us to share his experience with a ransomware event. This is a story you don't want to miss.



Feedback

Feel free to email us at Admin@gocybercollective.org.

If you have a suggestion on meeting topics, special interest groups, breakfast menu, or anything else we want to hear from you.

Event Sponsors



FORTINET®

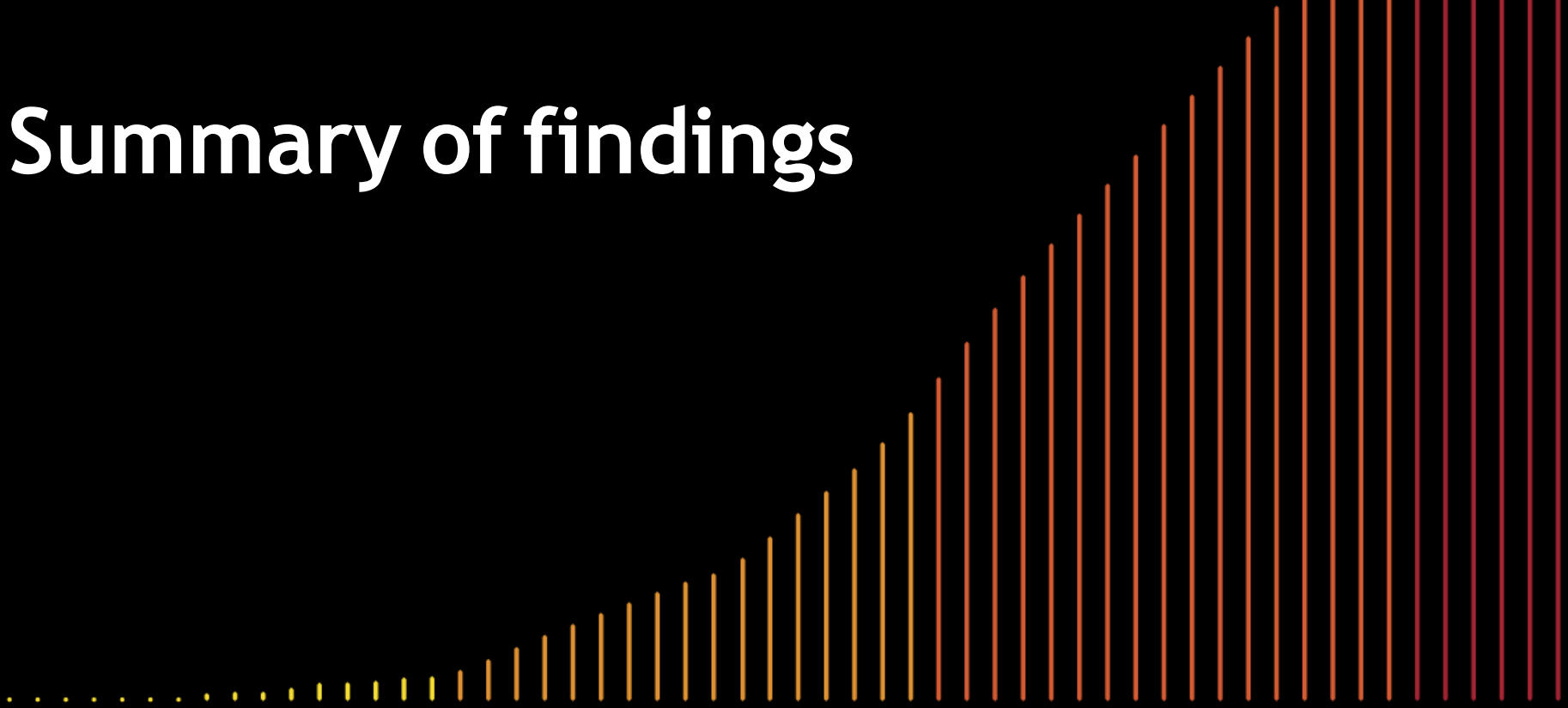
DBIR

2023 Data Breach Investigations Report Presentation

The authoritative source of cybersecurity breach information



Summary of findings



A comprehensive look at data security patterns

16

years

81

countries

16,312

incidents reviewed in
our 2023 report

5,199

data breaches analyzed
in the 2023 report



It's been a busy year for cybercriminals—and those who fight them. Here's what we saw.

Key paths to data breaches:



Stolen credentials



Phishing



Exploitation of vulnerabilities

Who are the culprits?

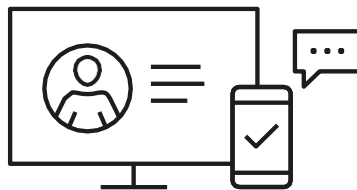
Organized crime is the leading source of cyberattacks.

74% of all breaches include the human element, through Error, Privilege Misuse, Use of stolen credentials or Social Engineering.

What are the motives?

#1 The number 1 motive was Financial gain, which was the driver for 95% of attacks.

#2 The number 2 motive was Espionage—but a very distant second place.

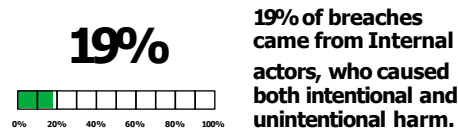
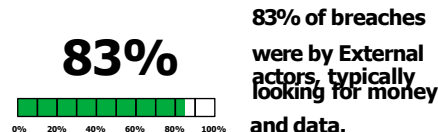
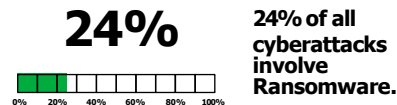


Pretexting rose.

50% of all Social Engineering incidents in 2022 involved

Pretexting—an invented scenario that tricks someone into giving up information or committing an act that may result in a breach.

What we found:



More than 32% of all Log4j scanning activity over the course of the year happened within 30 days of its release (with the biggest spike of activity occurring within 17 days).



Top data-driven findings

74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering.

83% of breaches involved external actors, and the primary motivation for attacks continues to be overwhelmingly Financially driven, at 95% of breaches.

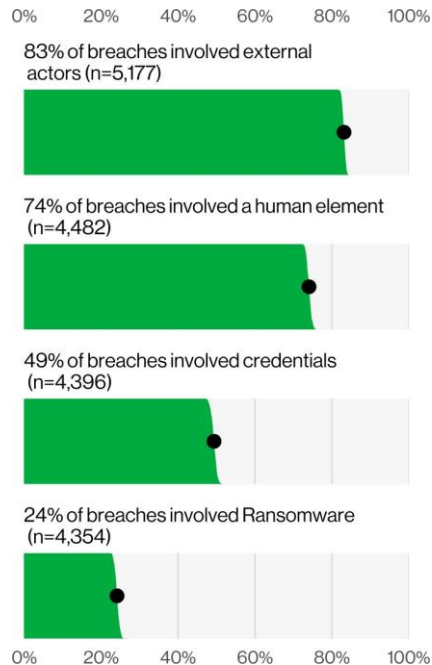


Figure 1. Select key enumerations



Ransomware

Ransomware continues its reign as one of the top Action types present in breaches, and while it did not actually grow, it did hold statistically steady at 24%. Ransomware is ubiquitous among organizations of all sizes and in all industries.

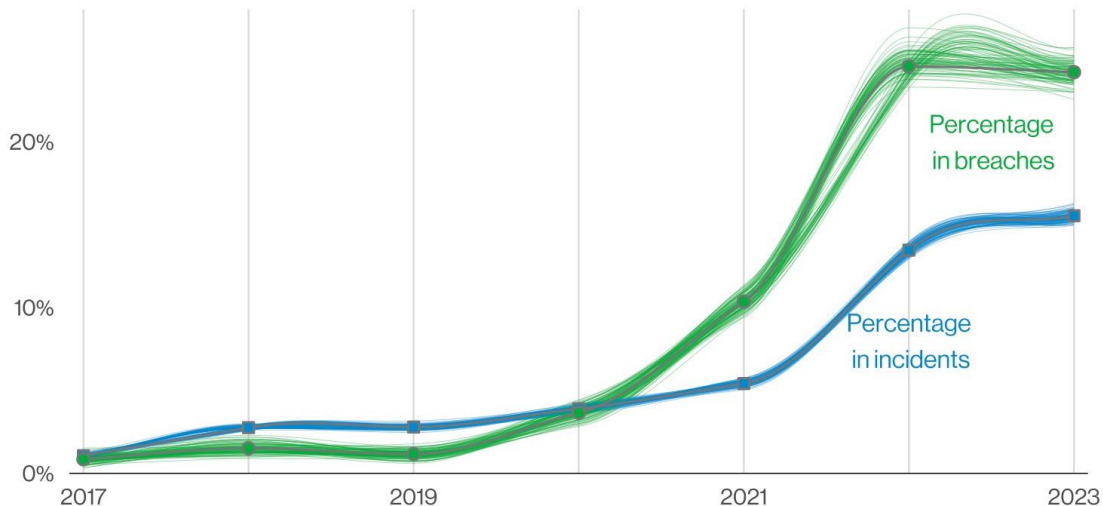


Figure 2. Ransomware action variety over time



Business Email Compromise (BEC)

Social Engineering attacks are often very effective and extremely lucrative for cybercriminals. BEC attacks (which are most of our pretexting attacks) have almost doubled across our entire incident dataset and now represent more than 50% of incidents within the Social Engineering pattern.

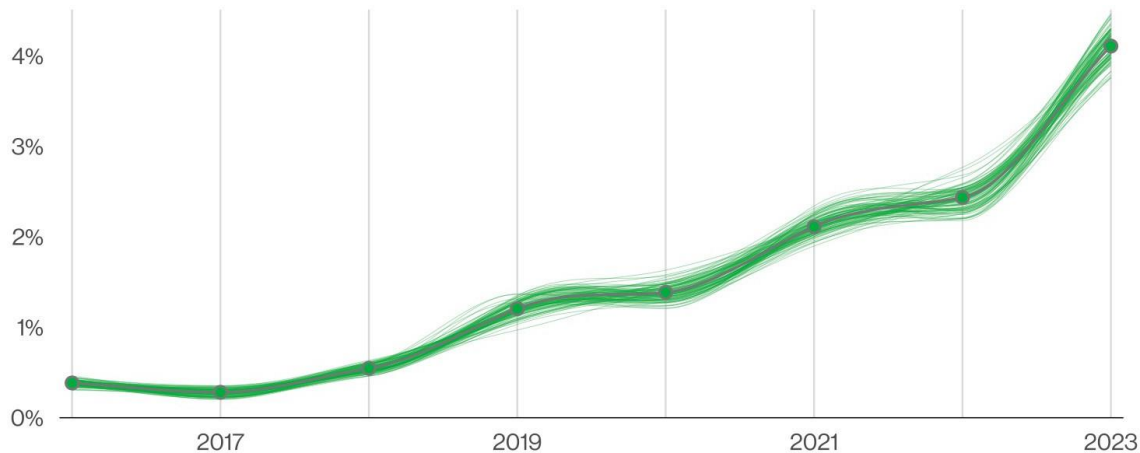


Figure 3. Pretexting incidents over time



Ways in

External actors leveraged a variety of techniques to gain entry to an organization, such as Use of stolen credentials (49%), Phishing (12%) and Exploiting vulnerabilities (5%). This is very much in line with last year's results, so what about Log4j? Wasn't it impactful?

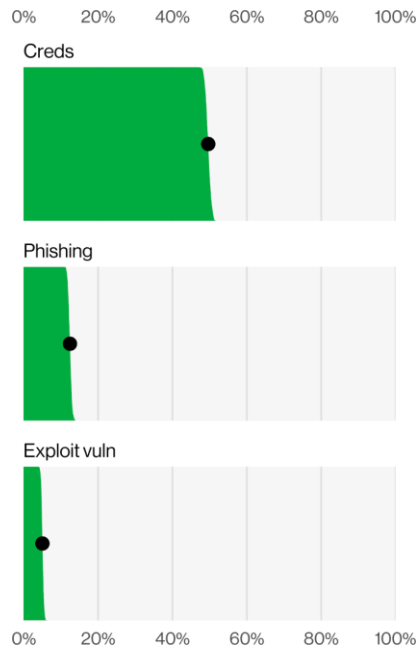


Figure 4. Select enumerations in non-Error, non-Misuse breaches (n=4,291)



Log4j

Log4j was identified as the culprit in 90% of breaches where a vulnerability exploitation was the way in and our contributors explicitly documented what vulnerability was exploited.

More than 32% of all Log4j scanning activity over the course of the year happened within 30 days of its release (with the biggest spike of activity occurring within 17 days).

Takeaway: Quick patch response by industry mitigated what could have been a much bigger disaster.

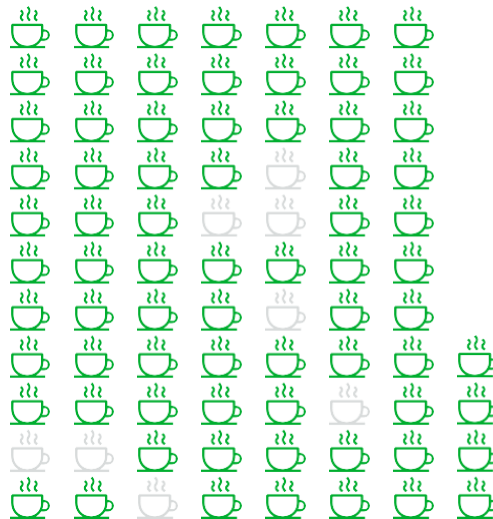


Figure 5. Percentage of identified Exploit vuln that was Log4j (n=81). Each glyph represents an incident.

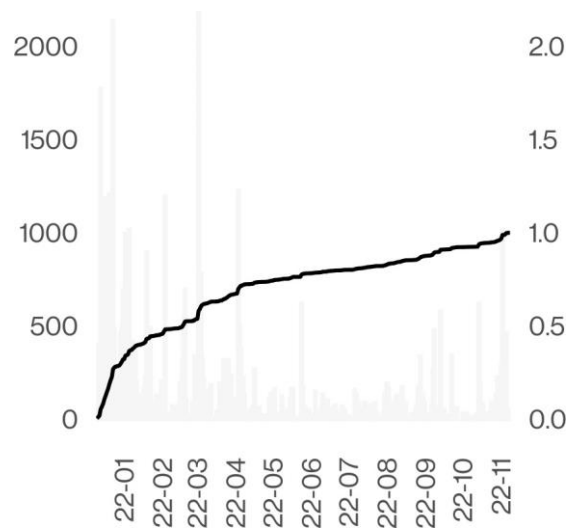
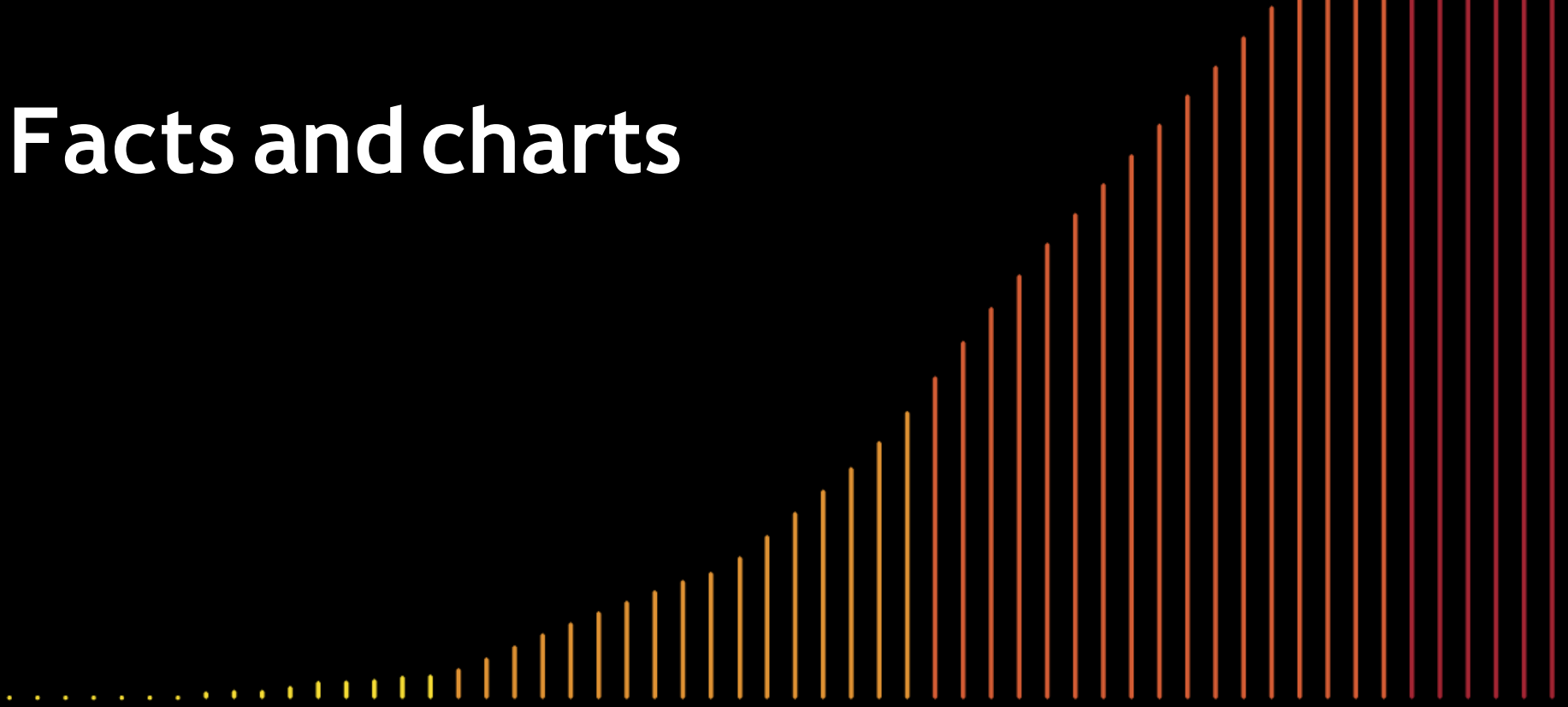


Figure 6. Percentage of Log4j scanning for 2022



Facts and charts



Incident patterns

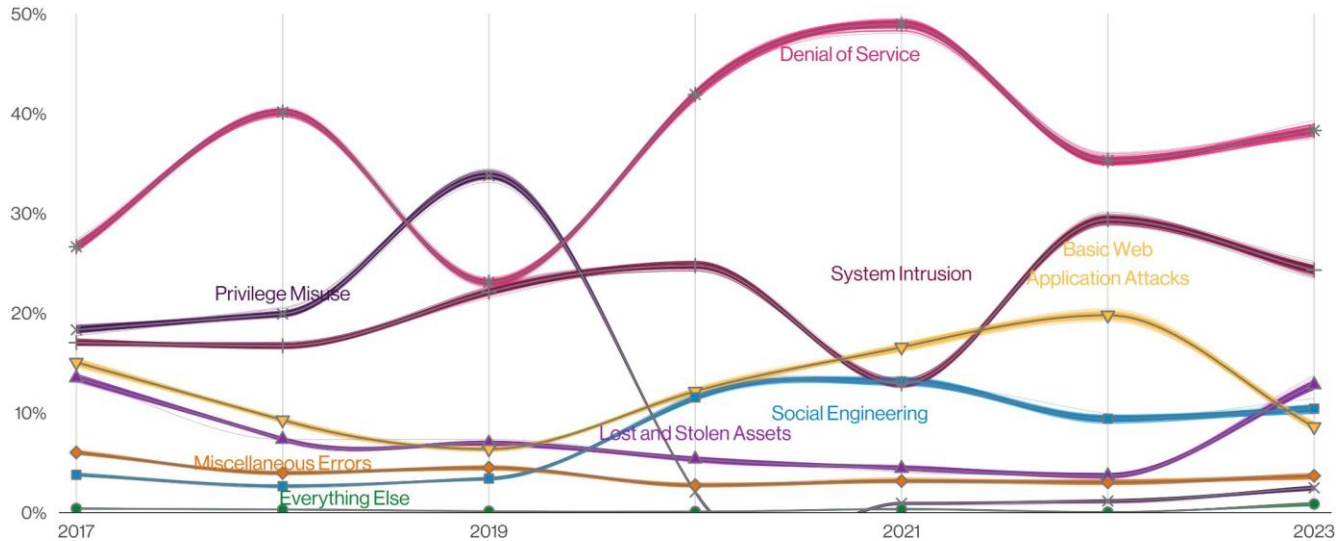


Figure 7. Patterns over time in incidents



Breach patterns

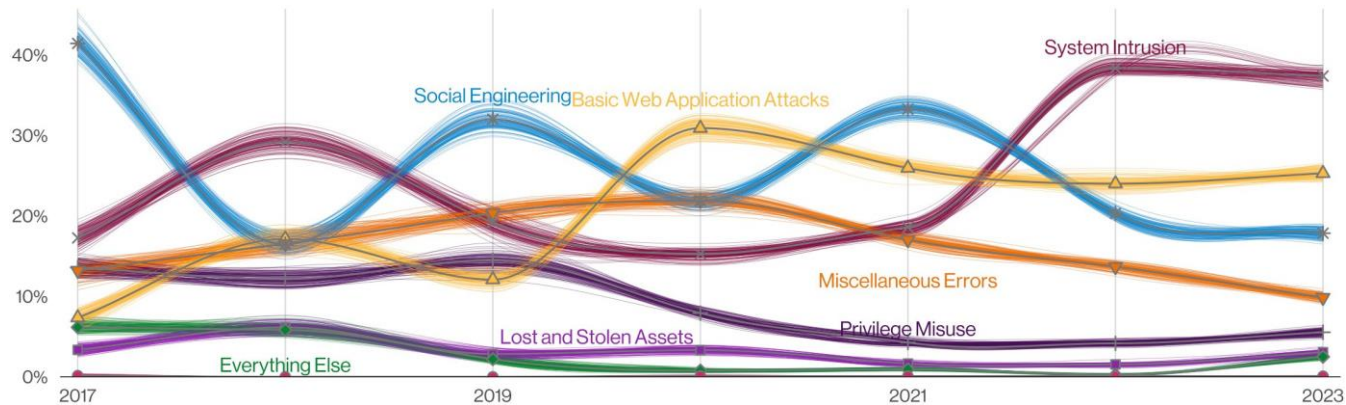


Figure 8. Patterns over time in breaches



System Intrusion

80% of System Intrusion incidents involved Ransomware as attackers continue to leverage a bevy of different techniques to compromise an organization and monetize their access.

91% of our industries have Ransomware as one of their top three actions.

While only 7% of Ransomware incidents reported losses to the FBI Internet Crime Complaint Center (IC3), the median loss more than doubled from last year to \$26,000, with 95% of incidents causing losses ranging between \$1 and \$2.25 million.

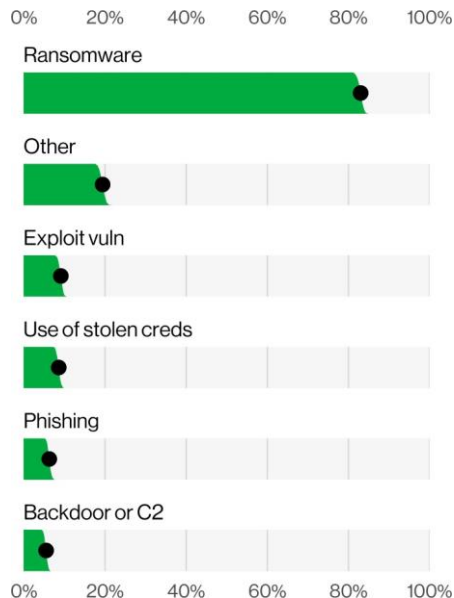


Figure 9. Action varieties in System Intrusion incidents (n=2,700)

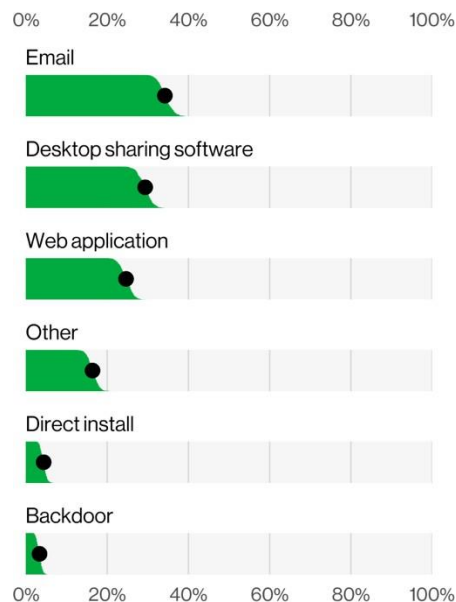


Figure 10. Action vectors for Ransomware (n=690)



Social Engineering

Social Engineering incidents have increased from the previous year largely due to the use of Pretexting—a tactic commonly used in BEC—which almost doubled since last year.

Social Engineering accounts for 17% of breaches and 10% of incidents.

Based on FBI IC3 data, the median amount stolen in a BEC has increased over the last couple of years to \$50,000.

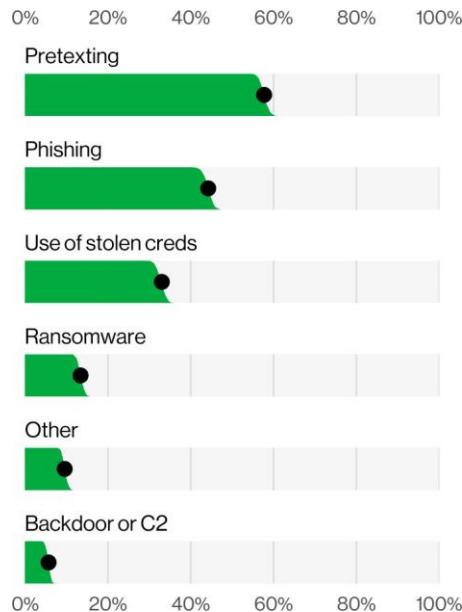


Figure 11. Action varieties in Social Engineering incidents (n=1,696)

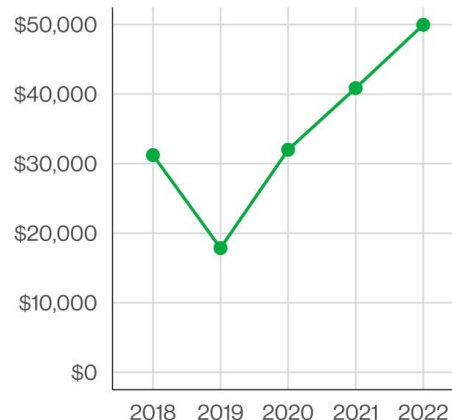


Figure 12. Median transaction size for BECs (n=73,420). Based on FBI IC3 complaints where a transaction occurred.



Basic Web Application Attacks

While representing approximately one-fourth of our dataset, Basic Web Application Attacks breaches and incidents tend to be largely driven by attacks against credentials and then leveraging those stolen credentials to access a variety of resources.

86% of Basic Web Application Attacks breaches involve the Use of stolen credentials.

10% of breaches in this pattern involve the Exploitation of a vulnerability.

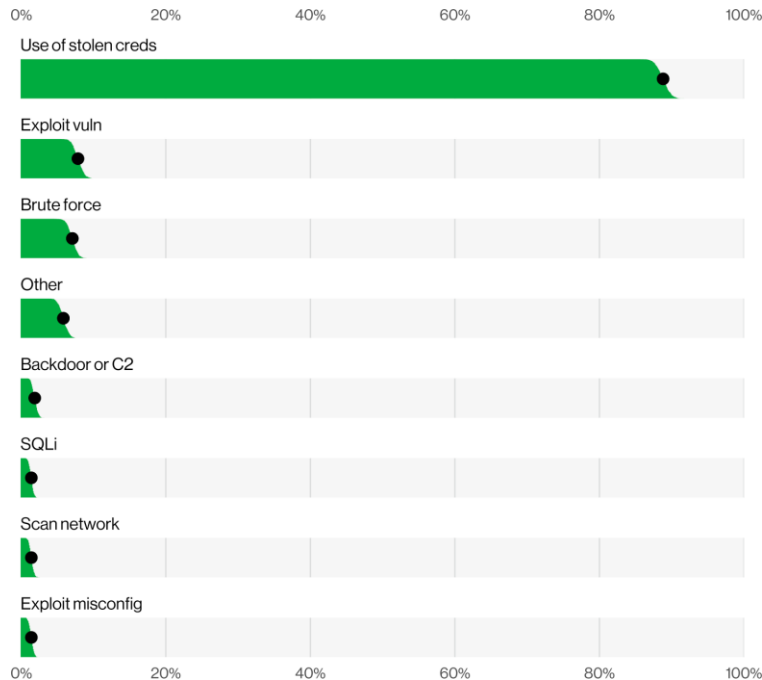


Figure 13. Top action varieties for Basic Web Application Attacks breaches (n=1,287)



Miscellaneous Errors

Error-related breaches are proportionally down to 9% as opposed to 13% last year.

The majority of errors that lead to breaches are committed by Developers and System admins.

Data compromised included Personal (89%), Medical (19%) and Bank (10%).

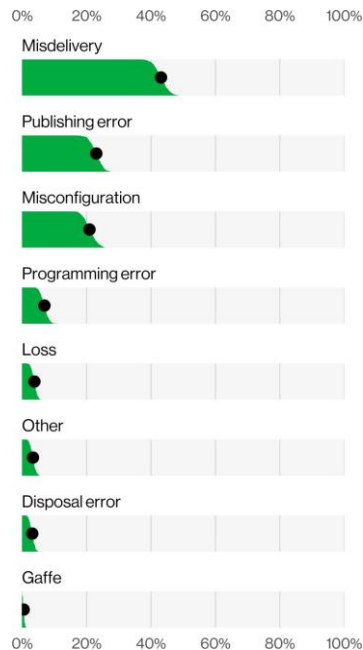


Figure 14. Top action varieties in Miscellaneous Errors breaches (n=450)

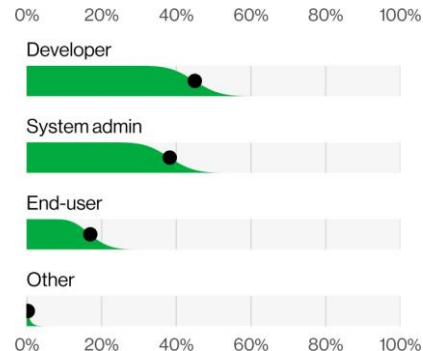
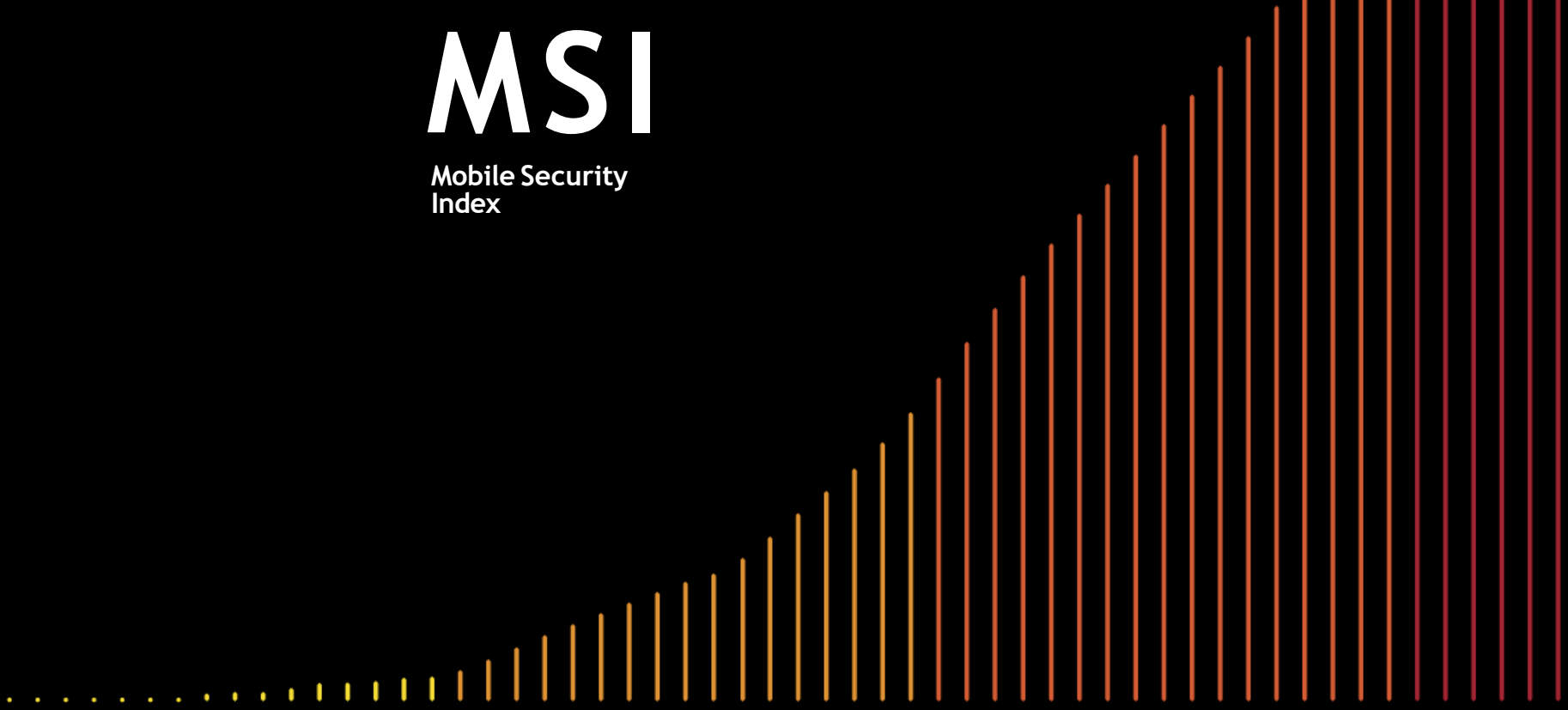


Figure 15. Top actor varieties in Miscellaneous Errors breaches (n=89)



MSI

Mobile Security
Index



According to a survey by Proofpoint, 64% of people have changed where they work. Changes driven by the pandemic have stuck. Sixty-eight percent of those surveyed have started working from home either full time or some of the time.² IT organizations did a stellar job enabling millions of people to work from home on short notice. New security approaches and tools mean that employees working from home can be just as secure as those working from the office.

And managing a mix of remote, home, hybrid and office-based employees doesn't need to be any more difficult either.

But companies are still struggling. Almost four-fifths of respondents agreed that recent changes to working practices had adversely affected their organization's cybersecurity.



79%

Almost four-fifths of respondents agreed that recent changes to working practices had adversely affected their organization's cybersecurity.

22%

Over a fifth (22%) of IT leaders in an Absolute study said that their primary reason for wanting employees to work from the office is to maintain a better corporate security posture.³

Almost two in three CISOs across all regions agree that remote working makes their organization more vulnerable to cyberattack.

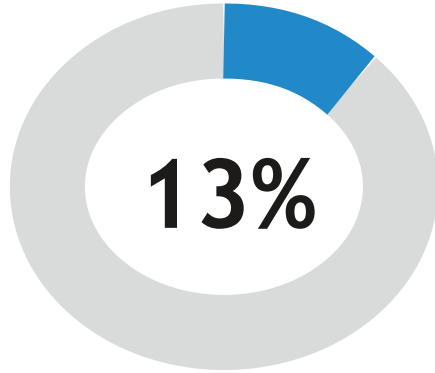


² Proofpoint, 2022 State of the Phish, 2022
³ Absolute, The Future of Work, 2022

Companies are more reliant on mobile devices.

This is partly driven by the shift toward more hybrid working, but there are several other factors too. For many, mobile devices are no longer a secondary device.

Only one in eight respondents said they had few (less than 10% of their workforce) people working from home or following a hybrid working model.



58%

We have more users using mobile devices than 12 months ago.

59%

Mobile users are doing more with the devices than 12 months ago.

53%

Mobile devices have access to more sensitive data than a year ago.

Many employees now have access to much of the same data—customer lists, banking details, employees’ personal data, billing information, etc.—and systems—messaging, enterprise resource planning (ERP), etc.—via their mobile devices as they would sitting at a desktop in the office. This means that the compromise of a mobile device can now pose a significant risk to customer data, intellectual property and core systems.

Security spend is rising in response.

Over three-quarters (77%) of respondents said that their security spend had increased in the preceding year. More than a fifth said that it had increased significantly.

Change in security spend

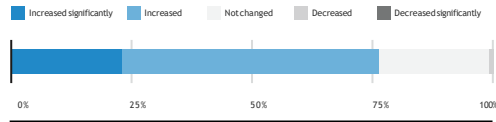


Figure 2. Year-over-year change in security spend. [n=632]

Factors driving increase in security spend

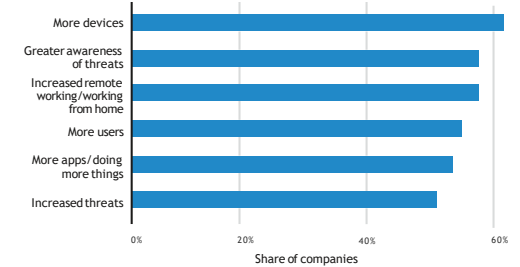


Figure 3. Factors that respondents said drove the increase in security spend that they had seen in the preceding 12 months. [n=626]

Mobile is NOW Critical

It's worth remembering that one of the early successes in the mobile device field was BlackBerry, and specifically BlackBerry Enterprise Server. The first thing that springs to mind when most people think of BlackBerry is the physical keyboard. But looking back, what's really interesting about BlackBerry is that security was central to how it was designed.

However, Blackberry's dominance, driven by enterprise users, was quickly overwhelmed by consumer-friendly devices from the likes of Apple. And that's when people started having better technology at home than at work. Executives around the world started putting pressure on IT teams to give them devices for work that were as user friendly as their personal devices. And it wasn't just hardware, it was apps too.

Today, few people even use the phrase "mobile phone"—unless you're well over 40, anyway—and laptops have become the norm. And it's not just the hardware that's changed, what we do with it has exploded.

Mobile devices are now critical to how we work. With increased capabilities and expansive connectivity, we now have access to far more information and tools than we ever did in the days of desktops and personal digital assistants (PDAs). Partly driven by the growth in cloud-based applications, a smaller screen no longer means less powerful.

Importance of mobile devices

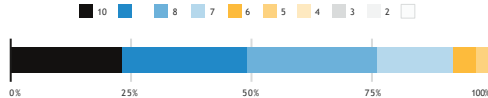


Figure 4. Responses to the question "How critical are mobile devices to the smooth running of your organization?" [n=632]

When asked how critical, on a ten-point scale, mobile devices were to the smooth running of their organization, 91% of respondents in our survey answered seven or above—and 78% answered eight or higher. The picture was very similar regardless of company operations (local, regional or global) and company size (small, medium or enterprise size). The difference was no more than two percentage points up or down.

85%

The vast majority of respondents said that flexibility in where they work and what devices they can use will be important to attracting the best new talent.

Where employees call "the office"

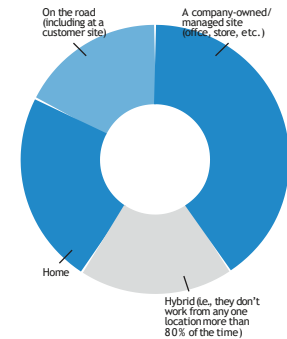


Figure 5. What proportion of your organization's staff work from each of these locations most (80% or more) of the time? [n=632]



Everywhere, all the time

Fifteen years ago when we wrote about mobility, we often talked about the new ability to work from anywhere at any time. Marketers came up with all kinds of clever phrases, like "Make work an activity, not a location."

Obviously, the COVID-19 pandemic had a dramatic impact on working practices. But it didn't create the trend toward more flexible working, it just accelerated it. On average, about two-fifths (40%) of employees work from the office most of the time (80% or more). About the same percentage (41%) work from home or "on the road" most of the time.

There is a downside. For many people, "any time, anywhere" has evolved into "everywhere, all the time." Sometimes, it's employers putting expectations on employees to be contactable outside, often way outside, working hours. In some cases, it's employees themselves slipping into the habit of checking messages, and more, at all hours of the day. It's easy to find ways to justify it to yourself: "This project is important," "I'd rather know now than worry about it all night," and countless more.

Prior to 2016, employers in France were able to dismiss employees for failing to respond to out-of-hours messages—and some did. Then the French government passed a law giving workers the right to disconnect.⁴ Since then, Ireland, Italy and Spain have enacted similar legislation. The province of Ontario is considering enacting a similar law.

Reasons for not being able to disconnect

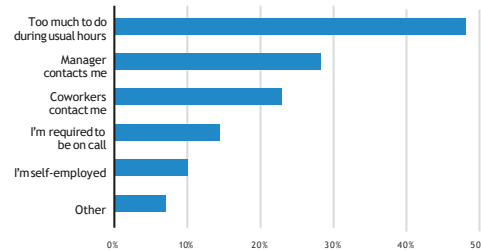


Figure 6. Reasons why employees feel unable to "disconnect" from work.⁴

Assembly of Ontario: Schedule 2 Employment Standards Act 2000

The Schedule amends the Employment Standards Act, 2000. The new Part V11.01 of the Act imposes a requirement on employers that employ 25 or more employees to have a written policy with respect to disconnecting from work. The term "disconnecting from work" is defined to mean not engaging in work-related communications, including emails, telephone calls or the sending or reviewing of other messages, so as to be free from the performance of work.

Figure 7. Extract from Working for Workers Act, 2021 in the Legislative Assembly of Ontario.⁵

⁴ LifeWorks, *The Mental Health Index* by LifeWorks, 2022

⁵ Legifrance, *Partie législative (Articles L1 à L8331-1)*, 2017

⁶ Legislative Assembly of Ontario, *Bill 27, Working for Workers Act, 2021*, 2021

Working excessive hours can affect mental health. LifeWorks found that the 21% of workers who disagreed with the statement "I am typically able to disconnect from work after usual work hours" had a Mental Health Index score 4.8 points lower than those that were able to switch off.⁷

Mental Health Index over time

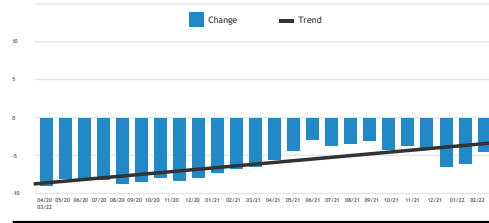


Figure 8. Global Mental Health Index score by month.⁸



2022 Payment Security Report



2023 Release – 8/25/2023

The challenges that organizations encounter, and the mistakes that occur during the planning and execution of PCI security compliance programs, can generally be divided into three stages of failure:


Stage 1: Failure of vision. These are “why” mistakes.

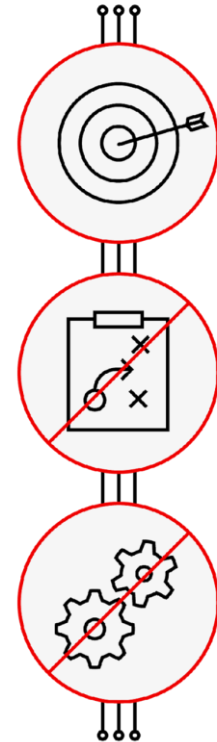
- Failure to understand why they are engaged in PCI security compliance and what their overall goals are
- This happens when leadership doesn’t establish a clear direction for security and compliance, with a clearly articulated vision of the goals and objectives necessary to achieve the required outcomes

Stage 2: Failure of strategy. These are “what” mistakes.

- Failure to design and execute a strategy in a manner that delivers the desired results
- Choosing the wrong “what” to make the strategy happen (i.e., wrong priorities and objectives). For example: not including the development of a sustainable control effectiveness capability as an explicit objective and weaving it into the fabric of every component of the management canvas

Stage 3: Failure of architecture and design. These are “how” mistakes.

-  Taking the wrong approach. Inappropriate strategy and management methods and frameworks



- 1. Capacity.** Limitations on the amount of resources that can be allocated to security and compliance
- 2. Competence.** The level of skill and experience at an individual level to support security and compliance
- 3. Capability.** The level of proficiency at team and organization levels—what people can achieve collectively
- 4. Commitment.** The pledge from stakeholders to undertake the actions needed to achieve security goals
- 5. Communication.** The frequency and quality with which stakeholders exchange information
- 6. Culture.** The sum of an organization's attitudes, actions and behaviors toward security and compliance
- 7. Cost.** The amount of time and money allocated and required to achieve objectives and goals



The risk and compliance landscape

28%

Fewer than one in three organizations achieved full PCI DSS compliance during their interim validation in 2019.¹

\$100k

Organizations found to be in breach of PCI DSS could be fined \$5,000 to \$100,000 per month.²

87%

The majority of consumers said they would not do business with a company if they had concerns about its security practices.³

99%

Nine out of 10 data breaches, and 99% in the retail sector, are financially motivated.⁴ And payment card data is a key target because it's easy to monetize.

1 2020 Payment Security Report, Verizon, 2020.

2 PCI Compliance Guide, PCIcompliance.org

3 The consumer-data opportunity and the privacy imperative, McKinsey, April 2020.

4 2019 Security Priorities Study, IDG, July 2019.



Delivers PCI DSS services in

61 countries*

Over

180 consultants in 30 countries

More than

16k assessments since 2009

Security consulting services since

1999

PCI DSS compliance services since

2003



* PCI Security Standards Council website

Conversation starters

- Do you have a programmatic approach for your PCI DSS program?
- How do you identify PCI DSS threat risks today?
- How do you measure PCI DSS risk and exposure to for your mission, operations and end -users and customers?
- How prepared are you and your team to meet the new PCI DSS v4.0 requirements?
- ✓
 - How long have you been working with the same

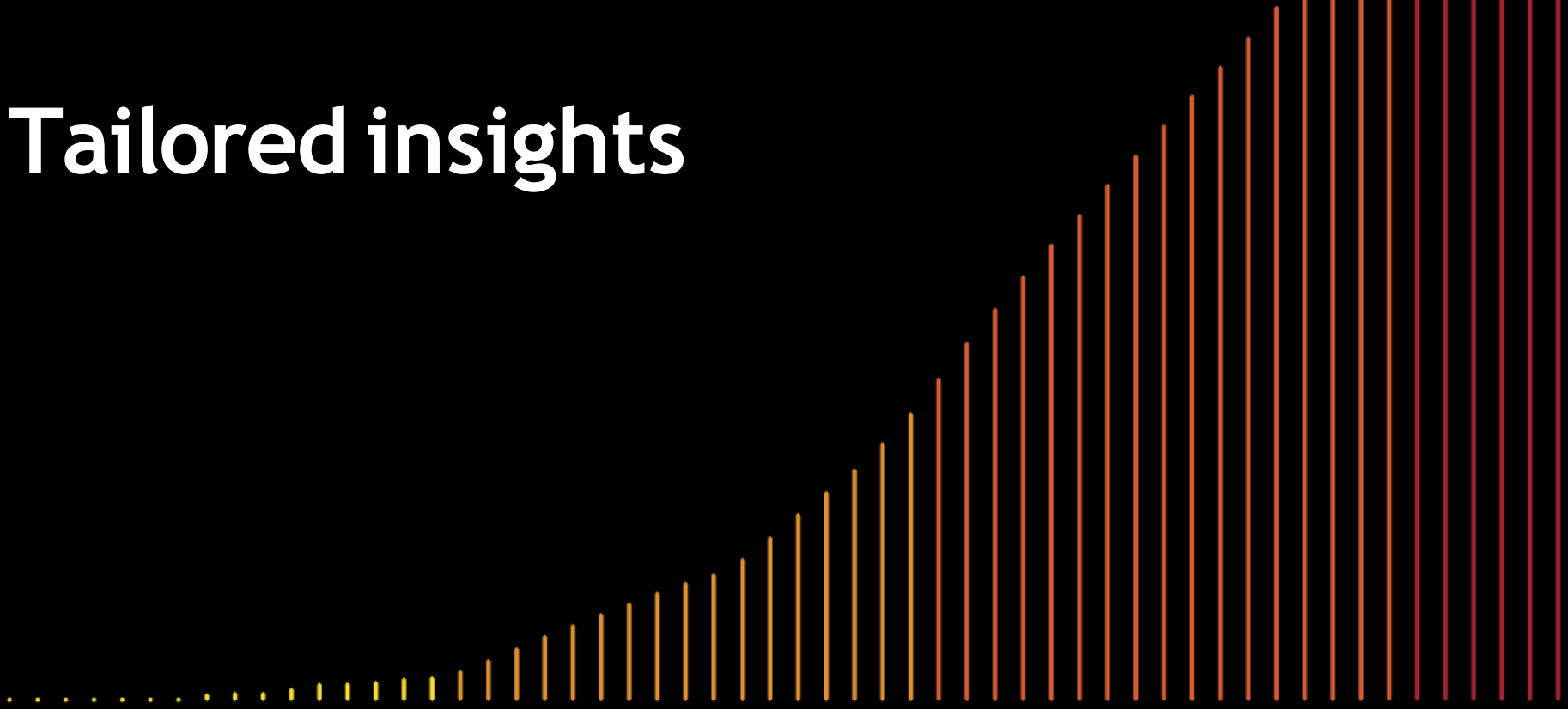




1	Do not delay.	5	Take care when selecting a customized approach.
2	Start strong: Meet PCI DSS v3.2.1.	6	Use control design and mapping templates.
3	Understand the PCI DSS v4.0 requirements.	7	Do early validation of control designs.
4	Choose your control design and validation option wisely.	8	Prepare for ongoing assessments.



Tailored insights



Accommodation and Food Services (NAICS 72)

Frequency	254 incidents, 68 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Social Engineering represent 90% of breaches
Threat actors	External (93%), Internal (9%), Multiple (1%) (breaches)
Actor motives	Financial (100%) (breaches)
Data compromised	Payment (41%), Credentials (38%), Personal (34%), Other (26%) (breaches)
What is the same?	We are seeing the same three attack patterns hitting this sector as we did last year—but the order has changed. External actors continue to target this industry because of the lucrative data the members hold.

Approximately one-third of cases involved the use of Ransomware, and much of the remainder consisted of RAM scrapers.

RAM scrapers targeting the point of sale is the favorite combo in this sector.

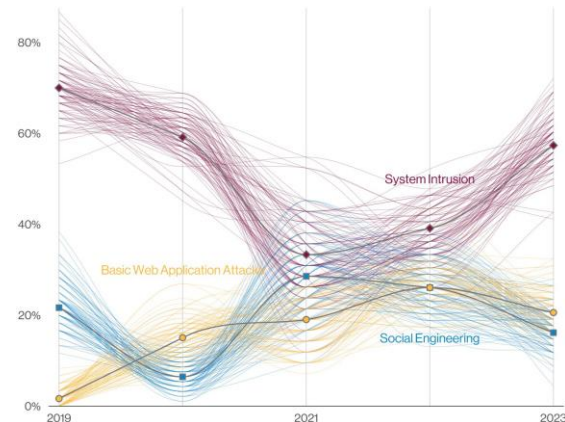


Figure 16. Patterns in Accommodation and Food Services



Educational Services (NAICS 61)

Frequency	497 incidents, 238 with confirmed data disclosure
Top patterns	System Intrusion, Miscellaneous Errors and Social Engineering represent 76% of breaches
Threat actors	External (72%), Internal (29%), Multiple (1%), Partner (1%) (breaches)
Actor motives	Financial (92%), Espionage (8%), Convenience (1%), Fun (1%) (breaches)
Data compromised	Personal (56%), Credentials (40%), Other (25%), Internal (20%) (breaches)
What is the same?	System Intrusion and Miscellaneous Errors are yet again two of the top three patterns for this industry. The ratio of External and Internal actors is nearly the same as last year.

System Intrusion is the number one pattern in Education, Miscellaneous Error is second and Social Engineering took the third-place position from last year's Basic Web Application Attacks.

Hacking was present in 40% of breaches, with Use of stolen credentials appearing in 31% of them.

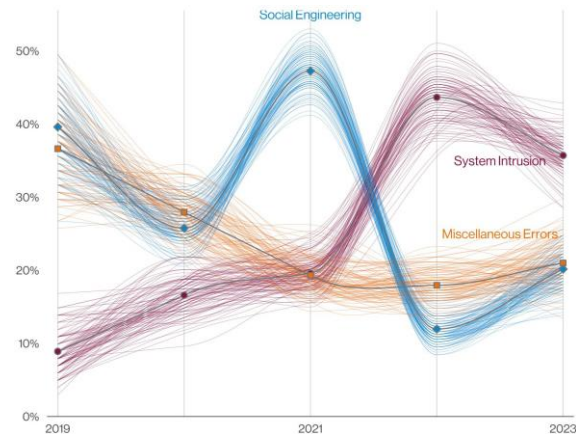


Figure 17. Patterns in Educational Services



Financial and Insurance (NAICS 52)

Frequency	1,832 incidents, 480 with confirmed data disclosure
Top patterns	Basic Web Application Attacks, Miscellaneous Errors and System Intrusion represent 77% of breaches
Threat actors	External (66%), Internal (34%), Multiple (1%) (breaches)
Actor motives	Financial (97%), Espionage (3%), Convenience (1%), Ideology (1%) (breaches)
Data compromised	Personal (74%), Credentials (38%), Other (30%), Bank (21%) (breaches)
What is the same?	The top three patterns remain the same, but their order of ascendancy has rearranged. Personal data, very useful for fraud, continues to be the most desired data type stolen.

The Basic Web Application Attacks pattern is the most prevalent in this sector.

A prominent attack involves Internal actors making mistakes. Misdelivery—where protected data is sent to the wrong recipient—is the most common.

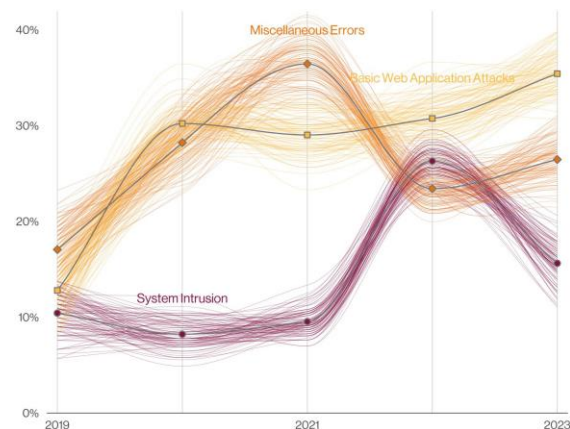


Figure 18. Patterns in Financial and Insurance



Healthcare (NAICS 62)

Frequency	525 incidents, 436 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Miscellaneous Errors represent 68% of breaches.
Threat actors	External (66%), Internal (35%), Multiple (2%) (breaches)
Actor motives	Financial (98%), Espionage (2%), Fun (1%), Ideology (1%) (breaches)
Data compromised	Personal (67%), Medical (54%), Credentials (36%), Other (17%) (breaches)
What is the same?	The top three patterns remain the same, although the order has changed. Internal actors making mistakes continue to trouble this sector.

This sector is beset by ransomware gangs, and there has been an increase of confirmed data breaches associated with criminals taking a copy of the data and releasing it as leverage to get their victims to pay.

Misdelivery continues to be the most common error type in this sector, with both electronic and paper documents being sent to the wrong recipients.

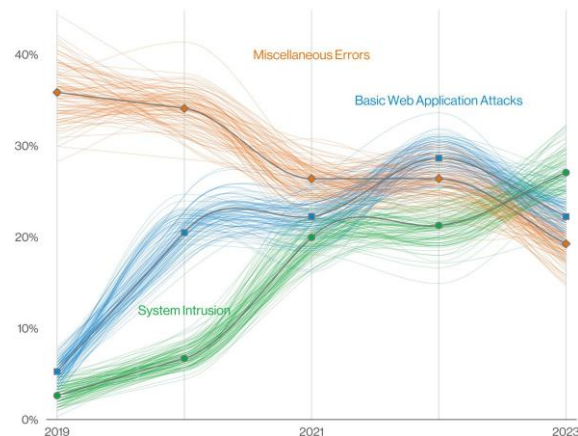


Figure 19. Patterns in Healthcare



Information (NAICS 51)

Frequency	2,110 incidents, 384 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Social Engineering represent 77% of breaches
Threat actors	External (81%), Internal (20%), Multiple (2%), Partner (1%) (breaches)
Actor motives	Financial (92%), Espionage (8%) (breaches)
Data compromised	Personal (51%), Credentials (37%), Other (35%), Internal (19%) (breaches)
What is the same?	System Intrusion remains the top pattern in this vertical, and it is still dominated by Financially motivated external actors.

Error continues to decline in this vertical as it has over the last few years and represents 13% of breaches, while Social Engineering has risen and accounts for 20% of breaches.

Phishing (15%) and Pretexting (11%) present very similar numbers in this vertical, although Pretexting is more common across the whole dataset.

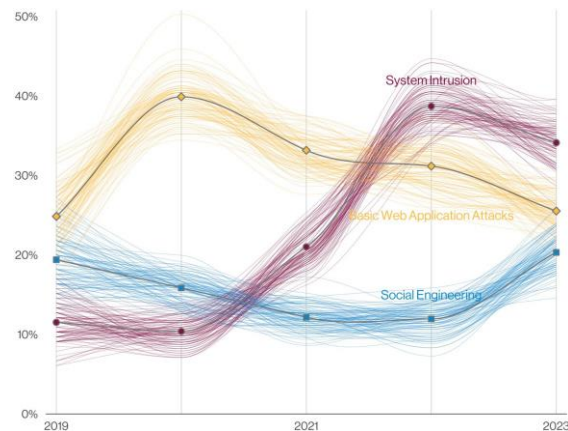


Figure 20. Patterns in Information



Manufacturing (NAICS 31-33)

Frequency 1,817 incidents, 262 with confirmed data disclosure

Top patterns System Intrusion, Social Engineering and Basic Web Application Attacks represent 83% of breaches

Threat actors External (90%), Internal (11%), Multiple (2%), Partner (1%) (breaches)

Actor motives Financial (96%), Espionage (4%), Convenience (1%) (breaches)

Data compromised Personal (60%), Credentials (38%), Other (37%), Internal (18%) (breaches)

What is the same? The top three attack patterns remain the same, but their order has changed slightly. Financially motivated external actors continue to wreak havoc in this industry.

Ransomware, which accounts for a large part of the breaches in the System Intrusion pattern, continues to slowly trend upward in this vertical for the third year in a row.

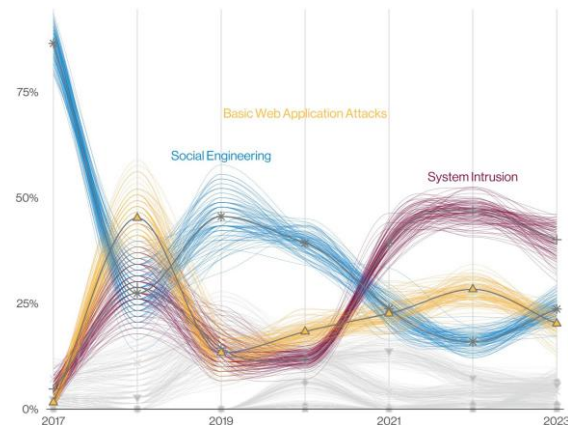


Figure 21. Patterns in Manufacturing



Mining, Quarrying, and Oil & Gas Extraction + Utilities (NAICS 21+22)

Frequency	143 incidents, 47 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Miscellaneous Errors represent 81% of breaches
Threat actors	External (80%), Internal (20%) (breaches)
Actor motives	Financial (63%–93%), Espionage (4%–32%), Grudge (1%–21%), Ideology (0%–15%), Convenience/Fear/Fun/Other/Secondary (0%–7% each) (breaches)
Data compromised	Personal (50%), Internal (33%), Other (26%), Credentials (24%) (breaches)
What is the same?	System Intrusion and Basic Web Application Attacks remain significant causes for concern in this industry.

Ransomware is responsible for approximately one out of three breaches in this vertical. Social Engineering, in spite of its overall rise, has decreased in this industry.

There was a substantial rise in Internal data being compromised, increasing from 9% last year to 33%.

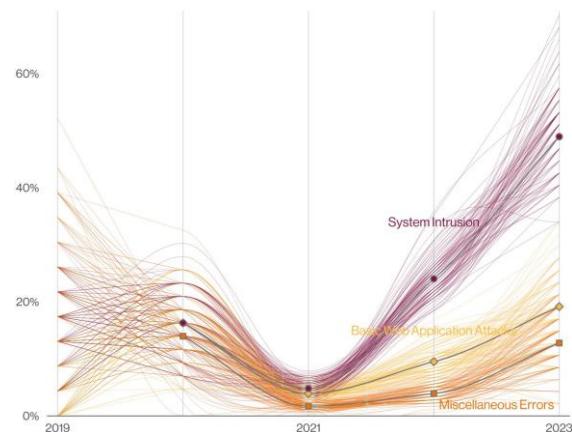


Figure 22. Patterns in Mining, Quarrying, and Oil & Gas Extraction + Utilities



Professional, Scientific and Technical Services (NAICS 54)

Frequency	1,398 incidents, 423 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Social Engineering represent 90% of breaches
Threat actors	External (92%), Internal (9%), Multiple (3%), Partner (2%) (breaches)
Actor motives	Financial (96%), Espionage (4%), Convenience (1%) (breaches)
Data compromised	Personal (57%), Credentials (53%), Other (25%), Internal (16%) (breaches)
What is the same?	System Intrusion, Basic Web Application Attacks and Social Engineering continue to be the main threats to organizations in this sector.

This industry is affected by the big three patterns of System Intrusion (47%), Basic Web Application Attacks (25%) and Social Engineering (18%).

This year, Ransomware accounted for approximately 23% of the incidents in this sector, which is a notable increase from last year's 14%.

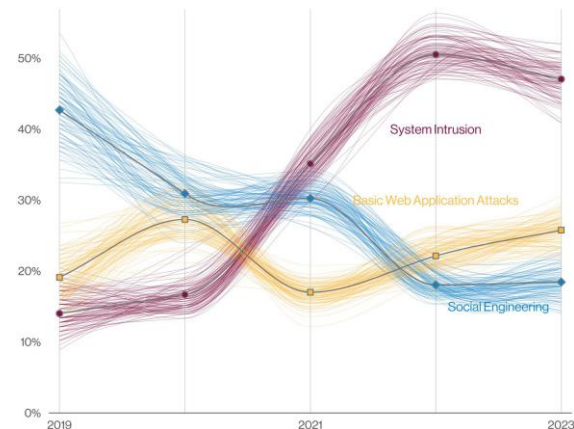


Figure 23. Patterns in Professional, Scientific and Technical Services



Public Administration (NAICS 92)

Frequency	3,273 incidents, 584 with confirmed data disclosure
Top patterns	System Intrusion, Lost and Stolen Assets, and Social Engineering represent 76% of breaches
Threat actors	External (85%), Internal (30%), Multiple (16%) (breaches)
Actor motives	Financial (68%), Espionage (30%), Ideology (2%) (breaches)
Data compromised	Personal (38%), Other (35%), Credentials (33%), Internal (32%) (breaches)
What is the same?	This sector continues to be targeted by Financially motivated external threat actors as well as spying Nation-states that are interested in what their rivals are doing. Personal data remains the most often stolen data type.

This is a sector where the Espionage motivation is the highest.

While ransomware continues to be an issue that disrupts the smooth running of government entities, we did see a slight decrease from last year's total.

Evidence of collusion with multiple Actor breaches was significant at 16% in this sector. Given that the overall dataset has just 2% of these kinds of cooperative breaches, it is concerning that Internal and External actors are combining forces to steal data from the public sector.

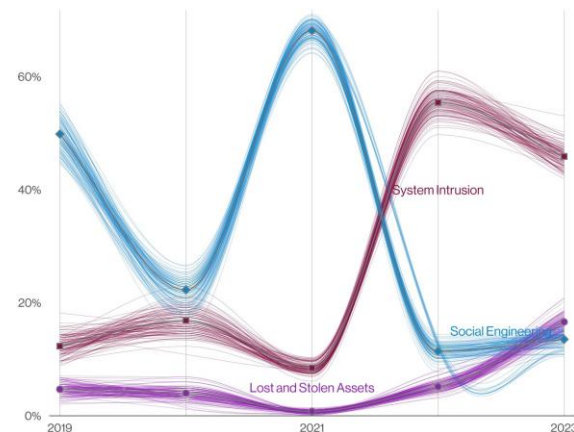


Figure 24. Patterns in Public Administration



Retail (NAICS 44-45)

Frequency	406 incidents, 193 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 88% of breaches
Threat actors	External (94%), Internal (7%), Multiple (2%), Partner (2%) (breaches)
Actor motives	Financial (100%), Espionage (1%) (breaches)
Data compromised	Payment (37%), Credentials (35%), Other (32%), Personal (23%) (breaches)
What is the same?	Retail organizations continue to be lucrative targets for cybercriminals looking to collect Payment card data.

Payment card data is one of the most common data types breached in this sector, accounting for 37% of breaches this year.

70% of Payment card breaches in Retail originated from Web applications, 17% from Gas terminals and 8% from Point-of-sale (PoS) servers.

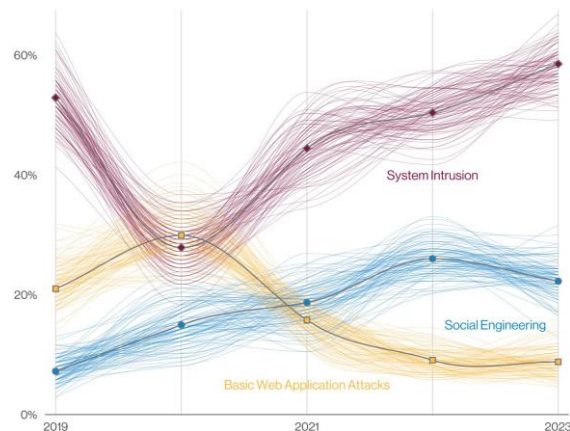
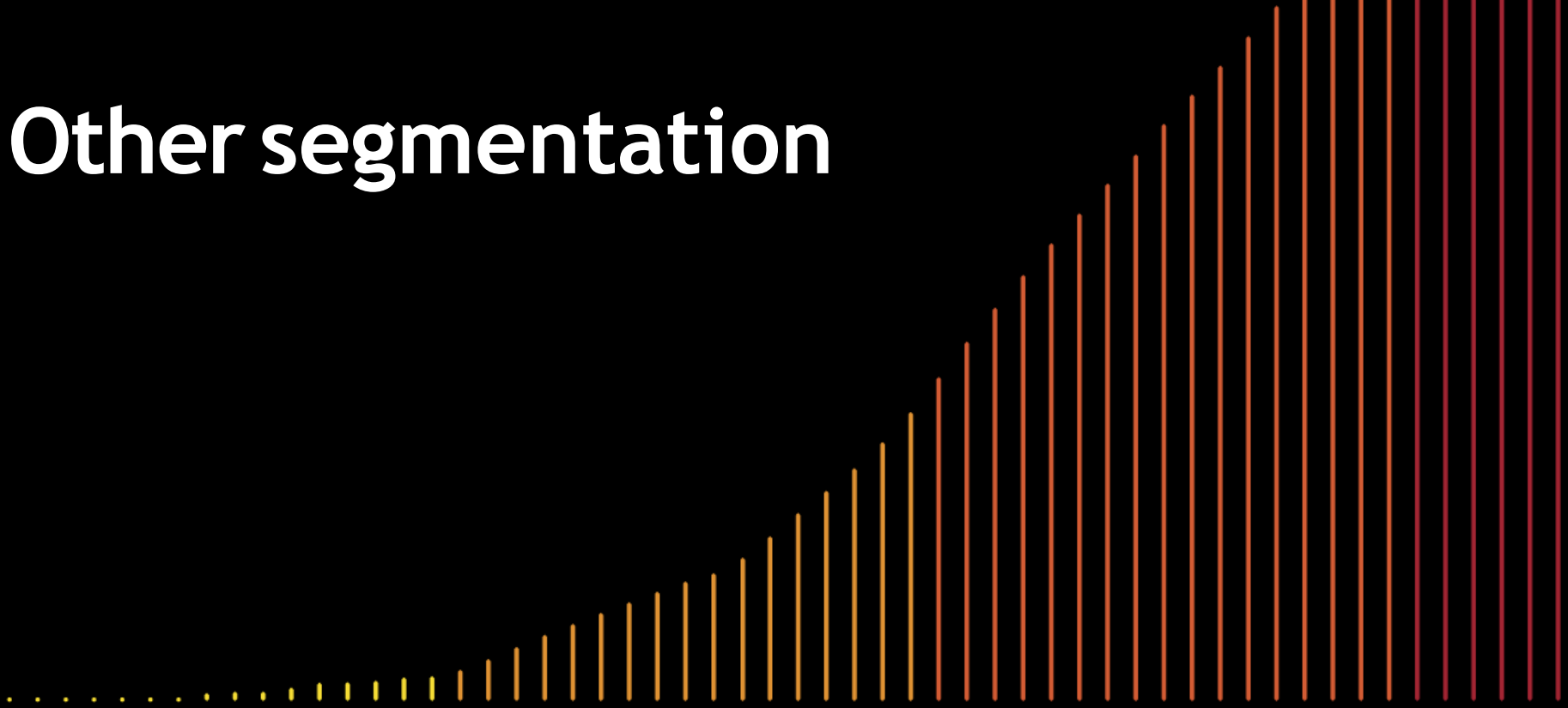


Figure 25. Patterns in Retail



Other segmentation



SMB (less than 1,000 employees)

Frequency	699 incidents, 381 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 92% of breaches
Threat actors	External (94%), Internal (7%), Multiple (2%), Partner (1%) (breaches)
Actor motives	Financial (98%), Espionage (1%), Convenience (1%), Grudge (1%) (breaches)
Data compromised	Credentials (54%), Internal (37%), Other (22%), System (11%) (breaches)

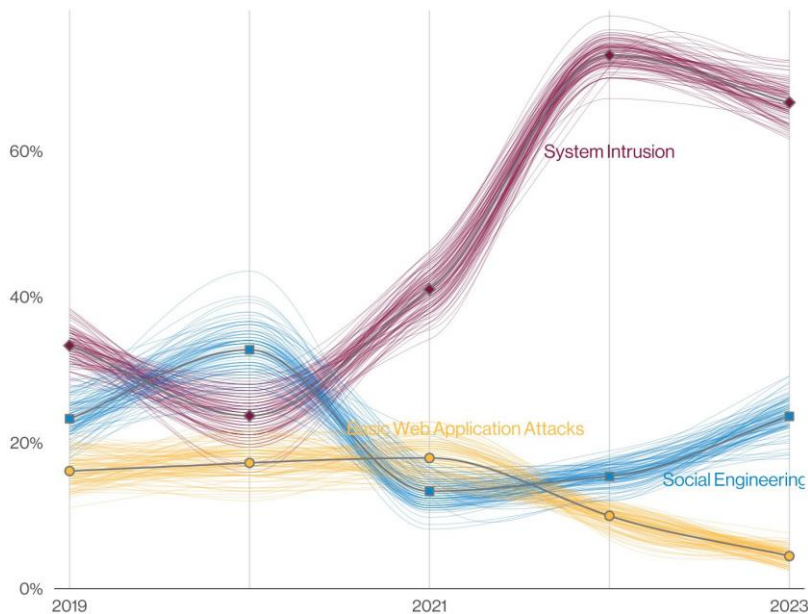


Figure 26. Patterns in SMB

SMB: small- and medium-sized businesses



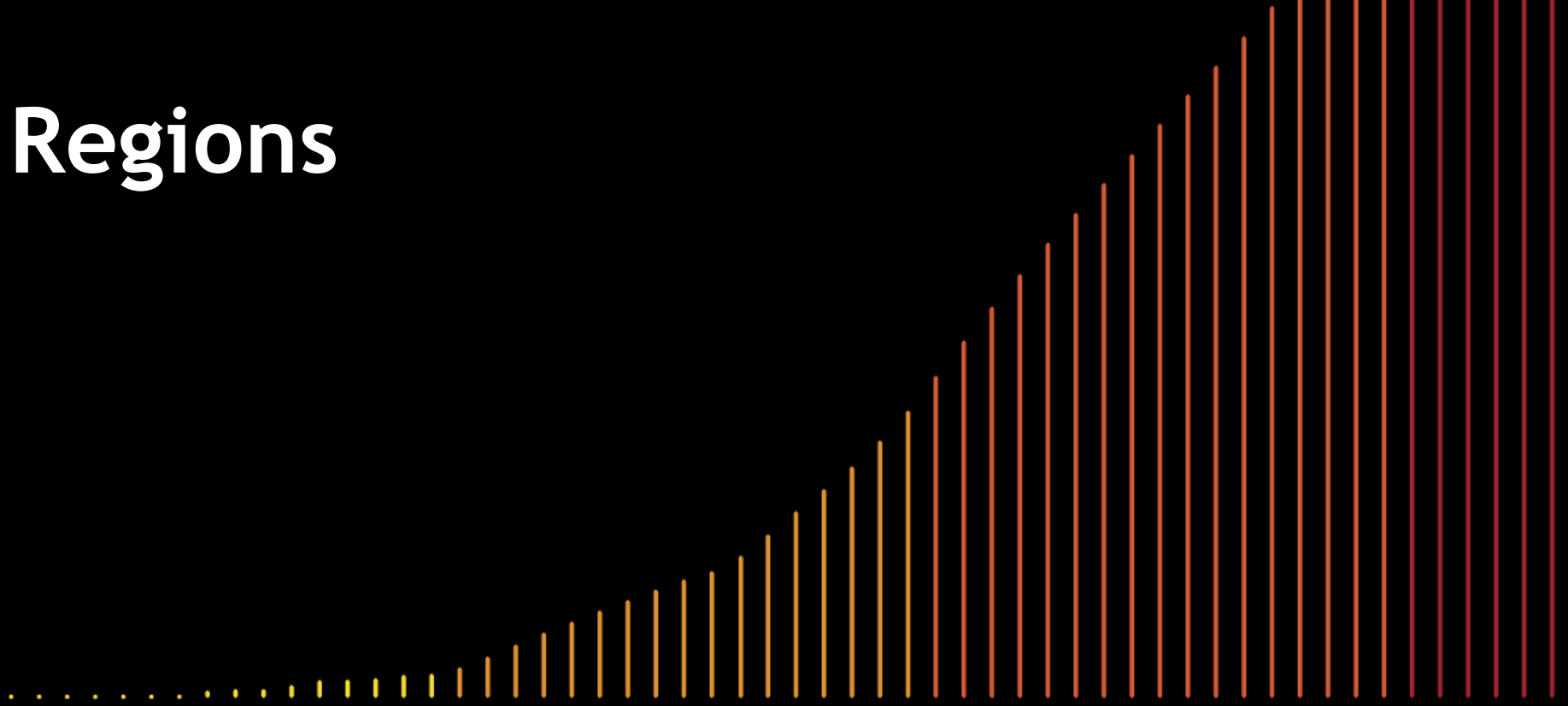
SMB (less than 1,000 employees) - recommended controls

CIS Control	IG	Description
14	IG1	Security Awareness and Skills Training Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.
11	IG1	Data Recovery Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a preincident and trusted state.
5	IG1	Access Control Management Use processes and tools to create, assign, manage and revoke access credentials and privileges for user, administrator and service accounts for enterprise assets and software.
17	IG2	Incident Response Management Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training and communications) to prepare, detect and quickly respond to an attack.
16	IG3	Application Software Security Manage the security life cycle of in-house developed, hosted or acquired software to prevent, detect and remediate security weaknesses before they can impact the enterprise.
18	IG3	Penetration Testing Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes and technology) and simulating the objectives and actions of an attacker.

CIS: Center for Internet Security
IG: Implementation Group



Regions



Regions - details

Region	Frequency	Top patterns	Threat actors	Actor motives	Data compromised
APAC	699 incidents, 164 with confirmed data disclosure	Social Engineering, System Intrusion and Basic Web Application Attacks represent 93% of breaches	External (92%), Internal (9%), Partner (2%), Multiple (2%) (breaches)	Financial (61%), Espionage (39%), Convenience (2%), Grudge (2%), Secondary (1%) (breaches)	Internal (56%), Secrets (42%), Other (33%), Credentials (29%) (breaches)
EMEA	2,557 incidents, 637 with confirmed data disclosure	System Intrusion, Social Engineering and Basic Web Application Attacks represent 97% of breaches	External (98%), Internal (2%), Multiple (1%) (breaches)	Financial (91%), Espionage (8%), Ideology (1%), Fun (1%) (breaches)	Credentials (53%), Internal (37%), System (35%), Other (15%) (breaches)
LAC	535 incidents, 65 with confirmed data disclosure	System Intrusion, Social Engineering and Basic Web Application Attacks represent 94% of breaches	External (95%), Internal (5%), Partner (2%), Multiple (2%) (breaches)	Financial (93%), Espionage (11%), Ideology (2%) (breaches)	System (55%), Internal (32%), Classified (23%), Credentials (23%), Other (19%) (breaches)
NA	9,036 incidents, 1,924 with confirmed data disclosure	System Intrusion, Basic Web Application Attacks and Social Engineering represent 85% of breaches	External (94%), Internal (12%), Multiple (9%), Partner (2%) (breaches)	Financial (99%), Espionage (1%), Grudge (1%) (breaches)	Credentials (67%), Internal (50%), Personal (38%), Other (24%) (breaches)



Regions - Northern America

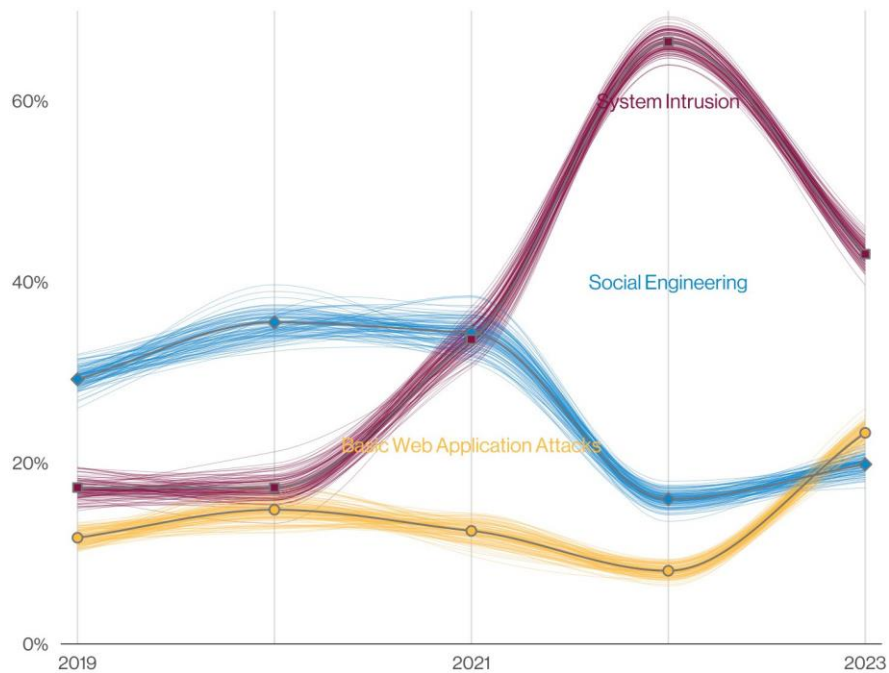


Figure 27. Patterns in Northern America



Regions - EMEA and APAC

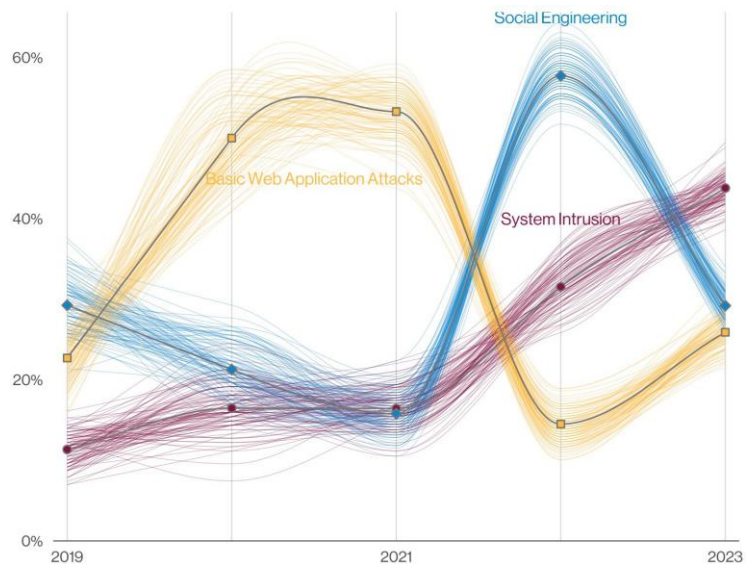


Figure 28. Patterns in EMEA

APAC: Asia Pacific
EMEA: Europe, Middle East and Africa

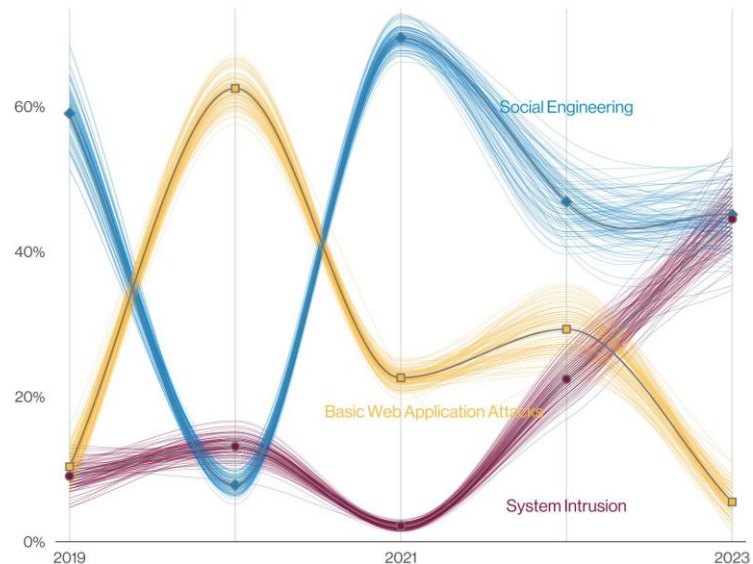
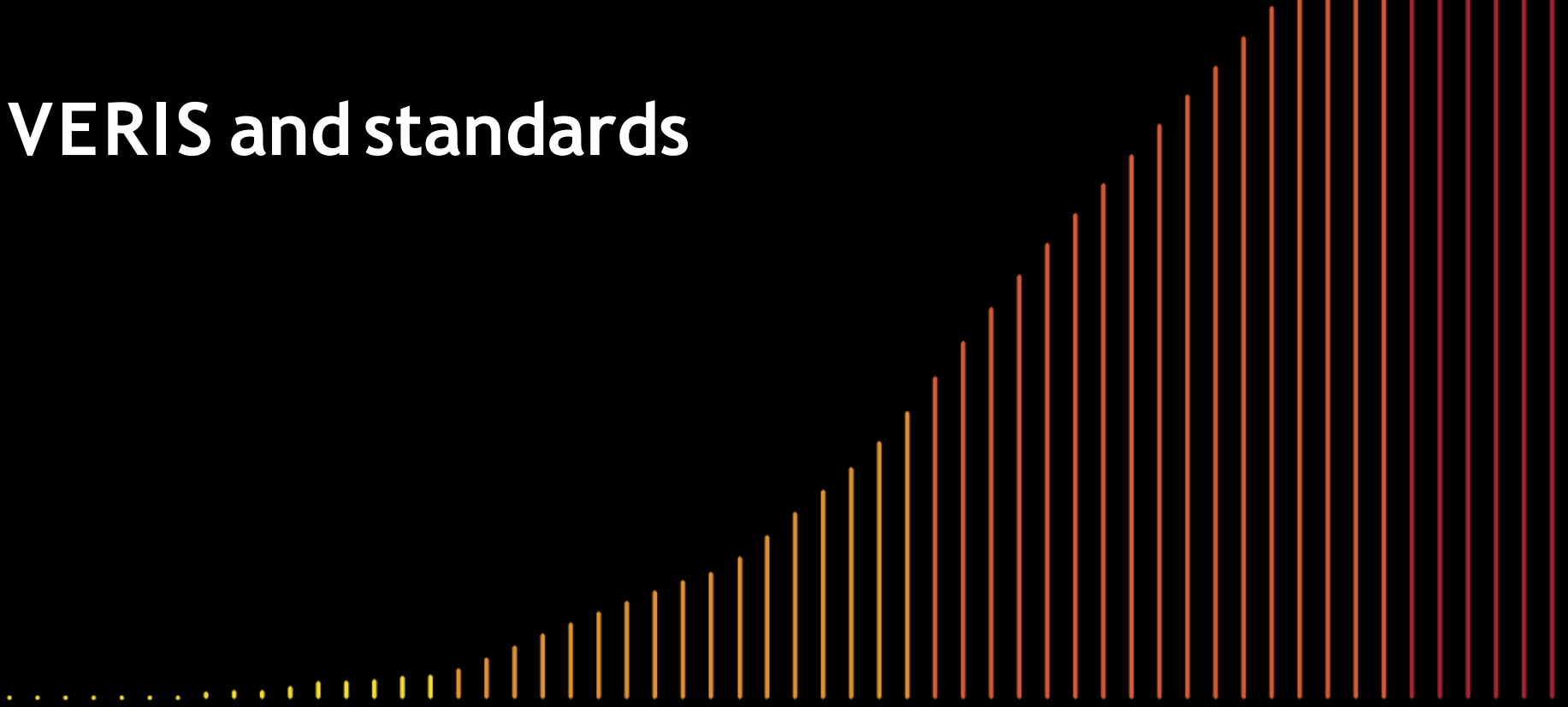


Figure 29. Patterns in APAC



VERIS and standards



VERIS and standards

- **Vocabulary for Event Recording and Incident Sharing (VERIS)**
- **Created to standardize collection of key incident information**
 - Victim
 - Actors, Actions, Assets, Attributes
 - Impact
- **Collaboration with Center for Threat Informed Defense (CTID):**
 - Mapping with MITRE ATT&CK update - April 6, 2023

Key links:

<https://verisframework.org/>

<https://www.github.com/vz-risk/veris>

https://center-for-threat-informed-defense.github.io/attack_to_veris/

https://github.com/center-for-threat-informed-defense/attack_to_veris/



VERIS and ATT&CK mapping update

VERIS + MITRE ATT&CK®

VERIS enumeration

VERIS enumeration breakdown

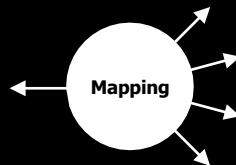
Threat action: hacking

Tactic used to cause or contribute to the incident: intentional, unauthorized access of information assets

Vector: desktop sharing software

The means through which the action took place: use of graphical desktop sharing

Action: hacking
Vector: desktop sharing software



ATT&CK Techniques

T1021.001
Remote Services:
Remote Desktop Protocol

T1021.005
Remote Services: VNC

T1133
External Remote Services

T1219
Remote Access Software

ATT&CK Technique summary

Adversary technique of behaviors

How an adversary achieves a tactical goal by performing an action

Remote access software and services

Leveraging of remote services to initially access, move laterally and/or persist within a network

Bidirectional mapping between VERIS and ATT&CK

Find out more:

https://github.com/center-for-threat-informed-defense/attack_to_veris



Questions?

DBIR: [verizon.com/dbir](https://www.verizon.com/dbir)

Email: dbir@verizon.com

If you are interested in becoming a contributor to the annual Verizon DBIR (and we hope you are), the process is very easy and straightforward. Please email us at dbircontributor@verizon.com.



verizon

The Last 2 Weeks In Cyber

The Last 2 Weeks in Cyber

[Android – Chisel Malware Analysis Report](#) – Active Exploit

[Vmware Tools Update Issued](#)

[CISA – Mounting a Defense Against DDoS](#)

[Citrix Netscaler – Current Exploits](#) – Active Exploit

[Nation State Actors Exploiting ManageEngine, Fortinet, ScreenConnect](#) – Active Exploit

[Barracuda – Submarine, Skipjack, Seaspray, Whirlpool and Saltware Backdoors](#) – Active Exploit

The Last 2 Weeks in Cyber

[CISA/FBI/NSA – Information on Deepfakes](#)

[Adobe Connect, Acrobat and Reader](#) – Active Exploit

[Microsoft Monthly Patches](#)

- Patch Tuesday Dashboard: <https://patchtuesdaydashboard.com/>
- Ask Woody - <https://www.askwoody.com/2023/september-patches-apple-headlines-and-browsers>

[Apple Updates](#) – NSO Pegasus Detected

[Cisco ASA and Firepower](#) – Active Exploit

[Google Chrome Updates](#) – Active Exploit

QR Code Problems

file with you

Scan the QR code with the camera program on your mobile device to access your files.

Microsoft

QR Code

soft Security Policy

soft 2FA Security Authenticator access expires soon.
Getting locked out of your account, scan the QR code below w
ide expires in 72 hours.

Example phishing page

Microsoft

Enter password

password

Forgot my password

Sign in with a security key

Sign in with another account

Sign in

Example initial landing page

I'm not a robot


reCAPTCHA

Privacy - Terms

Currently Being Exploited

Currently Being Exploited

 [Adobe Connect, Acrobat and Reader](#) – Active Exploit

 [Apple Updates](#) – NSO Pegasus Detected – Active Exploit

 [Cisco ASA and Firepower](#) – Active Exploit

 [Google Chrome Updates](#) – Active Exploit

 [Android – Chisel Malware Analysis Report](#) – Active Exploit

 [Barracuda – Submarine, Skipjack, Seaspray, Whirlpool and Saltware Backdoors](#) – Active Exploit

 [Nation State Actors Exploiting ManageEngine, Fortinet, ScreenConnect](#) – Active Exploit

 [Citrix Netscaler – Current Exploits](#) – Active Exploit

Breaches In The News

Breaches In The News

- MGM –
 - <https://www.bleepingcomputer.com/news/security/mgm-casinos-esxi-servers-allegedly-encrypted-in-ransomware-attack/>
 - 30 Million Ransom Paid
 - Okta involved
 - ESXi
 - Hackers could be English speaking Teens and young adults 16-22 years old



Breaches In The News

- University of Michigan
- Johnson and Johnson
- Airbus
 - [FBI Hacker Dropped Stolen Airbus Data on 9/11](#)
- Updates to LastPass Breach
 - [Experts Fear Crooks are Cracking Keys Stolen in LP Breach](#)
- Jeff Wyler
- Antioch University

Other News

Other News

iOS 17 Released – Reported Incompatibilities

.US Domain Continues Abuse

Update On Israel Trip

- Dave Evans – Ahresty
- Ken Carrier – City of Hamilton
- Joe Finley - Fortinet
- Mark Leff – Exclusive Networks
- Kyle Zech – Secure Cyber Defense

Other News

GCC Use of Signal - Testing

GCC Website Operational

GCC Board Appointments

- Shawn Waldman - Executive Director
- Kyle Jones - Vice President
- Gary Estes - Secretary
- Randy Miller -WPAFB - Treasurer

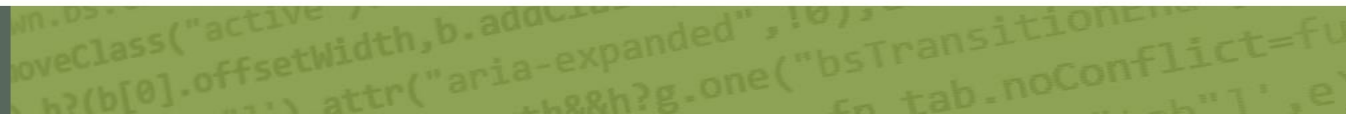
Sample Intelligence Sources

BLEEPINGCOMPUTER

Krebs on Security
In-depth security news and investigation



Deloitte.





Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Remote Access VPN Unauthorized Access Vulnerability



Advisory ID: [cisco-sa-asaftd-ravpn-auth-8LyfCkeC](#) [CVE-2023-20269](#)

First Published: 2023 September 6 16:00 GMT

Last Updated: 2023 September 11 18:21 GMT

Version 1.1: [Interim](#)

Workarounds: [Yes](#)

Cisco Bug IDs: [CSCwh23100](#)
[CSCwh45108](#)

CVSS Score: [Base 5.0](#)

[Download CSAF](#)

[Download CVRF](#)

[Email](#)

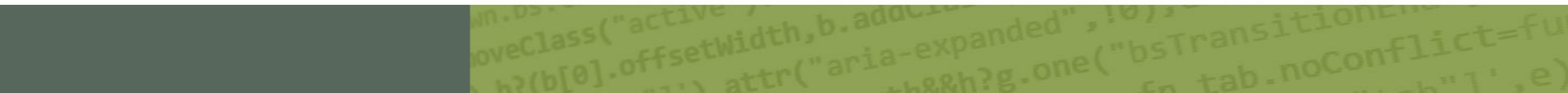
Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the [Security Vulnerability Policy](#). This document also contains instructions for obtaining fixed software and



Known Exploited Vulnerabilities Catalog

CVE-2023-20269	Cisco	Adaptive Security Appliance and Firepower Threat Defense	Cisco Adaptive Security Appliance and Firepower Threat Defense Unauthorized Access Vulnerability	2023-09-13
--------------------------------	-------	--	--	------------



Steps to Success

Event Sponsors



FORTINET®