FOUR KEY DATA PRIVACY CHALLENGES - AND THE SOLUTIONS

You can learn a lot from good TV. In the early 2000s, The West Wing speechwriter, Sam Seaborn anticipated the big issue for government and business today.

"In the '20s and '30s it was the role of government," said Sam. "50s and '60s it was civil rights. The next two decades are going to be privacy. I'm talking about the Internet. I'm talking about cell phones..."[1]

In this White Paper we are going to look at four of the key data privacy challenges that organizations face today. And we are going to explore how organizations are approaching those challenges in the real world.

01. PII - TOO MUCH (PERSONAL) INFORMATION

It's now clear many organizations have too much information. Much of that data is Personally Identifiable Information (PII) acquired via transactions or collected in search of marketing insights. However it got into the database, PII data can represent a serious business risk.

Accidental disclosure of that information can potentially expose businesses to stinging sanctions. For example, since the introduction of General Data Protection Regulation (GDPR) in 2018, European regulators alone have reaped over four billion euros in fines from organizations who had lost control of their customers' data (data to August 2023).

Considering 800,000 business or personal records are compromised each day, the scale of that risk is staggering. And that's before organizations confront the average total cost of a breach – estimated by IBM at over US$4 million. Let's have a look at how some organizations are dealing with those risks and those costs.

CASE STUDY: AN AUSTRALIAN BANK

Banks, by their nature, hold vast, comprehensive customer datasets crucial to the service they provide. But over time, they also accrue vast amounts of PII data that lies unencrypted and insecurely stored.

Nuix collaborated with a leading Australian bank to assist them in managing a critical PII risk. The bank had gathered millions of Tax File Numbers (TFNs) issued by the Australian Tax Office. These numbers are a powerful identifier in the Australian financial services system and by law, must be secured or destroyed once out-of-date.

The bank worked with Nuix to find and redact these identifiers amongst a database containing more than 240 million documents. These documents were in a wide array of file types – including handwritten application forms. Nuix's technology enabled the bank to secure those identifiers, negating a significant data and compliance risk.

CASE STUDY: A FORTUNE 100 COMPANY

Paradoxically, it was the arrival of the GDPR that drove one US Fortune 100 company to take control of its PII data. The company works across five continents and 100 countries with its employee and customer data just as widely spread across:

- multiple petabytes of information
- multiple systems – archives, content management systems, customer databases
- multiple formats – email, text, audio, images
- thousands of globally distributed endpoints and devices.

The company resolved to take a holistic approach to data and to managing e-discovery investigations that constantly crossed borders.

Their approach was three-pronged.

- **People** – hiring compliance and data professionals to upgrade data management and compliance practices.
- **Process** – updating data procedures and policies.
- **Technology** – deploying the latest data management and investigation technologies to cost-effectively identify, monitor and manage PII data.

Nuix's technology – driven by the scale of its processing power - enabled the company to ring-fence the PII risk by identifying and separating PII data from across the company's global network of systems across all formats.

That work also enabled the business to reduce external cyber risks to that data and establish processes that protected the PII data from internal threats – including poor data security behaviors or malign actions.

Deploying Nuix enabled the company to set alerts to flag potentially risky actions - such as bulk copies of sensitive files, off-hour use of IT systems or access from unknown endpoints. Working with Nuix, the company was able to build a security 'fence' specifically designed to meet its needs – especially the need to manage data across and through multiple locations.

02. PLAYING BY PROLIFERATING RULES – REGULATORY COMPLIANCE

As discussed above, the sanctions under GDPR are significant. Under Article 83(4), fines for 'less severe infringements' could cost an organization €10 million – or perhaps more worryingly, 2% of the firm's worldwide annual revenue.[4]

> GDPR set the tone for the world's regulators. According to Gartner research, more than 80% of organizations around the globe will need to comply with modern privacy and data protection requirements by 2024.[5]

In the USA, only five states (California, Colorado, Connecticut, Utah, and Virginia) have fully formed data privacy laws on their books. Michigan, Ohio, Pennsylvania, and New Jersey are working through legislation and some 20 states have legislation stuck in the sausage grind of state congresses.[6]

At the Federal level, the American Data Privacy and Protection Act (ADPPA) has support from both major parties but it too is still caught in Congress.

Australian organizations have a simpler regulatory framework to comply with but that compliance burden has recently been strengthened – and may be strengthened further, given a spate of high-profile data breaches at major telcos and healthcare companies publicized in the Australian media.

Meanwhile, in Canada, organizations face the toughest sanctions in the G7. For indictable offences fines can be worth up to CA$25 million or 5% of the organization's revenue – whichever is highest.[7]

This global regulatory race is keeping lawyers as well as technologists busy. According to a Gartner survey, nearly 60% of privacy leaders say keeping up with changing regulations is their biggest challenge.[8]

CASE STUDY: GLOBAL BANK

Over a period of years Nuix worked with a global bank which had been driven to undergo a complete reorganization of their data management practices due to a time-consuming and expensive money laundering investigation. Though the company was ultimately found to be blameless, the incident highlighted the costs, risks and management burden involved in sub-optimal data compliance. The bank launched itself into a comprehensive retooling of its compliance practices:

> It ran multiple compliance audits. Much of the data risk to the bank was tied up in 25 years of electronic content saved everywhere from shared drives to emails, to client databases, audio files, chats and texts.

> After identifying the amount and types of data it held, the bank launched a purge of its data, removing or neutralizing Redundant, Obsolete and Trivial data (ROT). This process enabled the organization to identify and isolate risky data, delete useless data and cut digital clutter – thus improving its efficiency.

> As it started to get control of its existing data, the bank also moved to protect itself from new risks by implementing technologies to monitor and protect endpoint devices across the organization.

> As part of these defensive tactics, the bank implemented technology solutions that gave it the ability to quickly respond to, investigate and remediate malicious activity targeting its systems.

> The bank was not only dealing with decades of data. It was dealing with data stored in multiple places, in multiple formats. For example, it collected and stored 10,000 hours of audio files each day. It needed technologies capable of tracking, reading and managing all sorts of data.

> In addition to deploying the latest investigation and data management software, the bank ran a business-wide program to upgrade compliance training and processes – especially around file handling and data storage.

A HOLISTIC APPROACH TO EFFECTIVE INFORMATION GOVERNANCE

As this case study highlights, all data privacy and governance strategies involve a mix of people, processes and technology.

In light of the growing focus on personal data, there may be commercial benefits for organizations that provide high levels of data protection. To begin with, consumers are increasingly sensitive to how brands manage their data. The ability to securely manage customers' personal information can be a key differentiator.

Brands are also increasingly keen to give consumers control over their own data and to reward them for sharing it – many brands now accompany requests for customer data with some form of value exchange.

03. FILLING THE BREACH – DATA CRISIS MANAGEMENT

Given the vast amounts of data that modern organizations deal with – and the range of internal and external threats they must address - even the best managed organizations will have to deal with a data breach at some point. This has a range of implications:

> As outlined above, organizations face the threat of significant – possibly crippling – financial sanctions if they are proven to have neglected their data management responsibilities or failed to notify the regulator within the regulated timeframe.

> They face reputational damage and loss of customer trust. In a global economy where cost-of-living is back in focus after decades of easy money, breaches may have another unwelcome characteristic – passing costs to customers. According to IBM, 60% of data incidents cause businesses to raise the costs for customers[9].

> They need to spend significant sums across their organization – refunding clients and paying damages, communicating with clients, re-mediating malfunctioning or at-risk systems and employing cybersecurity experts to analyze the breach.

> Another major cost of a data breach is business disruption. There's often an effect on day-to-day operations. Meanwhile, management focus moves off revenue, growth and operations and on to managing constant demands for information from the press, customers and regulators.

CASE STUDY: GLOBAL INSURER

One global insurer highlights the most effective way of dealing with a data breach – act to prevent it happening and minimize the damage if it does.

The insurer had assessed its data risk and calculated that, over 15 years, its document storage systems had gone from holding 1.5 million documents to 70 million documents. The insurer addressed the scale of the problem by buying a manage-in-place enterprise application and hiring a new records manager.

The record manager's first task was building consensus around the importance of records management. After using data management software to run a comprehensive ROT exercise he gained board support by quantifying the value of early wins:

- a reduced risk of data leakage and consequent fines
- a significant reduction in storage costs[10]
- enhanced productivity across the business as leaner systems facilitated faster data searches – a significant benefit in insurance where visibility of claims and pricing performance is crucial.

Using Nuix technologies, the insurer's data team was able to take complete control of the data by:

- implementing a sophisticated records management system that prioritized the areas where enhanced data management could have most impact
- optimizing database management
- rolling out data management training across the business. Part of that process involved working with staff to help them dispose of their ROT data. The other part focused on training in better data management practices including naming conventions, retention standards and more
- using Nuix content analytics to identify and categorize records according to very specific criteria – location, ownership, content topics, number and word patterns, file attributes, lifecycle status and other relevant data points. This analysis meant the data could be managed, safely deleted or archived
- moving all data into a controlled environment where all records are electronically registered.

By the end of this preparation process, the insurer's data systems and data governance practices were in far better shape. The risk of a breach was significantly lower and the ability to respond to any breach was improved thanks to smaller, cleaner, better-organized databases.

CASE STUDY: GLOBAL BANK

As the case study above highlights, minimizing the risk of a data breach is vital. Yet if a breach occurs, organizations must respond. For many that means having the ability to deploy advanced technologies and processing power into the task of analyzing and understanding a breach and meeting the information needs of customers, regulators and the media.

A US bank that recently suffered a data breach was able to harness the power of the Nuix to drive its investigation and remediation efforts. The bank was able to use multiple servers, searching many terabytes a day to quickly grapple with and report on the extent of the breach.

BEFORE AND DURING

As these two case studies suggest, managing breach risks is a two-pronged approach, involving enhanced risk management preparations that embrace people, process and technology solutions. But once a breach occurs, the ability to throw increased computing power at the problem becomes crucial.

IBM's analysis supports this two-pronged approach. They found that technology – specifically fully deployed security AI and automation – can reduce the financial damage from a typical data breach by around US$3 million. Organizations equipped with those technologies were also able to find and contain breaches an average of 74 days more quickly.[11]

04. MANAGING DATA IN M&A

In a modern economy, much of the value of companies we buy or sell is based on intangible assets. Assets you can't touch account for about 90% of the value of the S&P 500 Index.[12]

Nowhere is this clearer than in the mergers and acquisitions (M&A) process. During M&A, a company's understanding of the value of the asset it is buying or selling depends on its ability to delve into and understand a vast amount of data and to be able to separate that data into two categories:

- data that has value – IP, client records, strategic insights, ongoing research
- data that costs organizations money in storage, risk, slower systems and clogged up decision-making.

DUE DILIGENCE - IDENTIFY RISK, FIND VALUE

Nuix has worked with multiple companies that have deployed our technologies to help them value businesses they were assessing for acquisition. With our assistance those organizations were able to analyze vast stores of data and documents (across many formats) to understand a whole range of issues.

- What the target organization was actively working on.
- The sophistication of the target company's data management systems and processes. This could be crucial information, helping a buyer understand any embedded risk in the target's data management – including potential liability for fines and regulatory sanctions. It also provides a window into the target's flexibility and decision-making processes.
- That M&A is often as much about people as products. Nuix's analysis of data and documentation can identify the people who generate the most valuable IP within an organization.
- Nuix analytics – and expertise - can help companies assess the quality of a target company's IT system, databases and data-management practices. This can be a vital input to an M&A decision.

CASE STUDY: MAJOR PHARMACEUTICAL COMPANY

A large pharmaceutical company that Nuix worked with was selling a subsidiary and had a two-month window to identify and remediate data before it lost access to the subsidiary's servers.

Seeking to extract maximum value from the embedded IP, the pharmaceutical company used Nuix to process and index all its data and to find and remove valuable intellectual property from databases and email servers.

FATTENING THE PIG BY SLIMMING THE DATABASE

In many M&A situations, Nuix's technologies have been used to drive due diligence investigations into an asset. But they can also be used to make an asset more attractive. The pharmaceutical company was able to make the divested division more attractive to the buyer through a range of data-management activities.

- Running a ROT process to eliminate e-trash and reduce future data storage costs.
- Identifying applications, content and databases that could be managed more optimally post divestiture through dedicated and secure devices.
- Lawyers were able to prioritize their focus on the high risk, high value data in a short period of time.
- Completing a retention schedule and data mapping so it could more precisely value the information assets it was passing onto the acquiring company.

THE NUIX NEO DIFFERENCE

In this White Paper we have looked at four use cases where data management has become increasingly crucial – PII, M&A, compliance and managing a breach. Numerous organizations face these challenges – businesses big and small, NFPs and government agencies. They're all looking for a powerful but customizable Data Privacy solution.

At Nuix, we've been helping organizations manage data challenges for twenty years. Today we've brought everything we know, and every technology resource we have together in one solution– the **Nuix Neo Data Privacy Solution**. Here's how it works.

THE ENGINE UNDERNEATH

At the heart of that privacy solution is the Nuix Neo platform, a powerful and integrated platform designed for organizations who need a holistic solution to their data privacy challenges. And underpinning Nuix Neo is the Nuix Engine – a technology solution linking vast processing capability with responsible, ethical AI to give your organization the intelligent computing power it needs to manage data issues. Whether it is analyzing vast databases. Harnessing data for M&A valuations. Safeguarding PII. Or giving your organization the ability to quickly assess a data breach before it becomes a reputational disaster.

The Nuix Neo Data Privacy solution gives your organization the power to automate away repetitive tasks, prioritize data risks and dramatically cut the time needed to work through vast volumes of data.

PEOPLE POWER

As we've emphasized throughout this white paper, managing today's data challenges is often as much about people and processes as it is about technology. The Nuix Data Privacy Solution – and the Nuix Neo platform it sits on – align with that philosophy, giving your organization access to Nuix's accumulated expertise and thought leadership and to people who can tailor our technology and services to address your organization's specific problems.

A PLATFORM FOR YOUR ORGANIZATION'S SUCCESS

The data challenges facing modern organizations are unique to those organizations, shaped as they are by different histories, different technology and unique customer needs and organizational imperatives. That's why the Nuix Neo platform is designed so your organization can select the services you need to strengthen your internal processes.

- **Plug, play, faster** – the platform is ready when you are. The solution is designed for fast, easy configuration so your organization can act at speed and capture value fast.
- **Format flexibility** - For many organizations the data management task is all about investigating and managing old files. For others, the challenge is that every new technology increases the variety of formats in which useful data is presented. Nuix can ingest and read over 1,000 file types.
- **Easy to use** – The underlying technology is extraordinarily powerful and robust, but the Nuix Neo user interface is designed for flexibility, featuring a simple single sign-on so your staff can get to work quickly without extensive training.
- **The right kind of AI** - Nuix's work with AI solutions predates Chat GPT by years. We have always had a focus on AI solutions that works for customers. In Nuix Neo, our NLP and LLP capabilities are harnessed to meet very specific customer needs.

YOUR CHALLENGES, YOUR CHOICE.

Can Nuix Neo work for your organization? It can be tailored to your organization's budget, jurisdiction and business needs. And you can choose from hyperscale, private cloud, on-premises, or partner-supported deployment. To find out how Nuix Neo can help your organization turn data challenges into opportunities, contact us or visit www.nuix.com.

It's new, it's Nuix, it's Neo.

REFERENCES

[1] See The West Wing episode, The Short List

[2] https://www.enforcementtracker.com/?insights

[3] Cost of a Data Breach Report 2022, IBM Security

[4] Source: gdpr-info.eu.

[5] The State of Privacy and Personal Data Protection, 2020-2022, Gartner

[6] Data Privacy Laws: What You Need to Know in 2023, Osano

[7] Canada's new federal privacy bill C-27 – Summary of significant impacts and new proposals. Dentons, 2022

[8] Data Privacy Compliance, Gartner https://www.gartner.com/en/legal-compliance/insights/data-privacy-compliance

[9] Cost of a Data Breach Report 2022, IBM Security

[10] One client NUIX worked with cut 20% from its data storage program though a ROT exercise – and saved $800,000 in data storage costs.

[11] Cost of a Data Breach Report 2022, IBM Security

[12] See https://intheblack.cpaaustralia.com.au/business-and-finance/value-of-ip-and-why-it-matters

APAC
Australia: +61 2 8320 9444

EMEA
UK: +44 203 934 1600

NORTH AMERICA
USA: +1 877 470 6849