The Godfathers of Cybercrime: The 2022 Verizon Report

by Sharon D. Nelson, Esq., John W. Simek and Michael C. Maschke

Roughly Four in Five Breaches Emanate from Organized Crime

Granted, the three authors of this article are geeks. And yes, we get excited every year when Verizon releases its annual data breach investigation report (DBIR). The Verizon 2022 Data Breach Investigation Report, like all of its predecessors, is chock full of reliable information that law firms need to know.

One of the stunning revelations this year is that roughly four in five breaches arise from organized crime. The quaint notion of disheveled individuals sitting in a chair, drinking endless caffeine-laden beverages and eating lots of pizza while hacking away has given way to criminal cartels, which operate much as the American mobsters once did, right down to godfathers who make people an offer they can't refuse.

Many of the cartels, unsurprisingly, are in Russia, where their activities are tolerated and perhaps encouraged by the government. Just like the Mafia bosses, there is often some level of cooperation between the gangs – attacks and data leaks are coordinated, and they may share intelligence and even infrastructure.

By pooling their information about evading security software and dodging law enforcement, they increase their power and their ability to conduct successful attacks. Our government, at long last, is laser-focused on these cartels and sharing information with foreign governments, offering bounties for information about the gangs, upping its ability to trace cryptocurrency transactions and establishing new sanctions as well as imposing mandatory requirements on some entities to report data breaches.

New Data on Breaches – and the Human Element

The Verizon DBIR is now in its 15th year and was based on 23,896 security incidents. 5,212 of those incidents were confirmed intrusions. It will take you a while to get through the 107-page report, but this article may suffice in giving you the highlights.

A tiny slice of good news: Last year, there was a human element involved in data breaches 85% of the time. That percentage has dropped to 82% this year. Not much comfort there, even if the numbers are headed in the right direction.

What are humans doing? They are falling for social engineering attacks, clicking where they shouldn't click, opening documents they shouldn't open and trying to evade the restrictions imposed by their cybersecurity policies and technologies. They use weak passwords (if allowed). They share passwords and reuse passwords. They let their browsers remember their passwords. They resist any implementation of multi-factor authentication.

Notably, humans misconfigure cloud storage. Typically, a cloud breach is not the cloud's fault – a user configures things incorrectly and thereby issues an engraved invitation to the hacker world.

The list of human mistakes is truly endless. This is one reason why security awareness training is so vital – particularly for law firms, who hold the confidential data of many people and entities.

Insiders or Outsiders?

As the report notes, it is common to see stories about the prevalence of insider attacks. However, the statistics don't bear out that prevalence. Nearly three out of four cases exhibited evidence of the attack coming from an outside source. Internal sources accounted for only 18% of incidents.

While we find that statistic creditable, we note (as the report itself does) that insiders are sometimes very adept at keeping their malicious activity hidden!

Ransomware Stats

Law firms, like all other entities, have been targeted by ransomware gangs. Ransomware made up 25% of security incidents between November 1, 2020 and October 31, 2021 and was used in 70% of all malware infections.

How do they get through our defenses? They steal credentials or buy them on the dark web. They use phishing attacks and they exploit vulnerabilities.

Seventy five percent of ransomware incidents involved an intrusion exploiting desktop-sharing software (40%) or email (35%).

Perhaps the most dire warning emanates from the fact that ransomware attacks increased 13% year over year. That represents a larger increase than the previous five years combined. And still the hits keep coming.

Though law firms have heightened their defenses, the ransomware gangs have gotten smarter too, so we play an endless cat and mouse game, in which the mouse often, but not always, evades the cat.

Money Makes the World Go Round

Money makes the world go round as the song from "Cabaret" points out. So it is unsurprising that the report found that the motive in 89% of breaches was financial and 11% was espionage, perhaps a tribute to our troubled times. National-state affiliated cyber attacks continue to increase in sophistication.

While we are following a "Shields Up!" defense strategy as a country, we were late to the game – hopefully not so late that we cannot catch up. And as we remind lawyers all the time, law firms are a "one stop shop" for cybercriminals because they hold the data of so many entities.

We are encouraged by the strength shown recently by our government in its war against ransomware and other cybercrimes. It may take us some time to develop cyber defenses that result in unseating the godfathers of cybercrime. But that's ok. We have it on good authority that "revenge is a dish best served cold."

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA.* *snelson@senseient.com*

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm.* *jsimek@senseient.com.*

Michael C. Maschke *is the CEO/Director of Cybersecurity and Digital Forensics of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional.* *mmaschke@senseient.com.*