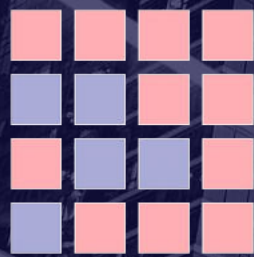


Surviving a Cyber Incident without damaging your Brand



IBRS

ANALYSIS
INSIGHT
JUDGEMENT

Dr Philip Nesci
Advisor

Headlines Oct 2016

NEWS

NEWS HOME >

Red Cross Blood Service admits to personal data breach affecting half a million donors

UPDATED FRI 28 OCT 2016, 5:41 PM AEDT

✉ f t w

Support The Guardian Subscribe

The Guardian

News Opinion Sport Culture Lifestyle

Australia World AU politics Environment Football Indigenous Australia More

Health

Red Cross Blood Service data breach: personal details of 550,000 blood donors leaked

MENU

The Sydney Morning Herald SUBSCRIBE 0

A Tiffany Mother's Day TIFFANY & CO. SHOP

Advertisement

POLITICS FEDERAL

Red Cross data leak: personal data of 550,000 blood donors made public

By Fergus Hunter, Tom McLroy, Rania Spooner

Updated 28 October 2016 -- 9:30pm, first published at 12:20pm

ABC ADELAIDE: BRETT WILLIAMS

Menu

FINANCIAL REVIEW
— NEWS WEBSITE OF THE YEAR

Oct 28 2016 at 1:38 PM
Updated Oct 28 2016 at 1:54 PM

☆ Save article My Saved Articles Print License article

Red Cross apologises after mass leak of Australian blood donor records

✉ G+ f t w

ABC News 24 Live Melbourne
Courtesy of ABC News 24

Australian Red Cross BLOOD SERVICE

Massive Red Cross breach

Latest Stories

- Musk buys \$13m of Tesla stock 13 mins ago
- Russia's Putin sworn in for fourth term 26 mins ago
- ASX poised to rise, alongside Wall St 38 mins ago

More

itnews Gartner Are API's the basis of your digital strategy? Learn more

GOVERNMENT IT SECURITY FINANCE IT TELCO BENCHMARK AWARDS

What are your biggest IT management challenges? Tell us for your chance to win

Australia's biggest data breach sees 1.3m records leaked

By Alle Coyne
Oct 28 2016 12:00PM

Medical data exposed.

More than one million personal and medical records of Australian citizens donating blood to the Red Cross Blood Service have been leaked.

11 Comments

Introduction

In October 2016 the LifeBlood (Blood Service) was made aware that some Donors' Personally Identifiable Information was available on the internet.

- What happened
- How the Lifeblood responded to the incident
- How Lifeblood responded to the need to rapidly improve the Information Security posture

Australian Red Cross Lifeblood

The Australian Red Cross Lifeblood is entrusted with the supply of Australia's blood and blood products.

- 1.3 million blood donations annually
- 500,000 active donors
- 3500 staff
- 80+ facilities
- 3 Manufacturing centres
- Federal Government Critical Infrastructure Classification

What Happened – The First Few Hours

- On Wednesday 26 October 2016 CIO notified by AusCERT – entire Donor database available on the internet.
- Informant advised that he would go public within 72 hours
- Immediate Internet access to server blocked and access denied
- Investigation pointed to information held by a third party - Precedent
- War room established by ICT and the Chief Executive and Board informed
- People brought in on a need to know basis, planning for next steps begun
- Engaged third party specialist support - Auscert, Idcare, Forensics, ACSC

What Happened – The First Few Hours

What we knew...

The incident was genuine

Enterprise Crisis Management Response Plan was in place

No specific Cyber Security Response Plan

What we didn't know...

Extent of the incident

- How it had occurred?
- How much data had been compromised?
- Who had accessed the data?
- Had it been copied or circulated globally?
- How would the donors be impacted?

The Response – Week 1

Day 2

- Adopted principle of maintaining trust and informing Donors
- Communications Plan established
- SMS and email to all Donors
- Press conference
- Scripts for the National Contact Centre
- Social media response team
- External Communications/Public relations expertise engaged
- Escalation process established to approve comms
- Independent Donor Helpline established – IDcare



The Response – Week 1

Day 3

- Midday Press Conference on site
- Take responsibility and no blame
- SMS and emails released to Donors subsequently
- Short, independent review of Blood Service response requested by Board.

Day 4 +

- 3000 responses required to enquiries
- Internal taskforce and communications team setup to triage and respond to individual donor queries
- Formulation of a broader Security Review underway
- Monitoring of Dark Web for unusual activities




Crisis Management and Governance

- Organisation wide response - a Team of Teams including ICT, Legal, HR, Internal Comms, Marketing and Donor Services
- Crisis Team was the Executive Team chaired by CEO
- CIO-CEO partnership
- CEO – Board Chair was communication channel for Board
- Various sub Teams were established in close proximity to crisis Team
- Board subcommittee established for ongoing oversight of the recovery.

governance


Response Week 1 – Social Media

 **Australian Red Cross Blood Service**
October 28, 2016 · 🌐

IMPORTANT UPDATE


We regret to inform the community that on 26 October we became aware a file containing registration information of 550,000 donors made between 2010 and 2016 was placed in an insecure environment. IDCARE, a national identity and cyber support service, has assessed the information accessed as of low risk of future direct misuse. Included in the file was information such as names, addresses and dates of birth. This information was copied, and then brought to the... [See More](#)

Like · Comment · Share

 [Redacted] An unfortunate mistake, but it won't stop me from continuing to donate - I'm booked in for Monday. As a nurse on a medical ward who administers blood products for unwell patients quite regularly, I appreciate the importance of blood donation, and I hope that this unfortunate event will not stop anyone from donating blood or plasma. Keep it up, lovely donors!

Like · Reply · 1y 40

View 2 more replies

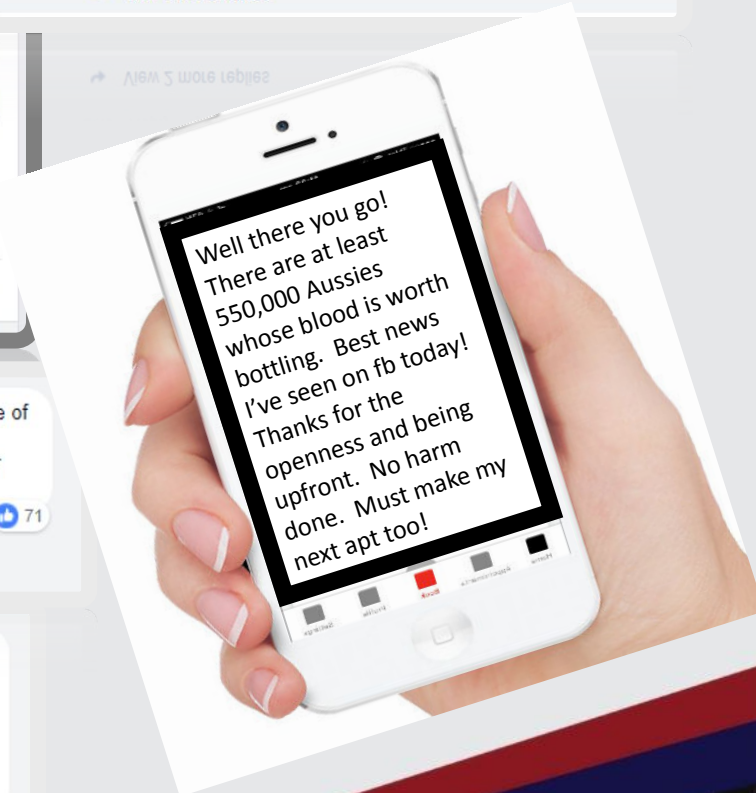
 [Redacted] The comments here certainly show the calibre of the people who donate blood! Thank you to you all for your donations. You've saved my life and continue to do so every four weeks!

Like · Reply · 1y 71

1 Reply

 [Redacted] I AM ANGRY THAT MY PERSONAL INFORMATION HAS BEEN STOLEN FROM A APPARENTLY SECURE SITE AND I HAVE TO READ ABOUT IT ON A FACEBOOK PAGE. I HAVE BEEN DONATING BLOOD FOR 26 YEARS AND THINGS LIKE THIS GIVE ME SECOND THOUGHTS OF DONATING AGAIN. HOW CAN WE TRUST THE SERVICE THAT THIS BREACH WILL NEVER HAPPEN AGAIN? VERY ANGRY

Like · Reply · 1y



The Response – Month 1

- A number of independent reviews were initiated
- Privacy Commissioner investigation commenced
- Tight controls on outbound information/data, external data stores hardened
- Multiple streams of work established
- Immediate approval of funding by the Lifeblood Board to commence security uplift.



Significant Outcomes for Lifblood

- ❌ Enforceable undertakings by Privacy Commissioner
- ✓ No widespread access to Donor data detected
- ✓ Overall maintained trust with Donors
- ✓ Significant investment and uplift in Cyber Security capability, breathing room for problem projects!
- ✓ Enhanced reputation for management of crisis and considered an exemplar
- ✓ Tight governance of information established
- ✓ Cultural change and awareness of cyber security across the organisation
- ✓ Significantly enhanced the motivation of teams involved in the crisis

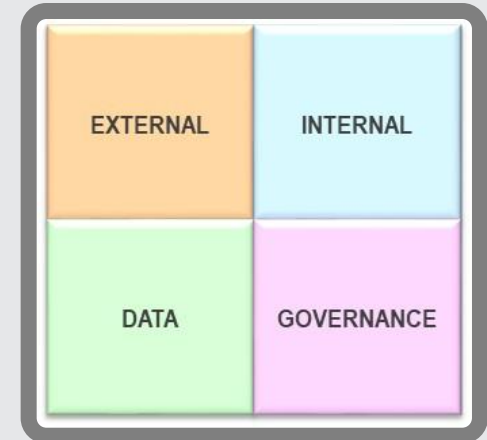
However

- Precedent exited Australia after 12 months
- Legislation passed for mandatory reporting

The Project Plan that moved

Initially determined four streams of work

- External – websites outside IT control
- Internal – detect and monitor capability, culture change
- Data – where is it and who has it
- Governance – policy and procedure review



The Ramp up

- Major impact on existing projects, operations activities and resources
- Program of works defined
- Significant staff uplift with external resources

Prevention is better than cure

- Get control of shadow IT through governance
- Know what data is stored outside your corporate network
- Know who has access to your data
- Review your Cyber Security Incident Response and Crisis Management Plans
- Management of vendors and their cyber posture
- Patch your systems
- Know what the Privacy Commissioner defines as reasonable steps and understand if you satisfy them



In Case of Cyber Incident

- Respond with enterprise crisis management urgency
- Access to specialist expertise
 - Forensics
 - Cyber Incident management – AusCERT, Federal Cyber Security Team
 - Dark Web
 - Communications/PR Specialists
 - Support for impacted stakeholders
- Transparency in communication and taking accountability
- Manage the health and well being of Executives and staff during the crisis!

The image is a composite background. The top half shows a city skyline at night with illuminated buildings. The middle section features a road with horizontal motion blur lines, suggesting speed. The bottom right corner shows a white maze with a small silhouette of a person standing in the center. A red and blue diagonal stripe separates the road from the maze.

Discussion