ATTITUDE IT
Keeping Your Technology On Course

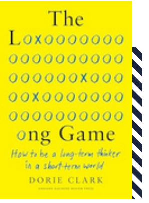
TRIVIA

What does the ZIP in ZIP file mean?

A. Zigzag Insertion Point
B. Zonal Integrated Process
C. Zero Information Packaging
D. Zipped Information Protocol

THE LONG GAME

By Dorie Clark



In a world where instant gratification rules and the pressure to achieve is relentless, Dorie Clark's *The Long Game* is a refreshing call to step back, think strategically and invest in your future self. Clark, a renowned business strategist and Duke University professor, makes a compelling argument for shifting our focus away from tempting short-term wins to more gratifying long-term successes. Clark shares practical frameworks and real-world stories that show how seemingly minor efforts lead to significant achievements if we're patient and persistent. With engaging storytelling and actionable insights, *The Long Game* encourages readers to step back from the daily grind, prioritize what truly matters and invest in their future selves.

Answer: A. ZIP in ZIP file stands for "Zigzag Insertion Point" because it compresses data like a zigzag.

ARE YOU MANAGING YOUR VENDOR SECURITY 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, 4.16 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, too, so old vendors don't have unwarranted access to your organization.

THE
ATTITUDE CHRONICLE
Insider Tips To Make Your Business Run Faster, Easier And More Profitably

WHAT'S NEW

Welcome to The Attitude Chronicle. Each month we focus on tips to help your business run safely, securely and more profitably.

Small businesses are the backbone of our local economy, and it is extremely hard for them to recover from data breaches and other cyber attacks.

Our hope is that YOU never experience the loss of revenue, trust, and reputation that comes with a cyber incident. However, in today's risk climate, there's a higher chance of your organization facing a cyber incident than not.

We want to make sure you are brilliantly prepared.

This monthly publication is provided courtesy of Brandon Jones, CEO of Attitude IT.

OUR MISSION:

We're on a mission to protect 10,000 Ontario businesses from data loss and cyber-attacks.

Yours could be next.

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.

1 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.

2 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.

continued on page 2…

...continued from cover

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.

3 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 in a bit). 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.

4 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.

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

5 Snowflake
(600 Million-Plus Recordings And 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.

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 credentials, 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.

MUST WATCH

HOW HACKERS ARE USING YOUR BUSINESS LIKE THEIR OWN BANK ACCOUNT... AND HOW TO STOP IT

You will learn the top ways criminals use to hack your business network and about some new scams being used today and how to identify malware. What is missing from your security if you have not implemented new procedures in the last 6 months. Learn how zero-trust networking can be applied to your business and what to do beyond MFA to protect your email from phishing attempts. There are some great resources to check-out for your team to check out and share. We have a live event in February details to come soon!

WATCH THE WEBINAR HERE: https://www.youtube.com/watch?v=L3NQ6fo2srk&t=438s

WEBINAR

NMA EXCELLENCE AWARDS

It was a full house tonight at Venture 13 in Cobourg Ontario to recognize and celebrate members of the Northumberland Manufacturers Association.
Congratulations on this year's Excellence Award Recipients:
Health, Safety & Environmental Award: Weir - ESCO Division
Investing in Employee Development: SABIC Corporate
High Performance Manufacturing: Custom Plastics International
Special thanks to our award sponsors: Baker Tilly Canada Resolution Staffing Inc. Cambium
Thank you Executive Chef Brad Murphy for the amazing service and delicious food! So great to see a our Durham partners show up in support of such a great event.

BEWARE OF WIFI SQUATTING

When did you last che s to your WiFi network? I e, you'll probably be surprised s hanging around. Managing your WiFi access is an important step to keeping your data safe because unwanted WiFi squatters could, at best, slow your WiFi 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 WiFi, 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 WiFi password and reconnect only the devices you trust.