THE DATA SECURITY CRISIS.

Why 'known unknowns' are your biggest risk.

> ”There are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns — the ones we don't know we don't know.”
>
> *Donald Rumsfeld, US Secretary Of Defence, 2002*

Donald Rumsfeld's famous 'unknown unknowns' line earned him scathing commentary back in 2002. With the benefit of hindsight it appears prescient and his formulation is often used in project and risk management. But nowhere is his advice more relevant today than in the data privacy space.

DATA BREACHES AND THEIR FULL COST

According to IBM Security[1] the average cost of a data breach around the globe is USD $4.35 million. A global survey of the Directors and Officers insurance market saw data risks – cyber-attack, data loss, cyber extortion – ranked as the top three risks across the US, UK, Europe, Latin America and Australia[2].

As the D&O insurers suggest, data privacy is a global problem. In June 2022, Massachusetts-based Shields Health Care announced a data breach of highly personal customer information – including names, social security numbers and medical records. And in July 2022, a hacker 'scraped' the personal information of nearly five and a half million Twitter users – including email addresses and phone numbers.

In Europe, in February 2022, an unknown person or group leaked data on 30,000 Credit Suisse account holders. Even not-for-profits are not safe. One hacker attacked the International Committee of the Red Cross and Red Crescent and leaked over 500,000 staff records – a breach that took nearly 10 weeks to be discovered.

In the UK, October saw the revelation that local councils in many Scottish cities have suffered more than 10,000 data breaches over the past five years. Meanwhile in Australia, large scale data privacy incidents at telecommunications provider Optus, retailer Woolworths and health insurer Medibank saw millions of individual records compromised.

Amplifying the business, operational and reputational damage of these incidents is the associated regulatory costs. Europe's General Data Protection Regulation (GDPR) went into force in 2018 with fines for 'less severe infringements' worth up to €10 million, or 2% of the firm's worldwide annual revenue. Since 2018, over thirty major economies have introduced or proposed their own data protection legislation - often with equally punitive sanctions.

WHERE IS THE RISK?

For many businesses it is **known unknowns** that represent the biggest cyber threat. "Many business leaders would struggle to answer questions such as 'what data are you holding?' 'why are you holding it?' and 'where is it held?'," says Nuix's Global Head of Customer Solution, Shane Jansz. "They know they have data that creates a risk – but they don't know where it is or what to do with it."

That's because few organizations have a complete picture of all the sensitive data in their company or where it resides. Data sets are enormous and information such as customer and employee data are captured and stored in a myriad of file types and a multitude of places.

"At Nuix we say, 'you can't protect what you can't see'," says Shane Jansz. "It sounds simplistic, but many organizations have neither the technology nor the knowhow to really protect their data. And that means they're flying blind when it comes to regulatory, reputational and revenue risk."

THE SOURCE OF THE PROBLEM

There are many reasons why organizations hold data that puts them at risk.

> There might be legitimate regulatory requirements for initially holding that data – such as for Tax File Numbers (TFNs) in the financial service space.

> The data may have been collected when the philosophy was “you can’t have too much information about your customers.”

> The data is ‘hidden’ - either because of poor data management, a myriad of systems or because the data resides within different databases in a merged entity.

> The business simply didn’t have the time, resources or focus to purge or manage their data.

“It’s not uncommon to find pools of data that were collected decades ago,” says Nuix’s Executive Vice-President, Customer Strategy & Innovation, Oliver Harvey. “Data privacy thinking was less advanced back then and so it can be all over the place, in computer logs, standard system reports, database outputs, even old accounting systems. There’s often large quantities of sensitive information residing in digital objects long forgotten.”

HOW TO TAKE CONTROL

Nuix is a global provider of software that helps organizations take control of their data. It uses vast amounts of processing power and the latest technologies - including Natural Language Processing and Artificial Intelligence – to give companies that control. But the process itself is relatively simple.

1. **Identify.** The prerequisite for control is the ability to identify and inventory data – both unstructured & structured data – wherever it is stored. “This is the point where our clients start to ‘see’ the data risk,” says Harvey. “They’re starting to make the unknown known and one reason they can do that is because our platform gives them the ability to read 1,000+ file types.”

2. **Understand.** Once the data is inventoried the focus turns to understanding the data and the risk it carries. That’s all about analysis that uncovers the age, ownership, format and content of each item. At this point organizations can start to see opportunities to cull/delete so-called Redundant, Obsolete and Trivial data using metadata including data ranges, file extensions, date and more. As a by-product of this activity, they can dramatically reduce the data they have to store, manage and navigate.

3. **Analyze.** At this stage, the focus turns to analyzing the data in context to determine whether it’s an asset or a liability. Nuix software can perform sophisticated functions – including turning audio and image data to searchable text. And run searches to find specific data types, including Personally Identifiable Information (PII) such as Tax File Numbers, Drivers License Numbers or Social Security Numbers.

4. **Act.** Understanding your data is crucial. Being able to act on it – at scale – is just as important. In this stage of the process Nuix users can focus on governance decisions: how to optimize storage; how to classify, move and protect data; or how to make it more readily available to the business. Nuix users have access to sophisticated workflow management systems that enable more informed, more accurate decisions – and rapid, defensible implementation of those decisions.

“The power of this process is the visibility and optionality it gives managers,” says Oliver Harvey. “We recently worked with a leading global bank as part of a large-scale information governance project. They knew there was highly sensitive customer information scattered across the company and that the data was unencrypted and largely unprotected. But they didn’t know where it was. It took us just 2 weeks to give them complete control of all that data.”

THE INEVITABLE CRISIS?

Unfortunately, there is no such thing as a ‘hack-proof’ company. More organizations will suffer breaches in the near future. As discussed above, these breaches have immediate effects on the revenue side of the business and often attract financial penalties from regulators.

But the cost of the crisis reaches way beyond those immediate effects. There is a cost in the loss of customer trust. There’s damage to the reputation and brand value of the business. And the oft-forgotten cost of lost executive focus as business leaders pivot from managing operations and driving strategy to remediation actions and dealing with regulators, the media, social media and public opinion.

So how can businesses minimize the costs – all the costs - of a data privacy breach?

1. FIND IT FAST

In 2019 Nuix ‘asked’ the hacking community how long it took an organization to discover what information had been taken following a breach. The average detection period was 200-300 days. Obviously, with every day that passes the risk of loss for customers increases – and at a compounding rate.

According to the IBM Security Report for 2022, organizations deploying security AI and automation dramatically reduce these risks, cutting the average breach cost by over 60% and discovering and containing breaches far faster – an average of 74 days faster.

2. GET IN FRONT OF THE NOISE

The second imperative is to respond quickly to the breach and to minimize the reputational damage it causes. Using a platform like Nuix enables organizations to quickly scour terabytes of data from thousands of endpoints, across hundreds of different file formats (e.g., PDFs, emails, Word documents) – and apply contextual intelligence to establishing links and relationships across widely varying datasets.

This analysis at speed is critical. It accelerates the speed at which containment strategies can be deployed. Just as importantly it allows the organization to report and respond quickly and comprehensively to regulators, the media and to customers. To obey the first rule of crisis management – “get ahead of the story.”

TWO ARMS OF THE SOLUTION

There's no doubt that the risk of a cyber-attack or cyber breach is perhaps the most material risk facing businesses. And that the risk is growing both in terms of incidence and cost.

To manage that risk, organizations need to get their own house in order – to develop a cyber-risk culture, to work with their peers and competitors and with government to make the general environment tougher for malign actors.

But underpinning all these efforts is the need for a technology platform that can take 'known unknowns' out of the risk matrix. Technology that ensures organizations understand their data – its value, its location and how much risk it entails. Technology that helps them reduce the risks built into holding that data. And technology that helps them respond decisively when a breach occurs.

SEE IT FOR YOURSELF

Get a personalized demo of our industry-leading solution and see for yourself how our innovative software can transform data into actionable intelligence and help solve your biggest regulatory compliance challenges. www.nuix.com/request-a-demo

REFERENCES

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

[2] *Directors' Liability Survey 2022, WTW and Clyde&Co*

CASE STUDY: REGULATORY AGENCY

A national government agency in Australia suffered a high-profile data breach that exposed sensitive data. In response, Nuix software was deployed to undertake a detailed audit of its stored data.

Nuix technology enabled the agency to review 300 terabytes of data [equivalent to 6.5m x 300 documents];

> to identify where its key and sensitive data was held and what data needed to be moved,

> what data should be securely stored and

> what data could be safely deleted.

"We chose Nuix for its phenomenal speed and accuracy when searching, indexing and finding sensitive data. We are very pleased with the outcomes which were achieved without degrading system performance and business-as-usual operations.

Agency Director

nuix

Nuix (www.nuix.com, ASX:NXL) is a leading provider of investigative analytics and intelligence software, that empowers our customers to be a force for good by finding truth in the digital world.

We help customers collect, process and review massive amounts of structured and unstructured data, making it searchable and usable at scale and speed, and with forensic accuracy.

APAC	EMEA	NORTH AMERICA
Australia: +61 2 8320 9444	UK: +44 203 934 1600	USA: +1 877 470 6849