THE GOOD SHEPHERD MODEL FOR CYBERSECURITY

Four strategies for Australian government organisations to minimise the potential for – and damage suffered from – data breaches

By Stuart Clarke, Lee Meyrick and Eddie Sheehy

nuix

Simple. Powerful. Precise.

CONTENTS

The high value and easy marketability of private data have made Australian government organisations, especially those that store citizens' information, a prime target for cybercrime

EXECUTIVE SUMMARY

The high value and easy marketability of private data have made Australian government organisations, especially those that store citizens' information, a prime target for cybercrime. There is also growing evidence of widespread state-sponsored cyber-espionage targeting intellectual property and confidential information. The costs of a single high-profile data breach can reach many millions of dollars or even have broad national security implications.

And now for the bad news: breaches are inevitable. Security researchers believe determined attackers can infiltrate any perimeter security system and lodge malware within organisations' networks. Knowing this, the Australian public service must adopt a new set of information security disciplines to protect high-value and high-risk data:

- Locating important data, understanding what it's worth and making sure it's protected
- Reducing the delay between when breaches occur and when they are detected
- Conducting rapid, thorough and effective post-breach investigation and remediation.

This paper will focus on the first discipline. It will examine how government agencies can reduce the extent and damage of cybersecurity breaches by becoming 'good shepherds' of their data.

Using information governance technologies to provide transparency into unstructured data reveals in detail where your organisation stores high-value and high-risk information and what it's worth. You can achieve this through four activities:

- Defensibly deleting data that has no business value
- Locating high-value documents and intellectual property, and migrating them to repositories with encryption, access controls and retention rules
- Protecting high-risk 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 authorised staff members have access to important data.

Through these efforts, government organisations can minimise the opportunities for malicious or accidental breaches of important information. If you know where your data is, you can respond efficiently to breaches by first targeting the high-risk storage locations. This in turn means you can close information security gaps quickly before they can be exploited again.

If you know where your data is, you can respond efficiently to breaches and close information security gaps before they can be exploited again

CYBERCRIME AND CYBER-ESPIONAGE: A DOUBLE THREAT

Government agencies, as a result of the highly important and valuable information they hold, may be targeted by criminal gangs with financial motives or by nation states and their proxies for cyber-espionage.

Verizon's 2015 Data Breach Investigations Report lists the public sector among its top three targets for data breaches, along with financial and information services companies.[i] Mandiant's report M-Trends 2015: A View from the Front Lines says government agencies are growing in popularity as a target for cybersecurity breaches, although Mandiant places the public sector further down its top 10 list of targeted industries.[ii]

The rewards of cybercrime

Cybercrime has become highly rewarding. A single live credit card number, accompanied by accurate identity details, can fetch up to US$100 on the black market.[iii] Private data is worth more to criminals than most organisations could ever spend protecting it from them. Even agencies that do not accept credit card payments still hold large volumes of citizens' private information that, when cross-matched with credit card numbers stolen from elsewhere, is extremely valuable to criminals.

The threats of cyber-espionage

Publicly known examples of cyber-espionage in Australia are few, but include reports that in 2013 state-sponsored hackers in China stole the plans for ASIO's headquarters in Canberra.[iv] China is "the noisiest threat actor in Cyberspace", and its targets include "proprietary information such as research and development data" as well as "intelligence access to sensitive communications", according to information security firm FireEye.[v]

FireEye has tracked one group, which it dubs APT30 (APT stands for 'advanced persistent threat'), which has exploited government and commercial targets across Southeast Asia for more than a decade.[vi] This group focuses on "acquiring sensitive data from a variety of targets, which possibly include classified government networks and other networks inaccessible from a standard Internet connection" or 'air-gapped' networks. From analysing the malware APT30 has created, FireEye researchers have seen evidence of a formal software development cycle, including version numbers. It deduces the group is extremely well resourced and "state sponsored—most likely by the Chinese government".

Time is money

According to Verizon's 2015 Data Breach Investigations Report, 60% of attackers were able to compromise their targeted information asset 'within minutes' and more than 90% within days. However, only around 25% of attacks were discovered within a similar timeframe. Mandiant's M-Trends 2015 report estimated that attackers were present on a victim network for a median of 205 days before being detected. This was an improvement on the previous year, when the median was 229 days.

A Ponemon Institute survey of 350 organisations in 11 countries, including 23 Australian organisations, found the average cost of a data breach for a local organisation was $2.82 million.[vii] In an earlier report, the Institute found that cybersecurity attacks took on average 27 days to resolve, once they had been detected, with an average cost of just over $500,000 during that time.[viii] Malicious insider attacks took 53 days, on average, to contain. The report showed that the faster an organisation resolved an incident, the less it cost overall.

The Ponemon Institute's Live Threat Intelligence Impact Report found that if organisations had actionable intelligence about cyberattacks within 60 seconds of a compromise, they could reduce the total cost of the breach by an average of 40 percent.[ix] As we will demonstrate later, this actionable intelligence could be as simple as knowing where your organisation stores its most valuable data.

CYBERCRIME AND CYBER-ESPIONAGE: A DOUBLE THREAT cont

SONY PICTURES ENTERTAINMENT: STATE-SPONSORED HACKING OR INSIDER ATTACK?

On 25 November 2014, details first emerged of a massively damaging cybersecurity breach at Sony Pictures Entertainment when a group calling itself Guardians of Peace posted four unreleased Sony films on several pirate websites. Over the following weeks, seven more data leaks revealed the vast and embarrassing extent of the breach.

The leaked details included:

- A list of the salaries of more than 6,000 employees, including executives and actors, which revealed marked gender and race gaps in employees' pay.[x]
- A spreadsheet listing the names, birth dates, and Social Security numbers of 3,803 employees, including all of the company's top executives.[xi]
- Another spreadsheet with names of employees who had been laid off in the past year, including reasons for their termination and performance reviews.
- Emails from senior executives, many of which were highly embarrassing to the studio, executives and other employees.[xii]
- Extensive details of the studio's computer networks including usernames, passwords, security tokens and certificates, instructions on accessing servers and lists of IT assets including network routers and switches.[xiii]

Very large numbers of computers across the studio's network were infected with ransomware that locked users out of their systems and malware that deleted the contents of PCs and servers containing the stolen data.[xiv] The studio was forced to take its entire computer network down, which significantly disrupted its business operations.[xv]

Reports quickly emerged that employees whose details had been released had fallen victim to credit card and identity fraud.[xvi] Former and current employees filed class-action lawsuits against Sony, alleging the studio was negligent because it didn't prepare for a large-scale cyber-attack despite previous breaches and warnings.[xvii]

After three weeks of investigation, US Federal Bureau of Investigation laid the blame for the attack on state-sponsored hackers from North Korea.[xviii] Several security researchers questioned the FBI's conclusion, noting that accessing and navigating certain systems within Sony's network would have required inside knowledge only available to employees.[xix]

Australia cannot be complacent

Unlike many overseas jurisdictions, Australia does not require businesses or government agencies to disclose if they suffer a data breach. Only 71 organisations voluntarily reported data breaches to the office of Privacy Commissioner Timothy Pilgrim in the 2013-14 financial year.[xx] The true number of incidents is likely to be much higher.

Under these circumstances, an organisation that suffers a breach might gamble it can get away with keeping things quiet. For example, online retailer Catch of the Day suffered a major data breach in 2011 but did not disclose this to customers or the Privacy Commissioner until 2014.[xxi]

We believe this legal and regulatory environment hides the extent of cybersecurity threats in this country. Further, it inhibits local organisations' ability to react to these threats. Organisations that underestimate the damage, business disruption, and financial costs they face will make poor investment decisions in technology, people, planning and breach insurance.

BREACHES ARE INEVITABLE ... NOW WHAT?

Gartner's bluntly titled report, Malware Is Already Inside Your Organization; Deal With It says "determined attackers can get malware into organisations at will".[xxii] It argues that "organisations must assume they are compromised, and, therefore, invest in detective capabilities that provide continuous monitoring for patterns and behaviours indicative of malicious intent".

If we cannot prevent malware from breaching perimeter security or information from leaking outside our virtual walls, how can we protect important, high-value and high-risk data in our care? It requires a change in mindset and a new set of disciplines around information security. This involves three core capabilities:

- Knowing where important data is stored, understanding what it's worth and making sure it's protected
- Reducing the delay between when breaches occur and when they are detected
- Conducting rapid, thorough and effective post-breach investigation and remediation.

One of the main reasons organisations take so long to detect and remediate breaches is they don't know where the high-value or high-risk data is stored, so they can't target those systems for investigation

Where is your data?

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

At its heart, this capability is an application of the classic information security triad:

- **Confidentiality.** Information is protected from being disclosed to people who should not see it.
- **Integrity.** Information cannot be modified by people who aren't authorised to do so.
- **Availability.** The right people can access information at the right time.

This is complicated by the fact that organisations store large volumes of unstructured data – typically 80% of the total – which is often in complex formats that are difficult to search and understand. To put it another way, you can't protect information if you don't know where it is and what's in it. It's also hard to decide how much to spend, or calculate the return on investment of security measures, if you don't know what the data is worth.

One of the main reasons organisations take so long to detect and remediate breaches is they don't know where the high-value or high-risk data is stored, so they can't target those systems for investigation. Instead, they must collect data widely, potentially including staff members' 'bring your own' laptops and other unmanaged locations, which takes time. Alternatively they can collect from a random sample of devices, which risks missing the compromised systems. Meanwhile the clock is ticking: data has gone missing, costs are building up and there is an ever-present risk that someone could exploit the same vulnerability again to do more damage.

THE 'GOOD SHEPHERD' MODEL

Thus information governance technologies become a powerful tool in reducing the costs and extent of cybersecurity breaches by delivering transparency into unstructured data and facts upon which security professionals can make informed decisions.

Information transparency can have huge impact on how secure your organisation is from data breaches and how effectively you can respond to incidents – internal or external, deliberate or accidental. It also gives you a clearer understanding of what data is worth so you can concentrate on protecting the high-value data and easily calculate the return on your security investments.

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

Organisations store large volumes of digital detritus – data that has no business value because it's duplicated, trivial, no longer used, past its retention period or potentially risky. While most organisations have strict compliance rules around how long they must retain data, once the retention period is over, the risks and costs it contains greatly outweigh any residual value. Deleting this low-value data, according to predefined and legally sanctioned rules, reduces risks and also minimises the volume of data that could be compromised. This in turn reduces the scope of a post-breach investigation.

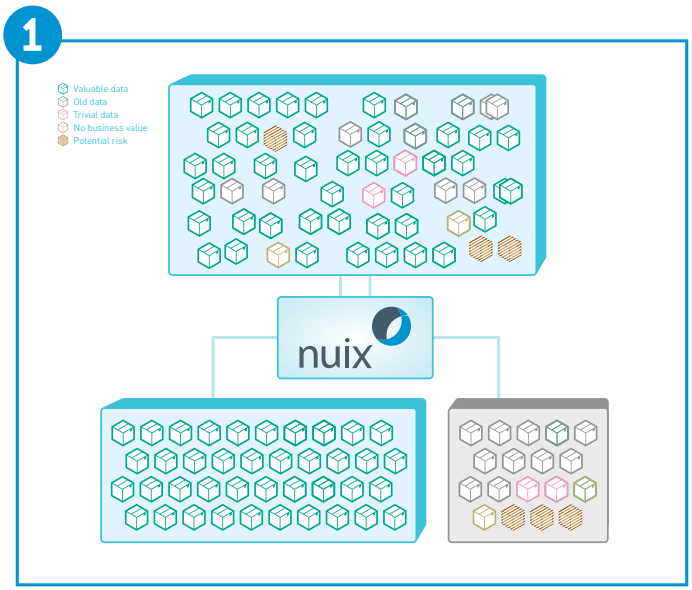

Fig 1: Deleting low-value data minimises risk and reduces the scope of post-breach investigations.

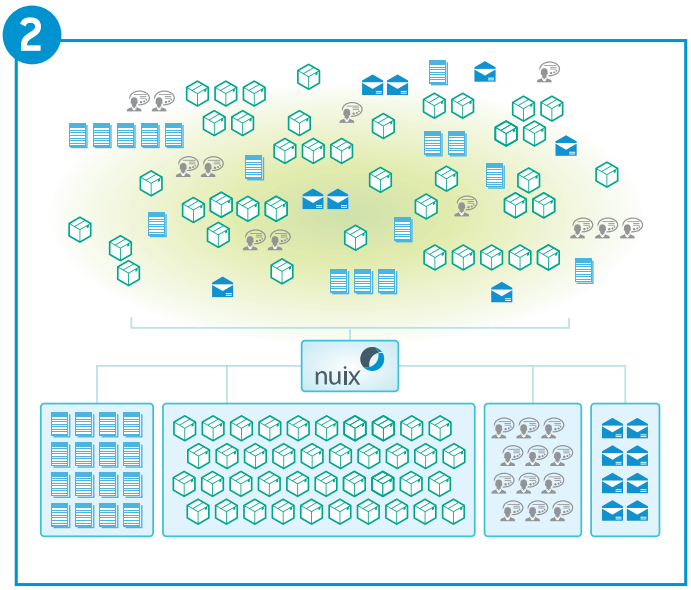

Fig 2: Locating records 'in the wild' makes high-value information less vulnerable to breaches.

2. Data herding

Organisations often have intellectual property and official records stored inappropriately in file shares, email attachments and employee-owned 'bring your own' laptops and mobile devices. Both records managers and end users struggle to find the time to ensure records are always filed correctly. Information governance technology can locate these records 'in the wild' and move them to controlled repositories with appropriate security, access controls and retention rules. This makes it much harder for anyone to gain unauthorised access.

3. Data security

Increasingly strict regulations around data privacy and financial information make it imperative to hold personal, financial and health details 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. And even if they dispose of this data correctly, it may still be retained in backups or archives.

By conducting regular sweeps of email, file shares and other unprotected systems, organisations can quickly locate and remediate unprotected private data. At the same time, understanding where this high-risk data is stored, organisations do not need to spend time and effort protecting data that doesn't need it.

4. Access controls

The key principle here is making sure the only people who can access high-risk data are those who need to for day-to-day work. This requires a combination of sound policy and constant vigilance. For example, many data loss incidents occur when a disgruntled employee leaves the organisation. By cancelling an employee's login and access credentials as soon as he or she leaves, this minimises opportunities for important information to go astray. (Nonetheless, it may be prudent to scan their recent emails for indications of company intellectual property or other important data).

It is also essential to regularly audit access controls on important systems and employees' security profiles to ensure the policy theory matches reality. For example, in one data breach investigation we worked on, employees had stumbled across a way they could 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.

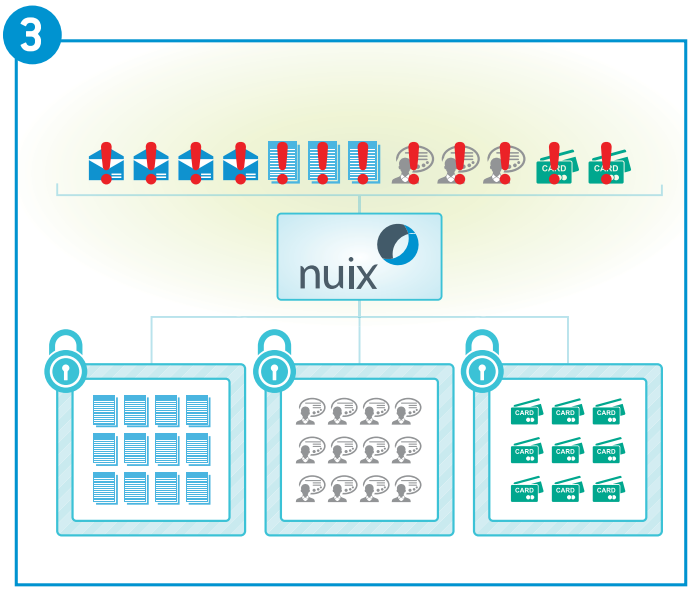

Fig 3: Keeping private, financial and health data within known, protected locations reduces business risks.

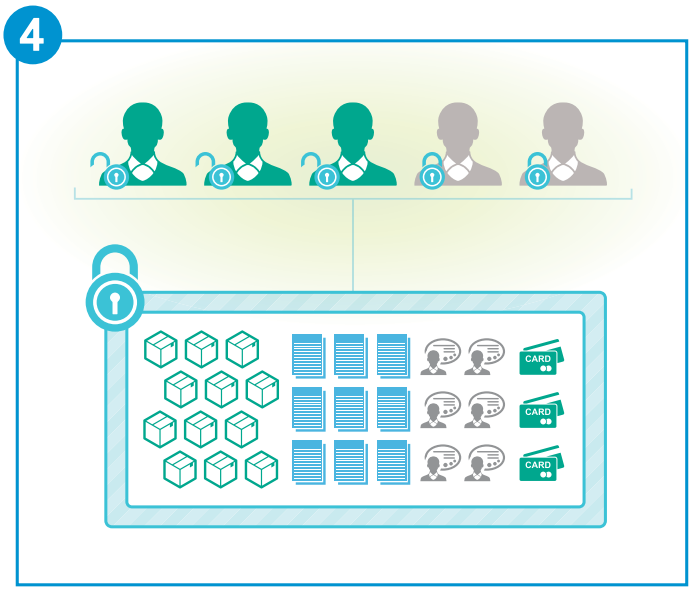

Fig 4: Regularly auditing access controls ensures security policy matches reality.

CASE STUDY

Investigating a datacentre breach the hard way

Nuix analysts worked with a major consulting firm to investigate a breach at a large datacentre. This firm 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 had to take some clients' servers offline and was losing money. And the incident was doing considerable damage to its reputation.

Realising 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 entities' 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 a signature of the attack 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 and were likely targets of the breach. 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.

These steps would have minimised the likelihood of future breaches and greatly reduced the time taken to locate them, protecting the firm's revenue and reputation.

A CHANGE OF MINDSET

While perimeter security defences remain essential, organisations must shift their information security mindset from 'How much do we have to spend to prevent breaches?' to 'How can we minimise the opportunities for breaches and the damage we suffer from them?' and 'How can we gain return on our security investments?'

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

- Know where important and high-risk data is stored and be confident it is only stored in those locations
- Minimise the opportunities for malicious and accidental breaches of important information
- Respond to breaches in a more targeted and effective way, by first targeting the high-risk storage locations and collecting much less peripheral data
- Close information security gaps quickly before they can be exploited again.

REFERENCES

i Verizon RISK Team, 2015 Data Breach Investigations Report, April 2015
ii Mandiant, M-Trends 2015: A View from the Front Lines, April 2015
iii Ken Westin, Stolen Target Credit Cards and the Black Market: How the digital underground works, Tripwire, December 2013
iv ABC News, China blamed after ASIO blueprints stolen in major cyber attack on Canberra HQ, 28 May 2013
v FireEye, WORLD WAR C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks, 2014
vi FireEye, APT 30 and the Mechanics of a Long Running Cyber Espionage Operation, April 2015
vii Ponemon Institute, 2015 Cost of Data Breach Study: Australia, May 2015
viii Ponemon Institute, 2013 Fourth Annual Cost of Cyber Crime Study: Global, October 2013
ix Ponemon Institute, Live Threat Intelligence Impact Report, July 2013
x Kevin Roose, Hacked documents reveal a Hollywood studio's stunning gender and race gap, Fusion.net, 1 December 2014
xi Kevin Roose, More from the Sony Pictures hack: budgets, layoffs, HR scripts, and 3,800 social security numbers, Fusion.net, 2 December 2014
xii Mark Seal, An Exclusive Look at Sony's Hacking Saga, Vanity Fair, March 2015
xiii Kim Zetter, Sony Got Hacked Hard: What We Know and Don't Know So Far, Wired, 3 December 2014
xiv Timothy Lee, The Sony hack: how it happened, who is responsible, and what we've learned, Vox, 17 December 2014
xv US Federal Bureau of Investigation, Update on Sony Investigation, 19 December 2014
xvi Mark Seal, op. cit.
xvii Ralph Ellis, Lawsuits say Sony Pictures should have expected security breach, CNN, 21 December 2014
xviii FBI, op. cit.
xix Jemima Kiss, Sony hack: sacked employees could be to blame, researchers claim, The Guardian, 31 December 2014
xx Office of the Australian Information Commission, Annual Report 2013–14, September 2014
xxi Ben Grubb, Catch of the Day caught out by hackers, Sydney Morning Herald, 21 July 2014
xxii Peter Firstbrook and Neil MacDonald, Malware Is Already Inside Your Organization; Deal With It, Gartner, February 2014

ABOUT THE AUTHORS

Stuart Clarke

Director of Cybersecurity and Investigation Services, Nuix

Stuart Clarke is an experienced consultant who has provided expert evidence in civil and criminal courts and across different jurisdictions including the Technology and Construction Court. Before joining Nuix, Stuart was Head of Forensics and Technical Operations at Millnet and previously Principal Consultant at PA Consulting Group (formally 7Safe). In these roles Stuart operated across digital forensics, eDiscovery and information security, and managed a diverse team of consultants.

Lee Meyrick

Director of Information Management, Nuix

Lee Meyrick has a decade of experience in data discovery, compliance planning and implementation. He advises organisations on eDiscovery techniques for retrieving information in unstructured data. Lee is an expert in the US Foreign Corrupt Practices Act, the UK Bribery Act and the discovery of risky data for remediation. He has also trained organisations on the use of Nuix for corporate investigations and eDiscovery.

Eddie Sheehy

Chief Executive Officer, Nuix

Eddie Sheehy has overseen Nuix's global expansion since the company commercialised its software in 2006. Eddie has been instrumental in securing public-sector and commercial customers across more than 45 countries, including law enforcement agencies, litigation support vendors, law firms, corporations, government agencies, and all the world's major corporate regulators and advisory firms. He has strategically guided the software's growing functionality from digital forensics to legal discovery, investigation, cybersecurity, information governance, and privacy.

To find out more about Nuix's cybersecurity solutions visit

nuix.com/cybersecurity

ABOUT NUIX

Nuix enables people to make fact-based decisions from unstructured data. The patented Nuix Engine makes small work of large and complex human-generated data sets. Organisations around the world turn to Nuix software when they need fast, accurate answers for digital investigation, cybersecurity, eDiscovery, information governance, email migration, privacy and more.

North America
USA: +1 877 470 6849
» Email: sales@nuix.com

EMEA
UK: +44 203 786 3160
» Web: nuix.com

APAC
Australia: +61 2 9280 0699
» Twitter: @nuix

nuix

CY1506UK1