Privacy Commissioner
Te Mana Mātāpono Matatapu

Testers as agents of TRUST

GOVIS Test Meetup

July 2024

Testers have a critical role in protecting our most valuable asset: personal information

What is at stake?

Loot from NZ ransomware attack being sold on dark web

Latitude makes $105 million first-half loss after devastating cyberattack

Privacy Commission says Latitude cyber attackers got away with data on 20% of the population

WEEK

CYBERCRIME

New Zealand Government Hit by Ransomware Attack on IT Provider

The New Zealand government this week confirmed being impacted by a ransomware attack on managed service provider (MSP) Mercury IT, which has disrupted businesses and public authorities in the country.

" business with only 25 employees, Mercury IT
arsecurity, IT, telecoms, and support services
rations in the country.

Massey University forced to cancel online exams due to technical probl

2:23 pm on 12 June 2024

Share this

John Gerritsen, Education correspondent
@RNZeducation john.gerritsen@rnz.co.nz

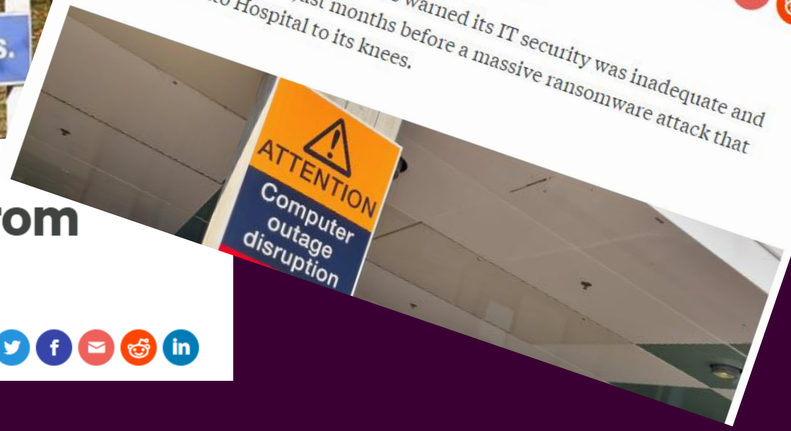
Waikato DHB warned a cyberattack 'catastrophic for patient safety'

9:21 am on 12 November 2021

Natalie Akoorie, LDR Editor
@NatalieAkoorie natalie.akoorie@rnz.co.nz

Share this

Waikato District Health Board was warned its IT security was inadequate and severely compromised just months before a massive ransomware attack that brought Waikato Hospital to its knees.



NEW ZEALAND / MONEY

Scammers took almost $200m from Kiwis last year - report

9:45 am on 13 November 2023

Share this

Poupou Matatapu: Doing Privacy Well

- Governance
- Know your personal information
- Security and Internal Access Controls
- Managing requests and complaints well
- Transparency
- Breach Management
- Building Capability and Awareness
- Assessing Risk
- Measuring and monitoring

Information privacy principle 5

Storage and security of personal information

An agency that holds personal information must ensure—

(a) that the information is protected, by such security safeguards as are reasonable in the circumstances to take, against—

(i) loss; and

(ii) access, use, modification, or disclosure that is not authorised by the agency; and

(iii) other misuse; and

(b) that, if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

121 Knowledge of officers, employees, agents, and members of agencies to be treated as knowledge of employers, principal agencies, and agencies

(1) Subsection (2) applies to processes and proceedings under this Act relating to the obligations under section 114 or 115.

(2) Anything relating to a notifiable privacy breach that is known by an officer, an employee, or a member of an agency is to be treated as being known by the employer or agency.

(3) Subsection (4) applies to processes and proceedings under this Act relating to the obligations under section 114 or 115 except a proceeding under section 118.

(4) Anything relating to a notifiable privacy breach that is known by an agent is to be treated as being known by the principal agency.

Why testing matters?

Testing systems with real data leads to breach

Sometimes it seems a good idea to use real production data in a test environment. But doing so means security becomes even more important if you want to stop things going wrong.

When testing a new system, it is always tempting to use a copy of real data from your existing system. The data is readily available, it has the variety of records needed, and it exists in a volume large enough to make it convenient for testing.

But in Britain a few years ago, the parenting retailer Kiddicare admitted the personal information of 794,000 people had been exposed on a version of its website set up for testing purposes and the incident has underlined the dangers of using real personal information.

The Kiddicare breach came to light after some customers reported receiving text messages that appeared to come from a subsidiary website of Kiddicare.com. A security company found the mobile phone numbers had come from a dataset used on a test website in November 2015. The messages invited Kiddicare customers to take an online survey - a tool often used by scammers to cheat people into signing up for fake schemes.

Close to home, we know of two other data breach 'near misses' which are examples of how using real data for testing a new system or website can be a risky thing to do.

In both cases, software developers took copies of their client organisations' data back to their own offices to use for testing. In one case, the software developer's own system was hacked and the organisation's data could have been exposed. In the other, the developer forgot to delete the data before uploading the software they had written (and the data!) to a public website.

Fortunately, neither of these incidents resulted in the sort of harm that flowed from the Kiddicare breach.

For this reason, it's usually much safer to generate fake data for testing purposes – just in case. The best practice for software testers is always to mask or transform the data in some way so that personal information cannot be exposed inappropriately and accidentally.

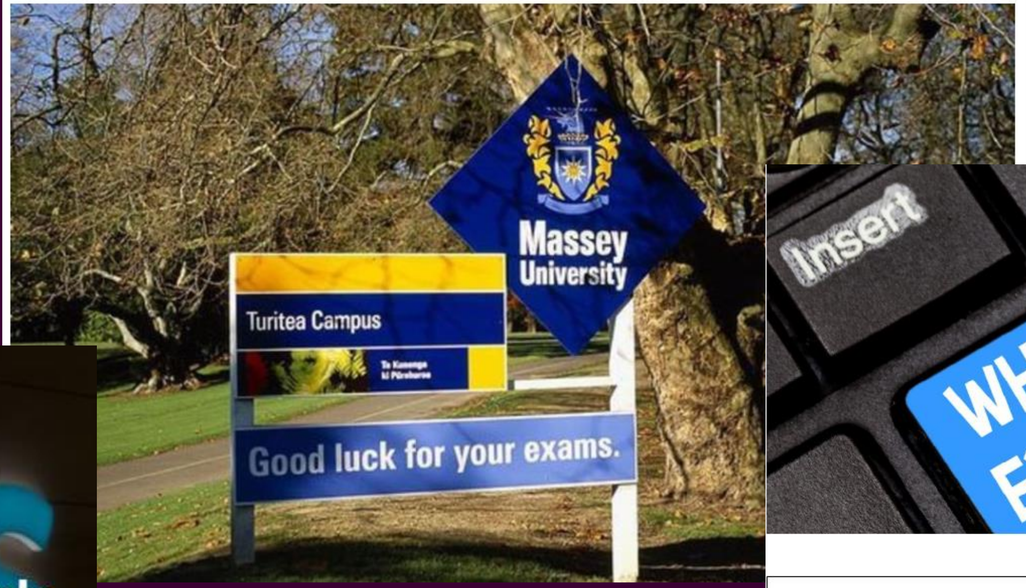
Why testing matters?

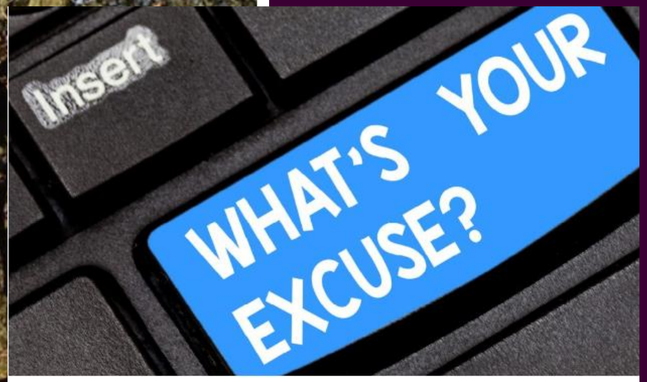
Massey University forced to cancel online exams due to technical problems

2:23 pm on 12 June 2024

Share this

John Gerritsen, Education correspondent
@RNZeducation john.gerritsen@rnz.co.nz





NZ: Massey University Experiences Serious Breach Of Security

Posted on March 31, 2009 by Dissent

The Massey University intranet system utilised by students from all across New Zealand, MyMassey, is under scrutiny after a severe breach of security left thousands of students able to access other people's highly sensitive information.

Rawa Karetai, President of the Albany Students' Association, was one of the first students to notice this critical error: "I was first made aware that the website www.mymassey.com started giving out personal information about other students at about 10.40pm. I immediately went and found a computer that was free and started to check to see if I was experiencing the same issues."

Karetai, like many other students, now had access to a variety of highly sensitive personal information that was not his own. Information at his disposal included, but was not limited to, the following: Massey ID numbers; Full names; Date of Birth; IRD Number; Academic transcripts as well as contact addresses and phone numbers. Students who had discovered this fault were also able sign the person whose information they could now access up for new papers or amend any of their contact details.

Read more on voxy.co.nz

Tester as vector for data breach

Ask yourself this question:

If we had a data breach could we prove that we have taken all reasonable steps to care for and protect the data that we hold or protect for others?

Poupou Matatapu: Doing Privacy Well

- Governance
- Know your personal information
- Security and Internal Access Controls
- Managing requests and complaints well
- Transparency
- Breach Management
- Building Capability and Awareness
- Assessing Risk
- Measuring and monitoring

Thanks!!

Privacy Commissioner
Te Mana Mātāpono Matatapu