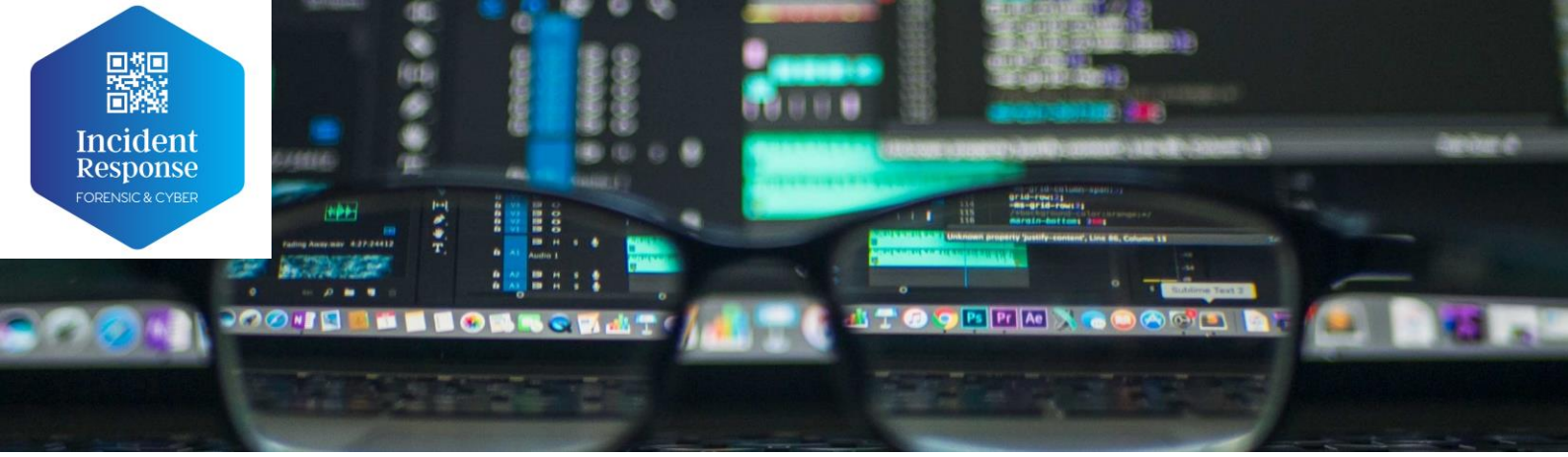


# NZ Incident Response Bulletin

April 2019

## In this issue:



## News:

*A high-level executive summary containing some of the most important news articles that have been published on Forensic and Cyber Security matters during the last month.*

### New Zealand

Commissioner Welcomes Select Committee's Privacy Bill Report

On 13 March 2019, the Justice Select Committee released its report on the Privacy Bill which New Zealand's Privacy Commissioner John Edwards has welcomed. *"The Committee has listened to submitters and the reported back Bill contains measures to ensure the law addresses some of the most pressing aspects of the modern digital economy".*

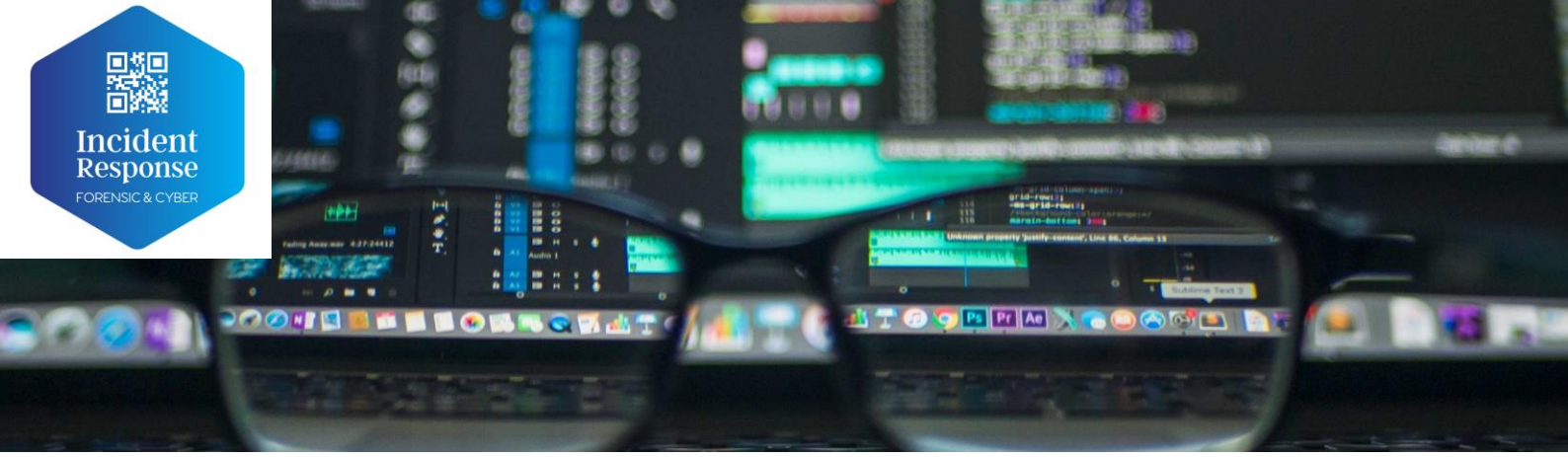
The Bill now clarifies the extent to which the Privacy Act will apply to overseas agencies or overseas activities:

- For a New Zealand agency, the Act will apply to any action taken and all personal information collected or held by it, both inside and outside New Zealand.
- For an overseas agency, the Privacy Act will apply if the agency is carrying on business in New Zealand. The Act will apply to any action and all personal information collected or held by the agency (regardless of where that may be) in the course of carrying on business in New Zealand.

Other key changes made during the select committee process include:

- Raising the notification threshold for privacy breaches so that notification is only required where the breach has caused, or is likely to cause, serious harm to affected people. Criteria are given for assessing whether or not serious harm has, or is likely, to occur.
- Expressly providing that agencies may not require a person's identifying information unless it is necessary for the lawful purpose for which the information is collected

Read the Select Committee report here.



# NZ Incident Response Bulletin

April 2019

[The Department of Internal Affairs – Response to the Christchurch terrorism attack video]

The Department has deemed the video file depicting the terrorist attack in Christchurch as being an objectionable publication under the Films, Videos, and Publications Classification Act 1993. The Department:

- Acted swiftly on Friday 15 March 2019 in its consideration of the video and issued a press release informing members of the public that it was likely to be objectionable and an offence to watch, share and/or possess.
- Has provided ISPs with information relevant to the hosting of objectionable material.
- Has been working closely with national and international stakeholders and law enforcement agencies to stop footage of the Christchurch attack from being circulated and further disseminated.

Prosecutions have been brought against people who have shared, distributed or possessed terrorism related and other objectionable material publications under the Act. The New Zealand Police are currently undertaking prosecutions regarding offences involving this video file. The Department will likely be progressing prosecutions under the Act and will consider these on a case by case basis.

## World

[Hackers Hijacked ASUS Live Update Utility to Install Backdoors]

According to security researchers at the threat intelligence firm Kaspersky Lab, hackers conducted a targeted malware attack on Asus customers, resulting in the installation of backdoors into thousands of Asus computers using the company's own software update platform. This attack is known as a 'Watering Hole' and was used in several recent big incidents including the NotPetya and the CCleaner compromises. Asus has released a diagnostic tool on its website for its users.

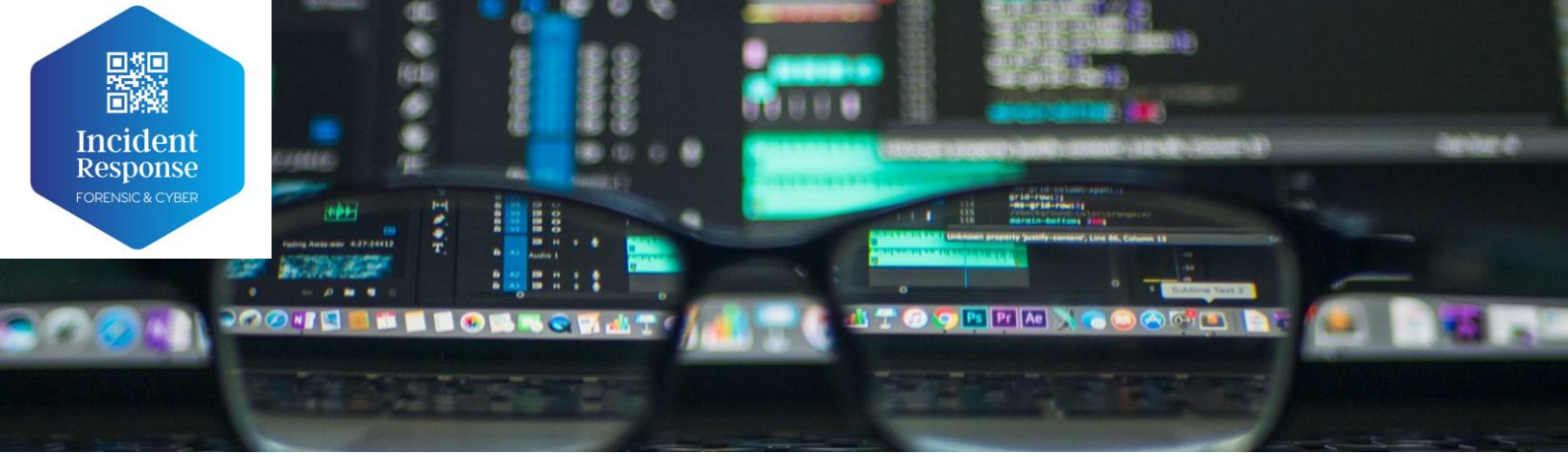
[UK Forensic Science Regulator calls for statutory enforcement powers]
The UK's Forensic Science Regulator (FSR) has reiterated calls for statutory enforcement powers to ensure forensic providers and police forces in England and Wales meet quality standards.

The FSR has urged the Home Office to put forward legislation to enforce quality standards. According to the FSR's annual report, dozens of police forces across England and Wales are making improvements in various areas of forensic science, including fingerprint comparison and areas such as crime scene examination and the extraction of data from digital devices.

However, both commercial forensic science providers and police forces in England and Wales are under financial strain, which represents a risk to the quality and sustainability of their work. In digital forensics, there are reports of police dropping cases because digital evidence is not available.

## Upcoming Events:

| Date | Event | Location |
|---|---|---|
| 3 May 2019 | ASIS New Zealand Women in Security 2019 | Wellington |
| 3-5 July 2019 | Australasian Conference on Information Security and Privacy (ACISP) | Christchurch |
| 11-13 September 2019 | ISACA 2019 Oceania CACS Conference | Auckland |



# NZ Incident Response Bulletin

April 2019

## Our Views:

*A selection of issues relevant to Forensic and Cyber Security matters during the last month. This month's theme is "Safety on Social Media".*

### Social Media - Privacy

Individuals should exercise caution when using social media. If you receive an invite from someone you don't know, check they are who they say they are. You should also think about your digital footprint, i.e. the entirety of information that you post including photos, comments and updates. Criminals conduct reconnaissance on your profile in order to launch targeted attacks.

The following lists the privacy and safety settings for each of the major social media platforms.

| | | |
|---|---|---|
| Facebook | Twitter | YouTube |
| LinkedIn | Instagram | Snapchat |

### Social Media – Harmful Content

It has been widely reported that New Zealand has experienced a surge in complaints relating to Harmful Digital Communications this month. The Harmful Digital Communications Act 2015 (the Act) aims to prevent and reduce the impact of online bullying, harassment.

Harmful digital communications include messages sent via various electronic formats such as email, apps and social media, which contain threatening or degrading material. A digital communication may be deemed harmful if it:

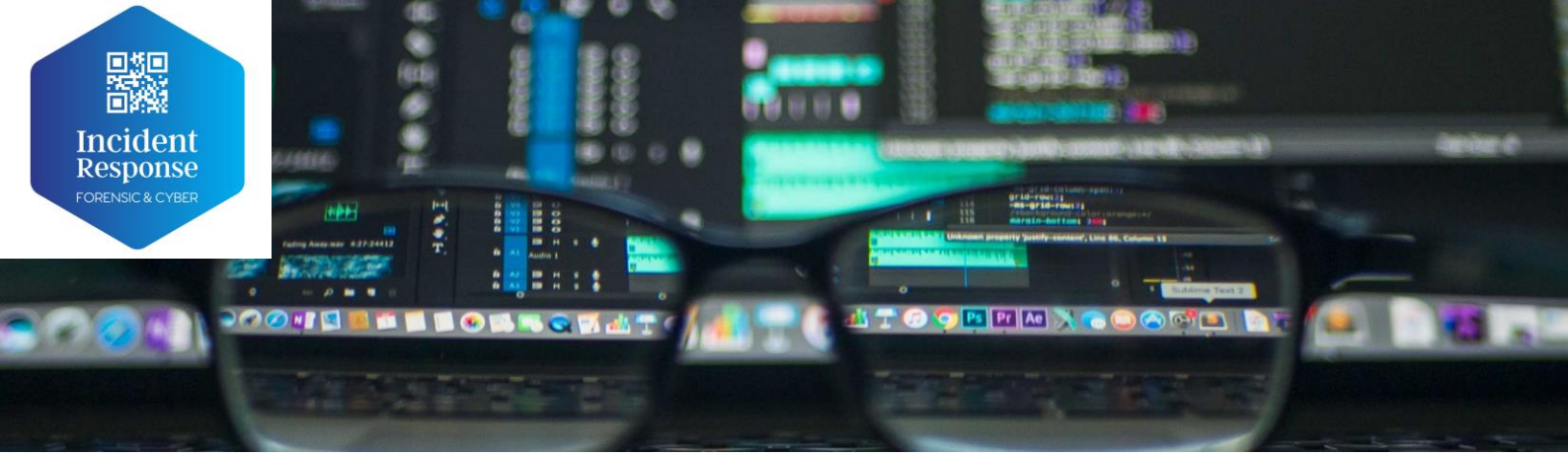
1. Is directed at an individual; and
2. Makes that person seriously emotionally distressed; and
3. It has or could seriously breach of one or more of the 10 communication principles in the Act.

Netsafe is the agency tasked with handling complaints and informs people about their options to remedy the situation. If you need support or assistance, more information is available on this website.

### Social Media – Reporting Content

The DIA has deemed the video file depicting the terrorist attack in Christchurch as being an objectionable publication. If you come across any the video please delete it or report it appropriately to the Censorship Compliance Team at the DIA here.

You can also report content directly to the websites, including Facebook and YouTube.



# NZ Incident Response Bulletin

April 2019

## About the Bulletin:

The NZ Incident Response Bulletin is a monthly high-level executive summary containing some of the most important news articles that have been published on Forensic and Cyber Security matters during the last month. Also included are articles written by Incident Response Solutions, covering topical matters. Each article contains a brief summary and if possible, includes a linked reference on the web for detailed information. The purpose of this resource is to assist Executives in keeping up to date from a high-level perspective with a sample of the latest Forensic and Cyber Security news.

To subscribe or to submit a contribution for an upcoming Bulletin, please either visit https://incidentresponse.co.nz/bulletin or send an email to bulletin@incidentresponse.co.nz with the subject line either "Subscribe", "Unsubscribe", or if you think there is something worth reporting, "Contribution", along with the Webpage or URL in the contents. Access our Privacy Policy.

## Share our Bulletin:

## About Incident Response Solutions Limited:

Our Purpose - We help you with specialist forensic, cyber security and crisis management expertise at all stages throughout the incident response lifecycle.

Our Promise - We will provide you with the confidence you require to prepare, respond and recover from forensic and cyber incidents.

Our specialist Forensic Technology expertise includes Computer Forensics, Cybercrime Incident Response, Social Media Analysis and eDiscovery. We have significant experience in providing expert witness reports and in delivering expert witness testimony at trial. Our background includes experience in Law Enforcement (NZ Police) and Big 4 Professional Services.

**Campbell McKenzie**
Director
Incident Response Solutions Limited
+64 9 363 7910
+64 21 779 310
campbell@incidentresponse.co.nz