Just like cybercrime, our 2010 Data Breach Investigation Report continues to evolve

As the Greek philosopher Heraclitus noted, “The only constant is change.” Today, that constant change is technology. Advancements in technology continue to improve the way things get done—including cybercrime. Modern-day criminals conduct sophisticated attack campaigns involving technical and social methods to gain trust, obtain access, and exploit valuable data. While it’s important to keep up with changing security tactics, it’s also important to remember the basics.

For example, a large e-commerce retailer suspected a breach when, in just two days, they found over 600,000 failed attempts to authenticate access to their online shopping cart. On try number 600,003, it worked. Through brute force and persistence, the attacker found the correct combination and nabbed 50,000+ credit card numbers, usernames, passwords, and other personal information. The application’s settings showed they allowed unlimited authentication attempts and the system’s log clearly showed the failed password attempts in alphanumeric order.

Our investigations into data breaches prove that while some things change, many remain the same, including cybercrime tactics like brute force. The release of our 2010 Data Breach Investigations Report marks our third report in a series that spans six years, 900+ breaches, and over 900 million compromised records. The report is a compilation of verified cases of data breaches, along with our analysis. It highlights trends showing who is involved, what they are after, and how they breached the data.

What makes this year’s report different is our collaboration with the United States Secret Service (USSS), and the addition of their data in our compiled findings. By using our VERIS (Verizon Enterprise Risk and Information Sharing) framework to capture and share key details of a data breach, we were able to integrate the two data sets for analysis.

USSS data provides new insights

The inclusion of the USSS data has changed the statistics we’re seeing in this year’s report. While organized crime has been and continues to be a leading factor in stolen data, the number of insider cases from the USSS data has given us new visibility to internal crime. Furthermore, cases involving bank account data rose significantly due to the addition of USSS cases involving insider misuse at financial institutions.

Although still the most commonly breached type, payment card data dropped from 81% of cases to 54% in 2009. Both Verizon and the USSS showed a similar result, within a few percentage points. Criminals place a high value on payment cards because they are an easy form of data to convert to cash. Personal information and bank account data were the second and third-most compromised data types. Like payment cards, both are useful to the criminal for committing fraud.

The staggering cost of a breach

The cost of a breach goes well beyond the initial value of the lost data. Because they involve more records per incident, external breaches have more impact than those committed internally. In fact, our study shows criminals outside the victim organization stole 98% of the actual data. Although insider breaches accounted for 48% of the cases, they involved only a small fraction of the data.

While cyber criminals do great damage by directly breaking into financial data streams and stealing data, there are additional and often greater costs associated with a breach. Additional costs could include potential legal expenses, compliance fines, and additional capital costs to upgrade technology. But perhaps the greatest costs could come as a result of damage to the brand. It can take many years to build a well-respected brand and a data breach can destroy it in a matter of days. With brand credibility damaged, current and future customers may steer clear of an organization that's had a data breach, resulting in lost revenue.

Preventing the preventable

In this third report, we continue to see a high percentage of preventable breaches. Considering the wealth of expertise and technology available today, we expected these numbers to continually decline. Such is not the case, however. Evidence of preventable breaches can be seen in the following statistics:

- 85% of attacks were not considered highly difficult
- 96% of breaches were avoidable through simple or intermediate controls
- 87% of victims had evidence of the breach in their log files
- 79% of victims subject to Payment Card Industry requirements had not achieved compliance

One of the first steps in better securing data is to identify where data exists. While this may seem obvious to some, we have found that many organizations don't always know where their data resides. IT and security managers may not have an up-to-date understanding of existing network connections, data, systems, and user privileges.

For example, we have found servers that organizations were not aware of or thought had been retired. These servers often contained data and were still connected to the network. Performing a discovery exercise can bring the understanding of an organizations data and connections current, and identify potential risk areas that are relatively easy to correct.

In the world of cybercrime, knowledge is power

Our intention with the 2010 Data Breach Investigation Report is to expand knowledge and awareness of who the attackers are, how they're getting in, and the assets they're targeting. Also, ongoing analyses of our global network activities offer additional insights. We feel strongly that it's important to share discoveries in order to stay one step ahead of criminals.

Finally, the breaches included in the 2010 Data Breach Investigations Report are not reflective of the risks in every business or industry. Ultimately, you need to decide which findings are most applicable to your organization. Get started now by downloading the full 2010 Data Breach Investigation Report at [URL].

Contact your Verizon Business account manager to learn more about how you can help ensure your organization is fully protected against the changing tactics of cybercrime.