Submission to the Serious Data Breach Notification Consultation

(Consultation closes 4 March 2016 — please send electronic submissions to privacy.consultation@ag.gov.au)

Your details

Name/organisation *(if you are providing a submission on behalf of an organisation, please provide the name of a contact person)*	Nuix Pty Ltd
Contact details *(one or all of the following: postal address, email address or phone number)*	Carolyn Betts Head of Government Relations

Publication of submissions

In meeting the Australian Government's commitment to enhancing the accessibility of published material, the Attorney-General's Department will only publish submissions to this website that have been submitted electronically.

Our preference is that submitters complete this template and send it to privacy.consultation@ag.gov.au.

However, if submitters choose to provide a separate document, the following formats are preferred:

- Microsoft Word
- Rich Text Format (RTF)
- txt format.

Please limit individual file size to less than 5MB. The department may create PDF documents from the above formats.

The department will still consider hardcopy submissions received by mail, but these submissions will not be published on the website.

Confidentiality

Submissions received may be made public on the Attorney-General's Department website unless otherwise specified. Submitters should indicate whether any part of the content should not be disclosed to the public. Where confidentiality is requested, submitters are encouraged to provide a public version that can be made available.

Would you prefer this submission to remain confidential? YES / NO

Your submission

Prepared by

Chris Pogue, Senior Vice President, Cyber Threat Analysis

Eddie Sheehy, Chief Executive Officer

Carolyn Betts, Head of Government Relations

Nuix Pty Ltd

2 March 2016

Executive summary

Mandatory data breach laws will address a major problem in Australia; while organisations are aware of cybersecurity threats, most do not take the problem seriously. In addition, as a nation we lack the in-depth skills required to get on top of cybersecurity threats and at present there is no pathway to improve these skills.

Nuix supports a clearly defined and uniform national breach notification scheme to avoid loopholes and legal ambiguities that would divert organisations' resources from fixing the problems to complying with laws, or worse, circumventing them. However, merely complying with the minimum requirements of the law has proven ineffective in protecting critical value data. Australian businesses and government agencies must do more to improve our national cybersecurity capability.

For these reasons, we recommend a program of incentives that would encourage organisations to follow the legislated process. These incentives would help offset the costs of post-breach activities that would help a breached organisation improve its cybersecurity posture; such as investigating and remediating the incident, conducting security posture assessments, designing and implementing cybersecurity strategies, and providing training on cybersecurity awareness and defence.

By raising these capabilities, the Australian Government can contribute to the safe, secure digital infrastructure that is the necessary foundation for an innovation economy.

Nuix enthusiastically offers our Australian-developed technology and global expertise to help the Government build up our national cybersecurity capability.

Contents

Breach notification must be mandatory and universal

Nuix congratulates the Australian Government on drafting the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 to enact a mandatory notification regime for serious data breaches. We understand that legislating in this area is difficult because there are no painless solutions. We strongly favour a mandatory breach notification scheme with as few exceptions as practical.

In 2014-15, only 110 Australian organisations voluntarily reported data breaches to the privacy regulator. However, one recent study estimated the probability that an organisation would suffer a breach of more than 10,000 records over a period of 24 months was 22% globally and 17% in Australia.[i] Thus there can be no doubt a much larger number of Australian organisations suffered data breaches but did not announce them. In our experience, sectors such as financial services view data breaches as simply a cost of doing business.

Our current system engenders a false sense of security by perpetuating the misconception that Australian businesses are not being targeted by cybercriminals. As a result, Australia lacks the depth of understanding we need to address the vast majority of cybersecurity issues. Most Australian organisations have an unrealistic view of the modern threat landscape and do very little to address cybersecurity. In our experience, many of them avoid even testing their cybersecurity posture because they believe they will fail and they lack the depth of skill to fix the problems.

The cybersecurity skills gap is an issue worldwide, but it seems to be worse here because we also lack a pathway within our higher education institutions for people who want to develop those skills to learn from industry experts. As a result, organisations have to import expertise and labour from overseas at great expense. Australia, while rated highly, is falling behind other countries in its cybersecurity maturity.[ii]

Enacting a uniform national notification scheme avoids the complications that have arisen in other jurisdictions. For example, organisations in the United States must deal with 47 different state-based breach notification laws – and failure to comply in any of those jurisdictions may lead to litigation and regulatory action. Breach notification laws in Europe are also diverse, although they will be unified under the European Union General Data Protection Regulation by 2018.

Overcomplicated legislation and regulation diverts resources from fixing the problems to complying with laws. A salient example is the lawsuit between the US Federal Trade Commission and the Wyndham Hotels group, which lost 600,000 customer records from 2008 to 2009. It took from 2012 to August 2015 for the appeals court to rule that the FTC had the authority to bring the suit. The original case is now under litigation..

For these reasons, we believe Australia's legislation must avoid caveats, exemptions and vague terms that create loopholes that benefit no-one but lawyers. Cybercriminals and cyberspies don't respect geographical borders or public–private–individual distinctions. To establish an appropriate and reasonable response capability that matches the current threat landscape, neither should our approach to cybersecurity.

Nuix recommendation: the stick is important, but so is the carrot

A mandatory notification scheme that relies solely on penalties to ensure compliance is unlikely to succeed. An organisation having suffered a data breach may well decide it is cheaper to pay a fine than suffer the losses of complying with the rules and disclosing the breach. Or the organisation may comply with the bare minimum required by law and then consider the matter settled, having established a legally defensible position of having taken reasonable action.

To achieve the ultimate goal of strengthening Australia's cybersecurity defences, government could provide incentives for organisations that follow the legislated process—and ensure these incentives contribute towards building national cybersecurity capability.

Incentives for breach notification

Such incentives might include subsidising or covering the costs of activities that improve the organisation's cybersecurity posture, such as:

- **Investigating and remediating** the data breach, and remediating any gaps in security defences that might be exploited again
- Conducting a complete **security posture assessment** that proactively identifies security weaknesses and provides practical advice about deflecting, detecting, and responding to cyberattacks.
- Implementing a **cybersecurity strategy**, based on the results of a posture assessment, that makes the organisation a smaller target for cybercriminals
- Providing **training** on cybersecurity awareness, countermeasures, analysis and investigation.

Cybersecurity strategy

In previous submissions to government on this issue, we have recommended the government develop a baseline cybersecurity strategy organisations could turn to when seeking to make themselves smaller targets for cybercriminals.[iii] An organisation seeking to develop a strategy should start by honestly assessing its current security posture, then creating a plan to improve it and to educate every employee on the role they can play in organisation's defences.

This strategy should include elements such as:

- **Identifying critical data and systems**, restricting access to them and understanding what people do with that data when they access it
- **Maintaining proper IT hygiene**, for example tracking down and removing copies of critical data stored in an unsecure location, or quickly removing access to critical data once employees leave the organisation
- Conducting regular **active penetration testing**, not just vulnerability scanning, and other advanced attack simulations to identify flaws in the organisation's security posture
- Acquiring **adaptive security technologies** that enhance the security of all devices that connect to the network, and provide a reliable real-time source of **threat intelligence**
- Creating detailed organisation-wide plans for **managing insider threats** and **responding to data**

breaches

- **Educating people** not to open unknown links or open files and making them aware of social engineering techniques – which target even small organisations.

Cybersecurity education

A typical education campaign might include:

- **Cybersecurity awareness** for all employees
- Basic **cybersecurity defence and countermeasures** for a targeted number of employees (perhaps 10% of the total)
- Intermediate cybersecurity investigation and analysis for 50% of IT staff
- **Advanced cybersecurity investigation and analysis** (such as Nuix's Hack It and Track It) for the top 5% of IT staff.

A cybersecurity awareness campaign should show people that their individual actions can have a global impact. It should cover basic IT hygiene – don't open unsolicited attachments or links – and examples of social engineering techniques.

Raise expectations

Prime Minister Malcolm Turnbull has expressed a strong desire for Australia to build a smart and agile innovation-based economy.[iv] In the same way that a peaceful, democratic and non-corrupt country leads to economic improvement, a safe, secure digital infrastructure will underpin an innovation economy.

As a country, we already have form in developing innovative cybersecurity policy and strategy. The Australian Signals Directorate's *Top four mitigation strategies to protect your ICT system*[v] is recognised worldwide as best practice for minimising the threat of data breaches.

There is an opportunity to recognise that cybersecurity is not just a business **problem** but also a business **opportunity**. By defining it this way, our government can raise expectations of what individuals, employees and the private and public sectors can do to improve cybersecurity. This would have three drivers or motivators:

- **National pride** – this approach to cybersecurity is something uniquely Australian and we are taking a leading role in the world.
- **Doing the right thing** – cybercriminals are a serious threat to the economy and national security.
- **Being part of the solution** – I can do things to make the problem better.

What Nuix has to offer

Nuix is excited to offer assistance to the Australian Government to help build up our national cybersecurity capability. We have an Australian-developed technology backed up by a global team of experts in digital forensics, incident response, penetration testing, security posture assessment, threat intelligence, counterintelligence, cybersecurity training and security strategy. We also have a strong local customer base, including a large number of Australian Government agencies.

We offer our expertise to help the nation and the region. We can help Australia grow a cybersecurity service industry that uses software such as ours in conjunction with industry standards, best practices and advanced countermeasures. Our assets include:

- Data from dealing with two decades of breaches
- Knowledge of industry leading security experts
- Teams of security and vulnerability researchers
- Capability to emulate threat scenarios
- An unmatched, supercharged, engine
- A marquee customer base – including government, corporate and advisory organisations – in more than 60 countries
- The ability to change the way security is viewed and approached for the next 20 years.

We have expert staff in Australia, the United States and the United Kingdom who could help Australian businesses and government agencies enhance their skills. Our staff already works with law enforcement and intelligence agencies in the US and the UK, offering skills transfer and force augmentation in:

- Basic, intermediate and advanced training
- Penetration testing and security posture assessment
- Malware analysis and reverse engineering
- Digital forensic and incident response
- Code review
- Security strategy development.

Our industry-leading investigation and incident response software is used to examine and remediate high-profile data breaches around the world. We are also developing:

- **Adaptive security** software to protect endpoints such as desktop computers from exploits and malware by blocking activity at the kernel level based on its behaviour, intelligence about common attack strategies and real-time awareness of activity across the network to stop malicious activity at the earliest stages.
- A **security intelligence and analysis** platform that searches from the binary level to the largest enterprise systems, from historical data to real-time feeds, to identify hidden relationships, reveal potential threats, catch malicious activity before it matters, and take decisive action to remediate it.

Next steps

We would be delighted to further discuss the contents of this paper with you. We hope the ideas we have presented are helpful in finalising the data breach notification laws.

For more information, please contact Carolyn Betts, Head of Government Relations, carolyn@nuix.com, 0418 487 469.

About the authors

Chris Pogue

Senior Vice President of Cyber Threat Analysis

Chris Pogue has investigated more than 2,500 breaches across the globe. Prior to joining Nuix in June 2014, he spent six years at SpiderLabs where worked as an incident responder, managing consultant, and director. He was previously an engagement manager at the IBM/ISS X-Force incident response and penetration testing teams. Before joining the private sector, Chris served in the United States Army for 13 years as a Signal Corps Warrant Officer and Field Artillery reconnaissance Sergeant.

Chris was the original creator of the Sniper

Eddie Sheehy

Chief Executive Officer

Eddie Sheehy has been CEO of Nuix since 2006. He has overseen the company's global expansion since the commercialisation of its software after seven years of research and development.

Eddie has been instrumental in securing public-sector and commercial customers across more than 60 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

Carolyn Betts

Global Head of Government Relations

Carolyn is responsible for Nuix's government relations and global marketing strategy and operations.

Prior to joining Nuix in 2007 Carolyn held executive positions in media, telecommunications and resources companies and was on the personal staff of two Australian federal government cabinet ministers.

As part of the Nuix global leadership team, Carolyn is driving the company's strategy to raise awareness in Australia about the problems and risks of cybersecurity and engaging

Forensics methodology, which has emerged as the industry standard among investigative agencies including the Federal Bureau of Investigation and the United States Secret Service. In 2010, he was the 41st security professional to be named as a SANS Thought Leader.	forensics to legal discovery, investigation, cybersecurity, information governance, email migration, and privacy Born and educated in Ireland, Eddie has two decades of experience working for and managing finance, technology, and legal technology companies.	with industry and government to contribute to the solution.

References

[i] Ponemon Institute (sponsored by IBM), *2015 Cost of Data Breach Study: Global Analysis*, May 2015
[ii] Tobias Feakin, Jessica Woodall, Liam Nevill, *Cyber Maturity in the Asia–Pacific Region 2015*, Australian Strategic Policy Institute, October 2015
[iii] This strategy is detailed in our submission to the Australian Government's Cyber Security Review
[iv] Peter Bradd, "Malcolm Turnbull's vision to rejuvenate innovation", *The Australian*, 22 September 2015
[v] Australian Signals Directorate, *Top four mitigation strategies to protect your ICT system*, October 2012