The Experts

If Companies Are More Prepared, Why Are Breaches Still Rising?

ORGANIZATIONS are spending more money than ever on cybersecurity—an estimated $188 billion globally in 2023, a figure expected to grow to almost $215 billion this year—yet hackers always seem to stay a step ahead.

The number of reported data breaches in the U.S. rose to a record 3,205 in 2023, up 78% from 2022, according to the Identity Theft Resource Center. Trends are similar in other parts of the world.

What can explain these two seemingly contradictory statistics? If awareness of and spending on cybersecurity is growing, why do data thieves remain undeterred?

Based on our research, three things are helping to drive the current increases:

- **Evolving ransomware attacks:** In traditional ransomware attacks, which I call Ransomware 1.0, hackers break into a computer system, "lock up" data by scrambling it and demand a ransom payment in return for the decryption key. To resume business, companies typically have a choice: Pay the ransom or try to re-create the frozen data. In these attacks, data isn't stolen, so there is no data breach to report.

But ransomware attacks are evolving in two key ways.

First, after a slight drop, these kinds of attacks are on the rise again due to the emergence of ransomware gangs that franchise their malware and make it available to budding cybercriminals. This trend is allowing more criminals, even those with minimal computer knowledge, to get into the ransomware game.

Second, these attacks are becoming more damaging in that many attackers are now stealing their victims' data, in addition to just locking it up. I refer to this new approach as Ransomware 2.0. The hackers threaten to disclose the private information if they don't receive a ransom payment. This results in large leaks of corporate and consumer data that didn't occur before.

- **Cloud misconfiguration:** More companies now store and maintain their corporate data in the cloud via services such as Amazon Web Services, Google Cloud and Microsoft Azure to avoid the expense of having to own and operate their own data centers. This is making the cloud an attractive target for hackers. In fact, 82% of breaches in 2023 involved data stored in the cloud, according to a recent IBM report.

Cybercriminals are taking advantage of the fact that many organizations migrated rapidly to the cloud without fully understanding all of the configuration settings and establishing procedures to keep their data safe. As a result, errors and glitches in these settings are common, and many firms have no idea that their sensitive data is exposed to the public internet until it is too late. Such misconfigurations have become one of the most common security issues when deploying new cloud-based applications.

- **Exploitation of vendor systems:** Almost every company, especially large companies, rely on a network of vendors to provide services ranging from maintaining the air conditioning to updating software packages. These vendors often have special access to the company's computers, which I refer to as "side doors," similar to a passkey given to the cleaning crew.

As large companies have become better prepared to repel cyberattacks, hackers have shifted their focus to vendors, often much smaller companies with limited cyber-defense resources and expertise. Attackers exploit those weaknesses to first get into the vendor's system, then use the vendor's privileged access to get into the computer systems of every company that uses the vendor.

A vulnerability in a single vendor system can threaten thousands of organizations. Security experts say more than 2,600 organizations were victims of the recent MoveIt attack, in which hackers exploited a vulnerability in a common file-transfer tool to gain access to personal data. Research by cybersecurity-ratings provider SecurityScorecard, meanwhile, found that 98% of organizations globally have a relationship with a vendor affected by a data breach in recent years.

Many firms fall victim to these attacks because they aren't aware of the risks they are taking, such as not confirming the quality of a vendor's security or monitoring whether their outgoing data traffic is being transferred to improper destinations. Companies can, and must, do these things better to stop the rise in data breaches.

*—**Stuart Madnick** is the John Norris Maguire Professor of Information Technologies at the MIT Sloan School of Management and the founding director of the Cybersecurity at MIT Sloan (CAMS) research consortium. Email him at **reports@wsj.com**.*

*The Experts are industry and thought leaders who write about topics of their expertise. Read more posts at **WSJ.com/Experts**.*