tripwire

WHITE PAPER

Key Takeaways from the Verizon 2020 Data Breach Investigations Report

Analysis by Breach Type and Industry, with Guidance on the CIS Controls

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

Each year, Verizon publishes the *Data Breach Investigations Report* (DBIR), giving the cybersecurity industry an in-depth analysis of the state of global cybersecurity across a number of industries, including retail, healthcare, financial and manufacturing. This year's report, sponsored by Tripwire and other industry leaders, revealed trends behind 32,000 cybersecurity incidents. Of those incidents, 3,950 were confirmed data breaches. What's new in this 13th edition is that the findings are broken down into 16 industry verticals and aligned with the MITRE ATT&CK framework and the Center for Internet Security's CIS Controls.

Misconfigurations

The fact that "misconfiguration" errors are in the top five action varieties for breaches is an important acknowledgment that not all incidents are the result of an exploited vulnerability. Misconfigurations actually lead to more breaches than exploited systems, but organizations often don't put the same effort into assessing them as they do while scanning for vulnerabilities. At a high level, the key things for every organization to worry about are brute force and stolen credentials, and web applications.

Cloud Security Threats

According to the report, cloud assets were involved in about 24 percent of breaches, while on-premises assets accounted for 70 percent of reported breaches. Cloud breaches involved an email or web application server 73 percent of the time. Additionally, 77 percent of those cloud breaches also involved breached credentials.

As businesses are adopting hybrid workloads, so too are criminals. These findings are not so much an indictment of cloud security as it is an illustration of the trend of cybercriminals finding the quickest and easiest route to their victims.

Cloud assets are still a minority of targets at 24 percent compared to on-premises 70 percent. Why change tactics if they're working? The cloud has a learning curve for criminals as well as enterprises.

IT vs. OT Cybersecurity

This year, the report began tracking Information Technology (IT) vs Operational Technology (OT) for assets involved in incidents. The findings were not particularly surprising: 96 percent of breaches involved IT, while the other four percent involved OT.

Although it might not sound like a lot, those breaches involving OT assets all constituted instances in which malicious actors might have attempted to disrupt the reliability and availability of highly critical services, such as the electric grid of water supply that rely on OT equipment. Clearly, there is an adequate cause for concern; relevant industries must take every precaution available to reduce the likelihood of a breach involving their OT assets.

Mobile Device Security

Nearly all (97 percent) of the incidents reported on mobile devices were errors, meaning a lost device. Despite being frustrating and a problem to tackle, this is not surprising. What is interesting is that the other three percent involved espionage and financial motives.

And while the financially motivated incidents range from theft to the use of the device as a vessel for pretexting, the espionage-related cases were exclusively malware-based compromises of mobile devices that were intended to further persistence and facilitate the exfiltration of data by advanced state-affiliated actors.

2020 DBIR Quick Facts

- Many believe internal actors to be the most common cause of breaches, but the DBIR's data shows that 70% of breaches this year were caused by outsiders.
- 86% of breaches were financially motivated, although espionage and advanced threats tend to receive the most buzz.
- Credential theft, social attacks (i.e., phishing and business email compromise), and errors caused the majority of breaches (67% or more).
- Ransomware accounted for 27% of malware incidents, and 18% of organizations blocked at least one piece of ransomware.
- Attacks on web apps were a part of 43% of breaches, more than double the results from last year. As workflows move to cloud services, it makes sense for attackers to follow. The most common methods of attacking web apps involved the use of stolen or brute-forced credentials.
- Personal data is getting swiped more often, or at least those thefts are being reported more often due to regulatory requirements. Either way, personal data was involved in 58% of breaches—nearly twice the percentage in last year's data. That's a big benefit coming out of GDPR.
- 81% of the reported breaches were contained in days or less, and 72% of the victims were large businesses.

If you're worried about mobile devices in your organization, the data says that your biggest concern should be theft or physical loss. Only three percent of incidents on mobile devices were anything other than that basic type of loss.

Asset and Vulnerability Management

The report findings indicate that hosts susceptible to major new vulnerabilities still also tend to be defenseless against many older vulnerabilities. While this finding seems to indicate that patching is working, it also serves as an indication that asset management is not.

Let's elaborate a bit more on this. The report found that organizations have approximately 43 percent of their internet-facing IPs in one network. However, the most common number of networks that an organization occupies is five, and half of all organizations are present on seven or more networks. The question is, do you know where these networks are—and do you have visibility into the assets of these networks?

If you don't, then you have an asset management problem. Therefore, it might not just be an asset management problem but also a vulnerability management problem on the assets you did not realize were there.

It's tempting to downplay vulnerability management based on this data, but the details show that, by and large, the organizations that are doing it reasonably well are safer, and the organizations that aren't are very, very vulnerable. One key lesson, though, is that an organization can do both. The old adage "you can't protect what you don't know about" is true for vulnerability management. Asset management is a prerequisite for vulnerability management.

How Many Steps to a Breach?

A very interesting section in the report is the one analyzing the courses of action criminals take to finally breach a company. The incidents and breaches analysis demonstrated that attacks come in numerous forms and sizes, but most of them are short, having a small number of steps. The long ones tend to be hacking and malware breaches, compromising confidentiality and integrity as the attacker systematically works their way through the network and expands their persistence (lateral movement).

Attackers prefer short paths and rarely attempt long paths. This means anything you can easily throw in their way to increase the number of actions they have to take is likely to decrease their chance of messing with the data. For example, although two-factor authentication is imperfect, it does help by adding an additional step for the attacker. The difference between two steps, and three or four steps, can be important in your defensive strategy.

The benefit in knowing the "areas" attackers are more likely to pass through in their journey to a breach gives you the ability to choose where to intercept them. One important lesson to take from the DBIR is that a compromise is often made up of multiple attacks, and so, as a defender, you have multiple opportunities to stop the attacker.

The concept of "defense in depth" is applicable here. The data provided about how the multiple steps in a compromise occur is vital. Malware is rarely the first step, and so if you catch malware in your environment, you have to look for what came before that. Hacking is much harder to deal with because it plays a role in the beginning, middle and end stages of a breach.

Industry Analysis

The industry analysis provided by the DBIR is invaluable. Being able to see which assets, actions, and patterns are most relevant for your industry

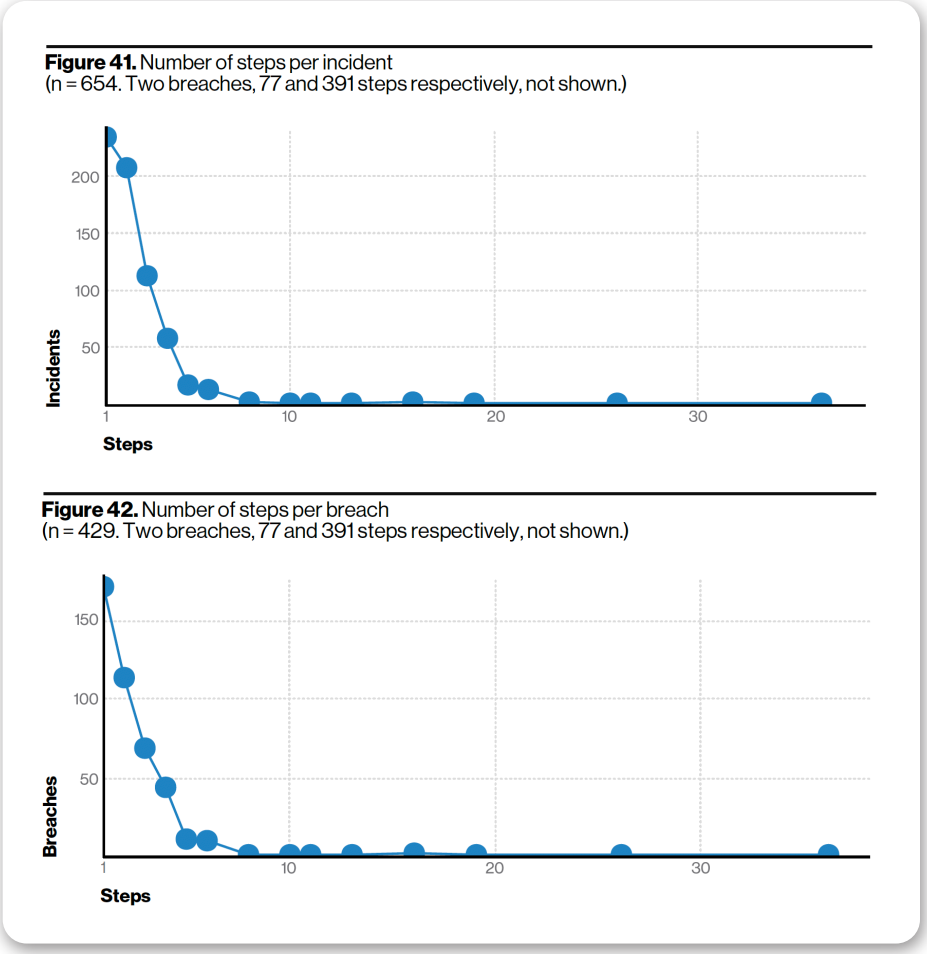

Fig 1. Number of steps per incident and per breach. Courtesy of Verizon.

allows you to take much more decisive action as a defender. For example, Manufacturing should be concerned about crimeware introduced through malware and social engineering more than any other industry. If you're in healthcare, errors figure much more prominently in your threat model than other industries. This year, the DBIR features a breakdown of findings from 16 industry verticals. Let's take a closer look at financial, manufacturing, oil and gas, public administration, and transportation.

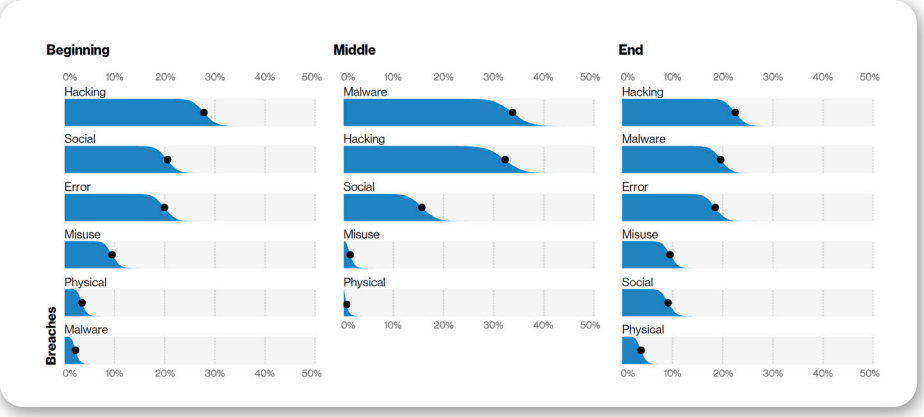

Fig. 2 Steps during a compromise. Courtesy of Verizon.

Financial and Insurance

The attacks in this sector were perpetrated by external actors who were financially motivated to obtain easily monetized data (63 percent), internal financially motivated actors (18 percent), and internal actors committing errors (9 percent). Web application attacks that leverage the use of stolen credentials also continued to affect this industry. Breaches caused by internal actors shifted from malicious actions to unintended errors, such as misdelivery, although both were still damaging.

Manufacturing

Manufacturing was attacked by external actors (75 percent) using password dumper malware and stolen credentials to hack into systems and steal data, the report revealed. While the majority of attacks were financially motivated (73 percent), there was an indication of cyber-espionage attacks in this industry, as well (27 percent). Internal employees (25 percent) misusing their access to get away with data also remained a concern for this vertical.

Public Administration

Ransomware was a large problem for this sector, with 61 percent of malware cases related to it. Ransomware was preferred by financially motivated attackers (75 percent) utilizing it to target a wide array of government entities. Misdelivery and misconfiguration errors persisted in this sector, too. When sensitive information goes to the wrong recipient and datastores are in the cloud without the necessary security measures in place to protect the data from unauthorized access, these can be serious problems.

Oil and Gas

Breaches in this sector consisted of a variety of actions, but social attacks such as phishing and pretexting dominated the incident data. Cyber-espionage-motivated attacks and incidents involving OT assets were also concerns for these industries.

Transportation

Financially motivated organized criminals utilizing attacks against web applications had their sights set on this industry. But employee errors such as standing up large databases without controls were also a recurring problem. These, combined with social engineering in the forms of phishing and pretexting attacks, were responsible for the majority of breaches in this industry.

Recommendations Based on the CIS Controls

To align the report findings with the corporate security efforts, the DBIR included a section where the findings were mapped to the CIS Controls. And there is a good reason for selecting the CIS Controls because they are a relatively short list of high-priority, highly effective defensive actions that provide a "must-do, do-first" starting point for every enterprise seeking to improve their cyber defense.

The inclusion of the CIS controls, after a hiatus, is a good addition for defenders. CIS is well-respected in the industry, and the controls provide enough information to be actionable but avoid being overwhelming at the same time.

Based on the report findings, the following CIS Controls are recommended:

- Continuous Vulnerability Management (CSC 3)
- Secure Configuration (CSC 5 and CSC 11)
- Email and Web Browser Protection (CSC 7)
- Limitation and Control of Network Ports, Protocols and Services (CSC 9)
- Boundary Defense (CSC 12)
- Data Protection (CSC 13)
- Account Monitoring (CSC 16)
- Implement a Security Awareness and Training Program (CSC 17)

Tripwire can help you meet the requirements of a number of the Controls to build a highly effective security program. Solutions such as Tripwire® Enterprise and Tripwire IP360™ leverage industry-leading file integrity monitoring (FIM), security configuration management (SCM), asset discovery, vulnerability management (VM), and more. Thousands of companies trust Tripwire to keep them in compliance and ahead of cyberthreats.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook

WPDBIR20a 2006