THE GOOD SHEPHERD MODEL FOR CYBERSECURITY, PRIVACY AND REGULATORY COMPLIANCE

Four principles for protecting private data to improve compliance with privacy regulations

EXECUTIVE SUMMARY

Organizations that store customers' private information have a duty of care to protect that data.

Credit card numbers and other personal details fetch a high price on the black market and unfortunately, organizations do a very poor job of keeping them out of the hands of cybercriminals.

Regulators in many countries are now levying considerable penalties against organizations that fail to protect people's private data. Under the European Union's General Data Protection Regulation (GDPR), for example, organizations face fines of up to €20m or 4% of annual turnover for exposures of European citizens' private data. They must also disclose breaches within 72 hours of discovering them.

And now for the bad news: Breaches are inevitable. Security researchers believe determined attackers can infiltrate any security system. Even so, many data exposures stem from internal causes: malicious insiders, loss or theft of devices, accidental misuse or simple errors by IT and security administrators.

If you can't prevent hackers or insiders from getting into your organization's network, it's vital to minimize the damage they can cause. Doing so requires a new set of information security disciplines:

- Knowing where important data is stored, understanding what it's worth and making sure it's protected
- Detecting breaches and discovering the extent of the damage much faster
- Conducting thorough and effective post-breach investigation and remediation.

This paper will focus on the first discipline. It will examine how organizations can use information governance technologies to reduce the cost and extent of cybersecurity breaches by becoming good shepherds of their data.

Information governance technologies provide visibility into unstructured data so you can understand where your organization stores high-value and high-risk private information. Strictly limiting access to private information – to malicious and inept insiders and external hackers – minimizes the risk that this high-risk data will be exposed. You can achieve this through four activities:

- Defensibly deleting data that has no business value
- Locating high-value documents and intellectual property, and moving them to repositories with encryption, access controls and retention rules
- Protecting high-risk personal and financial data with appropriate encryption and access controls, and ensuring this information does not leak from controlled repositories
- Applying policies and conducting regular audits to ensure only authorized staff members have access to important data.

If you know where your data is, you can respond efficiently to breaches by first investigating the high-risk and sensitive storage locations. This in turn means you can quickly discover and report on the extent of a breach and notify the regulatory body (and perhaps your insurer) as well as closing any information security gaps before someone can exploit them again.

REGULATORS SHARPEN THEIR FOCUS ON PROTECTING PRIVATE DATA

Organizations that hold customer data or intellectual property must contend with growing efforts to capitalize on their information. A report by the US Department of Homeland Security found "the cyber threat landscape is distinguished by an expanding set of actors" and attributed this to the "low barrier of entry for new actors" and the diffusion of expertise from former government and intelligence operatives and commercial practitioners to threat actors.[1]

In its 2021 Global Business Risk Barometer, global insurer Allianz found cybersecurity incidents were the third highest risk faced by businesses, after only business interruption and the COVID-19 pandemic.[2]

Owing to widespread awareness of cybersecurity and privacy issues, regulators are closely scrutinizing organizations' information security programs and imposing increasingly onerous fines for data breaches.

- In July 2019 Equifax agreed to pay at least $575 million for failing to take "reasonable steps" to secure its network. Regulators found Equifax culpable for failing to prevent a data breach that affected 147 million people.[3] The US Federal Trade Commission's complaint against Equifax alleged twelve shortcomings in its security program, including that it failed "to monitor or log privileged account activity across numerous systems."[4]
- In October 2020, the UK Information Commissioner's Office (ICO) fined British Airways £20 million, ICO's largest fine to date. ICO concluded British Airways had failed to protect customer data that was compromised in a 2018 cyberattack,[5] alleging the airline's failure to apply automated application blocking contributed to the breach.[6]
- Fines for breaches of the European Union's General Data Protection Regulation (GDPR) rose by nearly 40% between January 2020 and January 2021.[7]
- More broadly, data protection supervisory authorities across Europe have issued a total of EUR1.64bn (USD1.74bn/GBP1.43bn) in fines since 28 January 2022 – that's a year-on-year increase in aggregate reported GDPR fines of 50%. And in the US, 5 States (California, Colorado, Virginia, Utah, and Connecticut) have now passed privacy legislation, and there is currently a federal bill, known as the American Data Privacy and Protection Act ('ADPPA') making its way through Congress with bi-partisan support.

UNDERSTANDING THE NEED

In 2023, 65% of the world's population will have its personal information covered under modern privacy regulations such as GDPR, the California Consumer Privacy Act and Australia's Privacy Act, up from 10% in 2020.[8] By 2024, more than 80% of organizations worldwide will face modern privacy and data protection requirements.

Privacy regulations worldwide impose strict requirements on the way you govern and protect customers' and employees' personal data and how you respond to data breaches. If you suffer a breach that compromises citizens' data, you have as little as 72 hours to report that breach to the authorities in each jurisdiction you operate in.

Regulations in many countries give individuals a right to erasure or right to be forgotten, meaning they can ask an organization to delete any personal data it holds about them, provided the organization has no legal reason to keep it. Individuals may also ask for a complete record of the data an organization holds about them, known as a subject access request. Organizations must respond to these requests "without undue delay," which generally means within a month.

WHERE TO START? GAINING VISIBILITY TO ACT

Many organizations suffer the same challenge: Rapid data growth, teamed with an increasing number of storage devices, cloud technologies and working-from-home arrangements, all increase opportunities for data breaches.

Protecting personal information is complicated by the fact that typically 80% of the data organizations store is unstructured and often in proprietary formats and complex containers. This increases your risk exposure by adding difficulties when it comes to understanding your data, managing it as part of breach preparedness and responding appropriately to threats. To put it another way, you can't protect information if you don't know where it is and what's in it.

The fact that organizations don't know where they store personal data makes it much harder to comply with right-to-erasure and subject access requests. It makes it harder to reduce the risks of regulatory noncompliance by finding, classifying and remediating risky data. If you don't know personal data is there, you're much less likely to notice it's been copied or otherwise removed from outside your control. And when you do find out you've been breached, you won't know where to start your investigation.

This lack of visibility into personal data is one of the main reasons it takes so long to detect and remediate breaches. According to the frequently cited IBM Cost of Data Breach Report, breached organizations took an average 212 days to discover they had been compromised and a further 75 days to contain the breach.[9] Despite improvements in cybersecurity technology and awareness, this is more than two weeks longer than the average duration from five years earlier.

The new regulatory paradigm doesn't give you the luxury of a leisurely post-breach investigation. Once you've learned that data has been compromised, you need to find out what it was and who was affected and notify regulators. In Europe for example, you have 72 hours.

"ASSUME YOU ARE COMPROMISED" – NOW WHAT?

For many years, the information security industry sold the vision that the right combination of technologies could completely prevent data breaches. Antivirus software would prevent malware from executing on endpoints, firewalls would build a barrier between the inside of the network and the outside world, intrusion detection and prevention systems would detect and prevent attacks that had somehow got past the antivirus and firewall, and so forth.

In the past few years, the industry and its customers have come to realize this vision was a mirage. For example, antivirus software could block malware that had a known digital signature but cybercriminals found ways to modify files to have different signatures, develop new malware or acquire it on the black market, hijack software already installed on the target computer or deliver malware through a compromised software vendor's automatic updates process.

This is one reason why a majority (54%) of hackers and penetration testers surveyed in Nuix's Black Report said they could breach their target organizations, locate critical value data and exfiltrate that data within 15 hours.[10]

Nor is this a new or emerging issue. Gartner's bluntly titled report from 2014, *Malware Is Already Inside Your Organization; Deal with It* said, "determined attackers can get malware into organizations at will" and "organizations must assume they are compromised."[11]

PEOPLE ARE A PROBLEM

In addition, a large proportion of breaches result from the actions of people inside the organizational perimeter rather than those of external hackers.

The IBM Cost of Data Breach Report estimated that malicious insiders were responsible around 8% of the data breaches studied.[12] However, many other attack vectors involve insiders, often unwittingly, including compromised credentials (20% of breaches surveyed), phishing (17%), business email compromise (4%) and social engineering (2%). Cybercrime groups have been known to offer incentives of up to US$1 million for insiders to run malware[13] or provide administrator credentials.[14]

Data breaches can also stem from mistakes or poorly designed systems and processes. The IBM study found 15% of breaches were caused by cloud misconfiguration and another 5% by system errors.[15] (As Nuix has previously argued, system glitches are most often human errors by another name.[16]) And even in clear cases of criminality, human error is often involved – for example, opening a malicious attachment in a phishing email or giving away valuable information to a social engineering attack.

A NEW MINDSET

If we cannot prevent malware or hackers from broaching perimeter security, how can we protect high-value and high-risk private data in our care? How can we avoid falling foul of privacy regulations?

It requires a change in mindset and a new set of information security disciplines. This involves three core capabilities:

- Knowing where important data is stored, understanding what it's worth and making sure it's protected
- Detecting breaches and discovering the extent of the damage much faster
- Conducting thorough and effective post-breach investigation and remediation.

This paper will focus on the first capability: knowing where important data is stored, understanding what it's worth to your organization and making sure it's protected in proportion to this value and risk.

THE GOOD SHEPHERD MODEL

Information governance technologies are a powerful tool in reducing the cost and extent of cybersecurity breaches by providing visibility into unstructured data and delivering facts upon which security professionals can make informed decisions.

Information transparency can have a huge impact on how secure your organization is from data breaches and how effectively you can respond to incidents – internal or external, deliberate or accidental.

In this model, information security, information governance and records management specialists become good shepherds of their data. They know where all the sheep are, segregate them into separate fields, make sure the fences between fields are sound and regularly check to ensure the sheep are healthy and not due to be made into shepherd's pie. In this way, even if a wolf manages to get into one of the fields, most of the flock will be safe.

Applying these principles to data gives us four broad rules or areas of activity:

1. DEFENSIBLE DELETION

Most organizations just don't understand what data they have. They store large volumes of data that has no business value – it's duplicated, trivial, no longer used, past its retention period or potentially risky.

Many industries and jurisdictions have strict compliance rules around how long organizations must retain data. However, once that retention period is over, the risks and costs of keeping data greatly outweigh any residual value.

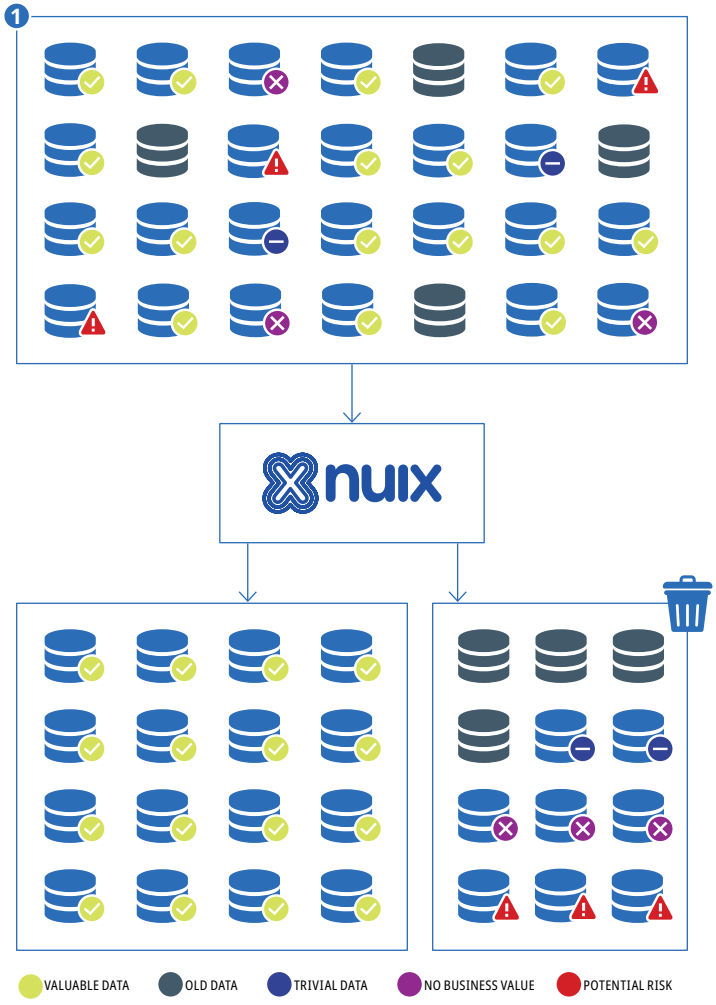

Figure 1:Deleting low-value data minimizes risk and reduces the scope of post-breach investigations.

Deleting this low-value data, according to predefined and legally sanctioned rules, reduces risks and minimizes the volume of data that could be compromised. This in turn reduces the scope of post-breach investigations, right-to-erasure and subject access requests.

In the longer term, information governance analysis can help you understand why this content is created or becomes low value in the first place.

2. DATA HERDING

Organizations often have intellectual property and company records such as contracts stored inappropriately in file shares or email attachments. Neither records managers nor end users have the time to ensure records are filed correctly.

Information governance technology can locate these records in the wild – often across dozens of storage systems and thousands of shares – and move them to controlled repositories with appropriate security, access controls and retention rules. This makes it much harder for anyone to gain unauthorized access.

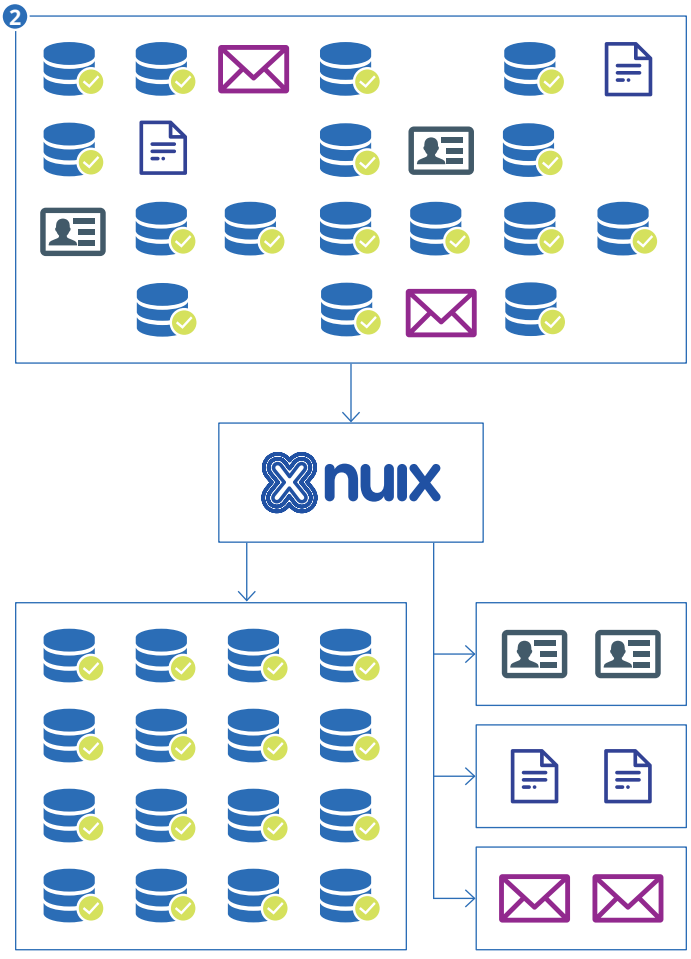

Figure 2: Locating records in the wild makes high-value information less vulnerable to breaches.

3. DATA SECURITY

Increasingly strict data privacy regulations make it imperative to hold personal data in the strictest confidence. Nonetheless, this information regularly escapes controlled repositories, whether through poor policies or employees not following the rules.

Employees may make convenience copies to work from home or as test data for a new application. They may find data that was generated for one purpose, such as legal discovery, and use it to fulfil other needs without understanding the privacy implications of doing so. And even if they dispose of this data correctly, it may still be retained in backups or archives.

By monitoring targeted data whenever it's accessed, copied or moved and by conducting periodic sweeps of email, file shares and other unprotected systems, you can quickly locate and remediate unprotected private data. Understanding where this high-risk data is stored also means you don't need to spend time and effort protecting data that doesn't need it.

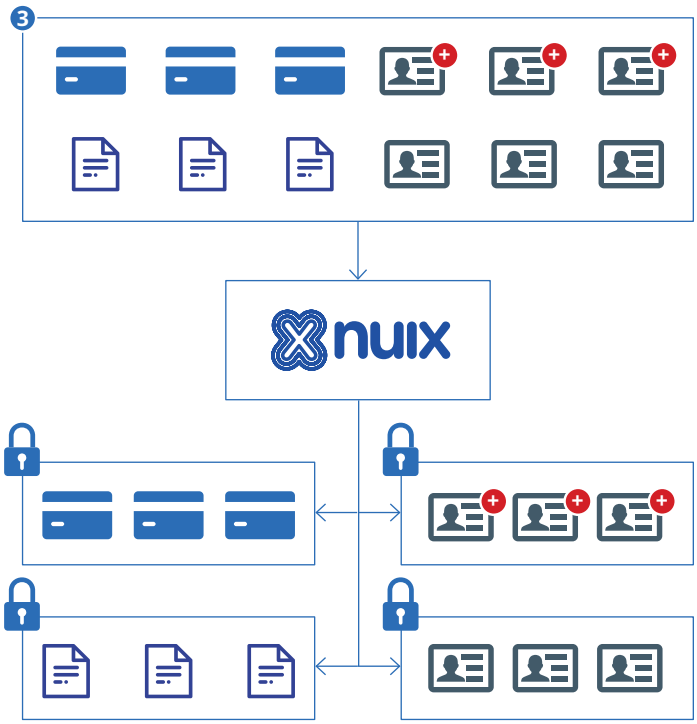

Figure 3: Keeping private, financial and health data within known, protected locations reduces business risks.

4. ACCESS CONTROLS

The final rule involves making sure the only people who can access high-risk data are those who need to. This requires a combination of sound policy and constant vigilance.

For example, many data loss incidents occur when a disgruntled employee leaves the organization. Canceling an employee's login and access credentials as soon as they leave minimizes opportunities for important information to go astray. It may also be prudent to scan their recent emails and other activity for indications they have mishandled personal information, company intellectual property or other important data.

It is also essential to audit access controls on important systems and employees' security profiles to ensure the policy theory matches reality.

For example, in one data breach investigation Nuix analysts worked on, employees had stumbled on a way to view salary information and other personal data on a human resources department network drive. It emerged that an IT admin had been updating the access controls to the drive and had mistakenly granted all users access to it during the process.

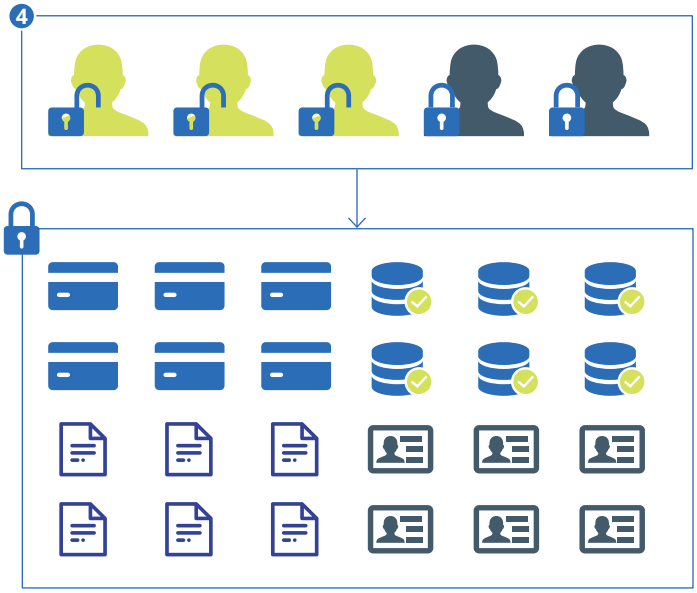

Figure 4: Regularly auditing access controls ensures security policy matches reality.

CASE STUDY: INVESTIGATING A DATACENTER BREACH THE HARD WAY

Nuix analysts investigated a breach at a large datacenter that had literally thousands of web, database and file servers belonging to individual clients with no visibility into their contents. It was impossible to know by examining the servers what roles they performed and which of them might contain credit card numbers or other personal data.

Fixing the problem was urgent. The company was losing revenue from having to take some clients' servers offline. And the incident was doing considerable damage to its reputation.

Realizing it would be impossible to scan all the servers within a reasonable time, Nuix analysts and the consulting firm staff took a random sample of the servers and used a named entity search to locate credit card numbers and other private data.

Fortunately, the gamble paid off and they located systems that had been compromised. This provided an attack signature they could use to find compromised servers among the remaining systems.

Had the hosting provider conducted regular sweeps, it could have quickly identified any servers that contained credit card numbers. It could have ring-fenced servers containing sensitive data and applied stringent encryption and access controls. Alternatively, it could have changed its policy so that credit card numbers and other private data could only be stored with a specialist third-party provider and conducted sweeps to ensure clients were complying.

Proactive measures yield downstream benefits. These steps minimize the likelihood of future breaches and greatly reduce the time taken to locate them, protecting the firm's revenue and reputation.

SECURITY AND PRIVACY ARE STRATEGIC

Regulators worldwide have made clear that businesses must dramatically change their posture of compliance in handling personal data. You need to build privacy into your systems by design and protect consumer data from mishandling. Organizations must shift their information security mindset from "Breaches only happen to other people – how much do we have to spend to look like we're doing the right thing?" to "How can we strategically minimize the opportunities for breaches and the damage we suffer from them?"

By adopting these four common-sense rules around deleting, herding, encrypting, and controlling access to data, you can:

- Know where personally identifiable information, business-critical records and high-risk data are stored – and be confident they are only stored in those locations
- Minimize the opportunities for malicious and accidental breaches of important information
- Respond to breaches in a more targeted and effective way, by examining the high-risk storage locations first and collecting much less peripheral data
- Close information security gaps quickly before they can be exploited again.

THE VISIBILITY TO ACT ON PRIVACY

Data is at the heart of privacy protection, making Nuix uniquely suited to help you ensure compliance with your regulatory obligations. Our technology enables you to:

- Identify collections of personal data across the enterprise to potential compliance risks
- Analyze and communicate threats to the organization, with visualizations for business users
- Collect and delete obsolete data to remediate risky information and transform to a compliant IT posture
- Search, review, and produce content related to a specific request for data (such as a subject access request), particularly if that request includes anonymization or the need to confirm you have erased data (right to be forgotten)
- Safeguard your data lifecycle with our governance, risk and compliance portfolio.

Nuix's suite of powerful, integrated tools allows you to deliver evidence with confidence. You can quickly and accurately collect, process and review data to satisfy any regulatory requests for information.

The more you know and can mitigate in a short period of time, the lower your risk exposure to regulator action and reputational damage.

REFERENCES

[1] US Department of Homeland Security, Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar, 2019.

[2] Allianz, Allianz Risk Barometer, 2021

[3] US Federal Trade Commission, Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach, July 22, 2019

[4] US Federal Trade Commission, United States District Court for the Northern District of Georgia Atlantic Division Document 2361, July 22, 2019

[5] Information Commissioner's Office, ICO fines British Airways £20m for data breach affecting more than 400,000 customers, October 16, 2020

[6] Information Commissioner's Office, Penalty Notice Section 155, Data Protection Act 2018, Case ref: COM0783542, October 16, 2020

[7] DLA Piper, DLA Piper GDPR Data Breach Survey 2021, January 19, 2021

[8] Nader Henein, Bart Willemsen, Bernard Woo, The State of Privacy and Personal Data Protection, 2020-2022, Gartner, August 26, 2020

[9] IBM, 2021 Cost of Data Breach Report, June 2021

[10] Chris Pogue et al., The Black Report 2018: Decoding the Minds of Hackers, April 2018

[11] Peter Firstbrook & Neil MacDonald, Malware Is Already Inside Your Organization; Deal With It, February 2014

[12] IBM, op. cit.

[13] ClearanceJobs, Tesla Insider Works with FBI to Turn the Tables on Russia's Million Dollar Attempt to Hijack the Network, August 26, 2020

[14] KELA, All Access Pass: Five Trends with Initial Access Brokers, August 2, 2021

[15] IBM, op. cit.

[16] Howard Solomon, Better trained people, not technology, will improve cyber security, SecTor told, IT World Canada, October 20, 2016

nuix

Nuix (www.nuix.com, ASX:NXL) creates innovative software that empowers organizations to simply and quickly find the truth from any data in a digital world. We are a passionate and talented team, delighting our customers with software that transforms data into actionable intelligence and helps them overcome the challenges of litigation, investigation, governance, risk and compliance.

APAC
Australia: +61 2 8320 9444

EMEA
UK: +44 203 934 1600

NORTH AMERICA
USA: +1 877 470 6849