THE EVERYWHERE THREAT

The five big data privacy trends – and how to get in front of them

Cybercrime and digital attacks on our privacy are now a near-universal, day-to-day threat.

In this White Paper we draw on conversations with Nuix partners and corporate and government customers to look at the changing shape of the threats to our privacy, and at what organizations can do to fight back.

TREND ONE: RELENTLESS ATTACK, RISING COST

According to IBM Security's 2022 *Cost of a Data Breach Report*, (**IBM Report**) the average cost of a data breach around the globe today is $4.35 million USD – up 13% since 2020[1]. Those data breaches affect 300 million people, and they have significant downstream effects.

The IBM Report states 60% of data breaches lead to higher costs passed onto consumers. Furthermore, the damage to brands and to the bottom lines of large multinational organizations is increasingly prevalent and widely reported in the public domain.

WHAT'S GOING WRONG?

The reasons for the explosion in data breaches can be broken down into three categories: the threat, the defense, and the environment.

The **threat** story is a simple one. Bad actors are encouraged by the potential rewards available from cybercrime, so their activities are proliferating. Their attacks are also becoming more sophisticated with the use of malware, ransomware, and techniques such as social engineering to psychologically build trust with an online user, and this trust is then exploited through various attack vectors.

On the flipside, many organizations don't have adequate security measures built into their operations to protect their systems and data from cyberattacks, with legacy systems that are unsupported and easy to hack or break, still in use.

The **environment** issue is more vexed – because it's almost unavoidable. We live in a digital world. That vast web of digital interconnections creates more opportunities for cyber criminals to access sensitive information and launch attacks on online users. If we work, live and play online, that's where crime is likely to occur.

The complexity of our interconnected digital systems also gives cybercriminals many more weak points to attack. It makes structuring digital and security defenses more difficult and costly. Even organizations with the latest technology – the highest and thickest firewalls and best security mechanisms – can be exposed.

In a sense, the digital environment is working against itself. Cloud computing is vastly more efficient and cost effective, however it has unleashed new security challenges. Organizations rely on third-party providers - and *their* providers - to store and manage their data. The IBM Report states 45% of data breaches occur in cloud environments.

TREND TWO: A TIDAL WAVE OF REGULATION

The centrality of the digital realm and the explosion in cybercrime are driving a surge in regulation around data privacy and cybercrime. A rapid increase in regulation and more draconian penalties means any organization serious about its reputation, and the state of its balance sheet, needs to understand their regulatory environment, operationalize compliance and manage the risks of sanctions.

For many organizations, the arrival of the European Union's General Data Protection Regulation (GDPR) marked the beginning of this trend. According to Gartner, by 2024, more than 80% of organizations around the globe will have to comply with modern privacy and data protection requirements[2].

The price of not doing so is heavy. Under GDPR, fines for 'less severe infringements' could cost an organization €10 million - or 2% of the firm's worldwide annual revenue[3]. To date (2023), fines in excess of A$3 billion have been issued by European regulators[4].

In the aftermath of major cyber breaches, the Australian government has also made 116 recommendations to improve the way data is held, processed and stored as part of a proposed regime that could impose a regulatory cost worth A$9 billion over the next ten years[5]. Other regulation classifies customer data as a 'critical asset' and could give the Australian Signals Directorate the legal cover to take over any company's IT systems in the event of a major cyber threat[6].

Further, in the United States of America, states such as California, Colorado, Virginia, Utah and Connecticut have now passed State-based privacy legislation and Federal legislation, the American Data Privacy and Protection Act (**ADPPA**) is working its way through Congress. The ADPPA – supported by both parties, seeks to govern how companies across different industries treat consumer data[7].

There's a global trend for more stringent and far-reaching regulation and as with any regulation, there's a risk of unintended consequences. That means organizations need to manage the risks and be part of the debate on future regulation.

TREND THREE: STOPPING THE ROT, CHANGING THE NAME

The world's data is doubling every three years and 80% of this data is unstructured[8]. For many organizations, this presents two key problems:

1. How to manage that volume.

A key part of managing the sheer volume of data is cutting the amount of Redundant, Obsolete, Trivial (**ROT**) data gumming up databases. That process has multiple benefits:

- It reduces the cost of storage[9].
- Since it eliminates a significant chunk of useless data, it reduces the work people and systems need to do to find valuable insights; and
- It means organizations can delete data that's useless to them but could still represent a security risk to their clients.

2. How to protect that data in the face of ever-more-stringent data regulation (see Trend Two).

To help reduce the risk involved in holding vast amounts of data, organizations are investing time, technology and resources in 'pseudonymization' and 'anonymization'.

Pseudonymization involves processing personal data so that it can no longer be attributed to an individual person who can be identified without the use of additional information.

Anonymization is the irreversible transformation of personal data. It aims not only to remove personal identifiers but to ensure it's impossible to determine who an individual is from the rest of the data. This process is designed to be permanent.

Both of these evolving processes are a big step forward from holding vast volumes of valuable, easily-identifiable, and hackable, personal data. Currently, pseudonymized data is considered personal data under the GDPR. Anonymized data isn't[10].

TREND FOUR: TROUBLE AT HOME – REMOTE WORK AND ITS RISKS

The pandemic lockdowns have had multiple negative effects on the global economy, education, hospital systems, mental health and more. Cybersecurity is now joining that long list. Remote working has not only increased the risk of breaches. It's made them more expensive. According to the IBM Report, where data breaches are associated with remote working, there's a $1 million USD additional cost for the organization[11].

Around the world, employees adapted surprisingly quickly to the possibilities of remote working, but so did cybercriminals. Roy Waligora, Head of Investigations Partner at KPMG Forensic has written: "Criminals immediately exploited new ways of working and living created by the pandemic, causing a huge spike in online fraud."[12]

Remote work means more personal devices interacting with corporate systems and more sensitive information travelling across less secure paths. Home offices are simply not as secure as controlled corporate networks. Data breaches associated with remote work not only create more threats for organizations, they often expose the personal data and identity of the remote worker.

TREND FIVE: PEOPLE AND CULTURE

Worldwide, there are currently 3.5 million cybersecurity roles that need to be filled[13]. That gives you an idea of the scale of the need for cybersecurity talent. There simply aren't enough cybersecurity professionals to go around and that's upping the price and the perks required to get cybersecurity staff on the payroll.

To meet this challenge, organizations are going to have to turn to technology solutions to protect their operations and their clients.

The other imperative is cultural. Even with the best cybersecurity staff and technologies, companies without a data security culture are at greater risk. Organizations must invest in education around data security and data management. They must have constant awareness programs and test and retest compliance. Most importantly they must make safe data practices part of 'the way we do things around here,' and that requires management commitment, training and soft skills.

SURFING THE TRENDS

Managing these interconnected trends is a key challenge facing organizations today. Indeed, respondents to the World Economic Forum's 2022 Global Risks Perception Survey cited cybersecurity failure as "a critical short-term threat to the world"[14].

One thing to remember is that cybersecurity is not all about downside risk. Today, a data security culture and a proven ability to manage client data securely puts you at a competitive advantage. Customers and partners will trust you and want to work with you.

SEE THE PROBLEM

At Nuix, we work with clients to build data privacy solutions that balance three imperatives:

- Organizations can easily manage and maintain the confidentiality and integrity of client data;
- That data is easily available for legitimate business and organizational purposes; and
- The management of that data is in line with ever-expanding global regulations.

To achieve these objectives, we focus on giving our clients a complete *view* of their data because 'you can't protect what you can't see.' The diagram below explains how we do it.

1. IDENTIFY

Nuix solutions help organizations to identify, collect and inventory unstructured & structured data – wherever it is stored and across 1,000+ file types across various source locations.

2. UNDERSTAND

With Nuix, organizations can understand the age, ownership, format, content, context and risk of each data item and giving it a score to help you prioritize. Nuix finds and understand private, sensitive or confidential data.

3. ANALYZE

Nuix analyzes the data in context to determine whether information is an asset or a liability. Then use sophisticated workflow management systems to make more informed, more accurate and more timely decisions.

4. ACT

Nuix helps organizations optimize storage; classify, move and protect data; defensibly delete the ROT data (Redundant, Obsolete, Trivial). Crucially, Nuix empowers organizations to make rapid, informed decisions in a data breach crisis or regulatory request

MORE BENEFITS OF CONTROL

As the diagram above indicates, Nuix technologies can help an organization understand the risk inherent in their data and help them manage those risks. Our technology, experience and massive processing power means we can provide this control even where your organization is working with vast amounts of data. And our automation tools means you can achieve this control without paying a huge extra cost in 'human time.'

In working with our clients, it's clear there are two often underplayed side-benefits of the Nuix approach to data security.

The data deep dive that's part of the process doesn't just give organizations control of their 'risky' data. **It can help them find and harness valuable intellectual property (IP) that's been 'lost' in the business.** That IP can be monetized by the business in its operations, or added to a valuation calculation when the business is on the market.

- The ability to interrogate and organize vast amounts of data means **organizations can quickly respond to regulatory requests for data**, or, in the worst-case scenario, get on top of a data-breach more quickly. According to the IBM Report, organizations deploying security AI and automation cut the average data breach cost by over 60%. They discovered and contained breaches an average 74 days faster[15].

WANT TO FIND OUT MORE?

The trends we've covered in this White Paper are almost universal. They affect business, utilities, government and not-for-profits. Staying ahead of these trends requires an investment in culture and training, in technology, recruitment and specialist expertise. If you'd like access to expertise in all these areas - so you can protect your organization and the people that rely on it, talk to Nuix.

REFERENCES

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

[2] *The State of Privacy and Personal Data Protection, 2020-2022*

[3] *GDPR Fines & Data Breaches Penalties*

[4] *GDPR Fines List: Find all GDPR fines & detailed statistics*

[5] *Privacy Act Review Report | Attorney-General's Department*

[6] *See the discussion in https://www.afr.com/technology/businesses-face-new-9b-cybersecurity-requirements-20230217-p5clf5. This regulation is also discussed by law firm Herbert Smith Freehills here: https://www.herbertsmithfreehills.com/insight/demystifying-australias-recent-security-of-critical-infrastructure-act-reforms*

[7] *https://crsreports.congress.gov/product/pdf/LSB/LSB10776*

[8] *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*

[9] *In one company Nuix works with, simply reducing ROT by 20% cut $800,000 from data storage costs in the first year.*

[10] *Anonymisation and pseudonymisation | Data Protection Commissioner*

[11] *IBM Security's 2022 Cost of a Data Breach Report*

[12] *Fraud Barometer 2021, A snapshot of fraud in the UK, KPMG*

[13] *'Hundreds Poached as Cybersecurity Talent Wars Rage on'*

[14] *World Economic Forum's 2022 Global Risks Perception Survey*

[15] *IBM Security's 2022 Cost of a Data Breach Report*