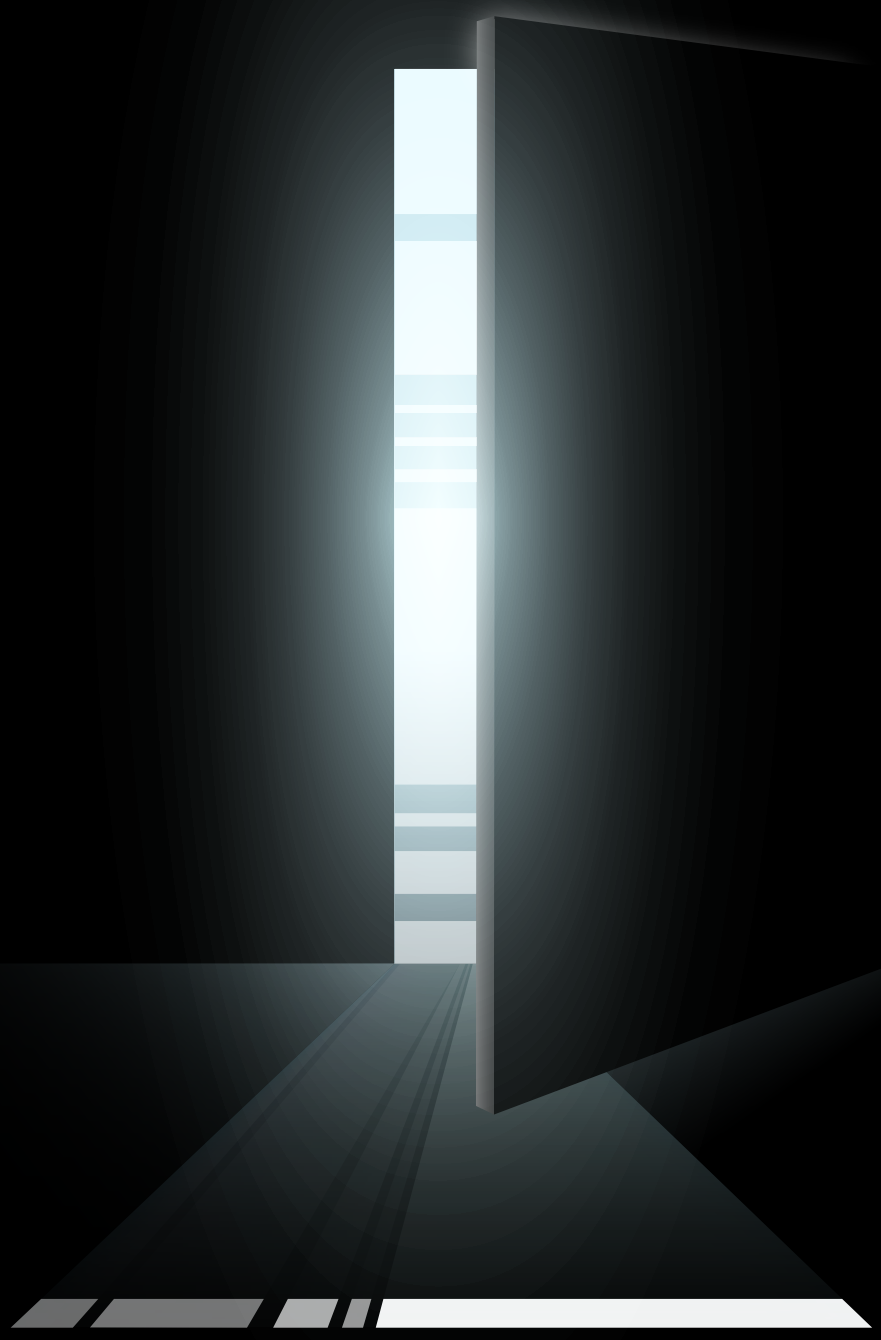
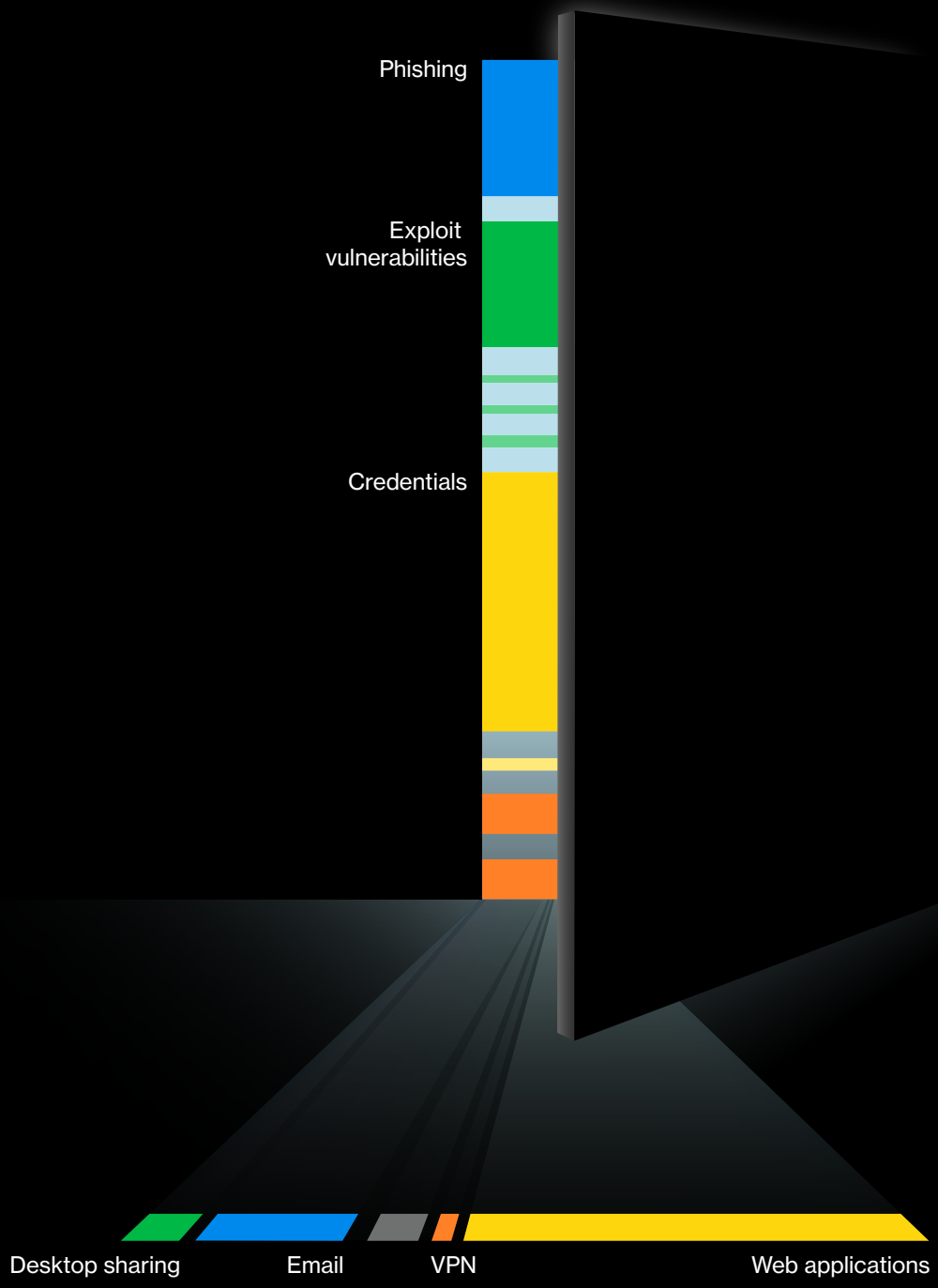
2024 Data Breach Investigations Report



verizon business


Phishing
Exploit vulnerabilities
Credentials
Desktop sharing
Email
VPN
Web applications

About the cover

This year, the report is delving deeper into the pathway to breaches in an effort to identify the most likely Action and vector groupings that lead to breaches given the current threat landscape. The cracked doorway on the cover is meant to represent the various ways attackers can make their way inside. The opening in the door shows the pattern of our combined “ways-in” percentages (see Figure 7 for a more straightforward representation), and it lets out a band of light displaying a pattern of the Action vector quantities. The inner cover highlights and labels the quantities in a less abstract way. Hope you enjoy our art house phase.

Table of contents

Introduction

Greetings! Welcome to Verizon's 2024 Data Breach Investigations Report (DBIR). This year marks the 17th edition of this publication, and we are thrilled to welcome back our old friends and say hello to new readers. As always, the aim of the DBIR is to shine a light on the various Actor types, the tactics they utilize and the targets they choose. Thanks to our talented, generous and civic-minded contributors from around the world who continue to stick with us and share their data and insight, and deep appreciation for our very own Verizon Threat Research Advisory Center (VTRAC) team (rock stars that they are). These two groups enable us to examine and analyze relevant trends in cybercrime that play out on a global stage across organizations of all sizes and types.

From year to year, we see new and innovative attacks as well as variations on tried-and-true attacks that still remain successful. From the exploitation of well-known and far-reaching zero-day vulnerabilities, such as the one that affected MOVEit, to the much more mundane but still incredibly effective Ransomware and Denial of Service (DoS) attacks, criminals continue to do their utmost to prove the old adage "crime does not pay" wrong.

The shifting landscape of cyber threats can be confusing and overwhelming. When, in addition to the attack types mentioned above, one throws in factors such as the human element and/or poorly protected passwords, things become even more confused. One might be forgiven for viewing the current state of cybersecurity as a colorful cyber Mardi Gras parade. Enterprise floats of all shapes and sizes cruising past a large crowd of threat actors who are shouting out gleefully "Throw me some creds!" Of course, human nature being what it is, all too often, the folks on the floats do just that. And, as with all such parades, what is left in the aftermath isn't necessarily pretty. The past year has been a busy one for cybercrime. We analyzed 30,458 real-world security incidents, of which 10,626 were confirmed data breaches (a record high!), with victims spanning 94 countries.

While the general structure of the report remains the same, long-time readers may notice a few changes. For example, the "first-time reader" section is now located in Appendix A rather than at the beginning of the report. But we do encourage those who are new to the DBIR to give it a read-through before diving into the report. It should help you get your bearings.

Last, but certainly not least, we extend a most sincere thanks yet again to our contributors (without whom we could not do this) and to our readers (without whom there would be no point in doing it).

Sincerely,

The Verizon DBIR Team
C. David Hylender, Philippe Langlois, Alex Pinto, Suzanne Widup

Very special thanks to:
– Christopher Novak for his continued support and insight
– Dave Kennedy and Erika Gifford from VTRAC
– Kate Kutchko, Marziyeh Khanouki and Yoni Fridman from the Verizon Business Product Data Science Team

Helpful guidance

About the 2024 DBIR incident dataset

Each year, the DBIR timeline for in-scope incidents is from November 1 of one calendar year through October 31 of the next calendar year. Thus, the incidents described in this report took place between November 1, 2022, and October 31, 2023. The 2023 caseload is the primary analytical focus of the 2024 report, but the entire range of data is referenced throughout, notably in trending graphs. The time between the latter date and the date of publication for this report is spent in acquiring the data from our global contributors, anonymizing and aggregating that data, analyzing the dataset, and finally creating the graphics and writing the report. The jokes, sadly, do not write themselves.

Credit where credit is due

Turns out folks enjoy citing the report, and we often get asked how to go about doing it.

You are permitted to include statistics, figures and other information from the report, provided that (a) you cite the source as "Verizon 2024 Data Breach Investigations Report" and (b) the content is not modified in any way. Exact quotes are permitted, but paraphrasing requires review. If you would like to provide people a copy of the report, we ask that you provide them a link to verizon.com/dbir rather than the PDF.

Questions? Comments? Concerns? Love to share cute pet pictures?

Let us know! Send us a note at dbir@verizon.com, find us on LinkedIn, tweet @VerizonBusiness with #dbir. Got a data question? Tweet @VZDBIR!

If your organization aggregates incident or security data and is 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**.

Summary of findings

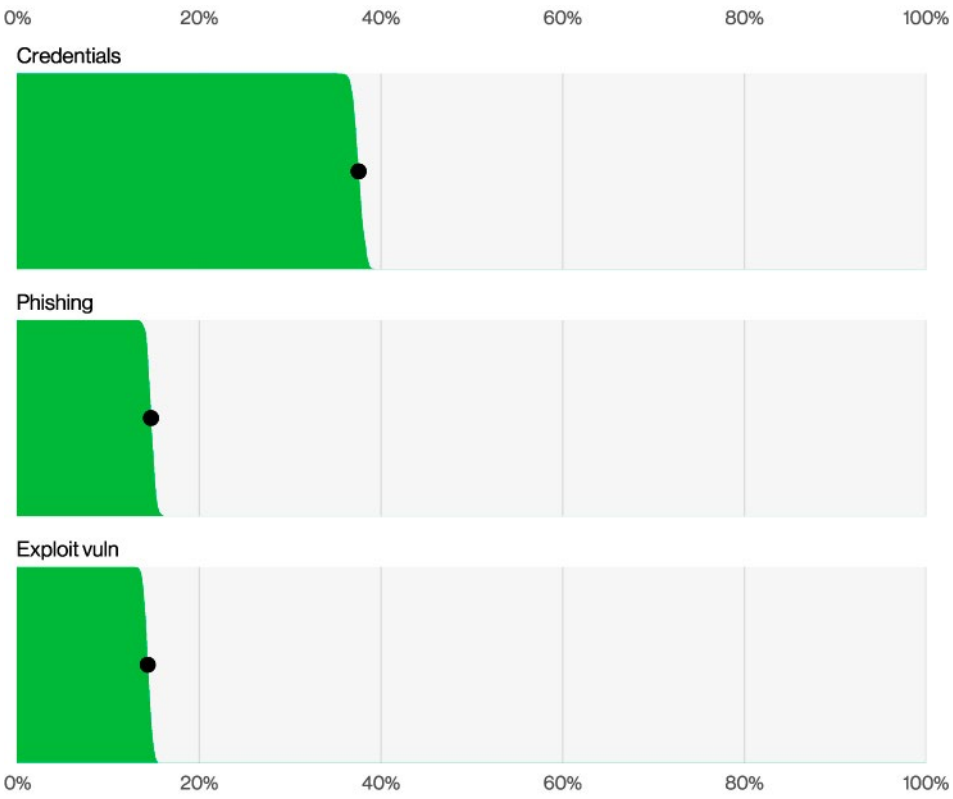


Figure 1. Select ways-in enumerations in non-Error, non-Misuse breaches (n=6,963)

Our ways-in analysis witnessed a substantial growth of attacks involving the exploitation of vulnerabilities as the critical path to initiate a breach when compared to previous years. It almost tripled (180% increase) from last year, which will come as no surprise to anyone who has been following the effect of MOVEit and similar zero-day vulnerabilities. These attacks were primarily leveraged by Ransomware and other Extortion-related threat actors. As one might imagine, the main vector for those initial entry points was Web applications.

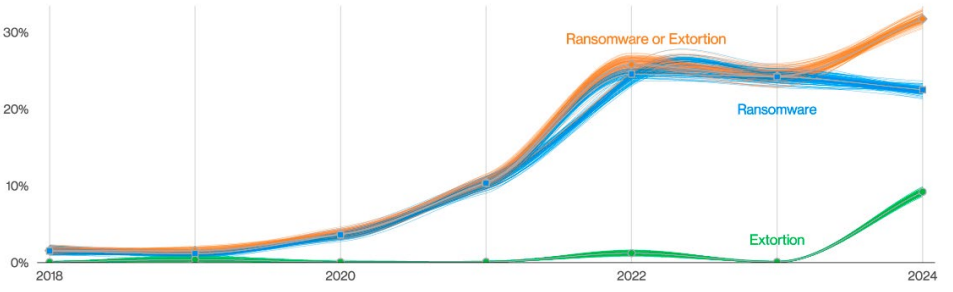


Figure 2. Ransomware and Extortion breaches over time

Roughly one-third of all breaches involved Ransomware or some other Extortion technique. Pure Extortion attacks have risen over the past year and are now a component of 9% of all breaches. The shift of traditional ransomware actors toward these newer techniques resulted in a bit of a decline in Ransomware to 23%. However, when combined, given that they share threat actors, they represent a strong growth to 32% of breaches. Ransomware was a top threat across 92% of industries.

Figure 3. Select key enumerations in breaches

We have revised our calculation of the involvement of the human element to exclude malicious Privilege Misuse in an effort to provide a clearer metric of what security awareness can affect. For this year's dataset, the human element was a component of 68% of breaches, roughly the same as the previous period described in the 2023 DBIR.

In this issue, we are introducing an expanded concept of a breach involving a third party that includes partner infrastructure being affected and direct or indirect software supply chain issues—including when an organization is affected by vulnerabilities in third-party software. In short, those are breaches an organization could potentially mitigate or prevent by trying to select vendors with better security track records. We see this figure at 15% this year, a 68% increase from the previous year, mostly fueled by the use of zero-day exploits for Ransomware and Extortion attacks.

Our dataset saw a growth of breaches involving Errors, now at 28%, as we broadened our contributor base to include several new mandatory breach notification entities. This validates our suspicion that errors are more prevalent than media or traditional incident response-driven bias would lead us to believe.

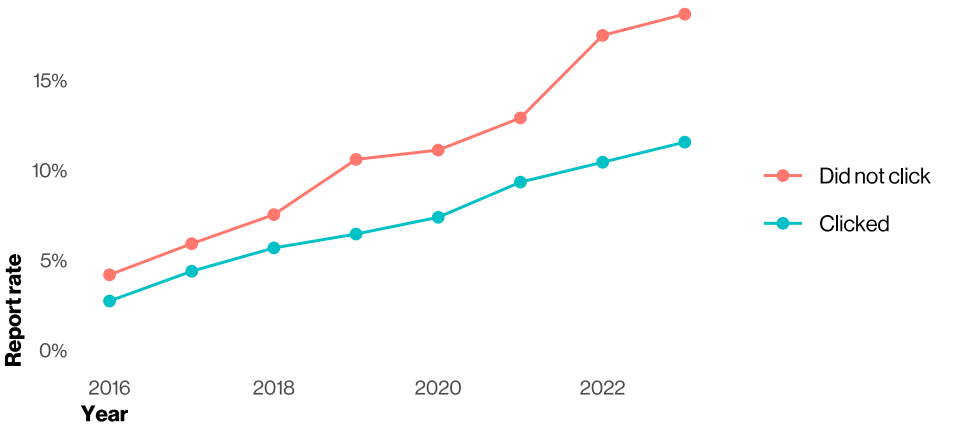


Figure 4. Phishing email report rate by click status

The overall reporting rate of Phishing has been growing over the past few years. In security awareness exercise data contributed by our partners during 2023, 20% of users reported phishing in simulation engagements, and 11% of the users who clicked the email also reported. This is welcome news because on the flip side, the median time to click on a malicious link after the email is opened is 21 seconds and then only another 28 seconds for the person caught in the phishing scheme to enter their data. This leads to an alarming finding: The median time for users to fall for phishing emails is less than 60 seconds.

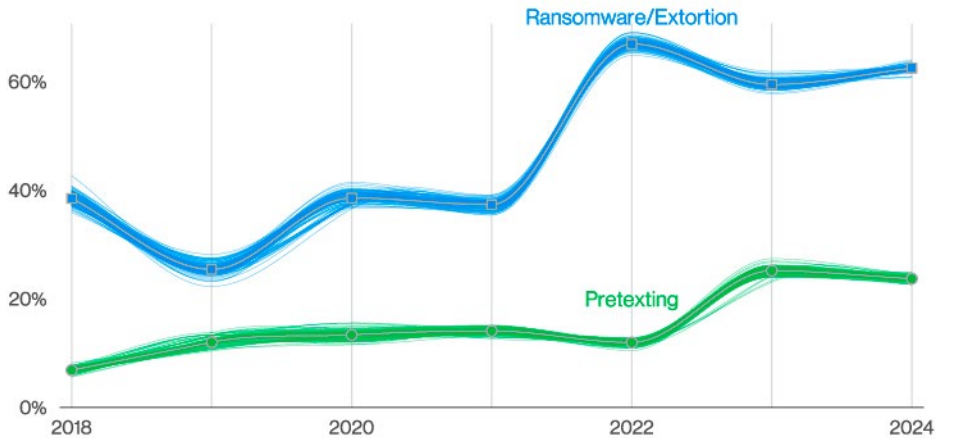


Figure 5. Select action varieties in Financial motive over time

Financially motivated threat actors will typically stick to the attack techniques that will give them the most return on investment.

Over the past three years, the combination of Ransomware and other Extortion breaches accounted for almost two-thirds (fluctuating between 59% and 66%) of those attacks. According to the FBI's Internet Crime Complaint Center (IC3) ransomware complaint data, the median loss associated with the combination of Ransomware and other Extortion breaches has been $46,000, ranging between $3 (three dollars) and $1,141,467 for 95% of the cases. We also found from ransomware negotiation data contributors that the median ratio of initially requested ransom and company revenue is 1.34%, but it fluctuated between 0.13% and 8.30% for 80% of the cases.

Similarly, over the past two years, we have seen incidents involving Pretexting (the majority of which had Business Email Compromise [BEC] as the outcome) accounting for one-fourth (ranging between 24% and 25%) of financially motivated attacks. In both years, the median transaction amount of a BEC was around $50,000, also according to the FBI IC3 dataset.

2
Results and analysis

Results and analysis: Introduction

Hello, friends, and welcome to the "Results and analysis" section. This is where we cover the highlights we found in the data this year. This dataset is collected from a variety of sources, including our own VTRAC investigators, reports provided by our data contributors and publicly disclosed security incidents.[1]

Because data contributors come and go, one of our priorities is to make sure we can get broad representation on different types of security incidents and the countries where they occur. This ebb and flow of contributors obviously influences our dataset, and we will do our best to provide context on those potential biases where applicable.

This year we onboarded a good number of new contributors and reached an exciting milestone of more than 10,000 breaches analyzed in a single edition.[2] It is an enormous amount of work to organize and analyze, but it is also incredibly gratifying to be able to present these results to you.

In an attempt to be more actionable, we would like to use this section to discuss some high-level findings that transcend the fixed structure of the Vocabulary for Event Recording and Incident Sharing (VERIS) 4As (Actor, Action, Asset and Attribute) and expand on some of the key findings we have been highlighting over the past few years.

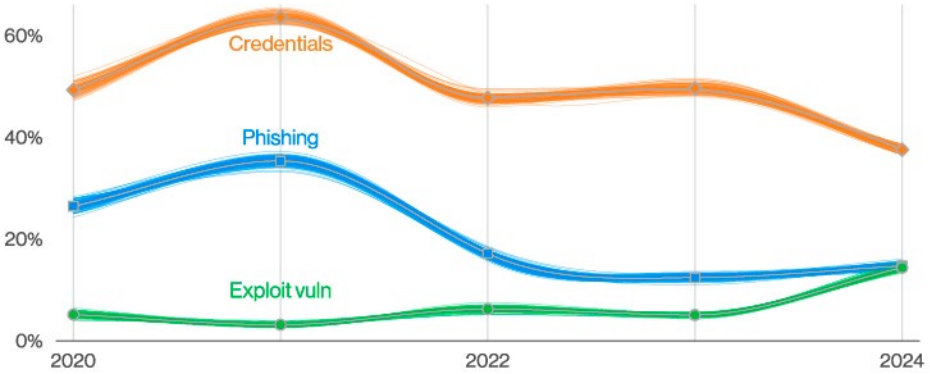


Figure 6. Select ways-in enumerations in non-Error, non-Misuse breaches over time

Ways into your sensitive data's heart

One of the actionable perspectives we have created has been the ways-in analysis, in which we try to make sense of the initial steps into breaches to help predict how to best avoid or prevent them. We still have plenty of unknown Actions and vectors dispersed throughout the dataset as investigation processes and disclosure patterns widely differ across our data contributors,[3] but this view of what we know for sure has remained stable and representative over the years.

Figure 6 paints a clear picture of what has been the biggest pain point for everyone this year. This 180% increase in the exploitation of vulnerabilities as the critical path action to initiate a breach will be of no surprise to anyone who has been following the MOVEit vulnerability and other zero-day exploits that were leveraged by Ransomware and Extortion-related threat actors.

This was the sort of result we were expecting in the 2023 DBIR when we analyzed the impact of the Log4j vulnerabilities. That anticipated worst case scenario discussed in the last report materialized this year with this lesser known—but widely deployed—product. We will be diving into additional details of MOVEit and vulnerability exploitation in the "Action" and "System Intrusion" pattern sections.

1 Have you checked out the VERIS Community Database (VCDB) yet? You should, it's awesome! (https://verisframework.org/vcdb.html)

2 We also passed our cumulative 1 million incident milestone as we forecast in the 2023 DBIR, but we are only mentioning this here in the footnote to not aggravate the report; it was very disappointed that 1 million is not enough to retire on in this economy.

3 We're not throwing shade—different types of contributing organizations focus on what is most relevant for them, as well they should.

To dig further into this concept of the ways in, we are presenting a new slice of the data, where we are overlaying those different types of Actions with their most popular vectors to help focus response and planning efforts. You can take a peek at those results in Figure 7.

Phishing attacks mostly having an Email vector is rather self-explanatory,[4] so we would like to focus on the concentration of the Web application vector prevalence for both credentials and exploit vulnerability. The presence of Credentials in the graphic should not be surprising as it carries a large share of the guilt for our Basic Web Application Attacks pattern (i.e., getting unauthorized access to cloud-based email and collaboration accounts). But recency bias might make folks doubt the prevalence of exploitation of vulnerabilities. Because this report is being written in the beginning of 2024, the focus has been on zero-day (or near-zero-day) vulnerabilities in virtual private network (VPN) software.[5]

Naturally, the share of VPN vector in the exploit vuln variety will likely increase for our 2025 report to reflect those trends, but the bottom line is again self-evident and self-explanatory. Anything that adds to your attack surface on the internet can be targeted and potentially be the first foothold for an external threat actor, and as such, the focus should be to try to keep footholds to a minimum.

No matter how you feel about your VPN software right now, having as many of your web applications as possible behind it might be a better strategy than having to worry about emergency overnight patching of the software—and all the other dependencies that power the web applications themselves. This will not completely mitigate the risk and will not be the right fit for all organizations, but in the worst-case scenario, the Cybersecurity Infrastructure and Security Agency (CISA) might have you rip out only one tool from your network as opposed to several.

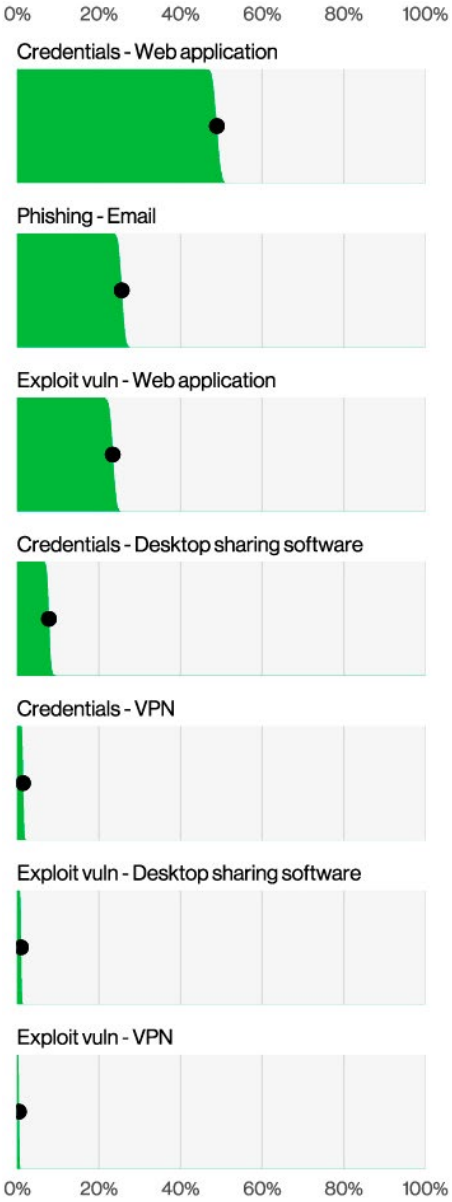


Figure 7. Select ways-in variety and vector enumerations in non-Error, non-Misuse breaches (n=2,770)

Anyway, all this nuance does not affect our opinion of having desktop sharing software directly connected to the internet. Go fix that pronto, please.

We are only human after all.

One other combined metric we have been tracking for a few years is related to the human element in breaches. There is a lot of focus on how fully automated attacks can ruin an organization's day,[6] but it is often surprising how much the people inside the company can have a positive effect on security outcomes.

This year, we have tweaked our human element metric a bit so its impact and action opportunities are clearer. You see, when DBIR authors (and the whole industry in general) would discuss this metric, it would be alongside an opportunity gap for security training and awareness. It is not perfect, but if you had a clear investment path that could potentially improve the outcomes of more than two-thirds of potential breaches, you might at least sit down and listen.

It turns out that our original formula for what was included in the human element metric built in Privilege Misuse pattern breaches, which are the cases involving malicious insiders. Having those mixed with honest mistakes by employees did not make sense if our aim was to suggest that those could be mitigated by security awareness training.[7]

4 And an incredible L for the *ishing portmanteau enthusiasts

5 Unless by now we have successfully ripped them out of our networks entirely and are back to our smoke signals and carrier pigeon ways.

6 We ourselves were just talking about the growth of exploitation of vulnerabilities as a pathway into breaches.

7 We dread to think what "awareness training" for malicious insiders would look like.

Figure 8 showcases the new human element over time (with malicious insiders removed) to provide a better frame of reference for our readers going forward. It is present in more than two-thirds of breaches as foreshadowed two paragraphs ago, more precisely in 68% of breaches. It is statistically similar to our findings last year, which means that in a certain way, the increases we had across the board in the Miscellaneous Errors pattern (human-centric) and as a result of the MOVEit vulnerability (automated) were similar in scope as far as this metric is concerned.

Fans of the "original flavor" human element are not missing much because the inclusion of the Misuse action would have brought the percentage to 76%, statistically only slightly more than the previous report's 74%. Still, we prefer the clearer definition going forward, and we will leave the analysis of those bothersome insiders and their misdeeds to the "Privilege Misuse" pattern section.

The weakest links in the chain of inter-connection

Finally, as we review the big picture of how the threat landscape changed this year,[8] we would like to introduce a new metric that we will be tracking going forward. As the growth of exploitation of vulnerabilities and software supply chain attacks make them more commonplace in security risk register discussions, we would like to suggest a new third-party metric where we embrace the broadest possible interpretation of the term.[9] Have a peek at Figure 9, where we calculated a supply chain interconnection influence in 15% of the breaches we saw, a significant growth from 9% last year. A 68% year-over-year growth is really solid, but what do we mean by this?

For a breach to be a part of the supply chain interconnection metric, it will have taken place because either a business partner was the vector of entry for the breach (like the now fabled heating, ventilating and air-conditioning [HVAC] company entry point in the 2013 Target breach) or if the data compromise happened

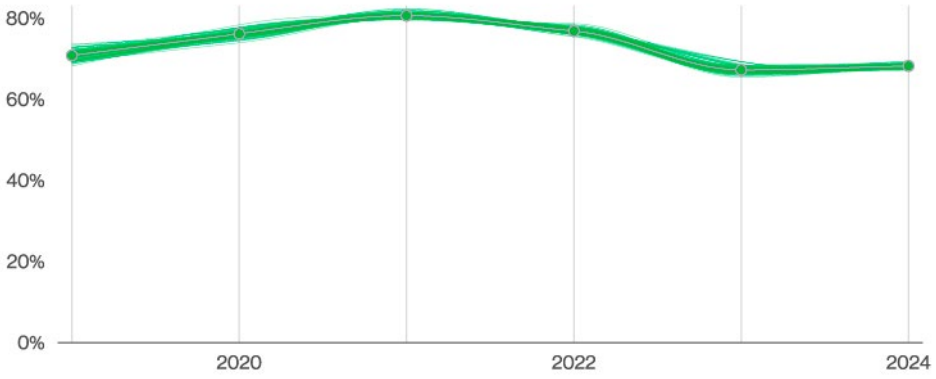


Figure 8. Human element enumeration in breaches over time

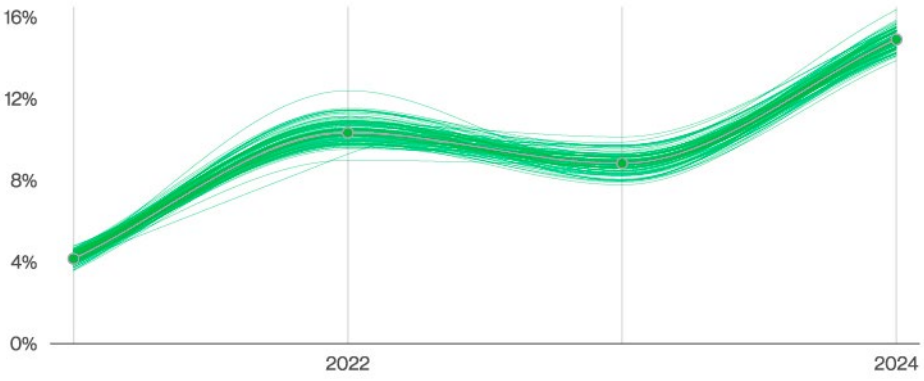


Figure 9. Supply chain interconnection in breaches over time

8 Number of times the word "MOVEit" is mentioned in this report: 25
9 In a surprising role reversal, as we are often very pedantic in our definitions

in a third-party data processor or custodian site (fairly common in the MOVEit cases, for instance). Less frequently found in our dataset, but also included, are physical breaches in a partner company facility or even partner vehicles hijacked to gain entry to an organization's facilities.[10]

So far, this seems like a pretty standard third-party breach recipe, but we are also adding cases, such as SolarWinds and 3CX, in which their software development processes were hijacked and malicious software updates were pushed to their customers to be potentially leveraged in a second step escalation by the threat actors. Those breaches are ultimately caused by the initial incident in the software development partner, and so we are adding those to this tab.

Now for the controversial part: Exploitation of vulnerabilities is counted in this metric as well. As much as we can argue that the software developers are also victims when vulnerabilities are disclosed in their software (and sure, they are), the incentives might not be aligned properly for those developers to handle this seemingly interminable task. These quality control failures can disproportionately affect the customers who use this software. We can clearly see what powerful and wide-reaching effects a handful of zero-day or mismanaged patching rollouts had on the general threat landscape. We stopped short of adding exploitation of misconfigurations in installed software because, although those could be a result of insecure defaults, system admins can get quite creative sometimes.

Figure 10 shows the breakdown of VERIS actions in the supply chain metric and, as expected, it is driven by Exploit vuln, which ushers Ransomware and Extortion attacks into organizations.

This metric ultimately represents a failure of community resilience and recognition of how organizations depend on each other. Every time a choice is made on a partner (or software provider) by your organization and it fails you, this metric goes up. We recommend that organizations start looking at ways of making better choices so as to not reward the weakest links in the chain. In a time where disclosure of breaches is becoming mandatory, we might finally have the tools and information to help measure the security effectiveness of our prospective partners.

We will keep a close watch on this one and seek to improve its definition over time. We welcome feedback and suggestions of alternative angles, and we believe the only way through it is to find ways to hold repeat offenders accountable and reward resilient software and services with our business.

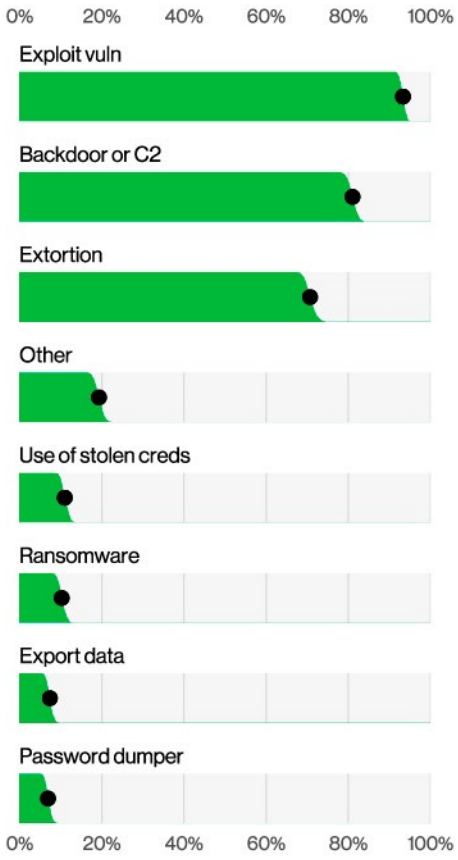


Figure 10. Action varieties in selected supply chain interconnection breaches (n=1,075)

10 We should stop watching those "Mission: Impossible" movies during DBIR writing season.

VERIS Actors

Hey, you, don't skip this section this year! We know we keep repeating, "It's always external criminals wanting your money" alongside dated pop culture references, but we have some interesting data points to discuss this year. Does this mean External actors are not the most prevalent? No, of course they are, silly. But since we got your attention, please read on.

This year, in part because of improved breach collection processes[11] and the onboarding of new data contributors documenting mandatory breach disclosures, it is finally time for Internal actors to shine. After all, why rely on outside help if you have the talent in-house?

We still have the External actors as the top catalyst for breaches at 65%, but we have Internal at a whopping 35%—a significant increase from last year's 20% number. Figure 11 showcases this development over the last few years.

However, before we call an emergency meeting and start pointing fingers at each other trying to figure out who the impostor is, it's important to realize that 73% of those Internal actor breaches were in the Miscellaneous Errors pattern, and we shouldn't really be holding their feet to the fire.[12] We will be discussing more about this Error renaissance[13] in the respective pattern section, but it showcases one long-standing suspicion of the team that mandatory breach disclosure at scale will help us better understand how mundane and preventable some of those incidents can be.

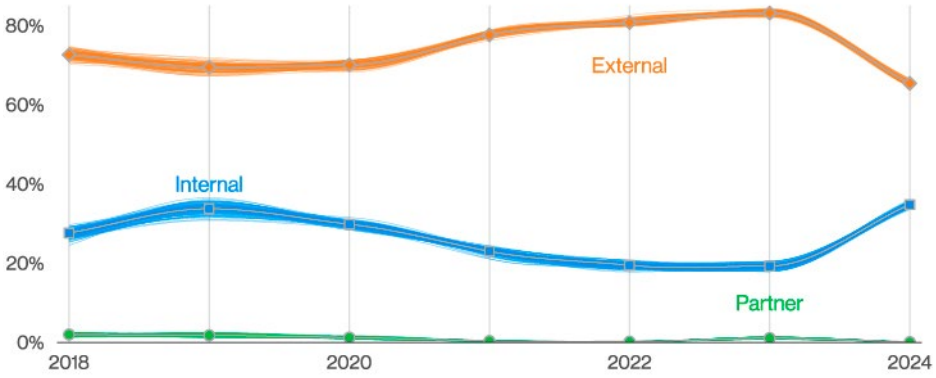


Figure 11. Threat actors in breaches over time

And speaking of disclosure, the numerous Extortion attacks used by ransomware actors have caused an influx of the numbers of external actor incidents we review each year because they tip the hands of their victims and force them to notify their customers of the breach. This helped us keep our dataset balanced. Further mandatory disclosure regulation trends in the world will help us all understand the causal landscape better.[14]

Before anyone gets excited by more groundbreaking changes in the "Actor" section, Figure 12 is pleased to inform you that the Actor motive ranking remains the same. Financial has the clear lead, but it is interesting to note that the Espionage motive has increased slightly over last year, from 5% to 7%. As was the case in the prior report, this motive is mostly concentrated in Public Administration breaches.

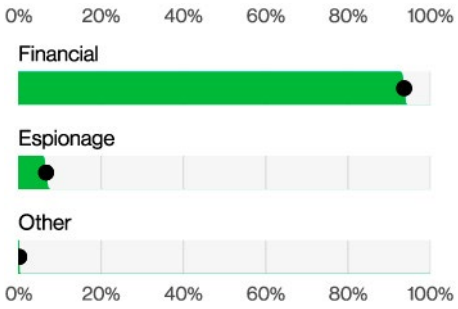


Figure 12. Threat actor motives in breaches (n=5,632)

11 Doubling the number of breaches we analyzed was no easy feat. We feel sorry for the poor DBIR authors who will have to outdo that number for the 2025 edition.
12 Unless carelessness and inattention to detail are wrong.
13 Errorssance? Age of Enerrorment?
14 This will also give threat actors new opportunities to be tattletales and report material breaches to organizations like the U.S. Securities and Exchange Commission (SEC).

We can find the same expected results when we consider the varieties of threat actors with which we are dealing. Figure 13 illustrates the lead that Organized crime-affiliated actors enjoy over their State-sponsored counterparts, as our analysis has shown for many years. Please don't misunderstand: This in no way means that the threat from those Actors should be taken lightly. State-sponsored actors are unusually resourceful and capable of adapting their tactics. Luckily for the average organization, they are less likely to target run-of-the-mill enterprises as often as your everyday, garden-variety criminal.

On a different note, End-user (in VERIS parlance, an average employee or contractor of an organization) has grown a lot, more than doubling from 11% to 26%. Those were mostly involved in Misdelivery errors and were part of the same growth in the Miscellaneous Errors pattern we discussed above. All in all, it's been an upsetting year for all detail-oriented perfectionists[15] out there.

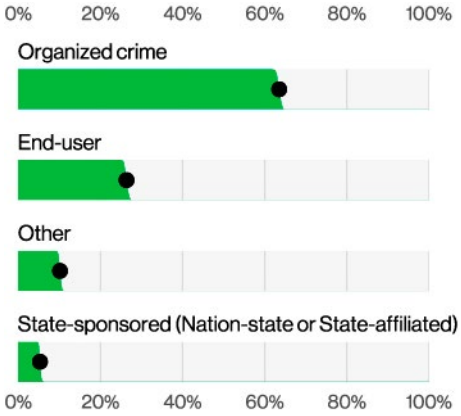


Figure 13. Threat actor varieties in breaches (n=7,921)

Actor categories[16]

External: External threats originate from sources outside of the organization and its network of partners. Examples include criminal groups, lone hackers, former employees and government entities. This category also includes God (as in "acts of"), "Mother Nature" and random chance. Typically, no trust or privilege is implied for external entities.

Internal: Internal threats are those originating from within the organization. This encompasses company full-time employees, independent contractors, interns and other staff. Insiders are trusted and privileged (some more than others).

Partner: Partners include any third party sharing a business relationship with the organization. This includes suppliers, vendors, hosting providers and outsourced IT support. Some level of trust and privilege is usually implied between business partners. Note that an attacker could use a partner as a vector, but that does not make the partner the Actor in this case. The partner has to initiate the incident to be considered the responsible party.

15 Just imagine what it would be like to work for one of those people. *[Editor's note: We resent that!]*
16 https://verisframework.org/actors.html

Artificial general intelligence threat landscape, emphasis on "artificial," not "intelligence"

Despite the pressure from a vocal minority of the cybersecurity community,[17] it seems that the DBIR team will not be adding "Evil AGI"[18] to the VERIS actor enumerations in 2024. However, it is still a very timely topic and one that has been occupying the minds of technology and cybersecurity executives worldwide.[19]

We did keep an eye out for any indications of the use of the emerging field of generative artificial intelligence (GenAI) in attacks and the potential effects of those technologies, but nothing materialized in the incident data we collected globally.[20]

After performing text analysis alongside our criminal forums data contributors, we could obviously see the interest in GenAI (as in any other forum, really), but the number of mentions of GenAI terms alongside traditional attack types and vectors such as "phishing," "malware," "vulnerability" and "ransomware" were shockingly low, barely breaching 100 cumulative mentions over the past two years. Most of the mentions[21] involved the selling of accounts to commercial GenAI offerings or tools for AI generation of non-consensual pornography. Figure 14 illustrates our findings.

If you extrapolate the commonly understood use cases of GenAI technology, it could potentially help with the development of phishing, malware and the discovery of new vulnerabilities in much the same way it helps your 10th grader write that book report for school or your average AI social media influencer pretend to create a website by taking a picture of a drawing on a napkin.

But would this kind of assistance really move the needle on successful attacks? One can argue, given our Social Engineering pattern numbers from the past few years, that Phishing or Pretexting attacks don't need to be more sophisticated to be successful against their targets, as we have seen with the growth of BEC-like attacks. Similarly, malware, especially of the Ransomware flavor, does not seem to be lacking in effectiveness, and threat actors seem to have a healthy supply of zero-day vulnerabilities for initial infiltration into an organization.

From our perspective, the threat actors might well be experimenting and trying to come up with GenAI solutions to their problems. There is evidence being published[22] of leveraging such technologies in "learning how to code" activities by known state-sponsored threat actors. But it really doesn't look like a breakthrough is imminent or that any attack-side optimizations this might bring would even register on the incident response side of things. The only exception here has to do with the clear advancements on deepfake-like technology, which has already created a good deal of reported fraud and misinformation anecdotes.

Incidentally, we did ask one of those GenAI tools what threats this nascent technology could amplify, and it ended up suggesting the same things as above.[23] It made it seem like it already had an outsize influence in those subjects and that "organizations must adapt their defense strategies to keep pace with the evolving sophistication of GenAI-driven threats."[24] This little experiment seems to indicate that even GenAI has a tendency toward beefing up its resume via the use of well-placed exaggeration.

Turns out it's really hard to escape the hype no matter where you sit on the natural vs. artificial divide.

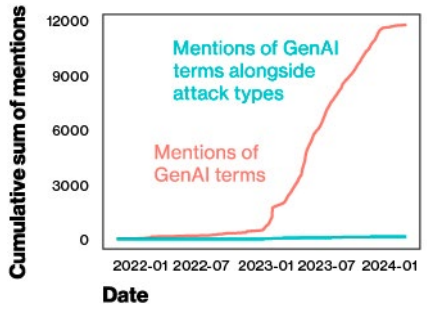


Figure 14. Cumulative sum of GenAI in criminal forums

17 Strange spelling for "unhinged marketing hype"

18 Artificial general intelligence. You know, HAL 9000, Skynet, Cylons, M3GAN ...

19 Just like real impactful technologies such as blockchain and the metaverse

20 But if we had been taken over by an evil AI technology, that is what we would say. Makes you think.

21 It is worth pointing out that while we were writing this section, Kaspersky came up with similar research that is worth a look: https://usa.kaspersky.com/about/press-releases/2024_new-kaspersky-study-examines-cybercrimes-ai-experimentation-on-the-dark-web

22 https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai

23 And when we asked it to do it again but in the voice of the DBIR, it seemed unhealthily fixated in circus and theater jokes and puns. Is that what we sound like?

24 We certainly know where we're getting marketing copy for our next cybersecurity startup.

VERIS Actions

A wise person[25] once said, "We are what we repeatedly do," and wouldn't they be impressed by the stoicism of how some of our top VERIS Actions keep showing up year after year? In all fairness, it does seem more an exercise of "if it ain't broke don't fix it" than any classical philosophical principle. But it highlights that we defenders have a lot of work to do, as usual.

Figure 15 has our top Action varieties in breaches, and it brings a lot to talk about. As we mentioned in the "Introduction" section, a big shift this year was the reduction of the Use of stolen credentials as a percentage of initial actions in breaches. It is still our top action at 24%, although it just barely passes statistical testing when compared to our good old Ransomware in the second spot, with 23%.

Ransomware is less representative than last year, although its common style of financially motivated breach is being complemented by Extortion, which now represents 9% of our action distribution. If you count Ransomware breaches and breaches with Extortion from ransomware actors as just two sides of the same coin,[26] we show a combined activity of 32% from those action varieties.

You can also see Extortion hand in hand with Exploit vuln at 10% of breaches, and the pair of them headline MOVEit's (and other similar vulnerabilities') impact, along with some other malware- and hacking-related varieties, such as Backdoor or C2 (command and control). That is double the exploitation of vulnerabilities of last year, and that obviously has had an impact in our ways-in metric as discussed in the introduction. Readers can find more details about this remarkable event in our "System Intrusion" pattern section.

One other thing worth noting is the clear overtaking of Pretexting as a more likely social action than Phishing. If you have been tracking our chronicle of the rise of BEC attacks, you know this is a viable and scalable way to address threat actor monetization anxieties.[27]

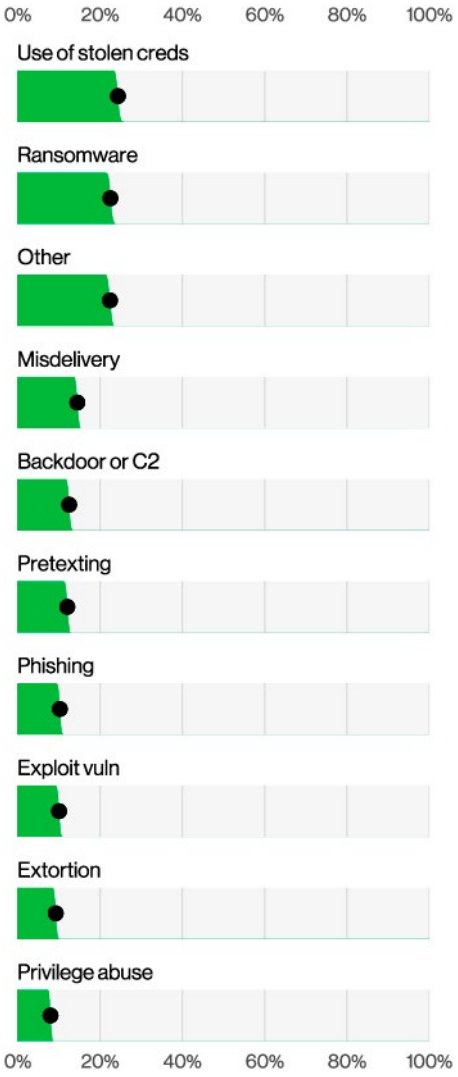


Figure 15. Top Action varieties in breaches (n=9,982)

Action categories[28]

Hacking (hak): attempts to intentionally access or harm information assets without (or exceeding) authorization by circumventing or thwarting logical security mechanisms.

Malware (mal): any malicious software, script or code run on a device that alters its state or function without the owner's informed consent.

Error (err): anything done (or left undone) incorrectly or inadvertently.

Social (soc): employ deception, manipulation, intimidation, etc., to exploit the human element, or users, of information assets.

Misuse (mis): use of entrusted organizational resources or privileges for any purpose or manner contrary to that which was intended.

Physical (phy): deliberate threats that involve proximity, possession or force.

Environmental (env): not only includes natural events such as earthquakes and floods but also hazards associated with the immediate environment or infrastructure in which assets are located.

25 Since every quote on the Internet is misattributed, let's just save some time and take the easy way out.

26 Which we kind of do in this issue of the report because it is exhausting to argue with people all the time about things like threat actor methodology details or tactics, techniques and procedures (TTPs) when everyone else seems to be doing it.

27 Unfortunately, everyone has to hit their quotas each quarter.

28 https://verisframework.org/actions.html

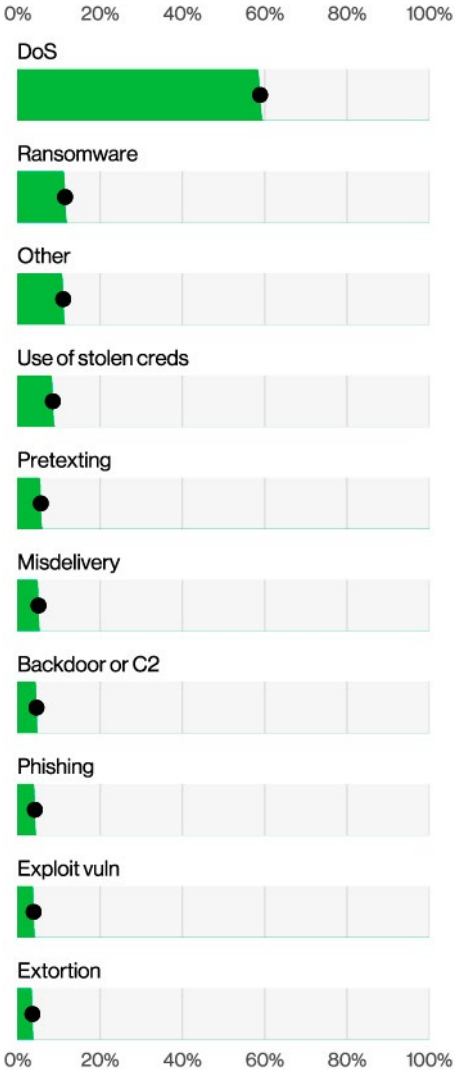


Figure 16. Top Action varieties in incidents (n=28,625)

Moving on to Figure 16, we have a chance to look into top Action varieties for incidents. It should not surprise any returning reader of the prevalence of DoS attacks in the top spot, being present in 59% of our recorded incidents. There is very little we can say about this Action variety that we haven't said before[29] as its lead has been quite stable over the years.

We can also observe the same phenomena in Ransomware that we saw in breaches. It is overall lower than last year, being present in 12% of incidents, but when you combine it with Extortion, we hit a similar ratio to last year's 15% of "Ramstortion."[30]

Figure 17 showcases the Action vectors in breaches, and the results are in line with what we have been discussing in the "Introduction" and "Actors" sections. There was considerable growth of Carelessness due to the increase in error breaches and an uptick in Email as a vector driven by the increase in pretexting. Web applications is hanging in there, though, and as we discussed in the introduction, it goes hand in hand alongside use of stolen credentials and exploitation of vulnerabilities to infiltrate your defenses.

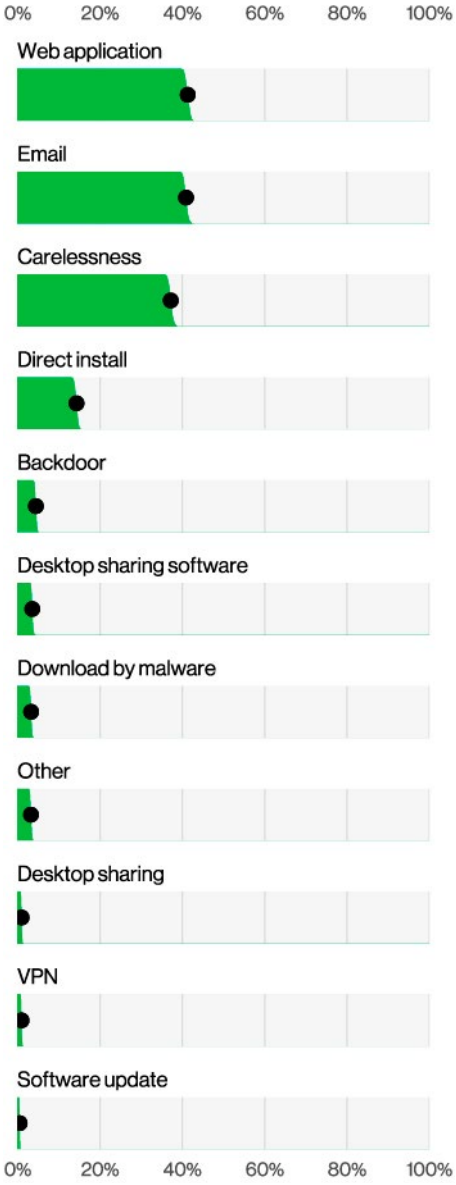


Figure 17. Top Action vectors in breaches (n=7,248)

29 We do try in the "Denial of Service" pattern section regardless.
30 "Extorware"? What would be the best couples name for this pair?

Speaking of ways in, it might also be interesting to explore a handful of goals and outcomes of those attacks.[31] Figure 18 describes the prevalence of ransomware/extortion and pretexting action varieties under the Financial actor motive. As we frequently point out, those are two of the most successful ways of monetizing a breach. The ransom duo has been hovering around the two-thirds mark (62%) for some time, while Pretexting made up nearly a quarter (24%) of goal actions over the past two years.

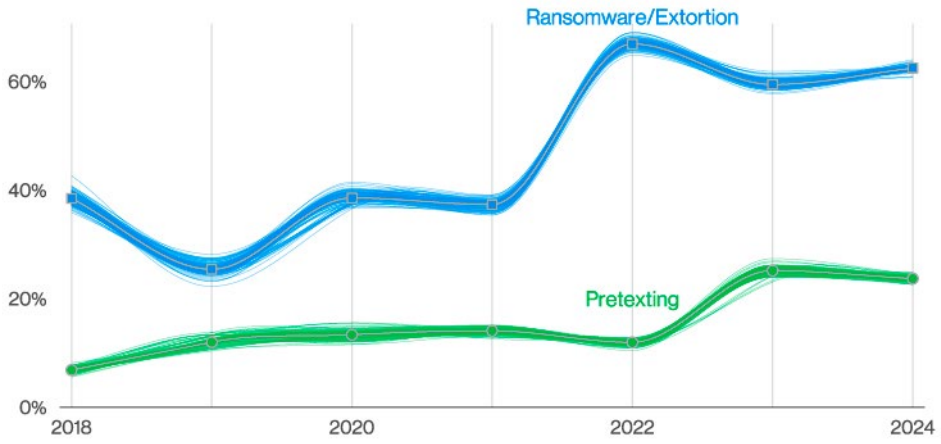


Figure 18. Select action varieties in Financial motive over time

Jen Easterly

Director Cybersecurity and Infrastructure Security Agency (CISA)

Over the past year, CISA has been leading the secure by design software development revolution. We have issued alerts documenting foreign intelligence agencies penetrating hundreds of critical infrastructure entities and establishing a foothold, possibly to be used in a future conflict. We have also published blueprints for what we need to change in order to establish a culture of technology development that puts security first without sacrificing innovation. These two efforts are different and necessary approaches to the same problem.

Today, the software industry is focused on the malicious actors and how they work. As a community, we talk about signature adversary moves, the amount of money made and the vulnerabilities that were exploited.

But it's that last point—vulnerabilities that were exploited—that doesn't get nearly enough focus. Most software vulnerabilities are not unknown, unique or novel. Instead, they fall into well-known classes of vulnerabilities, and unfortunately, we continue to see the same classes of vulnerabilities that have been identified for decades.

Our goal should be to shift away from focusing on individual vulnerabilities and to instead consider the issue from a strategic lens. By focusing on recurring classes of software defects, we can inspire software developers to improve the tools, technologies, and processes and attack software quality problems at the root. I hope that a deeper understanding of how attackers get in will be the catalyst to demand that our technology be secure by design starting today.

31 The obvious "ways-out" pun doesn't make sense here. Maybe if we had cyber getaway cars.

Exploitation moving swiftly in the threat landscape

The DBIR is entering its Vulnerability Era. One of the most critical findings we had this year was the growth of the Exploit vuln action variety. We have emphasized the fact that credential abuse is the big thing to focus on for several years now,[32] and even the most obtuse of us can see a trend when it is smacking us in the face.

We knew that the MOVEit vulnerability was trouble when it first entered the room, and we were able to identify 1,567 breach notifications that related to MOVEit by a combination of (very vague) breach descriptions and the timing of the breach itself. Reports from CISA[33] state that the Cl0p ransomware team had compromised more than 8,000[34] global organizations from a handful of zero-day vulnerabilities being exploited. It is important to mention this high number even if our sampled incident dataset does not account for all of that in either breach notifications or ransomware victim listings scraped from the threat actor's own notification websites.[35]

This love story between zero-day vulnerabilities and ransomware threat actors puts us all in a concerning place. By doing a survival analysis[36] of vulnerability management data and focusing on the vulnerabilities in the CISA Known Exploited Vulnerabilities (KEV) catalog,[37] (arguably an area of priority focus in vulnerability management), we found that it takes around 55 days to remediate 50% of those critical vulnerabilities once their patches are available. As Figure 19 demonstrates, the patching doesn't seem to start picking up until after the 30-day mark, and by the end of a whole year, around 8% of them are still open.

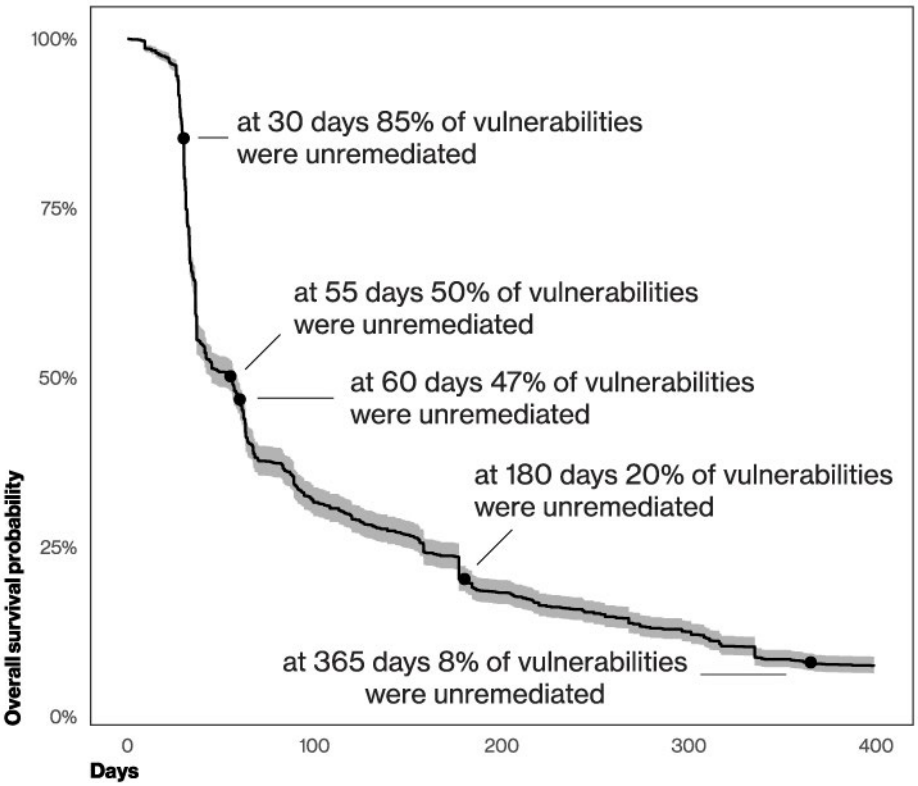


Figure 19. Survival analysis of CISA KEV vulnerabilities

But before organizations start pointing at themselves saying, "It's me, hi, I'm the problem," we must remind ourselves that after following a sensible risk-based analysis,[38] enterprise patch management cycles usually stabilize around 30 to 60 days as the viable target, with maybe a 15-day target for critical vulnerability patching. Sadly, this does not seem to keep pace with the growing speed of threat actor scanning and exploitation of vulnerabilities.

32 DBIR guided visualization: Picture blue team folks in jerseys at the Super Bowl chanting, "MFA! MFA! MFA!"
33 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a
34 Vegeta's power Scouter is still intact.
35 And just like a consultant will say, "It depends," our data scientists will say, "It's the sampling bias."
36 Hat tip to Jay Jacobs of Cyentia on the methodology: https://www.cyentia.com/why-your-mttr-is-probably-bogus
37 https://www.cisa.gov/known-exploited-vulnerabilities-catalog
38 Such as the one in https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-RemediateVulnerabilitiesforInternetAccessibleSystems_S508C.pdf

This is not enough to shake the risk off. As we pointed out in the 2023 DBIR, the infamous Log4j vulnerability had nearly a third (32%) of its scanning activity happening in the first 30 days of its disclosure. The industry was very efficient in mitigating and patching affected systems so the damage was minimized, but we cannot realistically expect an industrywide response of that magnitude for every single vulnerability that comes along, be it zero-day or not.

In fact, if you look at the distribution of when vulnerabilities have their first scan seen in internet honeypots on Figure 20, the median time for that to happen for a Common Vulnerabilities and Exposures (CVE) registered vulnerability in the CISA KEV is five days. On the other hand, the median time for non-CISA KEV vulnerabilities sits at 68 days. There is an obvious "no true Scotsman" fallacy comment to be made here because when exploitation starts running rampant, vulnerabilities get added to the KEV. There are few hindsight metrics as powerful as this one to guide what you should be patching first.[39] In summary, if it goes into the KEV, go fix it ASAP.

Even though this survival analysis chart looks bleak, this is the optimist's view of the situation. We must remind ourselves that these are companies with resources to at least hire a vulnerability management vendor. That tells us that they care about the risk and are taking measures to address it. The overall reality is much worse, and as more ransomware threat actors adopt zero-day and/or recent vulnerabilities, they will definitely fill the blank space in their notification websites with your organization's name.

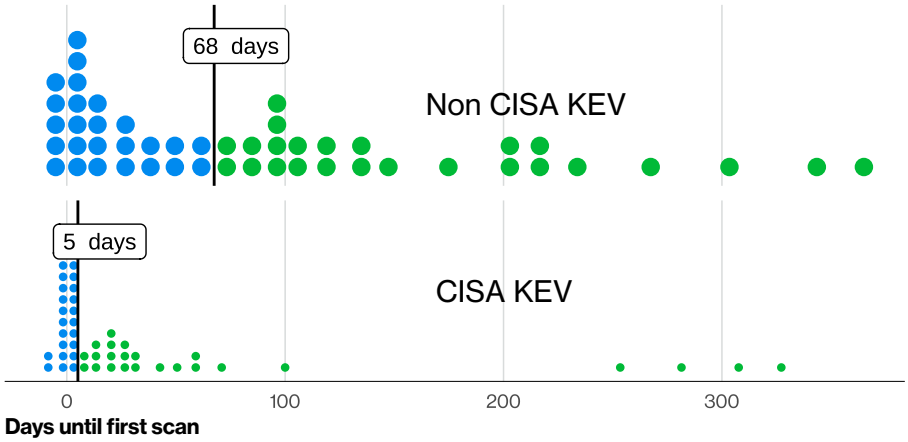


Figure 20. Time from publication of vulnerability to first scan seen (from 2020 onward)

If we can't patch the vulnerabilities faster, it seems like the only logical conclusion is to have fewer of them to patch. We realize this is the stuff of our wildest dreams, but at the very least, organizations should be holding their software vendors accountable for the security outcomes of their product, even if there is no regulatory pressure on those vendors to do better. The DBIR will emphasize this point going forward by expanding our third-party involvement in breaches metric to also account for the exploitation of vulnerabilities.[40] This helps illustrate that when choosing a vendor, software that is secure by design would make a difference.

We recommend that folks who are involved in both software development and software procurement take the time to review the recently updated "Secure by Design"[41] report by CISA and 17 U.S. and international partners. It shows how software can be made to have better security outcomes and what to look for as a buyer. The DBIR does not intend to foster any bad blood with software providers that might be falling short of their goals in keeping their products safe, but if there ever was a clear time to make a statement by prioritizing this elegant solution to a growing threat, this is it. We can see the costs of not acting all too well.

39 Eat your heart out, CVSS (Common Vulnerability Scoring System).
40 Have a look at the "Introduction" subsection in this "Results and analysis" section.
41 https://www.cisa.gov/resources-tools/resources/secure-by-design

VERIS Assets

Analyzing the VERIS Assets helps us understand where all those attacks we keep harping on are focused, and everyone sure needs help in prioritizing how to defend those assets. Even though those results might not be surprising as they have a good correlation with the VERIS Actions we just discussed, it is worthwhile to understand the year-to-year trends in the threat landscape.

Our asset power ranking[42] has not changed a lot from last year, but there are a handful of changes that are worth pointing out in Figure 21. Even though the order from the 2023 DBIR is the same and the prevalence of Server assets is roughly the same as well, we find substantial growth in both Person[43] and Media assets.

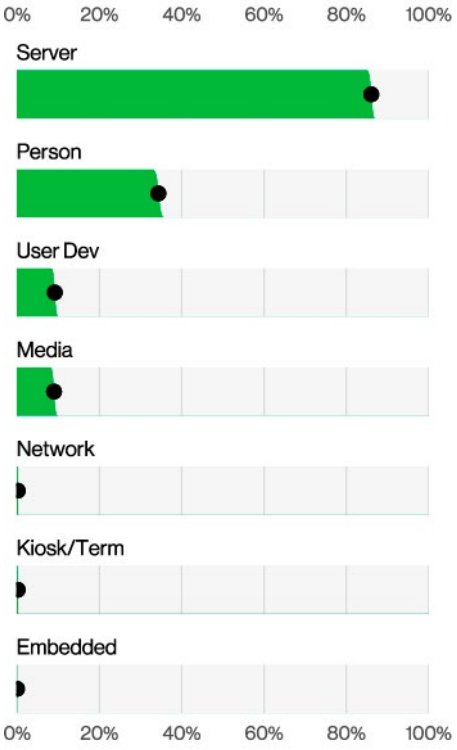


Figure 21. Assets in breaches (n=8,910)

Person as an asset has become more involved this year because of the growth of pure Extortion action-based breaches in our dataset. As a social action, Extortion demands a Person as the direct victim, and the dataset gnomes[44] are happy to oblige. What is interesting here is that the Ransomware action, where pure Extortion got its spin-off from, implied that there was an extortion phase where the money was requested without being connected to a Person asset.[45]

Thus, this growth in Person also makes sense as a more representative truth of the mechanics of such breaches. Your employees need to be aware of how to handle a ransom or extortion demand and follow whatever procedures were established by your organization to handle those. By the way, make sure you have those documented[46] just in case.

42 Who would win in a fight – an email server or a file server with prep time?
43 Perhaps not in maturity, as some people assets will have their security attributes compromised to avoid going to therapy.
44 The DBIR authors' pickleball team name
45 This is likely too much VERIS Standard inside baseball for the average reader, but we are amused very easily by things like this.
46 Just keep it on your file server. It should be fine, right? (Not really)

The Media growth is intrinsically tied with the progression in the Miscellaneous Errors pattern discussed previously. Some of those Misdelivery errors happen via physical documents and fax machines[47] which might limit their scope but does not make them any less breachworthy to regulators.

Digging deeper in Figure 22, we get a better sense of the Server asset breakdown. While the Web application and Mail servers are mostly involved in credential-theft breaches, the File server has been almost dominated by the MOVEit breaches, which explains why more than 95% of breached assets are servers.

All in all, a pretty standard year in the VERIS Assets world. We will be discussing more on how to help keep these assets safe in the "System Intrusion," "Social Engineering" and "Basic Web Application Attacks" pattern sections.

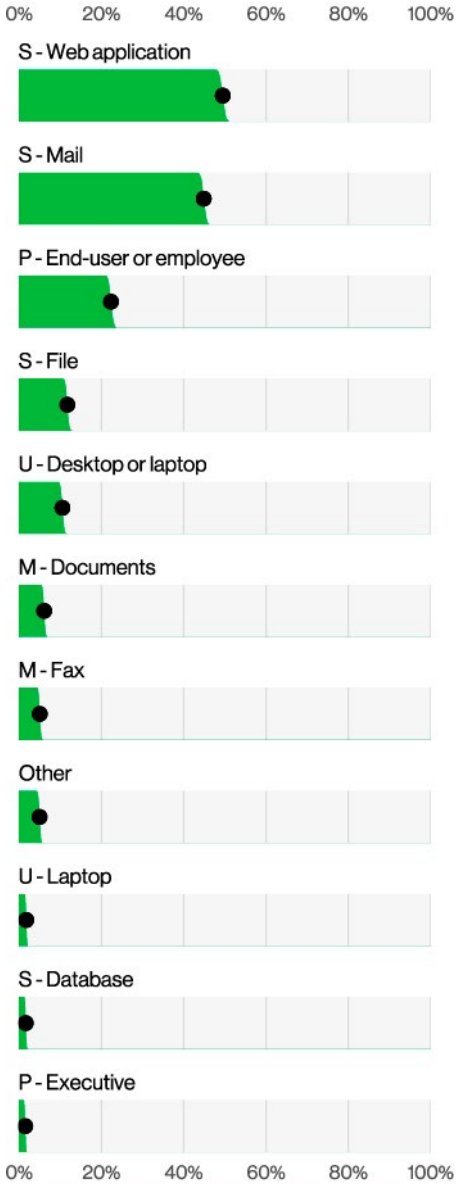


Figure 22. Top Asset varieties in incidents (n=6,606)

Asset categories[48]

Server (srv): a device that performs functions of some sort supporting the organization, commonly without end-user interaction. Where all the web applications, mail services, file servers and all that magical layer of information is generated. If someone has ever told you "the system is down," rest assured that some Servers had their Availability impacted. Servers are common targets in almost all of the attack patterns, but especially in our System Intrusion, Basic Web Application Attacks, Miscellaneous Errors and Denial of Service patterns.

Person (per): the folks (hopefully) doing the work at the organization. No AI chat allowed. Different types of Persons will be members of different departments and will have associated permissions and access in the organization stemming from this role. At the very least, they will have access to their very own User device and their own hopes and dreams for the future. Person is a common target in the Social Engineering pattern.

User device (usr): the devices used by Persons to perform their work duties in the organization. Usually manifested in the form of laptops, desktops, mobile phones and tablets. Common target in the System Intrusion pattern but also in the Lost and Stolen Assets pattern. People do like to take their little computers everywhere.

Network (net): not the concept but the actual network computing devices that make the bits go around the world, such as routers, telephone and broadband equipment, and some of the traditional in-line network security devices, such as firewalls and intrusion detection systems. Hey, Verizon is also a telecommunications company, OK?

Media (med): precious distilled data in its most pure and crystalline form. Just kidding, mostly thumb drives and actual printed documents. You will see the odd full disk drive and actual physical payment cards from time to time, but those are rare.

47 Believe it or not, this is not the 1994 Data Breach Investigations Report.
48 https://verisframework.org/assets.html

VERIS Attributes

As we often need to remind our very young children and grandchildren, actions have consequences.[49] Incidents and data breaches are no different,[50] and said consequences will often materialize as data leaks (confidentiality issue), unauthorized changes on your assets (integrity issue) or a loss of access to your data (availability issue).

More frequently than not, all of them can take a hit over the course of a multistep breach. Figure 23 demonstrates how often those three pillars were compromised over time in one of our charts with the most "DBIR charts do not add up to 100% because events are non-exclusive" energy thus far.

Roughly a third of the incidents we reviewed this year were data breaches where the Confidentiality of data was compromised. Figure 24 has the breakdown of data varieties that were leaked in breaches this year, and Personal data is unsurprisingly at the top of the list.

This continuous prevalence of Personal data in the top spot is in a way a self-fulfilling curse because the breaches that get more frequently disclosed will be the ones involving customer data where regulation requires the affected victims to be notified. Furthermore, customer data is so prevalent and hoarded without need or proper care that it will often be collateral damage in any sort of attack that might not even be specifically targeting it.

Internal company data (such as emails and business documents) and System-specific data also overshadow more exclusive targets such as Payment, Bank, Medical and Secrets. We have often described how the Ransomware (and now pure Extortion) breaches mean that the threat actors don't need to care about the data they are stealing because they will always have the victim organization as the main buyer. We dig into ransomware, ransom amounts and extortion economics in the "System Intrusion" pattern section later in the report.

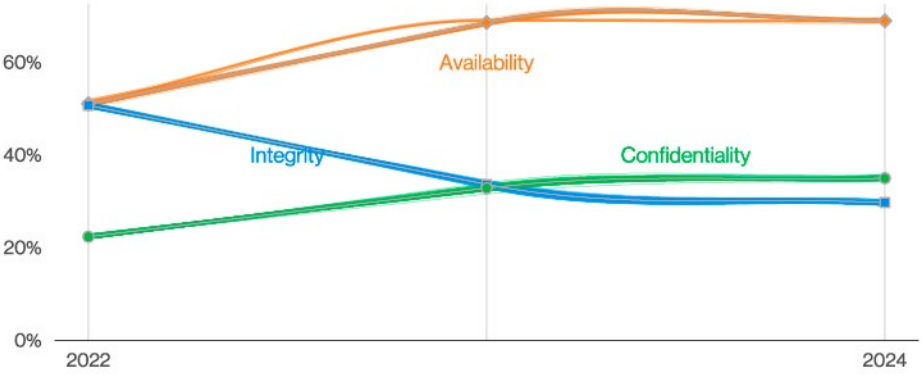


Figure 23. Attributes over time in incidents

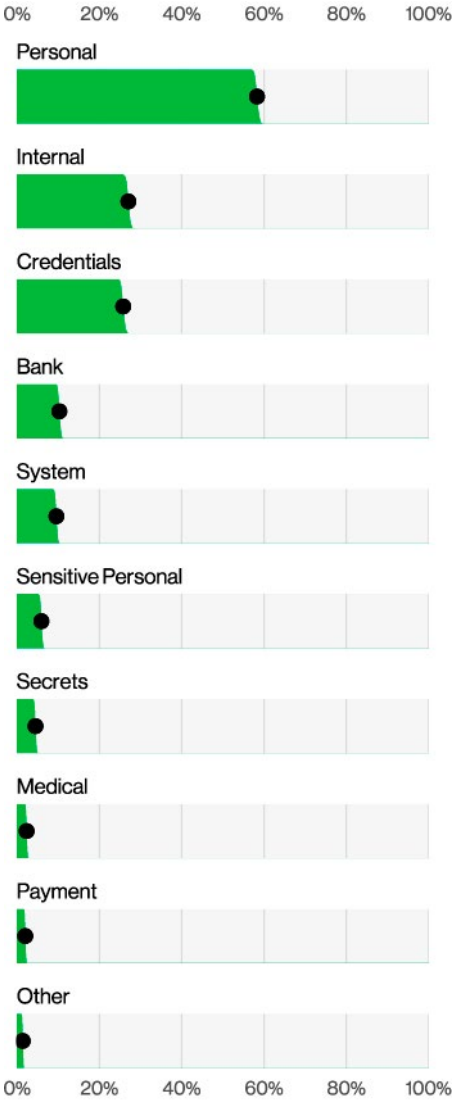


Figure 24. Top Confidentiality data varieties in breaches

49 Especially bad actions. Benevolent ones often go unnoticed.
50 Threat actors should also be sent to bed without TV if they misbehave.

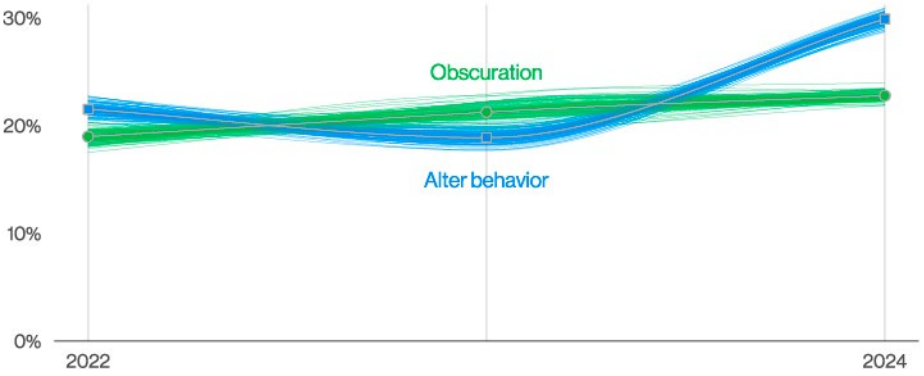


Figure 25. Select Attribute varieties over time in breaches

In addition, we are observing a decline in the Credentials data type from a percentage point of view. This is because the percentage of breaches caused by Error actions is rising (again as a result of our sample) as opposed to external actors who are exploiting weak credentials though credential stuffing or brute force attacks.

As a final curiosity, another side effect of the growth of extortion non-encrypting attacks has resulted in a significant bump in the Alter behavior variety under integrity. This is the integrity violation we get when Persons are influenced by external threat actors, and it is also a common outcome from a Phishing or Pretexting social action.

To see it overcome the Obscuration variety (the usual outcome of the Ransomware action) in such a sharp way in Figure 25 could be a harbinger of things to come. The consequence of which is that System Intrusion pattern attacks become more prevalent in the long run.

Attribute categories[51]

Confidentiality (cp): refers to limited observation and disclosure of an asset (or data). A loss of confidentiality implies that data were actually observed or disclosed to an unauthorized actor rather than endangered, at-risk or potentially exposed (the latter fall under the attribute of Possession or Control[52]). Short definition: limited access, observation and disclosure.

Integrity (ia): refers to an asset (or data) being complete and unchanged from the original or authorized state, content and function. Losses to integrity include unauthorized insertion, modification and manipulation. Short definition: complete and unchanged from original.

Availability (au): refers to an asset (or data) being present, accessible and ready for use when needed. Losses to availability include destruction, deletion, movement, performance impact (delay or acceleration) and interruption. Short definition: accessible and ready for use when needed.

Stephen Bonner

Deputy Commissioner – Regulatory Supervision, U.K. Information Commissioner's Office (ICO)

People need to be assured their information will be kept safe so they can participate in society, including having the confidence to share their data to access services and use products.

Our security incident trend data, which we have contributed to this report, shows cyber threats not only continue to exist but increase year on year. It is important to remember that there is no single solution to security, but organizations can improve their cybersecurity through our guidance and tools to better protect people's information.

We are also encouraging organizations to be transparent when a cyber incident happens, seeking early support and sharing information so the cyber threat landscape is improved for everyone. The ICO will soon publish a review of past security incidents to help organizations continue to improve their cyber resilience.

51 https://verisframework.org/attributes.html
52 https://en.wikipedia.org/wiki/Parkerian_Hexad