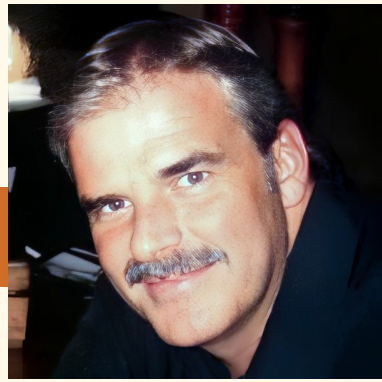
/// CYBER SECURITY ///

Debi Enright – Executive Director, Information Security, American Career Colleges
Louis Archbold – Managing Principal, Rapid Response Retainer, Verizon Threat Research Advisory Center



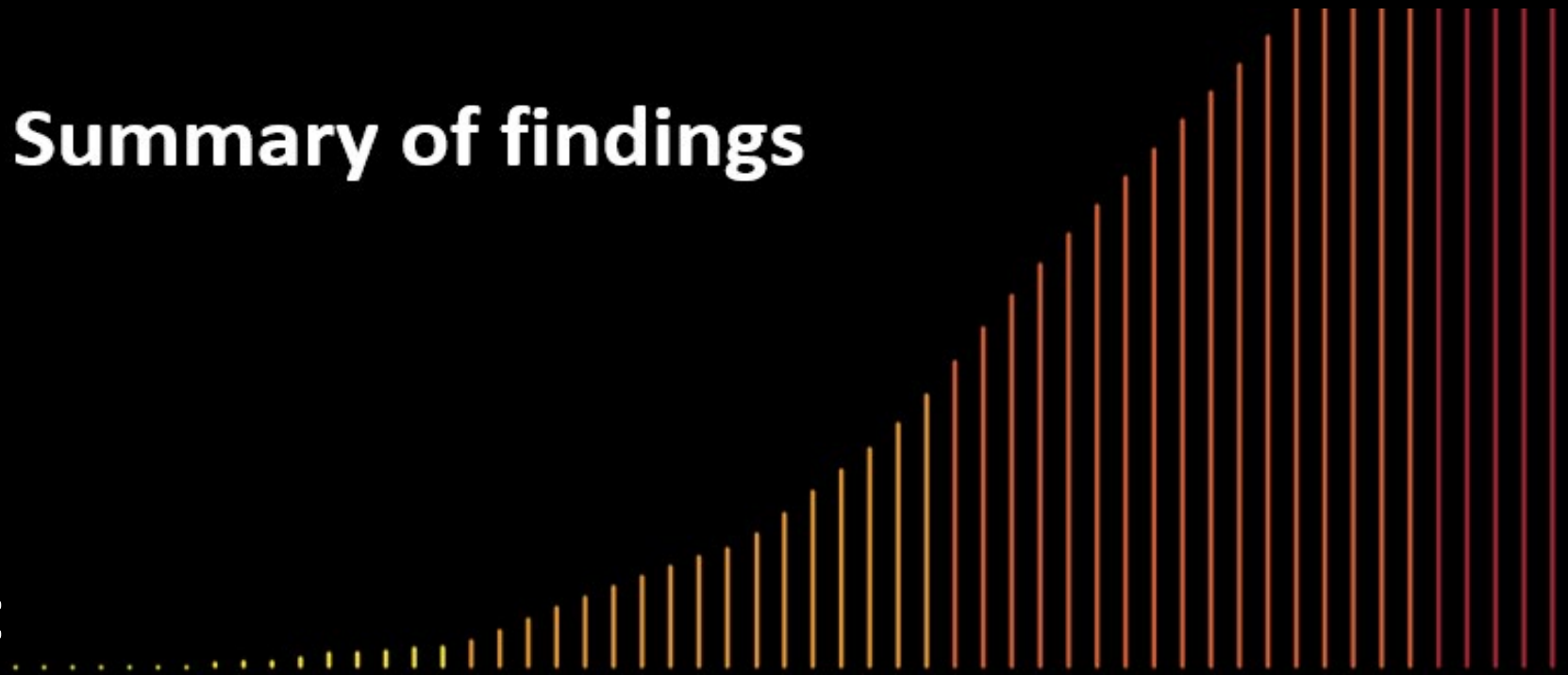
Today's High-Value Targets - Higher Education Institutions

"You cannot escape the responsibility of tomorrow by evading it today." – Abraham Lincoln

Summary of findings

DBIR

2023 Data Breach Investigations Report Presentation



The authoritative source of cybersecurity breach information

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?

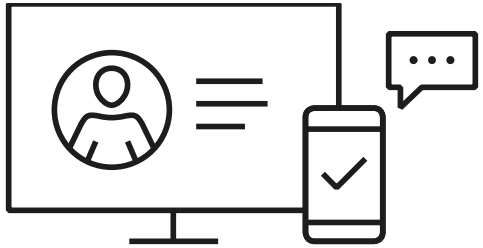
Organized crime is the leading source of cyberattacks.

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.

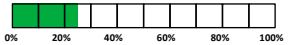


Pretexting rose.

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.

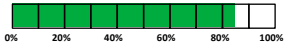
What we found:

24%



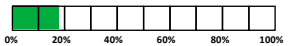
24% of all cyberattacks involved Ransomware.

83%



83% of breaches were by External actors, typically looking for money and data.

19%



19% of breaches came from Internal actors, who caused both intentional and unintentional harm.

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 included 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.

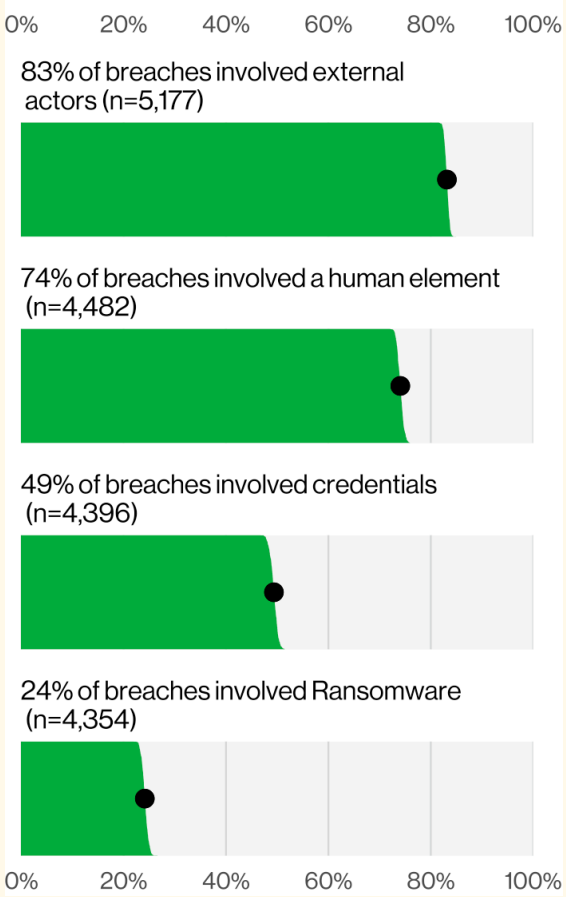


Figure 1. Select key enumerations

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.

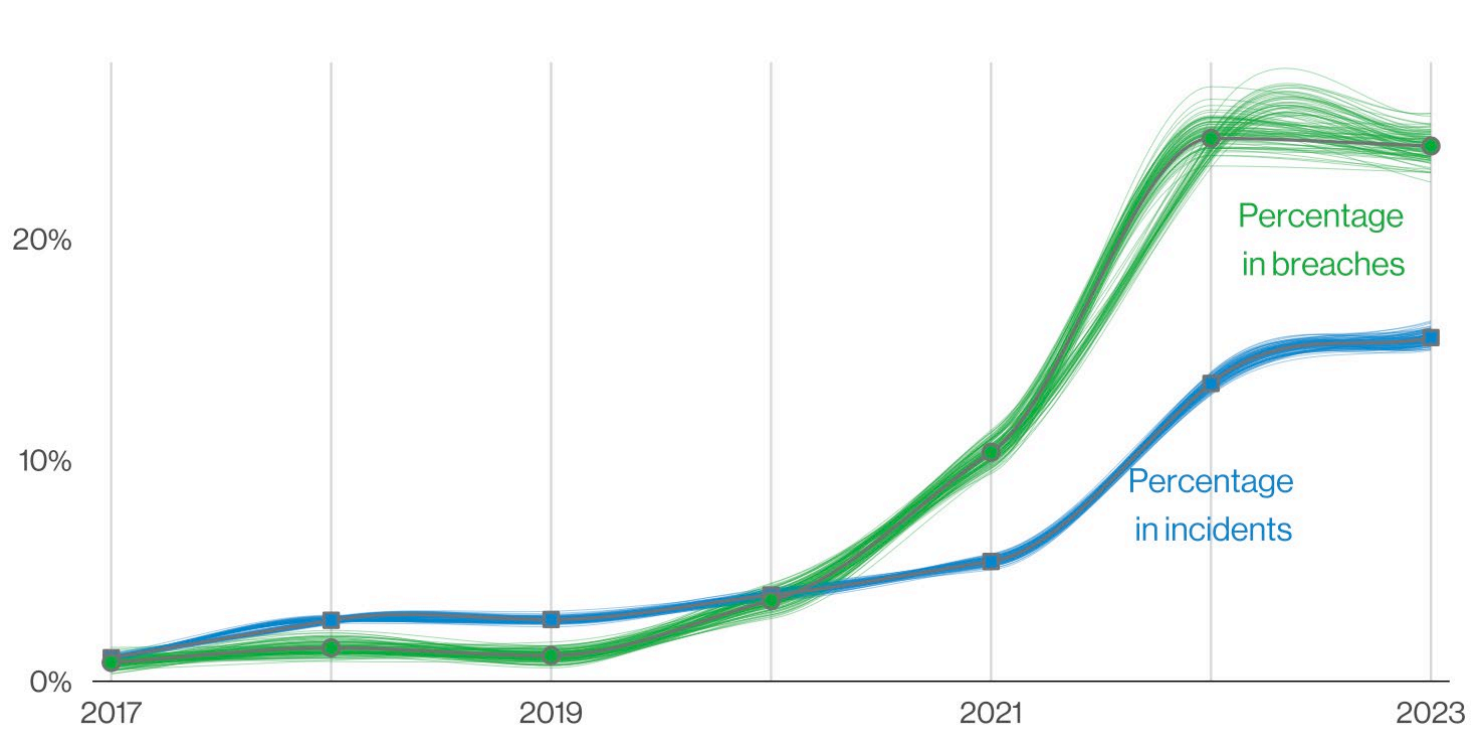


Figure 2. Ransomware action variety over time

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.

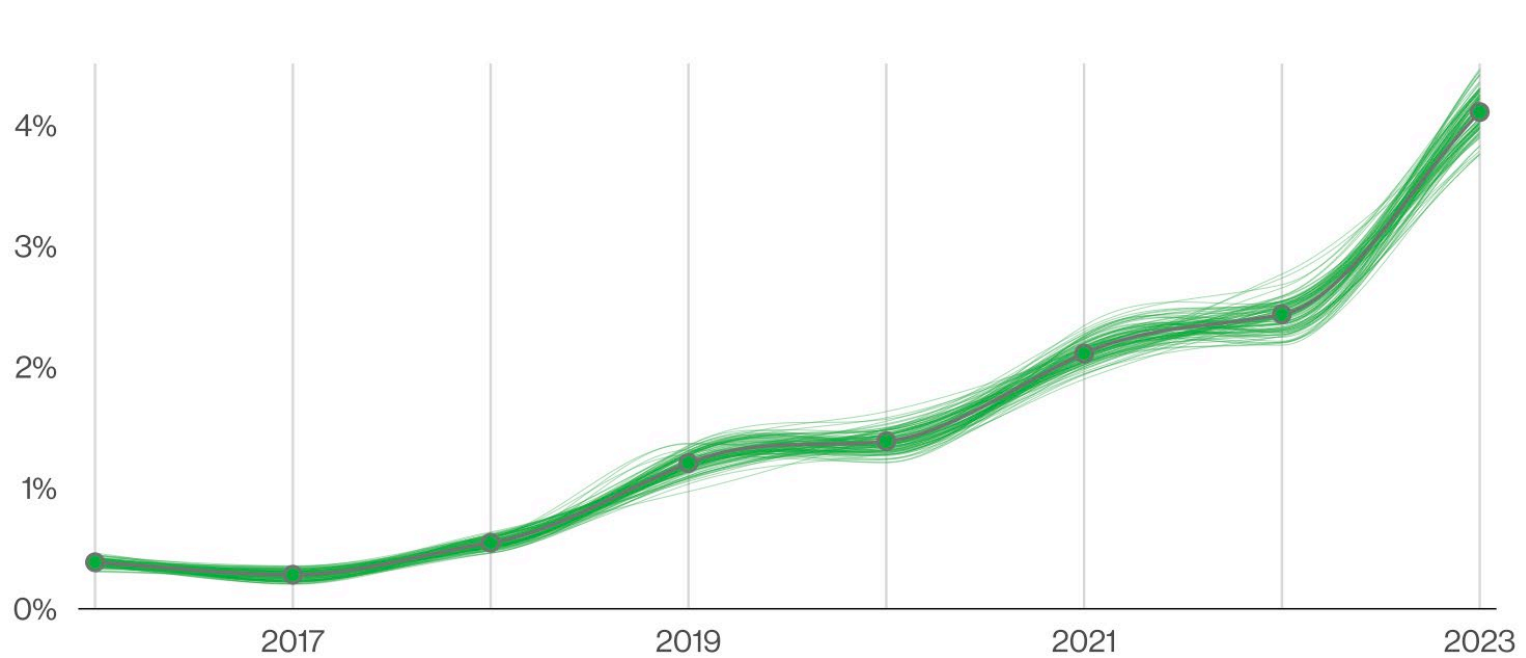


Figure 3. Pretexting incidents over time

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?

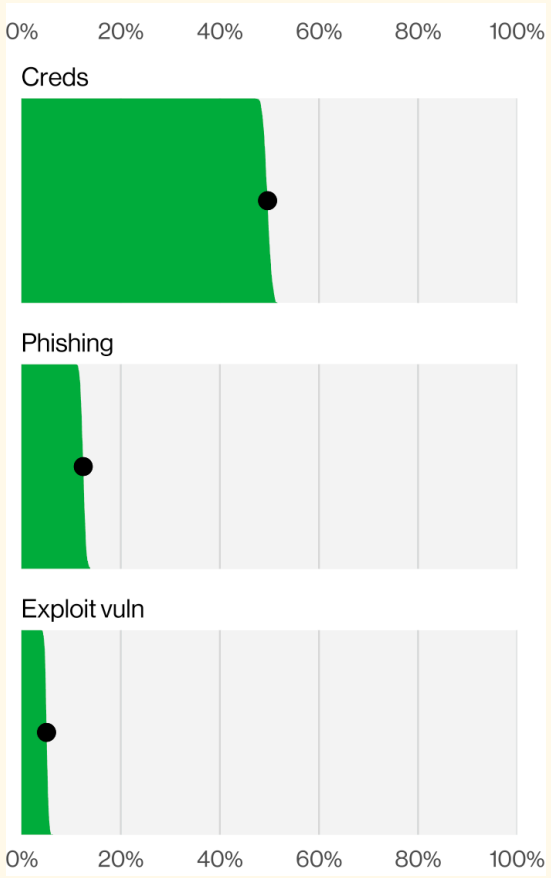


Figure 4. Select enumerations in non-Error, non-Misuse breaches (n=4,291)

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.

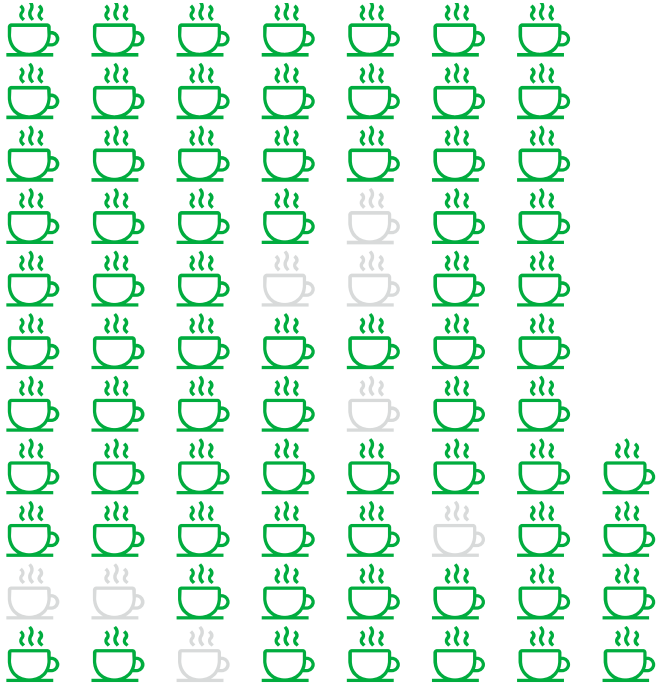


Figure 5. Percentage of identified Exploit vuln that was Log4j (n=81). Each glyph represents an incident.

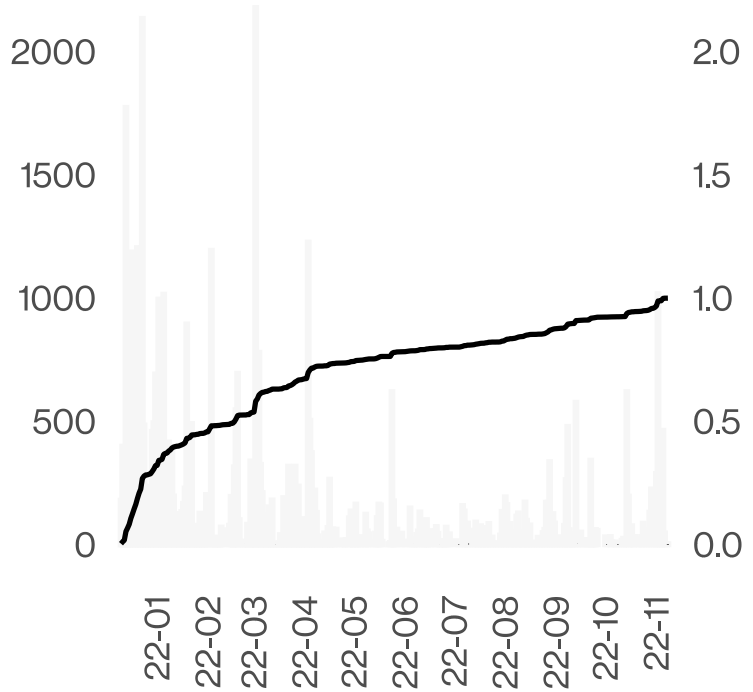
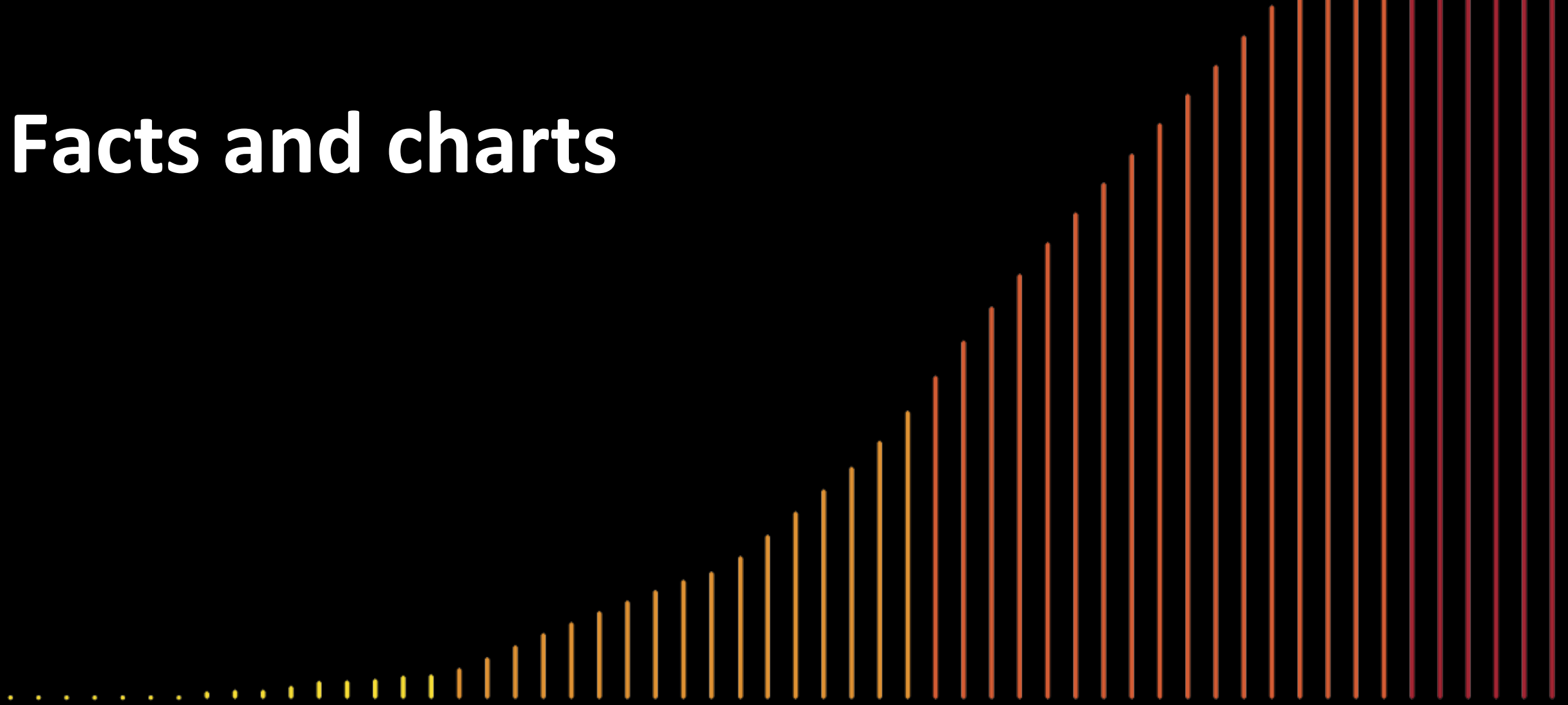


Figure 6. Percentage of Log4j scanning for 2022

Facts and charts



Incident patterns

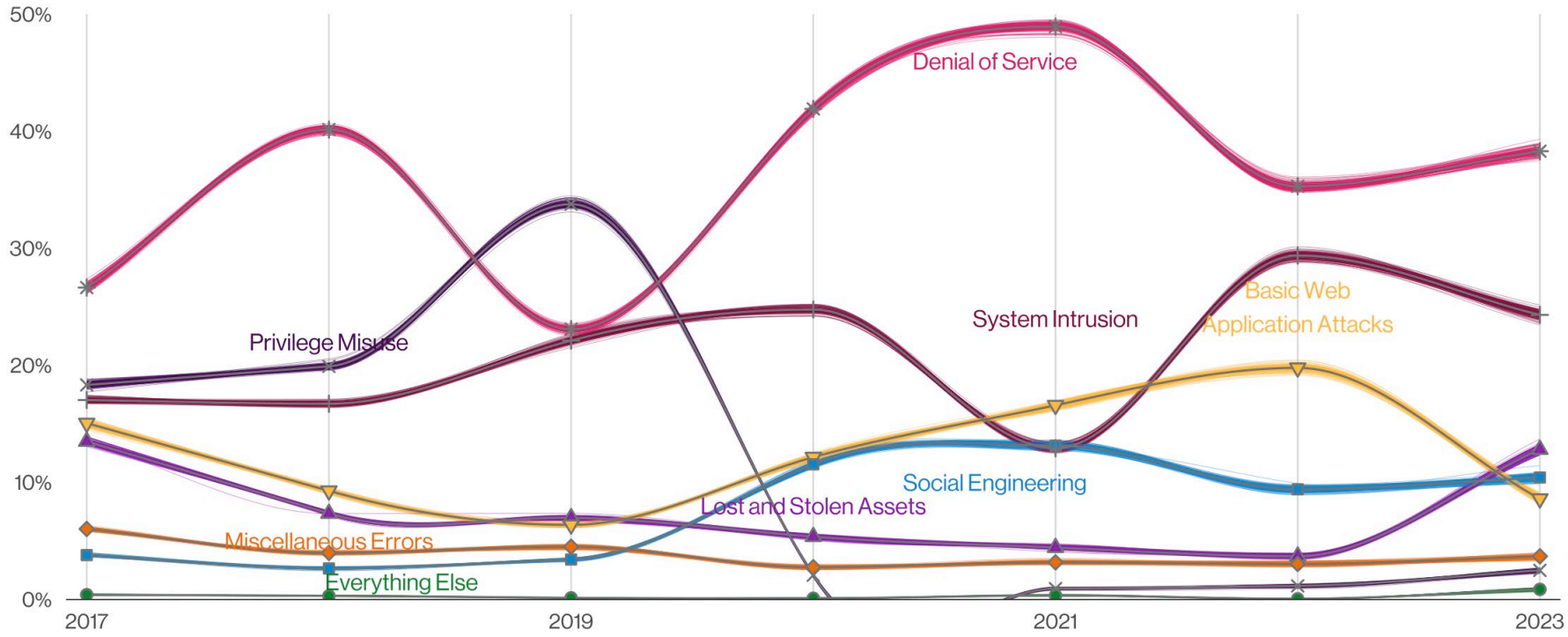


Figure 7. Patterns over time in incidents

Breach patterns

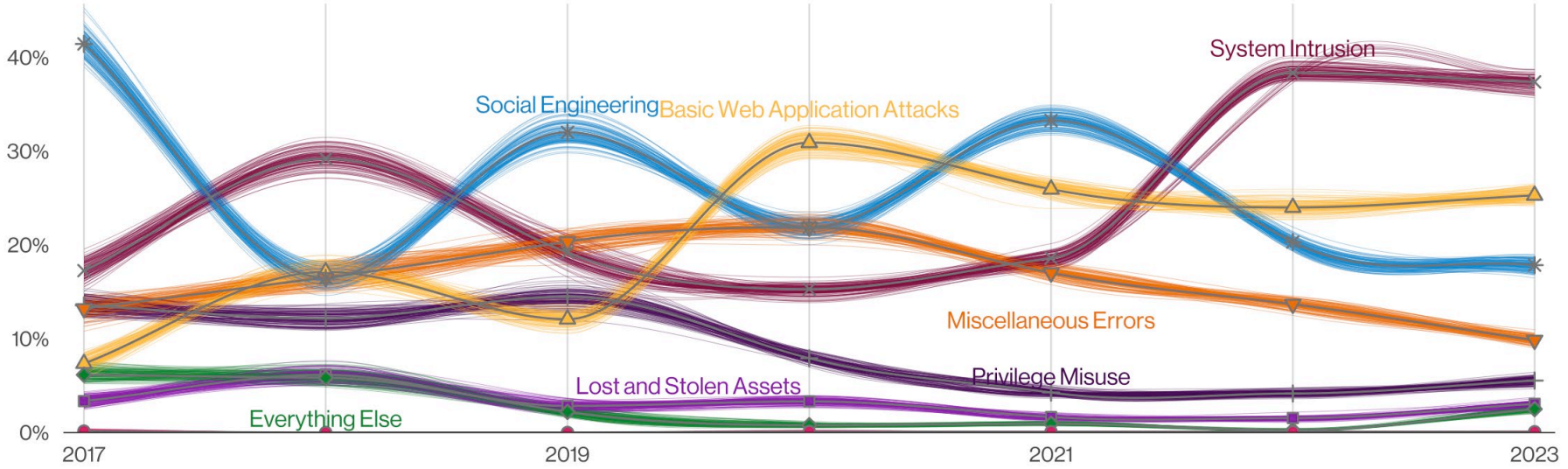


Figure 8. Patterns over time in breaches

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.

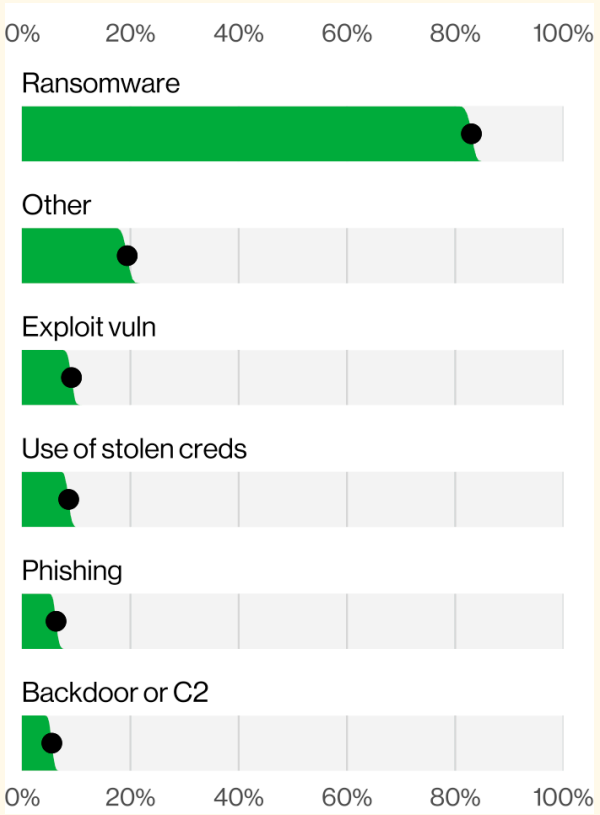


Figure 9. Action varieties in System Intrusion incidents (n=2,700)

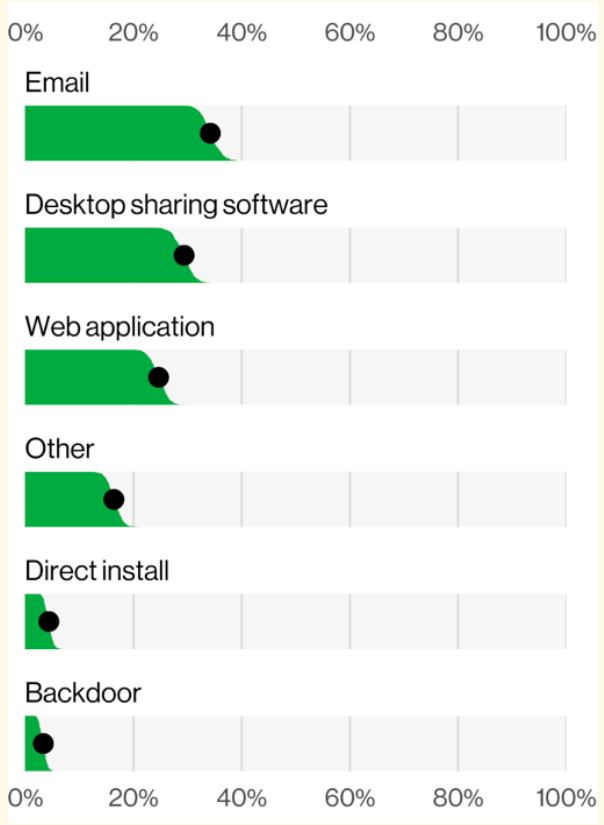


Figure 10. Action vectors for Ransomware (n=690)

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.

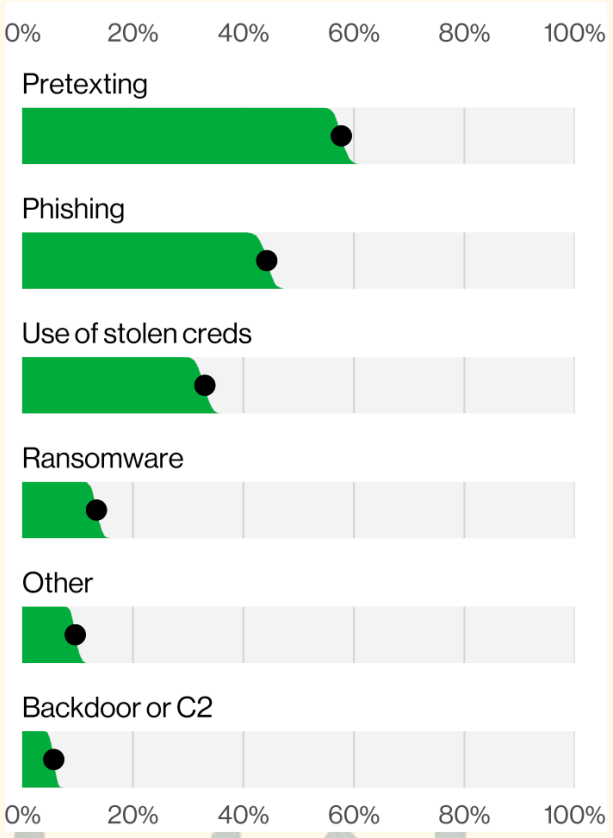


Figure 11. Action varieties in Social Engineering incidents (n=1,696)

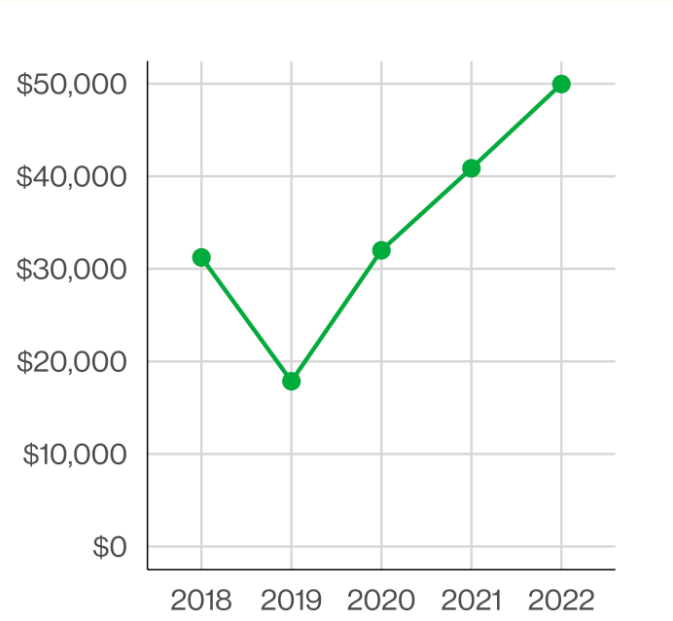


Figure 12. Median transaction size for BECs (n=73,420). Based on FBI IC3 complaints where a transaction occurred.

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.

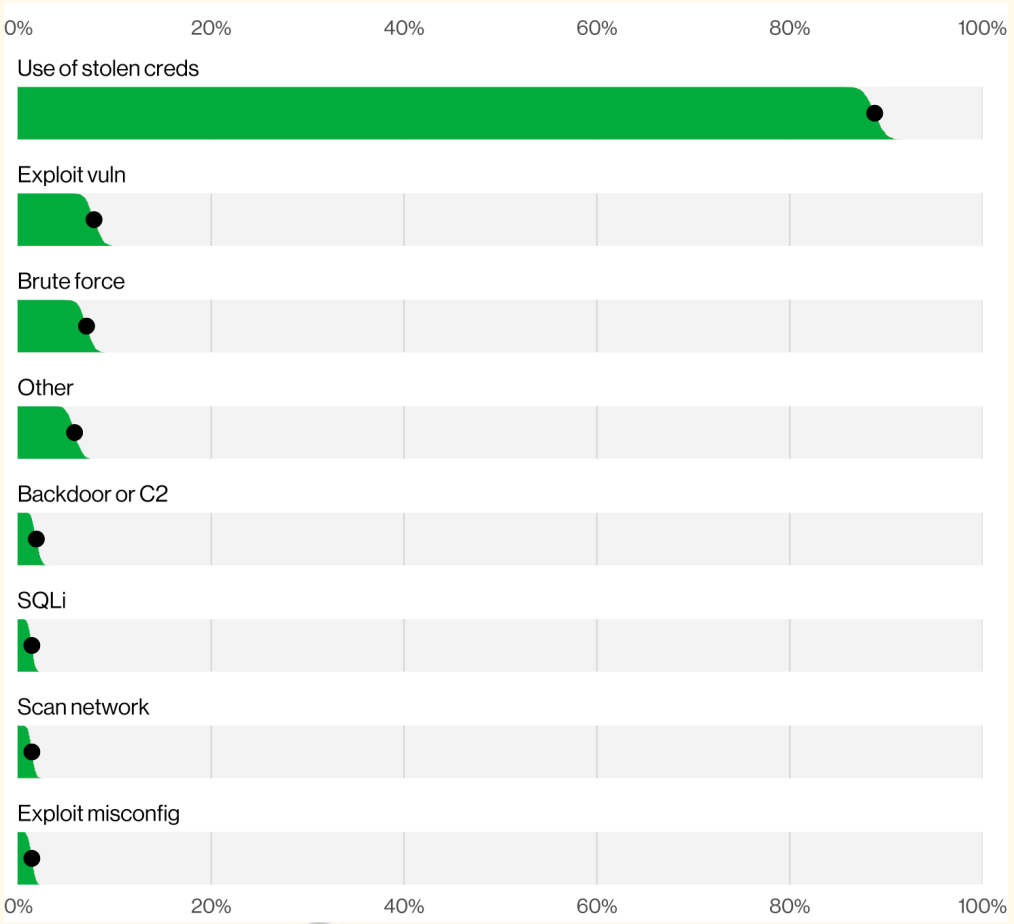
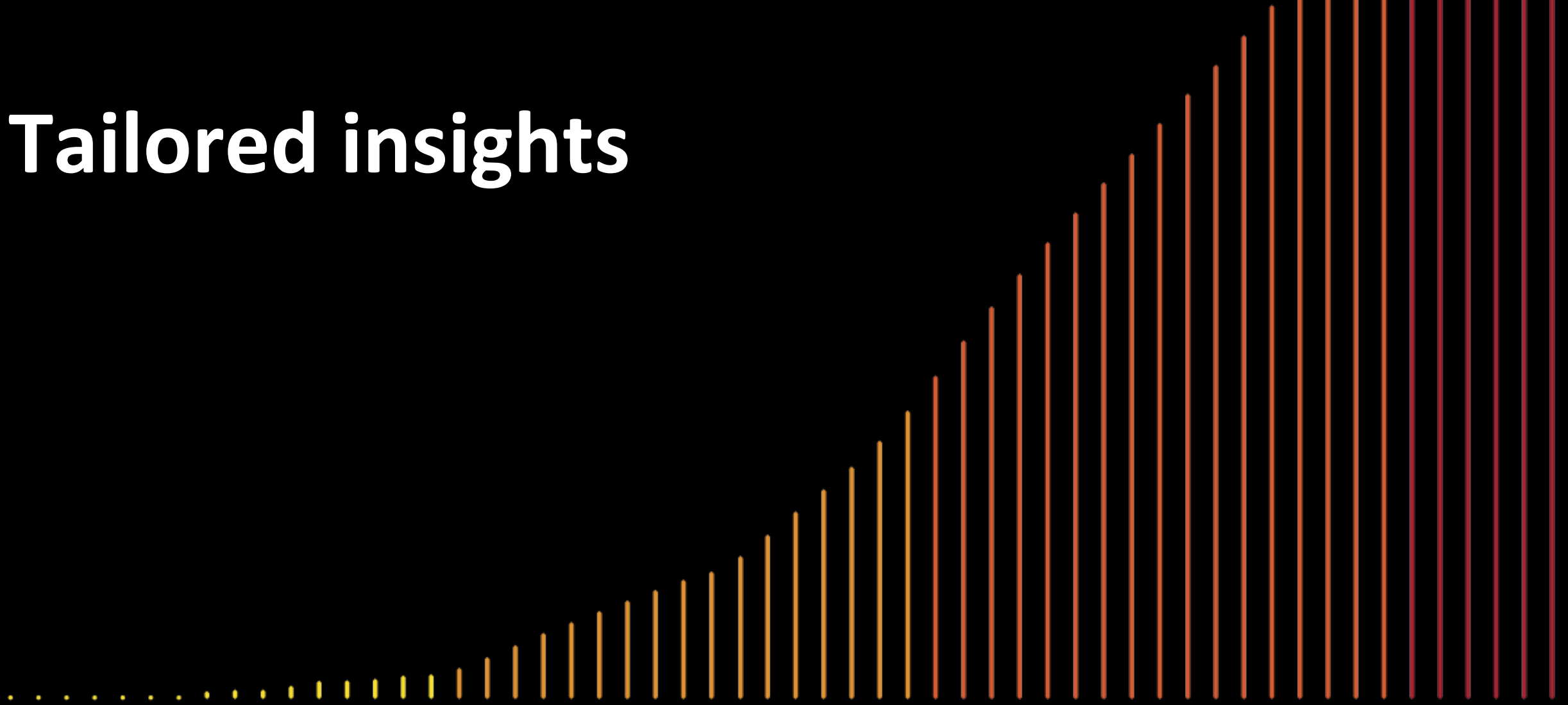


Figure 13. Top action varieties for Basic Web Application Attacks breaches (n=1,287)

Tailored insights



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.

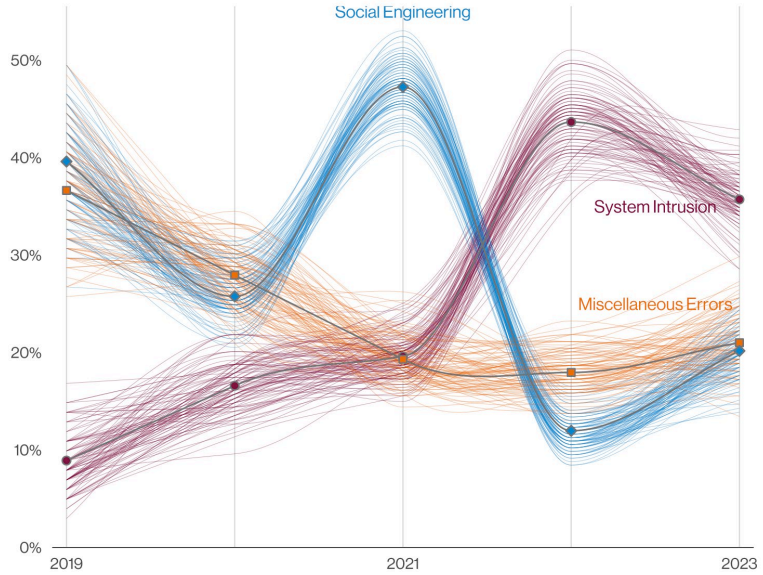


Figure 17. Patterns in Educational Services

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.

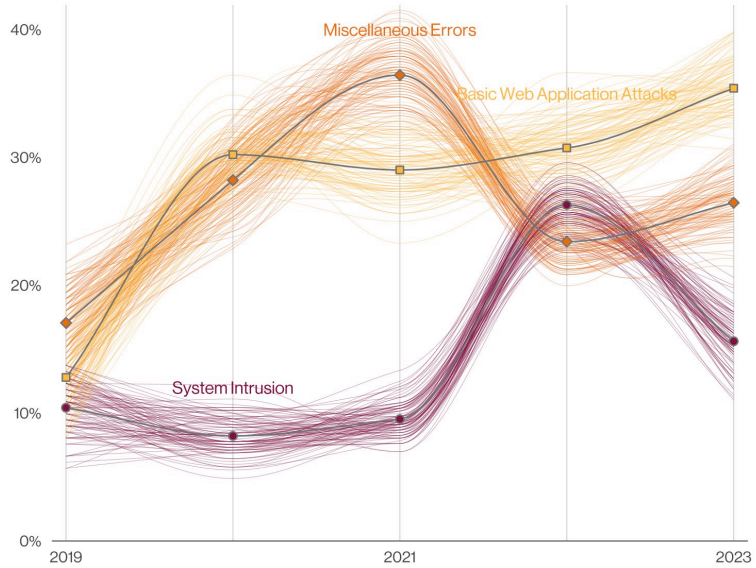


Figure 18. Patterns in Financial and Insurance

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.

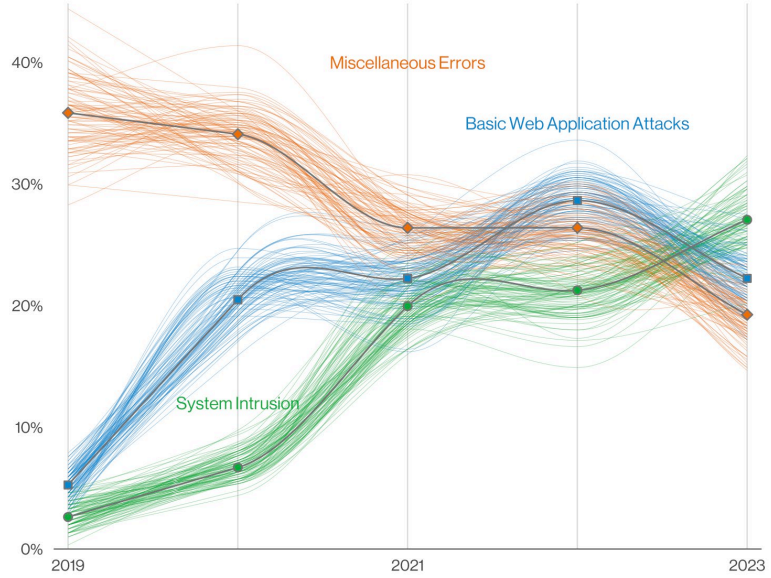


Figure 19. Patterns in Healthcare

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.

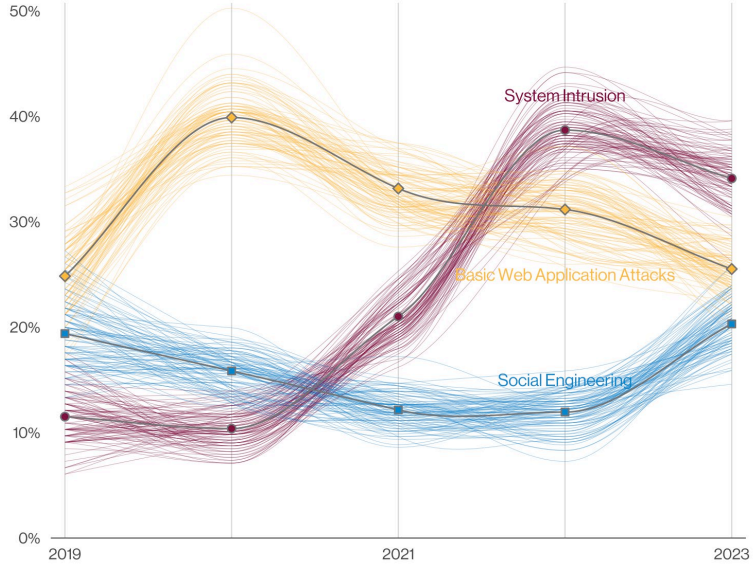


Figure 20. Patterns in Information

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%.

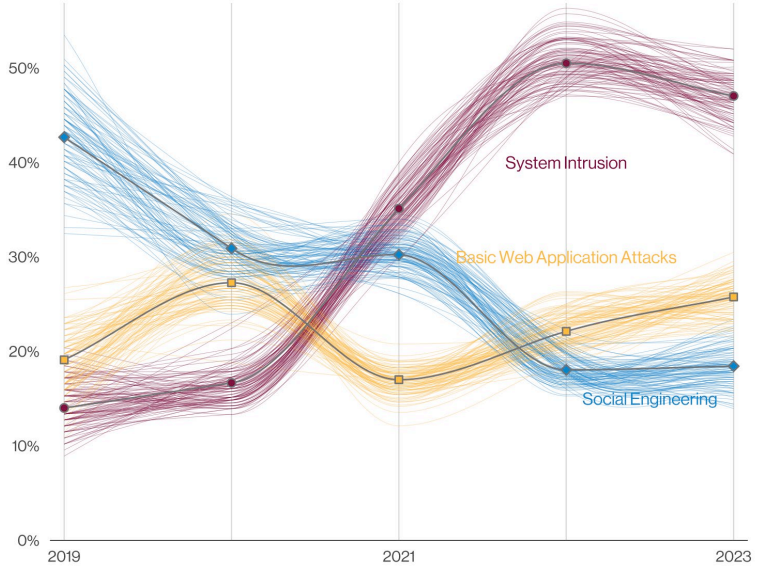


Figure 23. Patterns in Professional, Scientific and Technical Services

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.

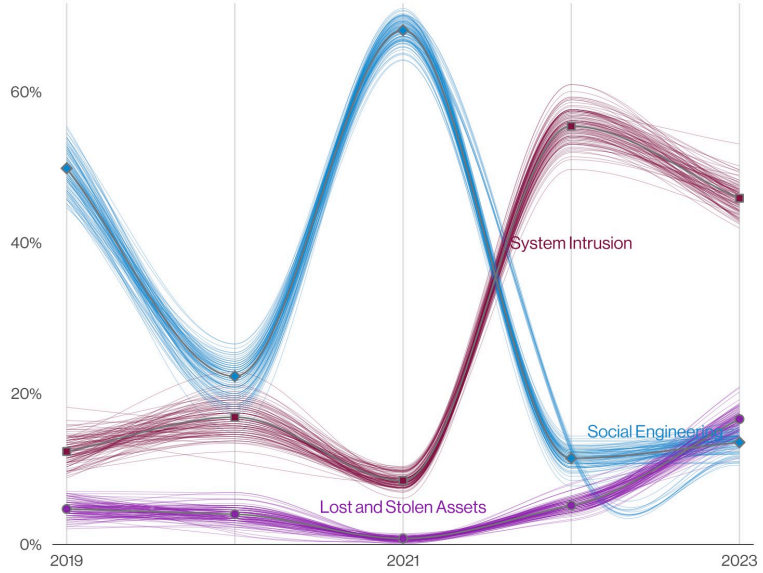
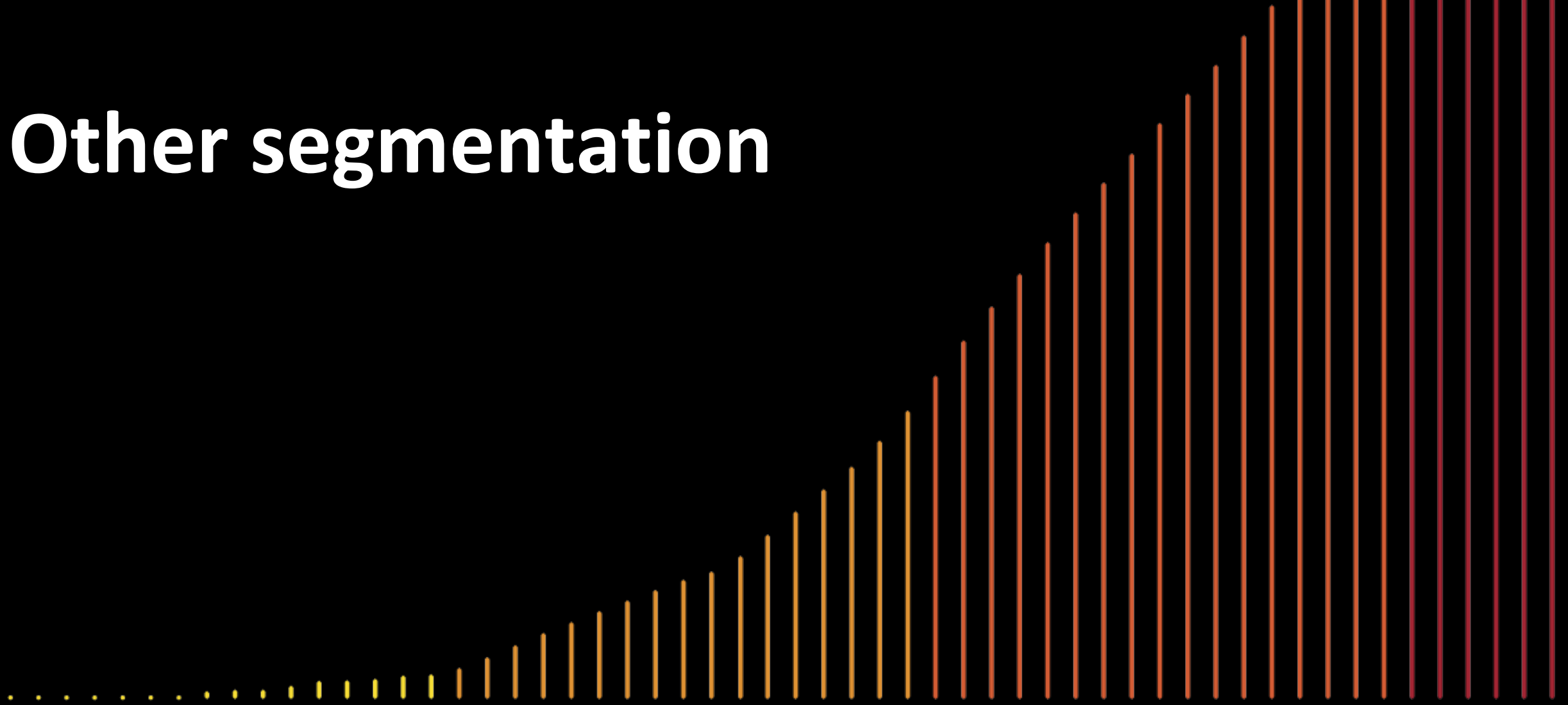


Figure 24. Patterns in Public Administration

Other segmentation



Small and medium business (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)

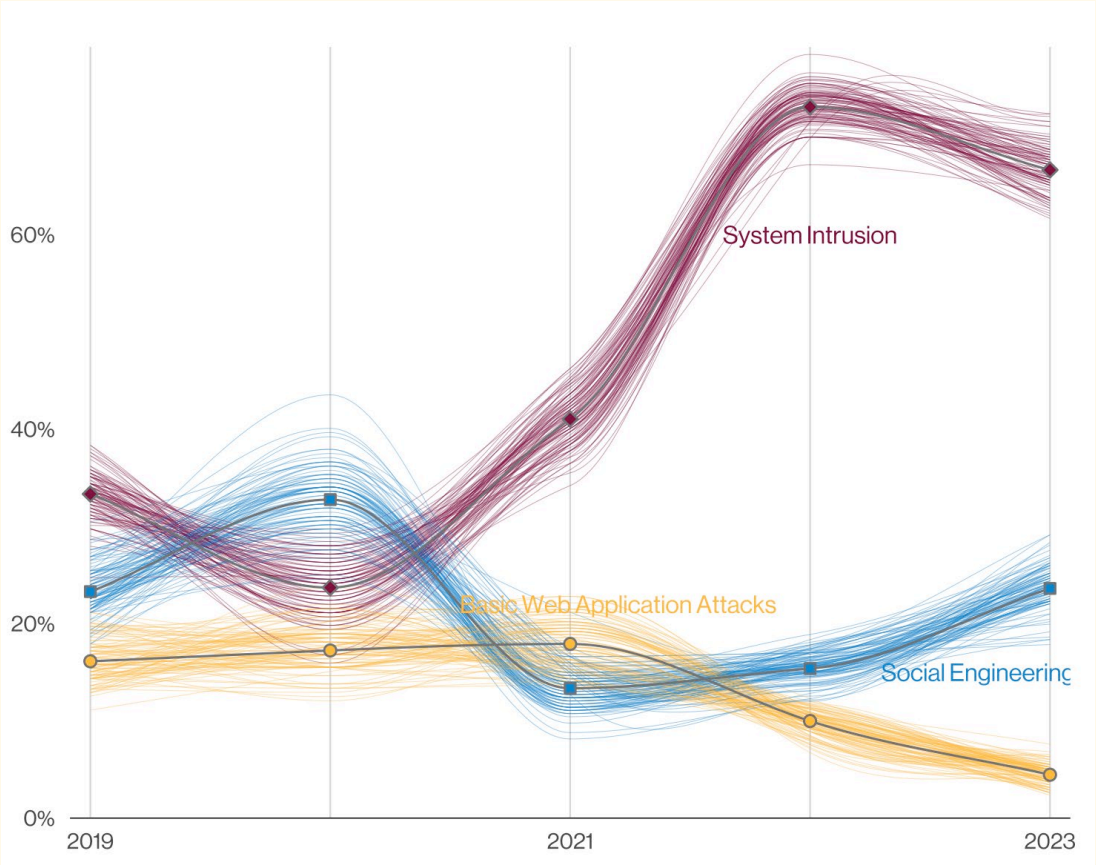


Figure 26. Patterns in SMB

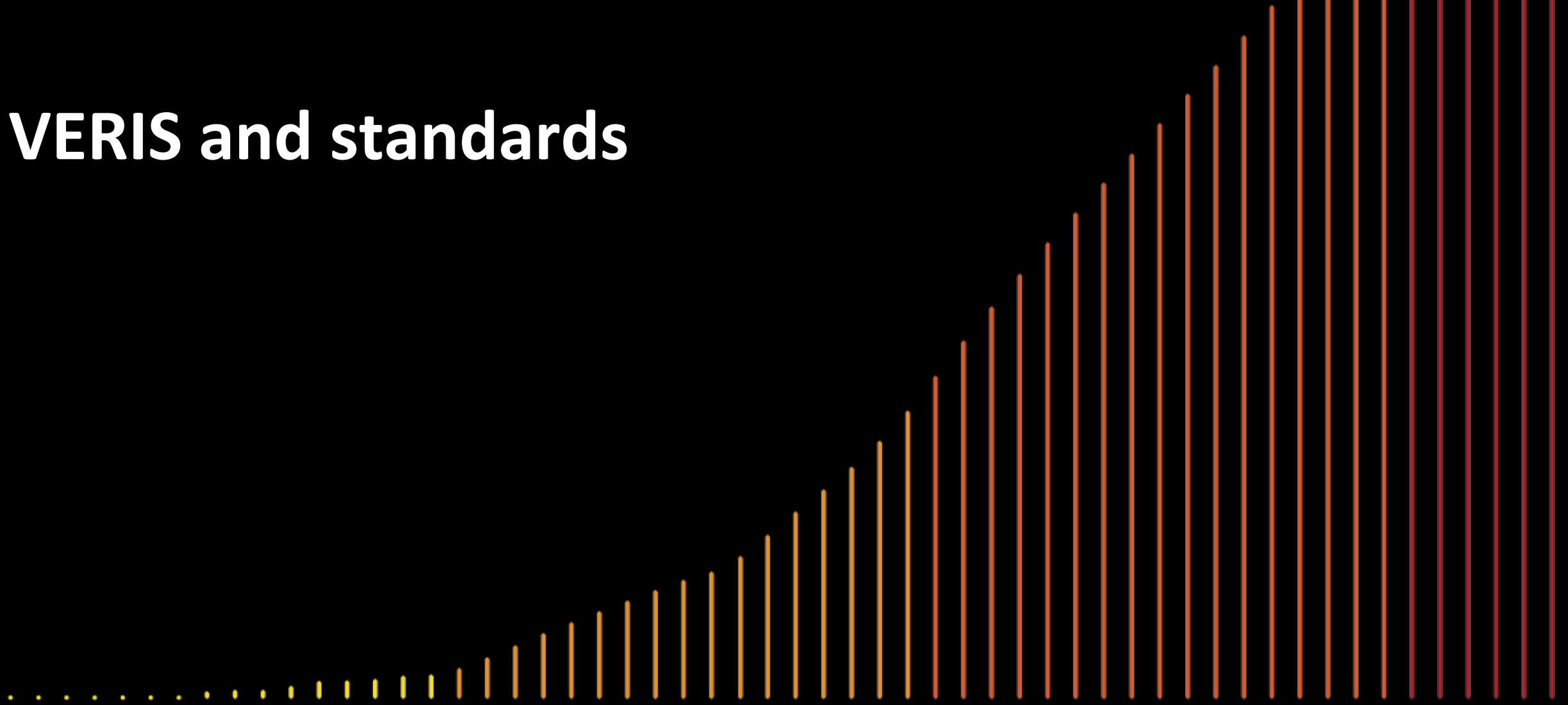
SMB: small and medium-sized businesses

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

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 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

VERIS enumeration

Action: hacking
Vector: desktop sharing software

Mapping

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

In the News

Home › News › Security › University of Michigan shuts down network after cyberattack

University of Michigan shuts down network after cyberattack

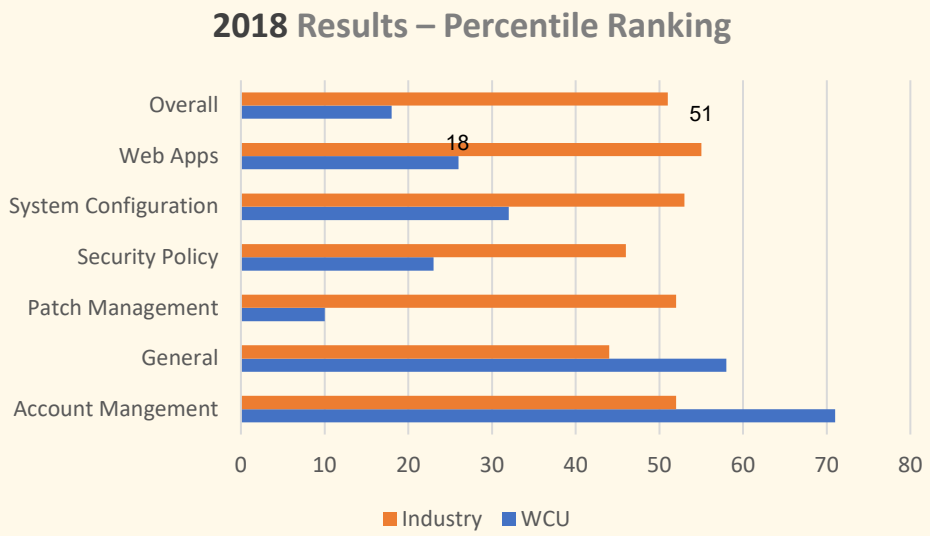
By **Bill Toulas**

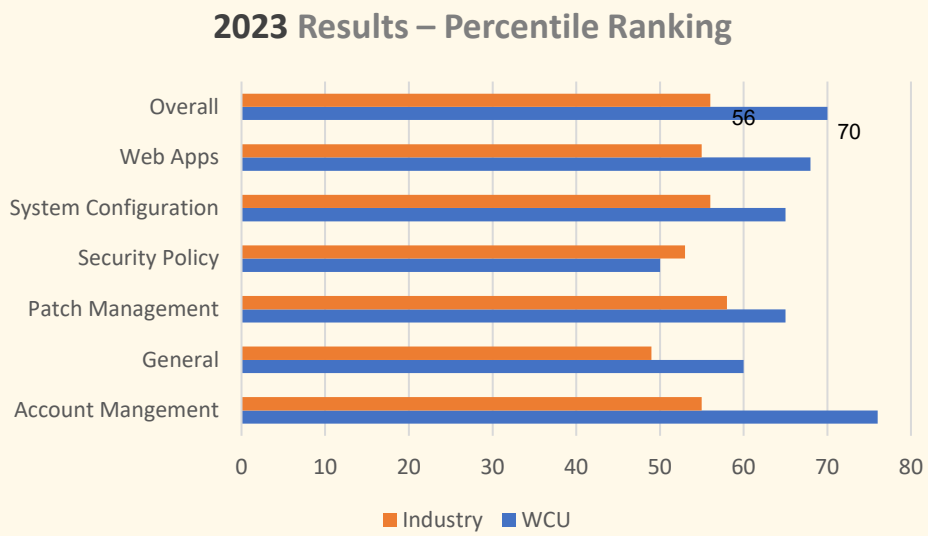
August 29, 2023 10:35 AM 0

Key take-aways to build your IT Security Footprint

- Develop Strategic Information Security Plan – 18 months to 2 years
- Identify Regulatory Compliance (GLBA, HIPAA, FERPA, CCPA, HiTECH, SOX)
- Create an Incident Response Plan to include a team
- CIS 18 Basic Controls – Align to this framework
- CyberSecurity Training Awareness to include Phishing Tests
- Conduct annual Penetration Testing

Information Security – PEN Test Results





Actual 5-year Comparison

Key Resources to get started:

Center for Internet Security (CIS 18 Controls)

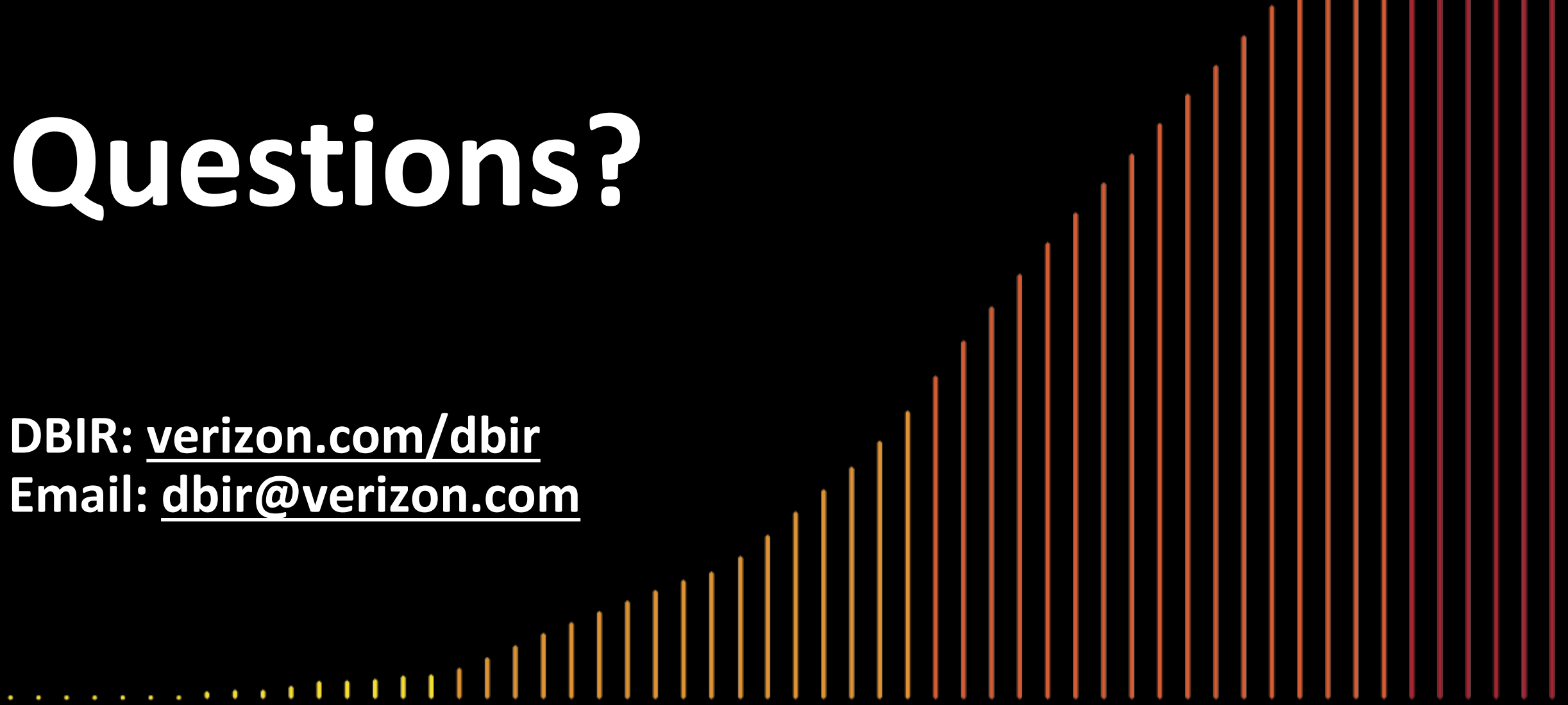
- https://www.cisecurity.org/controls/cis-controls-list
- https://www.auditscripts.com/free-resources/critical-security-controls/

National Institute of Standards and Technology (NIST) CyberSecurity Framework (CSF)

- file:///C:/Users/denright/Downloads/NIST-Cybersecurity-Framework-Policy-Template-Guide-v2111Online.pdf
- https://www.nist.gov/cyberframework/getting-started
- https://www.nist.gov/cyberframework/framework

Questions?

DBIR: 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.