ONE STEP SECURE IT

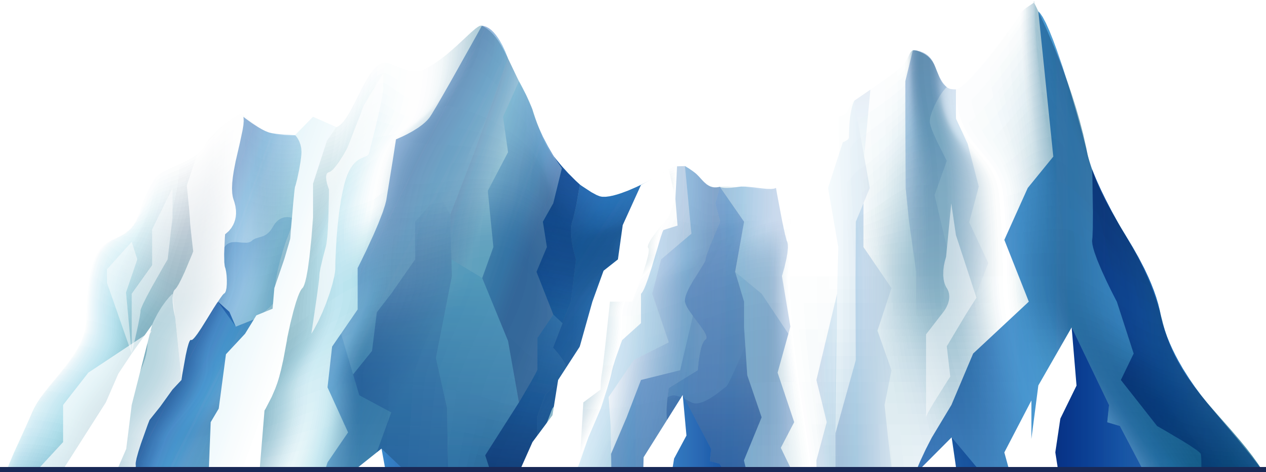
THE LATEST BYTE

The Cybersecurity Iceberg

Unseen Threats That Lie Beneath

Volume 1

2025



When it comes to cyber threats, what you see is just the tip of the iceberg.

Businesses often focus on the visible risks—installing anti-virus software and enforcing password policies—but these are now the bare minimum. Today, sophisticated cyber threats lurk beneath the surface, and cyber criminals work to exploit vulnerabilities.

With the rapid evolution of cyber crime, securing your business requires more than just the basics. To truly protect your organization, you need advanced measures like continuous network monitoring, mobile device management, remote employee safeguards, endpoint detection and response, and regular network maintenance.

The challenge?

Staying ahead of unseen security threats and ensuring your business isn't blindsided by what lies below.

Explore how to safeguard your business from the hidden dangers of the cybersecurity iceberg.

About One Step Secure IT

We are an outsourced IT company with over three decades protecting our customer's data from breaches to alleviate the dread of cyber attacks, costly downtime, and loss of customer trust.

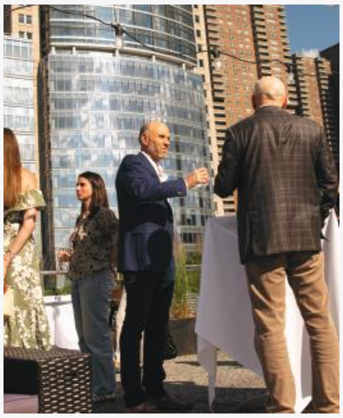
Our expertise includes Cybersecurity, Managed/Co-Managed IT, Information Security, and Compliance Services. We understand that as business operations evolve, so do the security threats. Our expert team collaborates closely with you to create a customized IT strategy, identify vulnerabilities, and strengthen your IT infrastructure.

Our corporate headquarters are in Phoenix, AZ, and we proudly serve businesses nationwide. To learn more about how One Step Secure IT can enhance your technology, visit our website at www.onestepsecureit.com.

2024

A YEAR IN PHOTOS!

This year, the One Step team traveled coast to coast, engaging with business leaders at major industry events across the country. We had the privilege of sharing our IT and cybersecurity expertise, helping organizations strengthen their operations and safeguard against cyber threats. Here's to another year of empowering businesses with the knowledge and tools to stay secure and efficient!



Uncovering the Cybersecurity Iceberg

Protecting Against Visible and Hidden Threats

At the surface, we see visible cybersecurity risks—phishing emails, compromised passwords, and other weak or outdated security measures. But what most people don't realize is that beneath this surface, a massive hidden network of more sophisticated threats lurks. These threats, often undetectable until too late, require action, diligence, and more complex solutions.

Let's take a look at some essential security tactics, starting with basic personal safety tips and progressing to advanced defenses for businesses. Whether you're an individual wanting to enhance your personal security or an executive with a business to safeguard, understanding how to protect against both visible and hidden threats can make all the difference.

Personal Cybersecurity Essentials

When it comes to personal cybersecurity, it's easy to think of passwords and two-factor authentication (MFA) as adequate protection. While these are foundational, today's threats demand more from us. Let's break it down from the basics to more advanced strategies.

Password Security and Multi-Factor Authentication (MFA)

Surface-Level Threats: Password breaches and weak login security are like the tip of the iceberg. Simply put, a compromised password is the most direct path for attackers to access your accounts.

Solution: Use strong, unique passwords for each account and enable MFA wherever possible to reduce your exposure. Adding MFA creates an additional layer of security, requiring a secondary confirmation that you're a legitimate user. Use a password manager to securely store your unique passwords.

Email and Phishing Protection

Surface-Level Threats: Phishing emails and social engineering attempts are common methods that attackers use to get access to sensitive information. These tactics might look simple but are extremely effective.

Solution: Be vigilant about unexpected emails, especially those urging immediate action. Consider using email aliases and filtering to limit direct exposure of your main accounts.

Beyond Basic Protections: Tracking and Privacy Controls

Deeper-Level Threats: Tracking technology, including phone and location tracking, is often overlooked but can expose personal information to criminals. These threats are subtler but can reveal critical data like travel patterns or geolocations.

Solution: Limit app permissions on your devices, avoid location sharing when not needed, and regularly review privacy settings across all devices.

Business Cybersecurity Essentials—Protecting Against Complex Threats

Businesses today face a unique and more daunting cybersecurity challenge. Holding vast amounts of customer data and handling significant financial transactions daily, companies are prime targets for cyber criminals. Here's how to address this from fundamental to advanced tactics.

Remote Work Protections

Visible Risks: Remote work environments are rife with vulnerabilities, including unsecured home networks, shared devices, and risky public Wi-Fi usage. These create easy entry points for attackers to intercept data or infiltrate company systems. While VPNs can protect connections, misconfigured or outdated VPNs may expose traffic to interception or unauthorized access.

Solution: Use up-to-date, encrypted VPNs alongside a zero-trust approach to validate every connection. Pair VPNs with endpoint detection tools, enforce multi-factor authentication (MFA), and provide secure, managed devices for remote employees—train staff on security best practices to minimize risks like phishing and unsafe Wi-Fi use.

Least Privilege Access

Hidden Threats: Attackers often exploit excessive permissions, gaining access to sensitive data or systems through compromised accounts. High-privilege accounts are especially vulnerable, as even a single breach can lead to widespread damage.

Solution: Enforce the principle of least privilege, granting users access only to the resources necessary for their roles. Use identity and access management (IAM) tools to assign and monitor permissions and regularly audit accounts to ensure privileges remain appropriate. For remote access, layer security with multi-factor authentication (MFA) to minimize risks while keeping permissions tightly controlled.

Data Encryption

Even Deeper Risks: Once attackers breach your systems, unencrypted sensitive data—such as customer records and financial information—can be stolen or misused, causing reputational and financial damage.

Solution: Encrypt all sensitive data in transit and at rest to ensure it remains secure, even if it is accessed by unauthorized parties. Use strong encryption protocols and update them regularly to defend against evolving threats.

Network Monitoring & Incident Response Planning (IRP)

Deeper Risks: Cyber criminals often infiltrate networks unnoticed, silently gathering data and probing for weaknesses. These hidden threats can go undetected without continuous monitoring until they cause significant damage, such as data breaches or system disruptions.

Solution: Deploy advanced network monitoring tools to detect unusual activity in real time, enabling early intervention. Complement this with a comprehensive incident response plan that outlines clear roles, responsibilities, and step-by-step procedures for handling breaches. Conduct regular vulnerability scans and update your IRP to ensure your team can respond swiftly and effectively to evolving threats.

Navigating the Cybersecurity Iceberg

Effective cybersecurity requires vigilance, advanced protections, and ongoing education. What you see is only a fraction of the threats—most operate quietly below the surface, with cyber criminals waiting for the right moment to strike. By being proactive, implementing layered defenses, and staying updated on best practices, you can protect yourself and your organization from sophisticated threats lurking out of sight.

FEATURED CLIENT CASE STUDY

Securing Financial Services

Learn how Landings Credit Union optimizes IT, enhances security, and upholds regulatory compliance through its partnership with One Step Secure IT.

For over 70 years, Landings Credit Union has successfully combined the resources of a large financial institution with a personalized touch in member service. With three locations spread across the bustling Phoenix metro area, their commitment to the community has always been unwavering.

As they expanded, the complexities of managing a growing IT infrastructure while adhering to stringent financial regulations began to mount.

The Search for the Right IT Partner

Rachel D. Causley, Landings Credit Union's CIO (Chief Information Officer) was searching for an IT partner that understood and met their needs. With over 30 years of industry experience and a decade spent at Landings Credit Union, she oversees all IT operations, including endpoints, servers, workstations, and user applications. When their previous Managed Service Provider (MSP) began to falter, Causley recognized it was time for a change.

> “
>
> *We were working with an MSP for several years, but they were a bigger entity that bit off more than they could chew. Their service was rapidly declining, and it felt like pulling teeth to get our needs prioritized.*

With a lean IT department of two other employees, Landings Credit Union needed a reliable IT partner to support their end users effectively.

Each time their team reached out for support, they were met with uncertainty. Help desk staff often didn't recognize or understand their situation, leading to unnecessary delays. The first 15 minutes of every call were frequently spent answering basic questions about the organization—information the MSP should have already known. This lack of familiarity wasted valuable time and fostered frustration among Landings Credit Union's team, who felt unsupported during critical moments when quick resolutions were essential.

A New Beginning with One Step Secure IT

After growing accustomed to the lackluster service of their previous MSP, partnering with One Step Secure IT felt like a breath of fresh air. The transformation was immediate and palpable. The stark difference in communication and support was evident, erasing the days of feeling like just another ticket in the system.

Since its inception in 1985, One Step Secure IT has been dedicated to providing top-tier IT, security, and compliance services. One Step strikes an excellent balance—small enough to offer personalized attention, yet large enough to support clients with a full team of experts.

Landings Credit Union decided to engage One Step Secure IT for co-managed IT services, allowing them to focus on more specific aspects of their IT operations while gaining access to a dedicated team of specialists.

One Step Secure IT took on key responsibilities such as...

Server Management

Network Monitoring

Regulatory Compliance Readiness

This allowed Landings Credit Union's IT team to refocus their efforts on user support, knowing that the critical back-end tasks were in expertly skilled hands.

This partnership brought invaluable resources to the table, including a **virtual CIO, Network Administrator, and Compliance Manager**—ensuring that Landings Credit Union has the specialized support they need.

Specialized Knowledge in Financial Services

In the world of finance, security is not just a priority; it's a necessity. One Step Secure IT's deep understanding of the financial sector and its specific regulatory requirements gave Landings Credit Union the reassurance they were looking for.

> “
>
> *The fact that they are knowledgeable in the financial sector—I feel like that has helped me feel more comfortable for our upcoming audits or exams.*

Causley emphasized the critical importance of protecting account information and Personal Identifiable Information (PII). Any breach could carry severe consequences, making strong security measures and strict adherence to industry standards paramount.

With One Step Secure IT, they felt confident that their sensitive data was in safe, capable hands.

A Partnership Built on Trust

Through this partnership, Landings Credit Union overcame its immediate IT challenges and established a foundation for sustainable growth. As they continue to serve their community with the personalized attention that has defined their organization, they now do so with the peace of mind that comes from having a dedicated IT partner at their side.

The decision was straightforward for Causley. "We considered other MSPs, but the level of service and the relationship we were building with One Step made the decision easy," she explained. The pricing was similar to what they had been paying, and the exceptional relationship and service quality made One Step the clear choice.

Causley highlighted their exceptional service, saying, "Even when it comes to account management, if I have any concerns or questions—especially about pricing—my account manager has been fantastic. They're incredibly responsive and always ensure everything is handled promptly. Those are all A-plus qualities in my book."

Since partnering with One Step Secure IT, Landings Credit Union has transformed its IT operations. The seamless blend of specialized knowledge, personalized service, and prompt communication has solidified One Step as a trusted partner in their journey.

This partnership has empowered Landings Credit Union's team to shift their focus back to what truly matters—serving its members with care. With the assurance that their IT infrastructure is not only secure but expertly managed, they're poised for a brighter future.

The Phoenix-based credit union is tackling today's challenges head-on and strengthening their tech foundation for a safer and more efficient future.

With One Step Secure IT by its side, Landings Credit Union is well-equipped to adapt and thrive, ensuring it continues to meet the needs of its community with confidence and dedication.

FREE DOWNLOAD

Get Your Copy of Our Latest eBook

Protect What You Connect: Security Starts with You

onestep
Secure IT Services

Protect What You Connect ::
Security Starts with You

Is your personal and business information safe from cyber threats?

Protect What You Connect is a practical, must-read guide for anyone looking to strengthen their online defenses.

This free eBook provides actionable steps to safeguard your digital world—from building stronger passwords to avoiding phishing scams.

Here's What You'll Find Inside:

- Simple Cybersecurity Tips Anyone Can Use
- How to Spot and Prevent Phishing Scams
- Securing Your Devices, Email, and Social Media
- Security Essentials for Both Home & Business

Download your free copy of the Cybersecurity Essentials eBook and start protecting yourself and your business today!

Cybersecurity | Fraud Prevention | Digital Protection

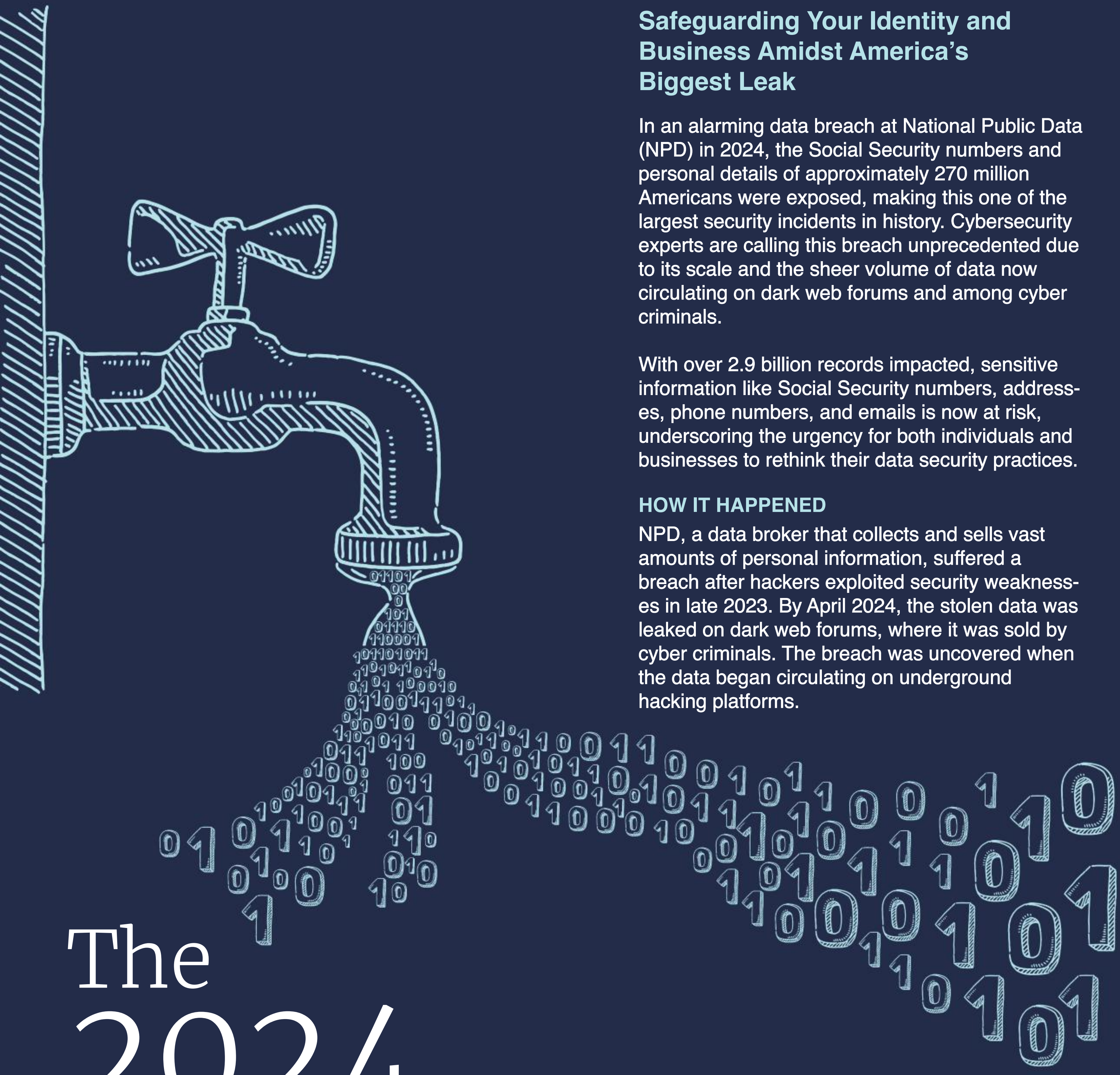
As cyber crime grows, so does the need for personal responsibility in cybersecurity. Empower yourself with insights, current trends, and practices you can start using to shield against cyber threats and fraud.

Visit www.OneStepSecureIT.com/cyber-ebook or scan QR code

onestep
Secure IT Services

(623) 227-1997

The 2024 NPD Data Breach



Safeguarding Your Identity and Business Amidst America’s Biggest Leak

In an alarming data breach at National Public Data (NPD) in 2024, the Social Security numbers and personal details of approximately 270 million Americans were exposed, making this one of the largest security incidents in history. Cybersecurity experts are calling this breach unprecedented due to its scale and the sheer volume of data now circulating on dark web forums and among cyber criminals.

With over 2.9 billion records impacted, sensitive information like Social Security numbers, addresses, phone numbers, and emails is now at risk, underscoring the urgency for both individuals and businesses to rethink their data security practices.

HOW IT HAPPENED

NPD, a data broker that collects and sells vast amounts of personal information, suffered a breach after hackers exploited security weaknesses in late 2023. By April 2024, the stolen data was leaked on dark web forums, where it was sold by cyber criminals. The breach was uncovered when the data began circulating on underground hacking platforms.

IMPLICATIONS FOR INDIVIDUALS

With personal information now exposed, we face heightened risks of identity theft, fraudulent applications, and social engineering scams. Cyber criminals are likely to use the compromised Social Security numbers to exploit weaknesses in financial and verification systems, putting not only individual identities at risk but also complicating verification processes across banks and financial institutions as this compromised data circulates.

PROTECTING YOURSELF FROM FRAUD

In light of this breach, there are critical steps you can take to reduce your risk:

FREEZE YOUR CREDIT

A credit freeze is a practical step to prevent fraudulent accounts from being opened in your name. This service is free through the major credit bureaus—Experian, Equifax, TransUnion, and Innovis—and can be temporarily lifted if you need to apply for credit. Given the magnitude of this breach, cybersecurity experts recommend keeping your credit frozen as a default.

WATCH FOR PHISHING AND SOCIAL ENGINEERING ATTACKS

With personal information widely accessible, attackers are likely to craft sophisticated phishing messages. Be cautious with unsolicited emails, calls, or texts asking for your details.

MONITOR YOUR FINANCIAL ACCOUNTS

Regularly check your accounts for any unauthorized transactions or credit applications. Immediately report any suspicious activity to your bank or credit institution.

WHY BUSINESSES SHOULD TAKE NOTE

The breach serves as a wake-up call for companies managing sensitive data. Even if you outsource your data storage or background checks, third-party incidents can tarnish your brand reputation and erode customer trust. Implementing proactive security measures, conducting regular audits, and investing in third-party testing can help reduce your vulnerability to similar incidents. When sensitive data is entrusted to other providers, your vigilance in choosing secure partners becomes paramount.

THE BIGGER PICTURE: STRENGTHENING DATA SECURITY PRACTICES

The NPD breach highlights serious vulnerabilities in handling and securing large data sets. As hackers continue to target centralized repositories, both businesses and individuals must adopt robust data protection and privacy practices to safeguard personal information against future breaches.

PROTECTING YOUR CREDIT AND IDENTITY

Your credit history and personal information are critical for financial activities like buying a car, applying for a loan, or securing a mortgage. Here are additional tools to protect your credit and identity:

Implement a Credit Freeze: A credit freeze is a free service that restricts access to your credit report, making it difficult for identity thieves to open new accounts in your name without affecting your credit score.

EQUIFAX 1-800-349-9960
www.equifax.com/personal/credit-report-services/credit-freeze

EXPERIAN 1-888-397-3742
www.experian.com/freeze/center.html

TRANSUNION 1-888-909-8872
www.transunion.com/credit-freeze

INNOVIS 1-800-540-2505
www.innovis.com/personal/securityFreeze

Lift a Credit Freeze as Needed: When applying for credit or employment, you may need to temporarily lift your freeze. Find out which bureau the provider uses and lift the freeze accordingly.

Review Your Credit Report Annually: By law, you are entitled to one free credit report per year from each U.S. credit bureau. Reviewing it can help you detect identity theft, unusual activity, or unfamiliar accounts. To request your free annual reports, call 1-877-322-8228 or visit the following website www.annualcreditreport.com.

Consider a Fraud Alert: If you suspect your information has been compromised, placing a fraud alert on your credit report can add an extra layer of security, especially useful if you have already experienced identity theft.

The NPD breach is a wake-up call, reminding us that the cyber risks are always everywhere. But here's the silver lining: by staying proactive, businesses and individuals can put up a solid defense against fraud and misuse. Don’t wait for your data to show up in the next massive leak—take charge now and stay one step ahead of cyber criminals.

One Step Secure IT
22520 North 18th Drive
Phoenix, AZ 85027

onestep
Secure IT Services

www.OneStepSecureIT.com | (623) 227-1997

Connect with us @OneStepSecureIT