comforte

HAVE YOU CHECKED OUT VERIZON'S LATEST?

# COMFORTE RECOMMENDS THE 2021 DATA BREACH INVESTIGATIONS REPORT

## VERIZON'S DBIR REPORT GIVES INSIGHTS INTO INCIDENTS AND BREACHES

Verizon has issued their comprehensive 2021 Data Breach Investigations Report. If you haven't given much attention to the report in the past, now is a good time to check it out. It provides insights into threat actors who perpetrate attacks, strategies and tactics they use to carry them out, and the repercussions, along with some witty conversation and asides along the way. The DBIR presents data very clearly, too, often with graphical representations to make the concepts abundantly clear. It's definitely worth a read!

We think the value of the DBIR report is two-fold: business and technical. So we've touched on both. At comforte, we deal with data security every single day, from finding and understanding your corporate data to implementing the right controls and protections, regardless of whether your data ecosystem is pretty straightforward or highly complex. We're here to talk with you about all this, if you need some expert advice and insights on data protection after reading the report.

According to the report...

**79,635** INCIDENTS

**29,207** MET QUALITY STANDARDS

**5,258** CONFIRMED BREACHES

**88** COUNTRIES

## USED BY CYBERSECURITY EXPERTS

The DBIR's strong track record of breach investigations across many years makes it a unique analysis record of hard breach risk facts. Trends across different threats, and the resulting impacts, can be quickly contrasted with macro trends like the introduction of data-centric security models, deeper cloud adoption, and faster and more accurate risk-detection techniques.

The report is thus a forecast of future breach risk concerns weighed against potential breach mitigation strategies, and also a record of the benefits of industry investment in enhanced security. For example, payment card data, regulated under PCI DSS, showed a sharp decline in breaches as more organizations implemented data-centric security like tokenization and point to point encryption, while personally identifiable, healthcare, financial data, and credential attacks and breaches dramatically rose in the last couple of years as data succumbed to accidents, misconfigurations, ransomware, and insiders, and increasingly from cloud platforms.

**MARK BOWER, SVP**
**COMFORTE AG**

According to the report...

> 85% of breaches involved a human element

> **IN THE INFORMATION INDUSTRY, MISCONFIGURATIONS ACCOUNT FOR 70% OF ALL ERRORS.**

# THE BUSINESS VALUE OF DBIR

Business is all about income and expenditures, profit and loss. A company's assets are a big component of these calculations, things such as land holdings, buildings, vehicles, and equipment. We even refer to employees as one of a company's most valuable assets. Another corporate asset that arguably may be of highest value—and also highly vulnerable—is data. Knowing how to collect, handle, process, and analyze data separates the great enterprises from the fair ones.

An enterprise's data says everything about their customers, their intellectual property, their employees, and their corporate strategy. This is the reason that threat actors salivate to get their hands on this golden stuff. Therefore, you need to protect your data assets, and one way to do that is to understand as much as you can about recent incidents

A well-run business needs to know where to put its investments, including cybersecurity generally and data protection in particular so that data assets are secured. This is where Verizon's 2021 DBIR Report really comes in handy. By breaking down concepts like who the threat actors are (external, state-sponsored, etc.), the types of data they went after, and the actions and methods used to get to that data, Verizon gives you not predictions (they are very careful to point out that they are not in the business of predicting the future) but rather detectable patterns backed up by clear data points.

For example, learning that the pattern continues in which threat actors deprioritize payment data in favor of getting at any data which can disrupt corporate operations is an important fact to know. As you can guess, a disruption in operations due to ransomware probably nudges the organization to just pay the darn thing and restore operations. Has your IT thought of that, and do they have a plan to prevent it? What investments in tools do they need to prevent this?

Verizon also gives you many different ways to look at and consume the information within the report. From a business perspective, what are the major takeaways? Threat actors are after your data, because your data is a high-value asset. The patterns they establish are worth investigating, and if your organization is trying to build a culture of data privacy and security, each employee should read the report, understand how and why threat actors are targeting them, and determine how they can help thwart incidents within your company. If nothing else, the report should encourage every enterprise to give special thought to protecting data beyond just traditional controls: data-centric security that focuses on data itself might just reduce or eliminate the negative repercussions of an attack, even if your most sensitive data does fall into the wrong hands. We at comforte can explain how!

According to the report...

> Because the only way to predict the future is to change it yourself

**BUILDING A CULTURE OF SECURITY IS ALL-IMPORTANT. ORGANIZATIONS NEED TO HELP WORKERS ADAPT BEHAVIORS TO PREVENT CREDENTIAL THEFT, SOCIAL ENGINEERING, AND USER ERROR.**

## THE TECHNICAL VALUE OF DBIR

According to Verizon's 2021 Data Breach Investigations Report, over the years the threats have not changed substantially. Incidents and breaches are for the most part attributed to privilege abuse and data mishandling all in an effort to get at personal information. Mostly this has been accomplished by some tech-savvy criminals that have become adept at social engineering to get to the information needed. Phishing and social engineering seem to be a prime examples.

We have all gotten that email that says our Netflix account has been suspended due to lack of payment, and without thinking, because who can live without Netflix? Click unwittingly on the message, of course. This and other examples of phishing and social engineering have become bread and butter to organized criminals trying to get access to personal information. These phishing expeditions happen in the enterprise in order to get users credentials.

It happens like this. You have rolled out some new application and accordingly you get an email the next day to change your username and password. Some tech-savvy threat actor (criminal) has been paying attention to your company announcements and has sent this email to half the company trolling for credentials. It's a fair bet that at least 10% of the people receiving that email will respond. With the use of these credentials, now the criminals are in your enterprise with unknown access to company and customer data.

In today's world, data breaches are deadly, to your reputation, to your stock and to your customers!  Without a means of protecting data, other than with user credentials, you open yourself up to a large risk. The technical value of this report is immeasurable: knowing the technical approaches that threat actors utilize, you can guard against them.

> "The DBIR points out that privilege abuse and data mishandling are common trends as factors contributing to incidents and breaches over the last 3 years."
>
> **SONNY COVINGTON, DIA, CISSP, CCSK**
> **COMFORTE AG**

## THE REPORT OBSERVES THAT CREDENTIALS ARE THE "GLAZED DONUT" OF DATA TYPES

## Secure Your Growth

comforte

www.comforte.com

You can download the Verizon 2021
Data Breach Investigations Report at:

www.verizon.com/dbir