INCIDENT RESPONSE SOLUTIONS

We help you Prepare, Respond and Recover from Forensic and Cyber Incidents

"Until you have experienced something like this, you don't realise just what can happen, just how serious it can be. I had no intuitive idea on how to move forward."

Maersk CEO Soren Skou on how to survive a cyber-attack
Financial Times, 14th August 2017

https://commons.wikimedia.org/w/index.php?curid=63512816

On 27 June 2017, Maersk staff saw "repairing file system on C:" or "oops, your important files are encrypted" on their screens, **demanding a payment** of $300 worth of bitcoin to **decrypt** each computer. The firm had just become a **victim** of the NotPetya campaign.

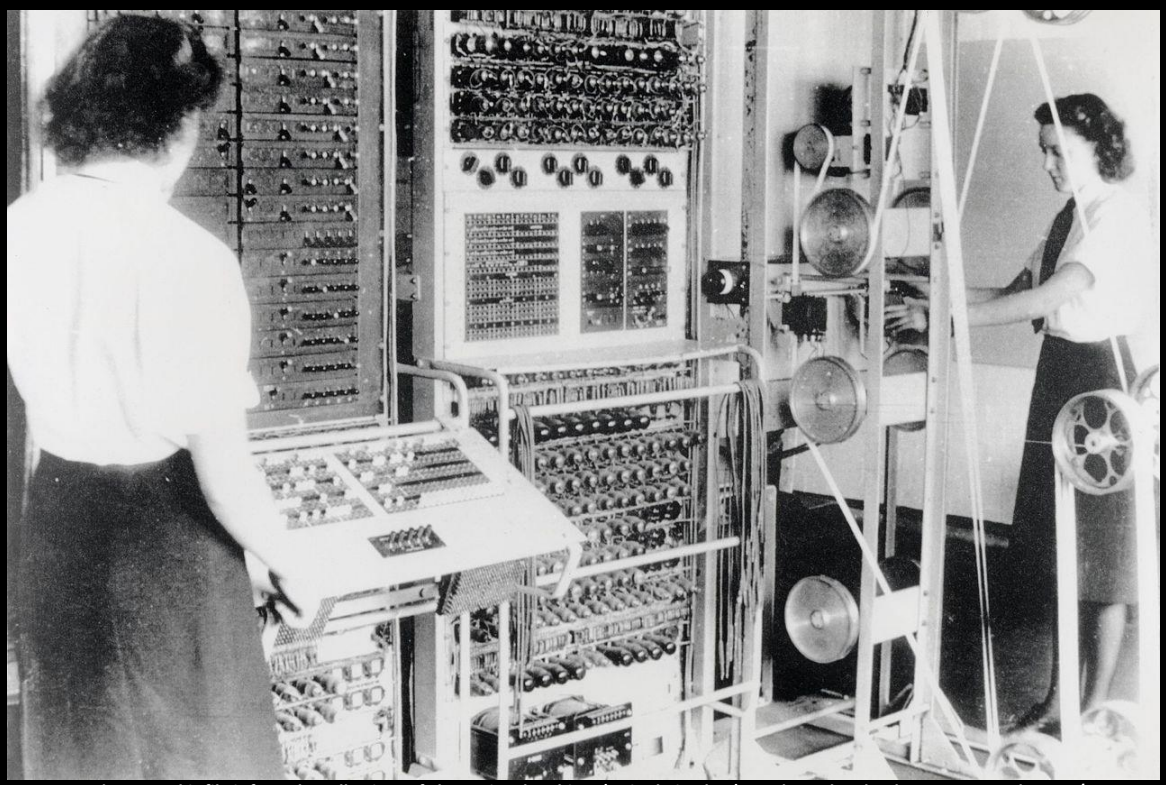
Only weeks earlier, this same exploit was used to spread WannaCry, which caused large-scale **disruption** to healthcare systems including the UK's National Health Service (NHS).

New Zealand **did not escape** the fallout resulting from these cyber-attacks.

THE PROBLEM IS NOT NEW

Encrypted electronic communications were used by the German High Command during World War II.

The Allies at Bletchley Park pioneered computer systems to successfully decrypt a vast number of these communications thereby reducing the duration of the war and saving countless lives.



By Unknown - This file is from the collections of The National Archives (United Kingdom), catalogued under document record FO850/234

About us

When faced with a problem requiring **Forensic Technology** or **Cyber Security** expertise, Incident Response Solutions helps turn your uncertainties into positive outcomes.

We help you **uplift** your capability, reduce your risk and immediately respond to actual events.

The core of our business is to provide the confidence you require to prepare for, respond to and recover from incidents, to a **Forensic** standard, i.e. the highest level of proof. We strive to make you look good, even in times of crisis.

We are **Forensic** and **Cyber** experts, with many years of proven experience.

Our wider network of experts is vast; whether you require a lawyer who specialises in cyber breaches or privacy, a public relations firm, or an introduction to the right technology vendor to solve your problem, we can help you in your time of need.

The result? Everyone is more **productive**, **less stressed**, and just a little **happier**.

Our technology

Whether an employee has **stolen your intellectual property** (IP), or your information systems have **suffered a cyber-attack**, we can assist.

We combine leading **forensic** and **cyber security** tools and technologies, along with our knowledge and experience of responding to incidents, to achieve the results you require. Our experts have solved numerous cases and are happy to share what has worked well.

Technology is also the key to updating all interested parties throughout an incident. We combine tools which specialise in **collaboration**, **automation** and **operations** to deliver you a seamless experience. From your phone call to us at 5 p.m. on a Friday, through to resolution.

What about data security? Well we certainly won't be transferring any data on an unencrypted USB stick! We offer you the choice to host your data in leading Tier 3 data centres, and we will also **encrypt** data in accordance with your policy and best practice.

How we help you

We can help you at any stage during your time of need. As there is no magic formula for technology, we've made it a little easier for you by creating this handy little guide to help us explain…

PREPARE

Strategy and plans

We develop and improve **incident response plans,** we can also help with your security strategy and policies.

Testing through simulations

Using forensic and cyber experts, we facilitate robust **tabletop exercises** to test and **improve** your incident response plan.

Panel of experts

We establish a suitable panel of **experts** including a breach coach, forensic, security, legal and public relations specialists who are **ready to assist** in your time of need.

RESPOND

Forensic technology expert witness

We have significant experience in providing **expert witness** reports and in delivering expert witness testimony at trial.

Electronic investigations and eDiscovery

We love finding needles in haystacks, using our **analytical** and **investigative** techniques to a **Forensic** standard. Our **eDiscovery expertise** is also recognised by the Courts.

Risk mitigation

We help you to **identify**, **contain** and **eradicate** risks from your business, e.g. if a staff member has stolen your IP, we can wipe it from their electronic devices and cloud storage.

RECOVER

Return to business as usual

You may require **data breach notification** services, assistance with your **cyber insurance** requirements, or general **security recommendations**.

Post-incident review and improvement plans

Following an incident, we **evaluate** your response to **correct** any weaknesses and **build** on your strengths.

"I don't think we've even seen the tip of the iceberg. I think the potential of what the internet is going to do to society, both good and bad, is unimaginable."

David Bowie in 1999

"I don't think anything is getting better, that much is pretty clear."

Troy Hunt - Security researcher who maintains 'Have I Been Pwned?'

"The knock-on effect of a data breach can be devastating. When customers start taking their business elsewhere, that can be a real body blow."

Christopher Graham, former Information Commissioner, UK

"In the very near future, cybersecurity exercises are going to be absolutely expected of all companies by regulators."

Michael Vatis, founding Director of the FBI's National Infrastructure Protection Centre, USA

Thinking Ahead. Being Prepared

In October 2018, the New Zealand National Cyber Security Centre (NCSC) published the results of its survey of 250 nationally significant organisations.

Key findings include:

i. An area of good practice that was identified is:

Readiness – Preparing the organisation to detect, respond and recover from a cyber-security incident.

ii. When an organisation becomes aware of an incident, being **ready** to respond can **reduce** its impact of a compromise.

iii. Having an **up-to-date plan** allows an organisation to react **quickly and decisively** when an incident occurs and serves as a framework to **preserve evidence** in the event legal action is sought following an incident.

iv. 63% of New Zealand's Nationally Significant Organisations have an incident response plan, but 33% have not **tested their plan** in the last year.

We are proud to be a 100% New Zealand owned and operated business.

Our Incident Response Retainer

When dealing with your health, you know in advance who your Doctor is.

For Forensic Technology and Cyber Security matters, you should also have a professional provider on an **0800 Speed Dial**.

With our Incident Response Retainer, you can take comfort knowing that in your time of need, you will quickly have access to Incident Response experts, along with a comprehensive network of associated professionals.

Retainer options

1. *A welcome pack and an initial consultation to explain how to maximise the service*
2. *Access to a panel of experts who are ready to help*
3. *Support desk for ad-hoc queries (up to 30 mins per month)*
4. *Our monthly Forensic and Cyber Bulletin – Premium Edition*
5. *Yearly forensic readiness assessment to prepare*
6. *Yearly assistance in drafting or revising your cyber incident response plan*
7. *Board briefing packs and deep dive presentations*
8. *Access to our Incident Response Portal and suite of Ops tools for managing incidents*
9. *Facilitation of a yearly cyber incident tabletop simulation*
10. *Discounted rates on our forensic technology expert services*

Benefits to you

24/7 on call support

Forensic collection and examination of data

Faster outcomes during your crisis

We have plans starting from $200 + GST per month

Email us at support@incidentresponse.co.nz
or phone 0800 WITNESS (0800 948 637) to start a conversation

Campbell McKenzie

Founder, Incident Response Solutions

I've always loved flying. It started with the obligatory Kiwi 'OE' on an Air New Zealand 747 Jumbo via LAX to London, then zig-zagging around the world back to Aotearoa via 33 countries on various airlines. I then learnt to fly a Cessna, but on becoming a Dad reverted to Microsoft Flight Simulator.

In recent years, I've done my fair share of flying. Before boarding, no matter what airline, airport or aircraft, I always try to eyeball the pilots in the cockpit while they conduct their pre-flight checks. I trust them totally with my safety, knowing they are highly trained, skilled experts in their field.

For me personally, the movie 'Sully' draws a similarity between **Flight Safety** and **Incident Response**. The movie is about Captain Chesley "Sully" Sullenberger's US Airways Flight 1549. Shortly after take-off, the plane strikes birds, losing both engines. They successfully land 'on' the Hudson River 208 seconds later with no loss of life. The movie is centred around the **Post-Incident Review** and how simulations show that the plane could have landed at an airport. However, when Sully asks for the **'human factor'** to be considered (thus adding a 35 second delay), it then proved that the plane would not have made it safely to any airport in New York.

The movie provides several lessons for Incident Response and shows how critical **'people'** are throughout the process. Firstly, when a crisis strikes, pilots refer to the response plan specific to that aircraft and follow it to completion. Secondly, pilots are regularly trained and tested using simulators. Finally, the flight industry conducts post-incident reviews in order to learn and make improvements.

We can help you understand and manage your technology risk, using easy to understand tools and techniques. When faced with a problem, we help guide you through what could become the most challenging time in your career.

Finally, as a guardian of critical data, let us help you ensure that **Security** and **Privacy** is at the forefront of every decision you make.

Thank you

Campbell

What next?

Start by asking yourself the following questions … and then get in contact with us.

- What is our current level of maturity within the Incident Response lifecycle?
- Do we have an Incident Response plan, and if so, have we recently tested it?
- Do we have a panel of forensic and cyber experts ready to act?
- Have we conducted a post-incident review of any previous incidents, applied lessons learned and made improvements to our plan?
- Do we fully understand what is included in an Incident Response Retainer and how it will assist us in addressing the above questions?

To find out more, please give us a call, send us an email, or visit our website.

Phone 0800 WITNESS (0800 948 637) or

021 779 310 (24 Hour Support)

Email support@incidentresponse.co.nz

Website https://incidentresponse.co.nz

Incident Response
FORENSIC & CYBER

INCIDENT RESPONSE SOLUTIONS