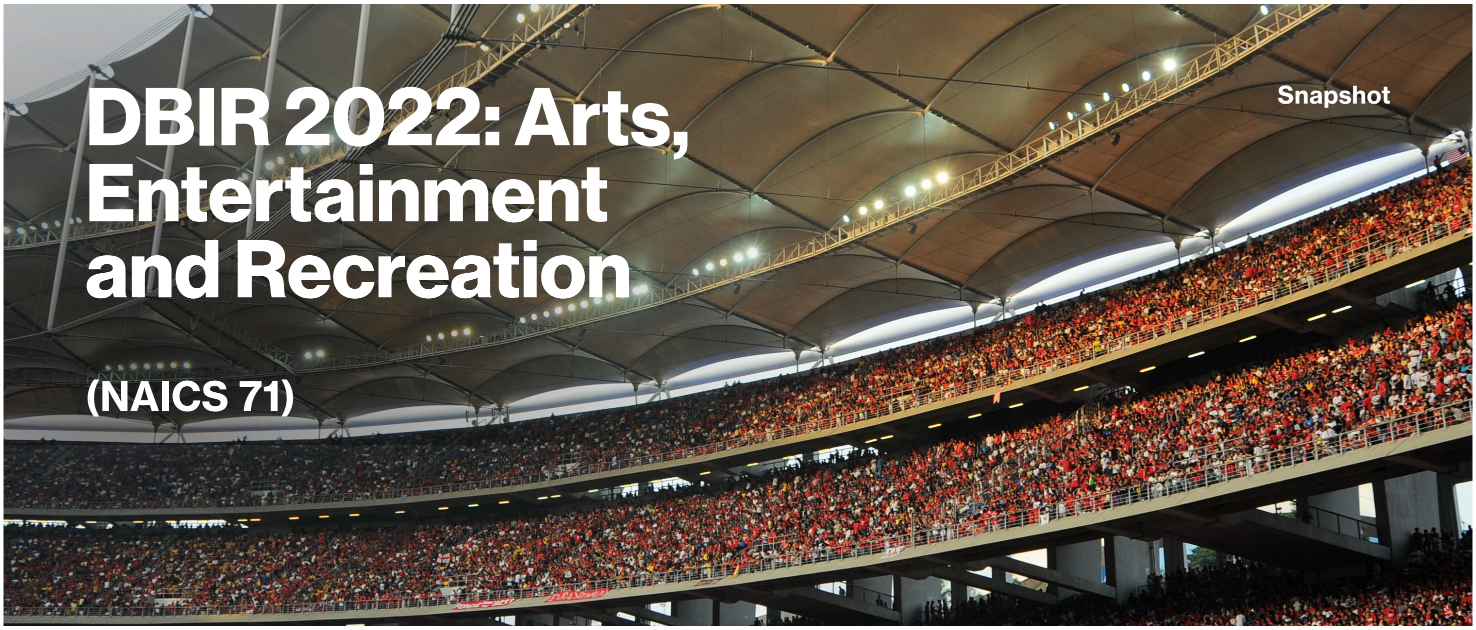

Snapshot

DBIR 2022: Arts, Entertainment and Recreation

(NAICS 71)

Welcome to the Arts, Entertainment and Recreation snapshot from the 15th annual Verizon Data Breach Investigations Report (DBIR). It is truly hard to believe that it has been 15 years since our inaugural report.

The DBIR examines common types of cybersecurity attacks and offers insights into how organizations can protect themselves. This year, we looked at 23,896 incidents. Arts, Entertainment and Recreation saw 215 of those incidents, 96 of which had confirmed data disclosure. This data represents real-world breaches and incidents investigated by the Verizon Threat Research Advisory Center (VTRAC) or provided to us by our 87 global contributors.

We hope that you can use this report and the information it contains to increase your awareness of the most common tactics used against Arts, Entertainment and Recreation, and to help prepare your organization.

Read on for report highlights related to Arts, Entertainment and Recreation. Also, please pass this summary along to colleagues and download the full report at verizon.com/dbir for a more detailed view of the threat landscape in 2022.

For all industry labels in the DBIR report, we align with the North American Industry Classification System (NAICS) standard to categorize the victim organization. The standard uses two- to six-digit codes to classify businesses and organizations. Our analysis is typically done at the two-digit level, and we will specify NAICS codes along with an industry label. Detailed information on the codes and the classification system is available here: census.gov/naics/?58967?yearbck=2012

Incident Classification Patterns

The DBIR first introduced the Incident Classification Patterns in 2014 as a useful shorthand for scenarios that occurred very frequently. Last year, due to changes in attack type and the threat landscape, we revamped and enhanced those patterns, moving from nine to the eight you see in this report.

These patterns are based on an elegant machine-learning clustering process, equipped to better capture complex interaction rules, and they are much more focused on what happens during the breach. That makes them better suited for control recommendations, too.

Social Engineering

Psychological compromise of a person that alters their behavior into taking an action or breaching confidentiality.

The human element continues to be a key driver of 82% of breaches, and this pattern captures a large percentage of those breaches. Additionally, malware and stolen credentials provide a great second step after a social attack gets the actor in the door, which emphasizes the importance of having a strong security awareness program.

- Fifty-nine percent of Social Engineering breaches compromised credentials, and 31% used stolen credentials. Credential compromise was three times more likely in Social Engineering breaches than in the rest of the patterns
- Phishing is more than twice as likely as Pretexting in the Social Engineering pattern
- A Financial motive is eight times more common than an Espionage motive in Social Engineering breaches

Basic Web Application Attacks

Simple web application attacks with a small number of steps or additional actions after the initial web application compromise.

This pattern continues to largely be dominated by attackers using stolen credentials to access an organization's internet-facing infrastructure, like web servers and email servers.

- Four out of every five web app attacks involved stolen credentials. This finding underlies the importance of password safeguards
- Espionage is four times more likely in Basic Web Application Attack (BWAA) breaches than in the rest of the patterns, indicating that Nation-states don't necessarily have to pursue complex attacks to leverage established and effective attacks to achieve their objectives
- Use of stolen credentials is six times more likely than Exploiting a vulnerability in BWAA breaches

System Intrusion

System Intrusion captures the complex attacks that leverage Malware and/or Hacking to achieve their objectives, including deploying ransomware.

This pattern consists of more complex breaches and attacks that leverage a combination of several different actions, such as Social, Malware and Hacking, and is where we find Supply Chain breaches and Ransomware, both of which increased dramatically this year.

- Ninety-two percent of System Intrusion breaches are Financially motivated
- Use of stolen credentials is four times more likely than Exploiting vulnerabilities in System Intrusion breaches

Miscellaneous Errors

Incidents where unintentional actions directly compromised a security attribute of an information asset. This does not include lost devices, which are grouped with theft instead.

This year's data shows it is all about your employees. Misdelivery and Misconfiguration are the top two varieties. Misconfiguration is frequently paired with the discovery method of "Security researcher."

- Misconfigured servers accidentally exposed to the internet or Misdelivery actions in which users send emails to the wrong recipient represent 13% of total breaches
- External cloud assets have decreased 83% since last year in Miscellaneous Errors breaches, potentially indicating a shift in technologies leveraging a secure-by-default approach
- Eighty-five percent of Miscellaneous Error breaches involved servers

Privilege Misuse

Incidents predominantly driven by unapproved or malicious use of legitimate privileges.

Most of these incidents result in successful data breaches. These actors are still motivated by greed (financial gain) and are stealing Personal data because it is easy to monetize.

- Documents are three times more likely in Privilege Misuse than in the rest of the patterns

Lost and Stolen Assets

Any incident where an information asset went missing, whether through misplacement or malice.

The prevalence of theft is driven by the Financial motive—we believe many of the perpetrators of theft are committing the crime with the intention of an immediate payoff by selling the stolen asset.

- The type of data affected by these incidents is the same (almost exactly) as last year. External actors typically perpetrate the thefts, while employees are responsible for losing track of their assets
- Unaffiliated actors are 14 times more likely in Lost and Stolen Assets incidents than in the rest of the patterns

Denial of Service

Attacks intended to compromise the availability of networks and systems. Includes both network- and application-layer attacks.

Large organizations are twice as common in Denial of Service (DoS) incidents than the rest of the patterns. While these attacks are a nuisance impacting a large range of organizations, some face these attacks on a regular basis, which may potentially affect their function.

Everything Else

Everything else isn't really a pattern at all. Instead, it covers all incidents that don't fit within the orderly confines of the other patterns.

Arts, Entertainment and Recreation

In the Arts, Entertainment and Recreation industry, the System Intrusion and Basic Web Application Attacks patterns exchanged positions, but the Miscellaneous Errors pattern held on to third place on the podium. For incidents, Denial of Service attacks remain a problem in the sector, particularly for the Gambling industry.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	No change	No change	No change
System Intrusion	No change	No change	Less
Miscellaneous Errors	No change	No change	Greater

Frequency	215 incidents, 96 with confirmed data disclosure
Top patterns	Basic Web Application Attacks, System Intrusion and Miscellaneous Errors represent 80% of breaches
Threat actors	External (74%), Internal (26%) (breaches)
Actor motives	Financial (97%), Grudge (3%) (breaches)
Data compromised	Personal (66%), Credentials (49%), Other (23%), Medical (15%) (breaches)
Top IG1 protective Controls	Security Awareness and Skills Training (CSC 14), Secure Configuration of Enterprise Assets and Software (CSC 4), Access Control Management (CSC 6)
What is the same?	The patterns are the same, but the order is not. Medical data continues to be compromised in this industry.

This industry mainly covers live performances, and whether dance, theater or sporting events, the common thread is that none are prerecorded for later broadcast. It also includes the gambling industry. One can only imagine the different attack surfaces that are present for the myriad organization types belonging to this NAICS code. Something many of them have in common, however, is that at least a portion of their infrastructure relies on the internet to perform critical functions, whether that is ticket sales or taking orders (or bets as the case may be). In any event, when a Denial of Service attack comes calling, it is a very unwelcome guest. Nevertheless, it is a frequent guest in this sector (particularly in the Gaming organizations in the Asia-Pacific region), and represents over 20% of incidents.

The inclusion of the Basic Web Application Attacks is concerning, given the less complex nature of these attacks. Conversely, the attackers have to try much harder to gain their prize in the System Intrusion attacks, where ransomware is always a favored tool. As we have seen in the past, every attacker loves credentials, and will use them to masquerade as a legitimate employee to evade capture for as long as it takes to get what they are after.

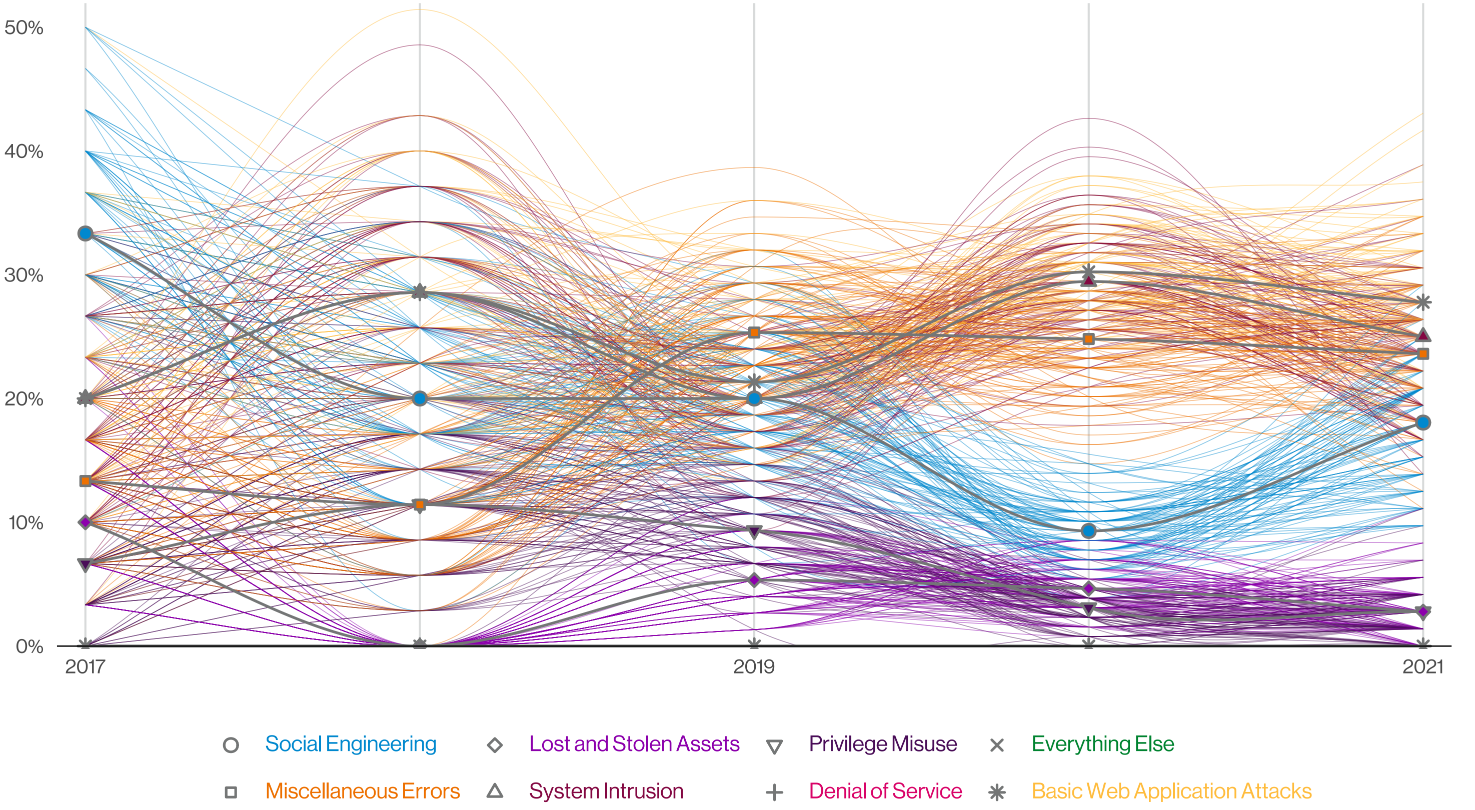

Figure 1. Patterns over time in Arts and Entertainment breaches

The most commonly taken data is Personal information (although it is down from a high last year of 83%) and Credentials. Oddly enough, Medical data is still being snarfed up (technical term) in 15% of the breaches in this sector. This was similar to last year (at 26%), but it remains a puzzling data type to find in a sector that has no medical affiliation. It may be that the data taken is from companies that are self-insured for their employee medical needs, and so have a need to store that kind of data, or it could possibly be from some form of workers' compensation data (on-the-job injuries). Additionally, this NAICS code includes sports teams which could account for a certain number of stolen medical records. Regardless, it is a rather counterintuitive finding.

Miscellaneous Errors remain in the top three patterns again this year (25%). The Misconfiguration error was the most common, representing approximately 15% of the breaches. It appears this sector simply traded one problem for another as Misdelivery errors (the most common last year) have dropped considerably.

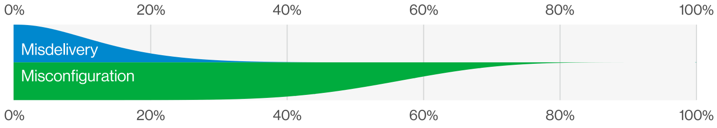

Figure 2. Misdelivery vs Misconfiguration in Arts and Entertainment industry Error breaches (n=16)

Being confident in our data

Starting in 2019 with slanted bar charts, the DBIR has tried to make the point that the only certain thing about information security is that nothing is certain.

The slant on the slanted bar chart represents the uncertainty of that data point to a 95% confidence level (which is standard for statistical testing).

Spaghetti charts, and our relative newcomer, pictogram plots, attempt to capture uncertainty in a similar way to slanted bar charts but are more suited for a single proportion.

Stay informed and threat ready.

Successfully navigating through the cyberthreats facing Arts, Entertainment and Recreation organizations today requires intelligence from a source you can trust. The full DBIR contains real-world details on the actors, actions and patterns that can help you to prepare your defenses and educate employees.

Read the full 2022 DBIR at verizon.com/dbir