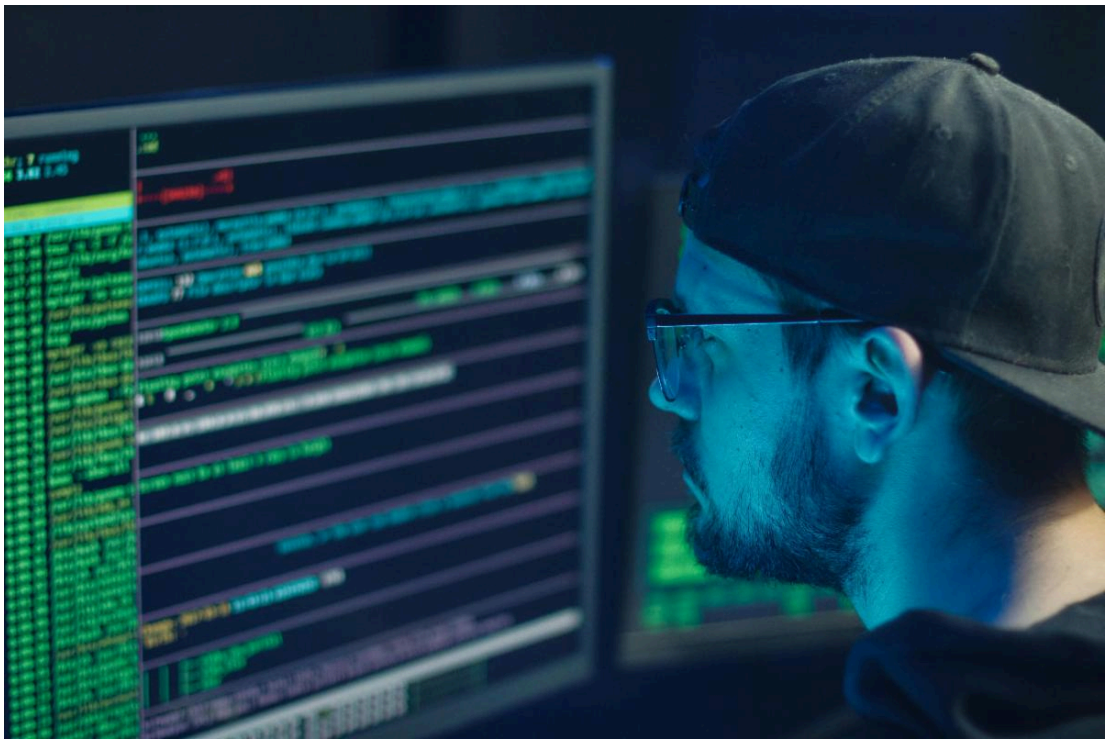
Volume 26 | Issue 6 | April 7, 2026

BCSI Investigations Inc.

The Investigator Newsletter

Data Breaches: Lessons from Recent Hacks



The Domino Effect: Hard Lessons from Recent Data Breaches

About Us

Since 2000, BCSI Investigations Inc. has performed thousands of successful investigations. Our integrated team of investigators and support services ensure that the investigations are conducted promptly with leading-edge techniques.

As we move through 2026, recent reports on major data breaches show a clear and worrying trend: most of the biggest hacks didn't happen because of "unbreakable" technology; they happened because basic security practices were ignored. From the massive leak of 16 billion credentials across major tech platforms to attacks on global logistics firms, the patterns are obvious and repeatable.

Weak Links: The Vendor Problem

One big lesson is that your security is only as strong as your weakest partner. In the past year, hackers often bypassed a company's main defenses by targeting a third-party service or shared software.

The takeaway is simple: don't just trust your vendors—verify them. Companies need to regularly verify that their partners

With over 40 years of combined experience, BCSI Investigations Inc. is the platinum standard for private investigations.

Contact us at 604-922-6572 or visit our website at www.picanada.ca to learn more.

Visit our Website

have strong security measures, because if a vendor is hacked, your data can be exposed too.

Identity Is the New Perimeter

Recent attacks show that it's not networks but identities that are the biggest target. Hackers use clever tricks, like pretending to be employees, to get helpdesk staff to reset security codes, making even strong firewalls useless.

The lesson: adopt Zero Trust. In this system, no one is automatically trusted, even if they're inside the company network. Users are granted access only to what they absolutely need, and their identities are constantly verified.

Backups Aren't Enough

Hackers today often steal data before locking it, using a tactic known as "Double Extortion". This means having backups helps you keep running, but it doesn't stop sensitive information from being stolen and sold online.

The solution: protect the data itself. Encrypt sensitive fields such as Social Security numbers or bank details so that even if hackers steal the files, the information is useless to them.

Be Proactive, Not Reactive

Finally, companies need to act before a hack happens. This includes running simulated attacks to find weaknesses and using AI-powered monitoring to detect suspicious activity quickly, sometimes in minutes rather than months.

The bottom line: security isn't just about stopping hackers at the door - it's about protecting data, monitoring activity, and verifying everyone who has access. Following these lessons can help prevent your company from becoming the next headline.

To stay up to date with scams, listen to Scams 360 wherever you get your podcasts.

Thank you for trusting **BCSI Investigations Inc.** to keep you informed and protected.

STAY CONNECTED

BCSI Investigations | 205-1868 Marine Drive | West Vancouver, BC V7V 1J6 CA