Harvard Business Review

Risk Management

Why Data Breaches Spiked in 2023

by Stuart Madnick

February 19, 2024

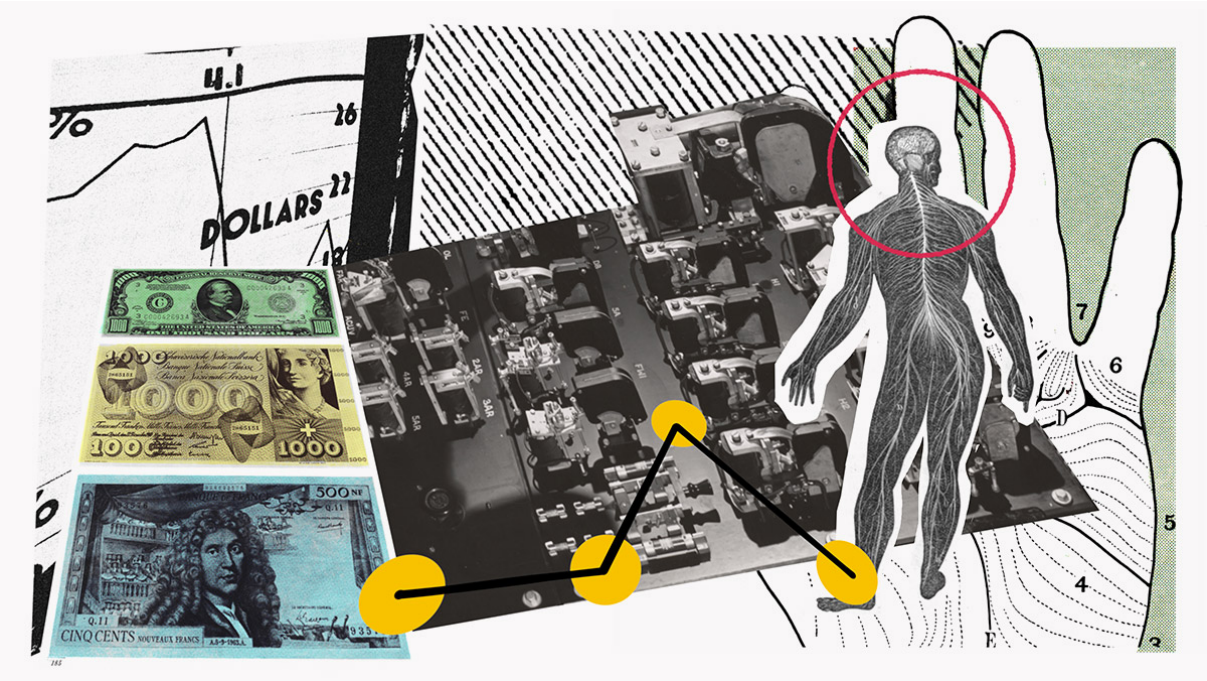

Illustration by Aaron Marin

Summary. In spite of recent efforts to beef up cybersecurity, data breaches — in which hackers steal personal data — continue to increase year-on-year: there was a 20% increase in data breaches from 2022 to 2023. There are three primary reasons behind this increased theft of personal data: (1) cloud misconfiguration, (2)

new types of ransomware attacks, and (3) increased exploitation of vendor systems. Fortunately, there are ways to reduce the impact of each of these factors.

close

For many years, organizations have struggled to protect themselves from cyberattacks: companies, universities, and government agencies have expended enormous amounts of resources to secure themselves. But in spite of those efforts, data breaches — in which hackers steal personal data — continue to increase year-on-year: there was a 20% increase in data breaches from 2022 to 2023. Some of the trends around this uptick are disturbing. For example, globally, there were twice the number of victims in 2023 compared to 2022, and in the Middle East, ransomware gang activity increased by 77% in that same timeframe.

Why has this cyber damage continued and expanded despite all our efforts? And what can we do? Based on what we have learned in my research group, there are three primary reasons behind this increased theft of personal data: (1) cloud misconfiguration, (2) new types of ransomware attacks, and (3) increased exploitation of vendor systems. Fortunately, there are ways to reduce the impact of each of these factors.

Cloud Misconfiguration

There are many benefits to companies for using cloud storage, as offered by Amazon, Google, Microsoft, and others: cost-efficiency, security, easy data sharing, synchronization, convenience, scalability, and disaster recovery, to name just a few. Understandably, companies put more and more of their data in the cloud. It is estimated that more than 60% of the world's corporate data is stored in the cloud.

That makes the cloud a very attractive target for hackers. In 2023, over 80% of data breaches involved data stored in the cloud. That is not just because the cloud is an attractive target. In many cases, it is also an easy target due of cloud misconfiguration – that is, companies unintentionally misuse the cloud, such as allowing excessively permissive cloud access, having unrestricted ports, and use unsecured backups. According to the NSA "cloud misconfigurations are the most prevalent cloud vulnerability" and can be exploited by hackers to access cloud data and services.

Why do people make such mistakes?

This is caused by several interrelated reasons: many companies have only recently moved to the cloud, so they do not have many years of experience; to address customer demands and competition, cloud providers continual increase their features and which correspondingly increase their complexity; furthermore, there is a desire to make the cloud easy to use, so the cloud providers have many settings being set by default. As a result, users might not realize what all the settings are and whether some, or all, of their data storage is being openly exposed to the public internet.

What can be done.

There is a lot of truth to the old saying: "Haste makes waste." In the drive to swiftly transition to the cloud and release new applications, many shortcuts are often taken by companies and not enough time is spent confirming that the cloud configuration is set correctly. The headlines frequently read, "This should not have happened." Take the time needed to carefully verify that cloud storage is being correctly used.

New Types of Ransomware Attacks

Almost everyone has heard of ransomware attacks. That is when hackers get onto your computer and "lock up" your data by cryptographically encoding it and requiring you to pay a ransom in order to get the decryption key needed to free up your data. In this type of ransomware attack, the data is not actually extracted – it remains on your computer, you are just not able to use it. As companies have been getting better at maintaining and using backups so that they could retrieve usable data without having the pay a ransom, it looked like ransomware would be reduced as a threat, in fact, there was a slight reduction in 2022. But the reality is that ransomware attacks have again increased and become more dangerous.

They are more dangerous because, to counter the possibility that a victim will refuse to pay the ransom because the data can be retrieved from backup files, the attackers make a copy of the data before encrypting in on the victim's computers. They then make an additional threat, pay the ransom or we will start to publicly disclose your private data, essentially using both *blackmail* and *kidnapping!* In this type of ransomware attack, there is an actual data breach, in fact, much more likely that massive amounts of data could be publicly disclosed!

Furthermore, the number of ransomware attacks has increased due to emergence of ransomware gangs and "ransomware-as-a-service." Essentially, the initial ransomware developers franchise their malware to make it easier and economically very attractive for other criminals to initiate ransomware attacks. In our research, we have seen many different types of franchise arrangements from the simple purchase of the ransomware malware, to monthly rental fees, to splitting the spoils.

Why do people make such mistakes?

Both of these failings are mostly caused by a certain amount of naivety or unawareness on the part of users. There is often an assumption that the protection methods they are using, such as firewalls, multi-factor identification, and such, will keep attackers out, so stealing data is not a concern. Likewise, it may seem simpler to process unencrypted data, so why complicate things by encrypting it.

What can be done.

Being diligent and effective in backing up all data and being fast and efficient in restoring the data is still important to address traditional ransomware attacks. To address the added risk of your private data being publicly exposed, you need to prevent the attacker from extracting the data from your system, usually called *exfiltration*, and then being able to expose that data.

In the first case, data transfers to sites outside of your systems must be monitored and illicit transfer must be promptly stopped. Sadly, this is frequently not done. In the second case, the data on your computers should only be stored in encrypted format, so that only you can read it. So, even if the attacker is able to exfiltrate your data, it cannot be read the data or blackmail you to prevent its disclosure.

Exploitation of Vendor Systems

Most companies have increased the cyber protection of their “front doors” through measures such as firewalls, stronger passwords, multi-factor identification, and such. So, attackers seek other — and sometimes more dangerous — ways to get it. Often, that means coming in via vendors’ systems.

Most companies rely on vendors to assist them, from doing air conditioning maintenance to providing software, including automatic updates to the software. In order to provide those services, these vendors need easy access to your company's systems — I refer to these as the "side doors." But, these vendors are frequently small companies with limited cybersecurity resources. Attackers exploit vulnerabilities in these vendor systems. Once they have some control over these vendor systems, they can use the side door to get into the systems of their customers.

These are often called "supply chain attacks." In fact, it is not just one customer that can be attacked, but essentially every customer that uses that vendor's services. Thus, a single vulnerability can threaten many thousands of organizations, such as in the 2023 MOVEit attack where already over 2,600 companies in more than 30 countries have admitted being attacked with more than 80 million individuals whose data has been compromised. In fact, 98% of organizations have a relationship with a vendor that experienced a data breach within the last two years. In some studies, the number of data compromises due to supply chain attacks in 2023 jumped 78% over 2022.

Why do people make such mistakes?

It is not surprising that people tend to trust their trusted vendors, such as giving a key to your home or office to the cleaning team. It usually does not occur to you that the key might be stolen from that vendor.

What can be done.

It is important that every company become more aware of the possibility of a supply chain attack. Of course, your company cannot completely control the systems and operations of other companies, but there are things that can be done.

First, understand the risk posed in engaging a vendor, by doing your own assessment of their cybersecurity effectiveness and/or make use of services, such as Bitsight or SecurityScorecard, that provide “cyber security credit scores” to evaluate the security of an organization before doing business with them.

Second, limit the scope of each vendor’s side door. For example, an air conditioning maintenance company should only need access to the areas where the equipment to be maintained is stored, not access to every office in the building.

Finally, as mentioned above regarding data exfiltration, limit what data vendors have access to, keep that data encrypted to make it useless, even if exfiltrated, and monitor data being exported from your systems to detection illicit exfiltrations.

• • •

Cyberattackers are remarkably resourceful, inventive, and creative. They will come up with new ways to attack your systems in the coming years. Many of the principles highlighted to address this wave of attacks will be helpful in addressing the new ones. In any case, stay alert and be prepared.

Stuart Madnick is the John Norris Maguire (1960) Professor of Information Technologies in the MIT Sloan School of Management, Professor of Engineering Systems in the MIT School of Engineering, and Director of Cybersecurity at MIT Sloan (CAMS): the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity. He has been active in the cybersecurity field since co-authoring the book *Computer Security* in 1979.

Recommended For You

Nudging Employees to Make More Sustainable Choices

What Does Banning Short-Term Rentals Really Accomplish?

The Future of Marketing Is Intergenerational

PODCAST
Apple's Dilemma: Balancing Privacy and Safety Responsibilities