2022 DBIR: Manufacturing

(NAICS 31–33)

Snapshot

Welcome to the Manufacturing 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. Manufacturing saw 2,337 of those incidents, 338 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 Manufacturing and to help prepare your organization.

Read on for report highlights related to Manufacturing. 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 creds. 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.

Manufacturing

Manufacturing continues to be a lucrative target for espionage, but is also increasingly being targeted by other criminals via the use of DoS attacks, credential attacks and Ransomware.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	Greater	Greater	Greater
Social Engineering	Less	Less	Less
System Intrusion	Greater	Greater	Greater

Manufacturing, with its hum of machinery churning out the key components that make our modern life possible, continues to be a valued target for espionage (mostly due to recent indiscriminate supply chain attacks discussed in the full report). However, it has also become a lucrative target for financially motivated criminals looking to make a quick dollar.

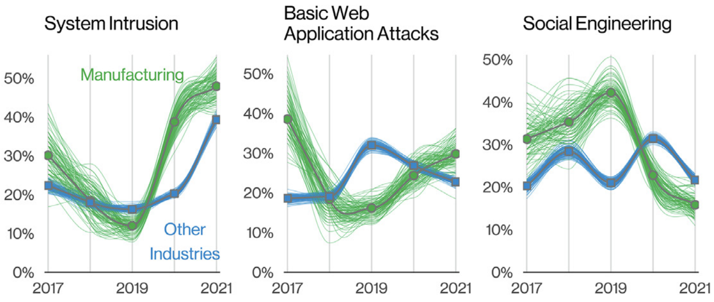

Figure 1. Top patterns over time in Manufacturing breaches

Frequency	2,337 incidents, 338 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Social Engineering represent 88% of breaches
Threat actors	External (88%), Internal (12%), Partner (1%) (breaches)
Actor motives	Financial (88%), Espionage (11%), Grudge (1%), Secondary (1%) (breaches)
Data compromised	Personal (58%), Credentials (40%), Other (36%), Internal (14%) (breaches)
Top IG1 protective Controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Secure Configuration of Enterprise Assets and Software (CSC 4)
What is the same?	System Intrusion and Basic Web Application Attacks continue to be among the main patterns this industry faces.

In previous reports, Manufacturing was largely targeted for its juicy schematics and secrets. For example, in 2016 over 55% of the incidents in this vertical involved Espionage (Figure 2), but that has been lower over the last few years. Or, conversely, the spies have upped their game to the point that they are no longer exposed.

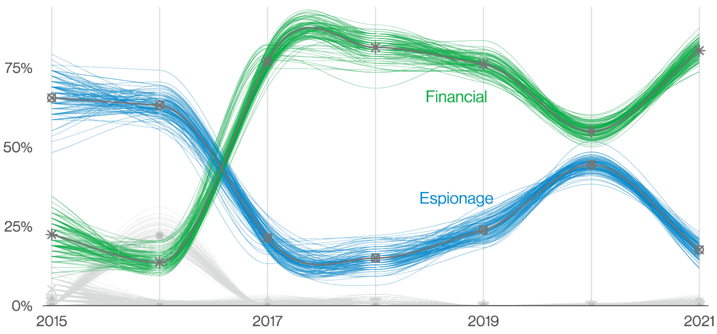

Figure 2. Motives over time in Manufacturing industry incidents

DoSing against the machine

For an industry where availability equals productivity, it's interesting to see the yo-yo pattern that has been taking place with DoS attacks over the years. While DoS attacks initially reached their former peak in the 2018 report (over 40% of incidents), they've been increasing since 2019 and now account for approximately 70% of incidents, which puts them more in line with what we see in other industries. This rise of DoS, while unlikely to prevent those key assets from actually running the manufacturing process, is still worth keeping in mind as integration increases between the OT side of the house and the IT side.

With regard to the breaches impacting this sector, one can find the usual suspects, such as stolen credentials (39%), Ransomware (24%) and Phishing (11%) demonstrated in Figure 4. These types of breaches appear to be impacting everyone regardless of industry. Implementing safeguards should be a priority for this vertical. Otherwise, you might find your organization unexpectedly seizing up due to a certain someone with an anime girl avatar.

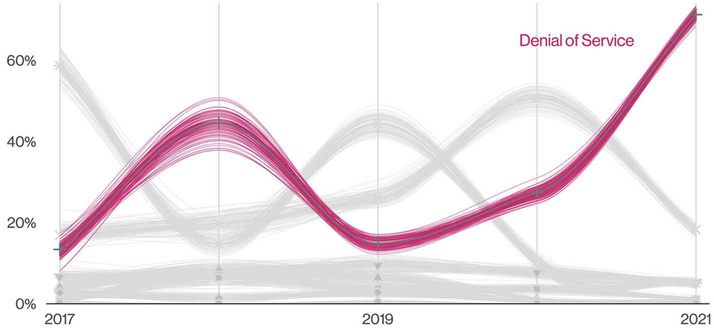

Figure 3. Patterns over time in Manufacturing industry incidents

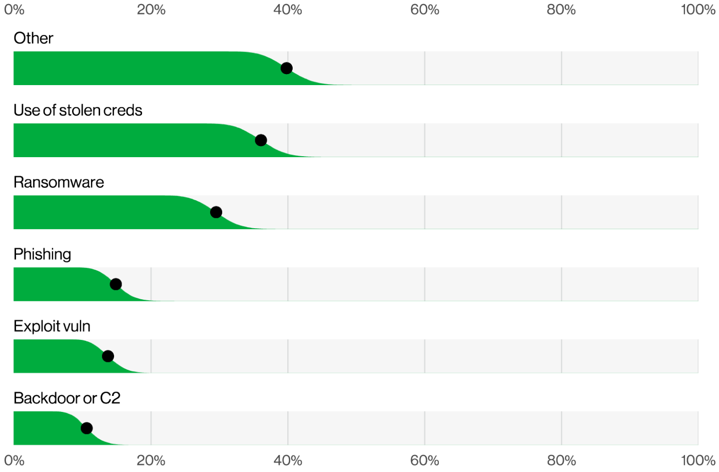

Figure 4. Top Action varieties for Manufacturing industry breaches (n=259)

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 Manufacturing 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