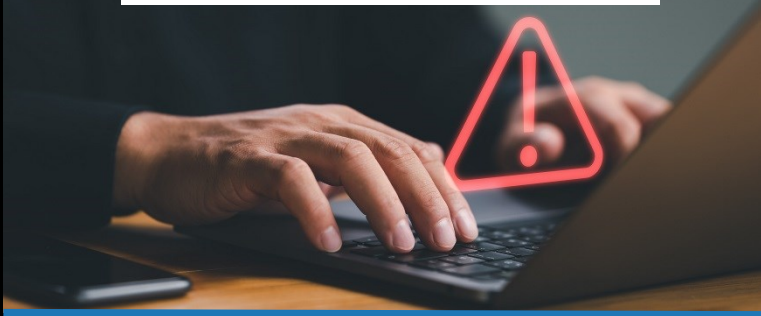


## This Year's Biggest DATA BREACHES



According to *TechCrunch*, this year has seen some of the most damaging data breaches in history. In 2024 alone, hackers stole billions of personal records, and it's almost guaranteed your data is among those stolen records. Let's look at this year's record-breaking attacks and what you need to know about protecting your information.



### National Public Data (2 Billion-Plus Records)

**What happened:** In December 2023, hackers accessed the systems of National Public Data, a background-check company. In April, 2.7 billion records with highly sensitive data for 170 million people were leaked onto the dark web.

**Who is exposed:** The stolen data includes records for people in the US, Canada and the UK.

**Compromised data:** 2 billion-plus records containing full names, current and past addresses, Social Security numbers, dates of birth and phone numbers.



### Change Healthcare (38 Million Records)

**What happened:** In February, the UnitedHealth-owned tech firm Change Healthcare was hacked by a Russian ransomware gang that gained access through systems unprotected by multifactor authentication. The attack caused widespread downtime for health care institutions across the US and compromised data for many, *many* Americans. UnitedHealth paid \$22 million to prevent data leaks, but another hacker group claimed to still have some of the stolen Change Healthcare data.

**Who is exposed:** Estimated data exposure for one-third of the American population (likely more).

**Compromised data:** Payment information, Social Security numbers and medical data, including test results, diagnoses and images.

*Continued on pg.2*



December 2024



HAPPY  
*Holidays*

From our team to yours,  
may this season bring you  
happiness and a bright  
start to the new year!



This monthly publication provided courtesy of  
David Luft, CEO of LDD Consulting, Inc.

#### **Our Mission:**

*We promise to provide knowledgeable, courteous and prompt service. We care as much about your business as you do. If you are not completely satisfied, be sure to let us know. If we cannot resolve the issue, we will refund your money.*

... continued from cover



### AT&T (Hacked TWICE)

**What happened:** In March, hackers released data for more than 73 million past and existing AT&T customers going back to 2019. Then, in July, data was stolen from an AT&T account the company had with data giant Snowflake (more on that below). Reportedly, AT&T paid a ransom to the hackers to delete the data. However, if this data is leaked, it could expose the data of anyone called by AT&T customers, including noncustomers.

**Who is exposed:** 110 million-plus past and current customers and, potentially, noncustomers.

**Compromised data:** Personal information, including Social Security numbers and phone numbers.

**Compromised data:** 300 million patient interactions, including blood test results for HIV and cancer, going back many years.



### Snowflake (600 Million+ Records & Growing)

**What happened:** In May, cloud data giant Snowflake announced a system breach caused by stolen employee credentials. Hundreds of millions of customer records were stolen from Snowflake customers, including 560 million from Ticketmaster, 79 million from Advance Auto Parts and 30 million from TEG.

**Who is exposed:** Millions of customers from many of Snowflake's 165 corporate customers, including those mentioned above, plus Neiman Marcus, Santander Bank, Los Angeles Unified School District and many more.

**Compromised data:** Customer records.



### Synnovis (300 Million Patient Interactions)

**What happened:** In June, a UK pathology lab, Synnovis, was attacked by a Russian ransomware gang. The attack resulted in widespread outages in health institutions across London. Reportedly, Synnovis refused to pay the \$50 million ransom.

**Who is exposed:** Past and existing patients in the UK.

## How To Protect Yourself

You can't stop companies from getting hacked. However, you can prevent the situation from worsening for YOU by taking a few extra steps to protect your data. Here's what to do:

- ✓ **Review your health-related communications:** With so many breaches affecting health institutions this year, pay attention to your statement of benefits and look for services you didn't receive. If you spot something fishy, tell your health care provider and insurance company right away.
- ✓ **Freeze your credit:** This will stop criminals from opening a credit card or loan in your name.
- ✓ **Update your log-in credentials:** If you know what accounts were hacked, change your credential, and also change the credentials to major accounts like your bank. Set up alerts too, so you're immediately aware of any unusual activity.
- ✓ **Be wary of e-mails:** After a breach, hackers access all kinds of information and may use that to send fraudulent e-mails. Slow down, read carefully and verify requests before taking any action.

### Free Cybersecurity Risk Assessment Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now



At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cybersecurity risk assessment to uncover loopholes in your company's IT security.

After the assessment is done, we'll prepare a customized Report Of Findings that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed. This report and action plan should be a real eyeopener for you, since most of the businesses we've assessed discover they have some exposures to various threats in a number of areas.

To Claim Your Free Cybersecurity Risk Assessment Now, Visit  
[www.iddconsulting.com/cyberaudit](http://www.iddconsulting.com/cyberaudit)

## HERE LIES WINDOWS 10...



GONE TO THE GREAT TECH BEYOND

UPGRADE NOW  
SUPPORT ENDS  
OCTOBER 2025

# PASSION ISN'T ENOUGH

## Tim Grover Explains Why Obsession is Key to Success



Passion is the key to success – that's what many of us have been taught to believe. If you want to be great, you must be passionate. However, Tim Grover believes we've been told wrong.

Tim Grover is a renowned speaker, author and performance coach with over 20 years of experience speaking to businesses, entrepreneurs and leadership teams aiming to be the top in their fields. Known for his work with athletes like Michael Jordan, Kobe Bryant and Dwyane Wade, Grover teaches audiences the mindset of elite professionals so they can apply it to their own success. At a recent industry conference, Grover shared his secret to success: It's not passion that equates to success. It's obsession.

### Be Obsessed

Grover draws a clear line between being interested in something and being obsessed with it. "Interest is passive," he explains. If you want to take your business to the next level, you must be all in because when you're obsessed, you pay attention to every tiny detail. As a performance coach, Grover read every injury report for his athletes so he knew how to lace their shoes. He watched hours of video footage and knew every step and landing so he could design training plans. "That's obsession," he says. "That's why they kept me around for such a long time."

### Act On Your Passions

"You don't follow your passion," Grover explains. "You act on it. You excel at it." In business, hesitation can lead to missed

opportunities. Once a decision is made, you must fully commit to it because excellence is a long game. There will be moments of pressure driving you beyond your comfort zone and moments that feel very isolating. "Excellence creates distance. It creates distance between you, your friends, your enemies, your family, your free time," Grover says. This isolation isn't necessarily negative; it's a byproduct of striving for greatness. It will separate you from everyone who is average – from people who don't understand the behind-the-scenes work it takes to truly succeed in your passion. People will try to pull you down, either out of jealousy or a lack of understanding, but excellence requires a singular focus that many won't understand.

### Balance Is A Myth

People often say that successful people need balance. Grover argues that if you try to balance everything – work, life, relationships – while striving for success, you'll be mediocre at all of them. You'll never grow if you're pulled in too many directions. The key to success is ditching balance, focusing on fewer, more important priorities and cutting out distractions. "Everyone has time for what they put first," he explains.

Excellence is a long-term journey that demands obsession, action and a refusal to settle for mediocrity. "Write your own story," Grover says. Put down the self-help books and "look deep down inside yourself and stop looking for everybody else to get you to that next level."

## Client Spotlight

### Affordable, Reliable IT Support for Schools

As a public charter school, staying within budget is essential, yet we need robust IT security for students and staff. David Luft and his team at LDD deliver excellent service at fair prices. They handle all our equipment needs, ensuring it stays current with industry standards. Their recommendations are always spot-on, so we never have to worry. If your business needs reliable IT support within budget, I highly recommend LDD.



*Jackie Danfelser*  
Financial Assistant  
Public Academy for Performing Arts  
Albuquerque

## BEWARE OF WIFI SQUATTING

When did you last check who has access to your Wi-Fi network? If it's been a while, you'll probably be surprised by who's hanging around. Managing your Wi-Fi access is an important step to keeping your data safe because unwanted Wi-Fi squatters could, at best, slow your Wi-Fi speeds and, at worst, have access to any device or file connected to your network, like household security cameras. To see who has access to your Wi-Fi, find your router's IP address (you can find instructions online about how to do this), type the IP address into your browser and log in. Next, look for a list called "DHCP Client" or "Connected Devices." Review the list, and if any unknown devices are on it, update your Wi-Fi password and reconnect only the devices you trust.





**Making Technology Work for You**  
 2420 Midtown PL NE, Suite K  
 Albuquerque, NM 87107

PRST STD  
 US POSTAGE  
 PAID  
 ABQ, NM  
 PERMIT 1187

Return Service  
 Requested

## Inside This Issue



«Name»  
 «Company Name»  
 «Street Address 1» «Street Address 2»  
 «City», «State» «Postal Code»

Year in Review: Are You In It? | 1

Michael Jordan’s Trainer Reveals Why Passion Isn’t  
 Enough for Success | 3



# ARE YOU MANAGING VENDOR RISKS?

As the year winds down, innovative businesses often reflect on what’s gone right – and what needs improvement. Beyond wrapping up projects and planning for next year, one critical task shouldn’t be overlooked: **managing vendor security risks**. Vendors play an essential role in your business’s success, but they also present a severe cybersecurity risk if you don’t vet and monitor them effectively, especially if they handle sensitive data.

## What’s A Vendor Risk?

Many businesses rely on trusted vendors, such as cloud services or file-sharing tools, to carry out day-to-day operations. If that vendor gets hacked, your sensitive data is suddenly – and dangerously – exposed. A perfect example is the 2023 MOVEit Transfer breach, where attackers exploited vulnerabilities in the vendor’s software, giving them access to critical data like customer information and business records for thousands of organizations. BlueVoyant’s *State of Supply Chain Defense*

*report* showed that organizations experienced, on average, 4.2 supply chain breaches in 2023 that impacted operations.

Vendor breaches are more than annoying – they could also lead to data loss, diminished customer loyalty or even legal issues. This year, consider adding these best practices to your end-of-year review to manage your vendor risk:

### 1. Review Vendor Contracts

Like you, vendors need to be held accountable for following industry-standard practices like encryption, secure data storage and incident response protocols. Start your vendor risk review by checking to see if your contracts have the necessary security clauses, and make sure your agreements outline these expectations clearly so you and your vendors know what’s at stake.

### 2. Conduct Vendor Security Audits

If you haven’t done it recently, it’s time for a thorough security audit of your high-risk vendors. This will help you understand if

they’re implementing strong cybersecurity measures, such as multifactor authentication, encryption and regular system updates. Knowing where your vendors stand gives you a better handle on your own security.

### 3. Monitor For Emerging Risks

Cyberthreats evolve quickly and so do the risks your vendors face. Regular monitoring of your vendor’s security practices, like tracking vulnerabilities or breaches, will keep you on top of any emerging threats.

### 4. Update Your Vendor List

Now is a good time to clean house. Cut ties with vendors who aren’t living up to your security standards and tighten your relationship with those who are proactive about protecting your data. Consider creating standardized onboarding and offboarding processes for vendors to prevent old vendors from having unwarranted access to our organization.

