Lance Spitzner

2021 Verizon Data Breach Incident Report Insights

This year's key finding is loud and clear, the human element is by far the largest risk.

June 17, 2021

Once a year every year, the Verizon Security team releases what is known as the Verizon Data Breach Incident Report , also known as the VZ DBIR. This annual report is known and respected as one of the world's best data driven reports on incidents and breaches at a global level. What I love about this report is

- It's truly vendor neutral, there is no product or service to promote.
- It's truly global, the Verizon team collects data on thousands of incidents from around the world (29,207 for this year to be exact).
- They then use this data to better understand the most common drivers for breaches and incidents today and share their analysis. As their data set is global they look at both technical and human risk.
- They are very transparent on both the sources of their data and the processes they used to analyze the data, clearly pointing out areas of uncertainty.

There are several special things about this year's report. The first is I had the opportunity to interview two of the authors behind the report, Alex Pinto and Gabriel Bassett. Alex and Gabriel were kind enough to help us better understand their thought process and findings. Second, we are very excited to announce that both of them will also be speaking at the SANS Security Awareness Summit this 5/6 August, further discussing the topic of human risk.

For 2021 one key finding is loud and clear; the human element is by far the largest risk. In fact, the report clearly calls out that human interaction was involved in over 85% of breaches. By human interaction the report means breaches that involved actions such phishing attacks, cyber attackers using easily guessed passwords, human error, intentional misuse of privileges, or even bad decisions leading to malware infections.

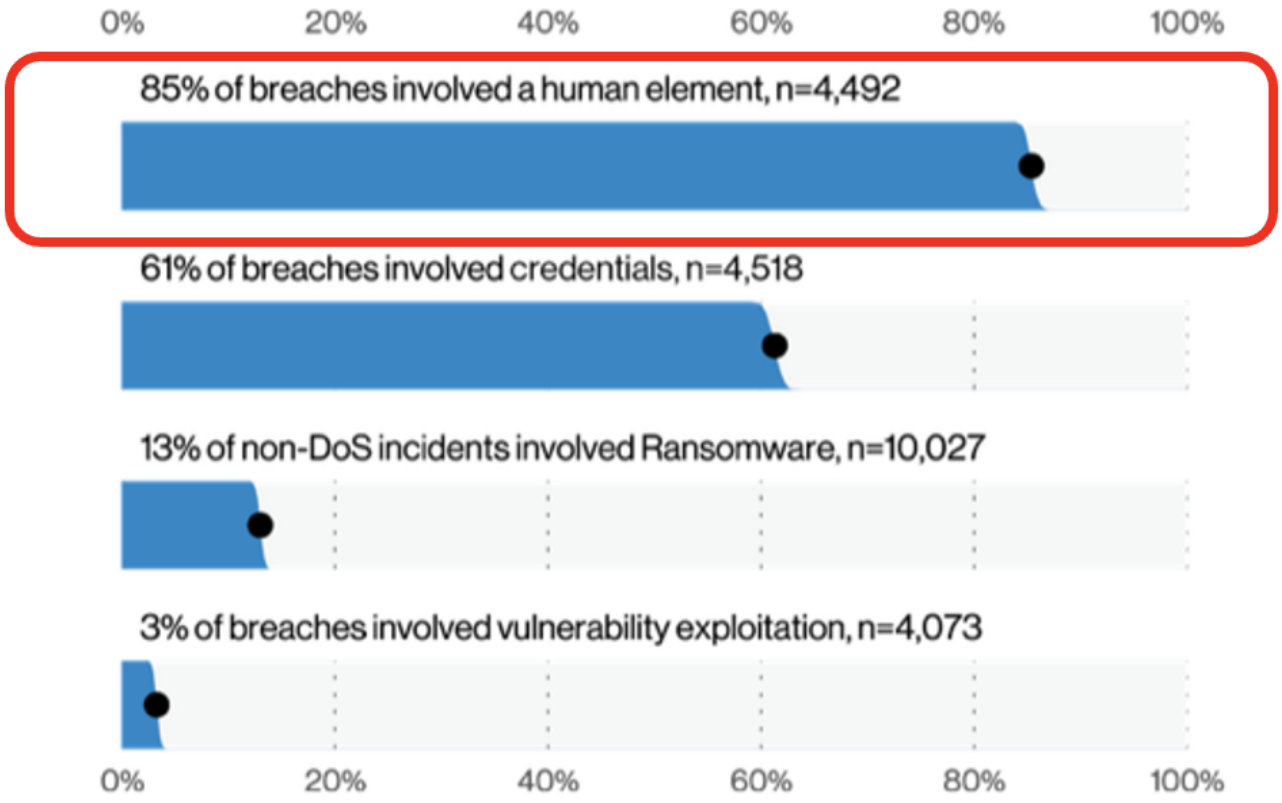

Figure 7. Select action varieties (n=4,073)

In addition, human risk has become such a common element in incidents and breaches at a global level that after fourteen years the VZ DBIR had to change how they structure their report to include changing their infamous “Patterns” to include “Social Engineering” (p. 31 of the report). As security awareness professionals, there are two key ways you can leverage this data-driven report.

1. **Prioritize**: Use the report to better understand the different elements of, and drivers for human risk, prioritize your top human risks and then focus your awareness program on just those top risks. As a result, you can be far more effective in how you manage your human risk.
2. **Support**: Use this report to demonstrate to leadership just how important human risk has become and the key role awareness plays in managing that risk.

Here are the key points I took away from the report.

- **Human is the Top Risk (p. 07)**: Human interaction was involved in 85% of breaches. If your organization is taking a purely technical approach to your security program, you are crippling your ability to effectively manage your organization's risk. To quote Gabe Bassett, "*Your job is not to secure your computers but your organization. And if you're not securing your people, you're not securing your organization*."
- **Top Two (p. 15)**: For the third year in a row, the top two risks are phishing and passwords. If you don't know what to focus on in your awareness program or if you don't know how to best manage your human risk, start with phishing and passwords. If these are not a key part of your awareness program, you should have a good reason as to why.
- **Error (p. 43)**: Far too often we focus on just deliberate threat actors such as Cyber Criminals or Nation State, yet human error represents almost 20% of breaches, good people trying to do the right thing. The two most common examples of error are misconfiguring Cloud accounts resulting in your data accidentally being shared with the world and causing email delivery being sent to the wrong person (for example, due to auto-complete). Far too often security teams feel accidental is not their responsibility, even when it represents as many breaches as System Intrusions. Make sure you have someone responsible for, and a program to address human error.
- **Top Control (p. 64)**: With so much data, the VZ DBIR can identify key drivers of incidents and breaches at the industry level, this year they do this for eleven different industries. Based on the data for each industry they also recommended the top three Center for Internet Security controls that can most effectively manage each industry's overall risk. Security Awareness and Training was the only control recommended for all eleven industries.

There is a huge wealth of knowledge in the report that we have not even touched on. For example, to include data on SMBs (Small-to-Medium Businesses), data based on Region and in-depth descriptions of their approach and methods used for data analysis. I highly recommend this report for any organization attempting to manage their cyber risk, for me it's the gold standard for actionable reports.

To learn more about SANS Security Awareness' product offerings and free resources visit us here!

Tags: Security Awareness