CASE STUDY: eCensus Cyber-Attack was the wake-up call needed to compel Australian business and government to ensure their security safeguards were up to scratch

Executive Summary

Australia owes the Australian Bureau of Statistics a debt of gratitude because in real terms, the cost of the targeted attack was negligible. Any doubters need only look to the parlous state of data breaches globally. Neither confidential data nor privacy was compromised as a result of the orchestrated attack against the ABS. The upside was that the incident grabbed national headlines and did more to bolster cybersecurity awareness in Australia than any other single event. The hope is that this incident marks the low-point and ensures our nation leads the world protecting citizen's data entrusted to third parties.

What the media unkindly dubbed #CensusFail was an important wakeup call for all Australians and has heightened awareness of the vital importance of data security. It's not overstating the case to say that prior to the eCensus incident, many "C- Suite" executives didn't view cybersecurity as an existential threat to their business survival. The episode exposed how vulnerable organisations are to denial of service attacks and offered a salutary lesson that demonstrated how even minor security lapses can compound and cascade into a public relations disaster. More alarming though was the evidence provided of how "tick-in-the-box" compliance was a determining factor in the scope of the failure. As a result, the government's compliance culture has been replaced with a comprehensive risk strategy, increased levels of inter-agency cooperation and greater collaboration between government and business.

An independent review was scathing of what many in private enterprise view as normal daily operations, particularly the "cosy relationship" between the ABS and technology partner IBM. In the corporate environment claims like "they know our network better than we do" are viewed as the mark of a successful, collaborative relationship. Business sees technology as an enabler that frees them to focus on customers and channel their energies towards sharpening competitive core operations. The business drivers are compelling for engaging with technology partners like IBM and guarantees access to subject matter experts at a much lower cost than employing personnel themselves. It hardly seems fair when government agencies are instructed by politicians to behave more like business, only to sacrifice them to the altar of public opinion when things go wrong.

So what practical insights have we learned from the ABS denial of service attack? Scrutinise partnerships and dependencies because security safeguards are only as strong as the weakest link. An avoidable partner oversight was pivotal in taking the census website offline for nearly two days. This error was attributed to using outdated government guidelines and compounded with ABS's unquestioning acceptance of partner IBM's advice. People make mistakes. They always have, and always will. By soliciting a wider range of expert views and opinions, the outcome may have been very different. The old maxim, "trust but verify" is still valid and should be baked into the DNA of every IT professional in business and government.

The other important takeaway from the event saw the ABS re-invent their approach to risk management. The traditional vector in government was to triage compliance mandates first. This is now outmoded, particularly in the fast-changing security landscape. The ABS now prioritise agility, adaptability and apply a laser like focus towards risk management as their best defence in warding off cybersecurity threats. The ABS learned to their detriment that in spite of their detailed analysis and planning, gaps and weaknesses still pose a grave security risk. To defeat this possibility the ABS actively collaborate with other government agencies to disseminate insights and share knowledge across the whole of government. For taxpayers, this is a change that will reap dividends for decades to come.

- ABS have gifted the nation by helping recast cybersecurity risk awareness from an abstract concept to an existential national threat
- The catalyst for security change within the organisation was traumatic – a compelling, avoidable event
- The ABS attack spurred changes across government that have transformed policy and increased resilience against orchestrated cyber attacks
- Technology partnerships must be reviewed and audited regularly and it's vital that trust and verification is a key pillar of the relationship
- The MacGibbon Review censured the ABS for some practices that are commonplace and rhapsodised in private enterprise
- The security landscape is dynamic and evolving. What was relevant yesterday may be outdated tomorrow. An inability to act with agility across every facet of your security operations and strategic direction may result in infelicitous outcomes
- No organisation is immune from attack so plan to fail and ensure that management and stakeholders actively bolster policy, safeguards, and awareness initiatives

Part I
The Incident

Digital First
Census 2016 was a watershed moment for the ABS. Over the two preceding censuses the transition from paper forms to online entry had succeeded to the point where in 2016, the ABS felt confident enough to transition away from paper forms by setting online entry as the default. Old fashioned paper responses were still an option, but most respondents preferred the ease and simplicity of the online approach. For taxpayers, applying "digital first" yielded massive savings and was a sustainability winner to boot.

Census Technology Partner IBM
The ABS and IBM were very confident that the project would proceed without a hitch based on their previous triumphs flawlessly delivering the census. Contracted census IT partner IBM were tasked with ensuring eCensus would be delivered successfully. More importantly, they were a trusted partner and committed to provide services delivering the census at a competitive price.

The Geo-Blocking Mitigation Measure
The ABS's primary safeguard was geo-blocking. Referred to internally as "Island Australia", this proposed mitigation control would theoretically offer enough protection to prevent Distributed Denial of Service (DDoS) attacks. They were wrong. This safeguard was based on IBM's recommendations and in compliance with the 2014 version of the ISM manual, the current and applicable version at the time RFT's were requested.

Attack!
Unknown assailants launched an intense SYN Flood DDoS attack that sent a torrent of data requests to the ABS webservers which couldn't be fulfilled. The process was repeated again and again until the systems froze. This initial attack was combined with a UDP Flood which randomly attacked the servers. When combined, these lethal attacks proved devastating, overloading ABS webservers and preventing legitimate respondents filling out their online eCensus forms. Based on the irreconcilable situation they were faced with, the ABS IT team shut down their servers and triggered their recovery plan.

The Router Failure
As the ABS and IBM were recovering services a Router restart failed, causing further delays. The Router configuration (a small data file) had inexplicably not been saved. This further compounded the difficulty in recovering services and further complicated to the outage's remediation complexity.

Exfiltration - Data Theft Alert - False Alarm
Just as there appeared to be some light at the end of the tunnel an alert was flagged. This was a potential security risk that the ABS sought to avoid at all costs to ensure the privacy and trust of Australian citizens was maintained. This was the worst possible outcome for the ABS. Data removal of census data would rank the entire eCensus a failure of epic proportions. As the investigation continued the conclusion was drawn that this was a false alert and there was never any risk of compromise.

Success: Systems Back Online
The outage lasted forty-three hours and occurred under the glare of a feral media and scrutiny from politicians with a very limited grasp of technology. No data was lost nor any privacy breached. The ABS then went through a very humiliating public post-mortem.

Part II
The Post-Mortem

The Media Pile-On
The media were merciless in deriding the ABS and their technology partner IBM. The pile-on from many uninformed pundits fuelled conspiracies and was further exacerbated with poorly briefed' politicians speaking independently with limited coordination or unified messaging. As cooler heads prevailed and the communication became more coordinated, a regimen of managed media disclosure began.

If just one incident within the sequence of events had occurred in isolation, geo-blocking measures could have mitigated potential DDoS attacks seamlessly and the episode may never have occurred.
Sadly, for the ABS and IBM, Murphy's law prevailed creating an extended, highly visible outage. So, what went wrong?

Geo-Blocking Mitigation Control Failure
IBM had implemented geo-blocking controls to mitigate DDoS attacks but this was never fully tested to learn if it would defeat a sustained attack. Load stress testing was undertaken but not scaled sufficiently to simulate the intensity of the type of intensive attack the ABS underwent. This oversight proved fatal. Until the incident occurred the ABS had not experienced DDoS attacks and although they had considered the threat in the planning phase, they lacked hands-on experience in dealing with an assault of this type. It was classic case of hypothetical versus reality. The threat is known but until the experience becomes lived, it's just an abstract concept.

Australian Government Information Security Manual (ISM)
The ISM manual is the standard reference that government, defence, and their contractors rely on to meet good practice security guidelines within government. The manual comprises three documents that target different audiences to bolster security compliance and executive awareness. If you could choose one oversight that was pivotal in enabling the DDoS event then it was IBM's reliance on an outdated version of the manual which omitted orchestrated DDoS attacks. The ABS believe that the lack of flexibility and agility in the contract to keep track of changing requirements and threats was a contributing factor to the failure. This change to the contract would have enabled the system to be built in accordance with the later revision of the ISM, but more importantly, updating the threat and risk assessment would have identified DDoS attacks as a potential risk and allowed a more thorough review of controls to be conducted and changes made proactively. The issue was comprehensively covered in the version of the manual that IBM later referenced. By the same token it's hard to put all the blame on IBM. The other unheralded offender was the mind-set that permeated government thinking. A tick in the compliance box.

Compliance and the dreaded "tick in the box"
Cybersecurity is evolving constantly to face-off indeterminate foes. The opponent is anonymous, usually very smart, located behind multiple layers of obfuscation and intent on creating mischief or harm. As government and businesses battle to curtail costs, traditional service delivery has transitioned from people and telephones to web-based self-service. The paradox is that increased customer convenience also expands our digital attack surface, increasing the challenge required to protect digital assets. The reality is that ticking a box isn't enough to protect organisations from motivated criminals, unknown foreign actors or ideologically driven activists.

The Outage That Shouldn't Have Happened
The ABS were prepared for the 2016 census and their security safeguards and testing aligned with industry best-practice. The ABS underwent security audits, penetration tests, and independent security assessments undertaken by IRAP certified practitioners. Government entities are exposed to some of the most rigorous oversight to safeguard taxpayers' investments. Their personnel are rewarded with generous career development budgets well in excess of the private sector. If one single safeguard had failed, the ABS website may have gone offline for a short period. But three? In spite of all the reviews, recriminations and remorse, bad luck still played a big part in the eCensus event. Random events still create good and bad outcomes in spite of all best efforts or well laid plans. To achieve exceptional success, organisations must be willing to accept failure, lick their wounds and get back to work. The ABS have shown their mettle and should be respected for how they came through for taxpayers in a situation the nation had never faced before.

Part III
Learning From Failing

Knowledge Transfer

The ABS have been generous sharing what they learned from their experience. ABS staff have mentored other agencies and been a catalyst in building inter-government knowledge exchanges. Their community contribution has helped create a more robust government security landscape. Most importantly, the ABS were candid, transparent and shared their insights openly. For many in government, the attack exposed how vulnerable we are as a nation to cyber-threats. The government acted quickly by establishing the MacGibbon Review to dispassionately appraise the incident and offer counsel to limit the chance of a recurrence.

The MacGibbon Review

Alastair McGibbon, the Prime Minister's Special Advisor on Cyber Security was asked to lead an enquiry into the eCensus incident. His report was excoriating and is mandatory reading for every C-level manager and board member. The reports' stinging criticism held both ABS and IBM jointly responsible for the census outage and offered a roadmap for change that organisations can use as a risk management template. All of the recommendations were implemented by the ABS and are equally applicable to both government and private enterprise. Senior management must accept that IT security must be deep-seated into their culture and that it's incumbent on them to understand the risks as part of an overall strategy. Security failures are now viewed as management failures: the days of blaming technology practitioners for security meltdowns are over.

Key points that the ABS learned from the MacGibbon review;

Partnerships and Contracts

The ABS must manage outsourcing contracts better and seek independent assurance to benchmark performance against expectations. Maintaining "cosy relationships" can make the business accord more pleasant but steadfast oversight, regular auditing and dispassionate reviews will prove more effective protection measures.

Inter-Agency Collaboration

The ABS have shown leadership in their quest to share knowledge and break down the silo structure that permeates government culture. By pooling experience and resources, improvements to information security can be realised and national cybersecurity fortified.

Privacy Concerns

It's postulated that the DDoS attack was initiated because of the ABS's indelicate handling of privacy concerns. We may never know but the ABS has completely revised their privacy and media policies to ensure stakeholders and the responsible ministers are fully informed and media interaction is focused and unambiguous. Speculation is anathema to controlling the media message.

Communication and Incident Management

During the incident there was limited coordination between the politicians, IBM and ABS. This was unhelpful in keeping stakeholders appraised and also raised the spectre of conspiracy, fuelled by social media conjecture. Other contributing factors to improve planning and make clearer any individual roles and responsibilities during crisis management response should improve outcomes. Planning to fail has changed the organisation's forward-looking perspective.

Testing and Compliance – Assurance

The ABS has formulated a more rigorous approach to security and testing that has filtered across the whole of government. Independent assessment and increased levels of staff training have permeated the ABS culture, guaranteeing staff are in a permanent state of security readiness.

The Nebulous Cloud

One key recommendation was harnessing the power of "The Cloud". This is now a contentious issue in the industry because the Cloud is not the silver bullet that the marketing hype promised. The adaptability and scalability of Cloud infrastructure may appear a perfect solution, but as the maturity of the technology increases, concerns and limitations have become more apparent. Contributing factors that must be analysed include security and privacy controls provided by the Cloud provider and mutual obligations about roles and responsibilities for overall security in the Cloud ecosystem. Lack of clarity can impede best possible outcomes. A detached review of the possible value and the benefits Cloud computing delivers must be weighed up carefully in any comprehensive evaluation.

Part IV
Observations

Who was behind the attack?

Since the attack of August 9, 2016 many lines of investigation have been followed up by Australian Federal Police. Suspicions are held that the attackers were political activists, but to date no charges have been laid. The case remains open.

Twelve Months to Triumph

Beaten and bloodied the ABS battled on to fulfil the same sex marriage postal survey. As a result of their success, marriage between same-sex couples is enshrined in Australian law. This mammoth task was a technical triumph and logistics success. New technical systems were implemented and existing infrastructure improved to deliver this demanding project on time.

Key deliverables included;

- Broader engagement with industry and government experts including Australian Cyber Security Centre and Digital Transformation Agency
- Adopt "Agile" delivery methodology thus ensuring security was a core structural component of every solution from inception
- Prioritise risk management focus over compliance and constantly strive to drive down risk exposure.
- Utilise Cloud services for all external facing elements to provide the resilience and scalability needed to serve the public and defend against attacks

Some of the key services the ABS built to make the postal vote possible included;

- Interactive Voice Response system
- Secure barcode generation
- Offline form management for remote areas
- Online request and enquiry system
- Logistics and supply-chain control systems
- Vendor systems – data capture and coding
- GIS dissemination
- Contact Centre knowledge base management systems

Part V
Conclusion

The MacGibbon review and ABS candour have helped the Australian government and private enterprise learn from the episode. The eCensus security incident made senior government officials apply an unflinching focus on the ramifications of a major security event and comprehend how the situation was resolved. It demonstrated how a cybersecurity occurrence could adversely affect their business, damage reputations and potentially harm brand value. The genesis of the problem was a single oversight caused by using an outdated technical manual. This fact alone still stuns people. Full credit must be given to ABS staff for bouncing back after their public humiliation and media evisceration. The MacGibbon review is mandatory reading for anyone who's in management or aspires to be. It's informative, and should give many managers and administrators a real jolt into commissioning their own organisational review. The key takeaway from the incident was that Cybersecurity isn't just an IT problem, but an existential risk that must be infused into the DNA of every employee, manager and board member. Information security must be managed better and viewed as a comprehensive business risk and not a technology issue.

Links and Resources

- Australian Government Information Security Manual (ISM)
- The Mandarin article referencing activism and its impact on security.
- Australian Bureau of Statistics website
- Australian Statistician's speech regarding 2016 Census
- Quality of the 2016 Census report
- Australian Information Security Association (AISA)

" You cannot outsource risk "

David W Kalisch - Australian Statistician

About The ABS

Founded in 1905, the Australian Bureau of Statistics (ABS) is entrusted with measuring and recording key national metrics. The data they gather enables lawmakers, industry and the community to make informed decisions and benchmark Australia's economic performance against international peers. The ABS publish their statistical data in a series of releases that informs interested parties about Australia's demographic trends and addresses financial performance and provides statistical insights into industry, labour, health and the environment. The ABS also play a key role in guiding regional neighbours through knowledge exchange, mentoring and thought leadership that helps drive economic efficiency across the South Pacific.

Employees: 2,500
Locations: 9
Established: 1905
Headquarters: Canberra, Australia

Australian Bureau of Statistics

About this case study

After attending an ABS presentation at the AISA annual conference in October, 2019 I was inspired to document the eCensus incident as a labour of love and set out the facts as dispassionately as possible. Mike Ryan - Brass Razoo

Thanks to the ABS

Thanks to Craig Lindenmayer of the ABS for his candid and entertaining presentation and the time he generously allocated for interviews and fact-checking.

About brass razoo

brass razoo specialise in producing technology content focused on enterprise information technology. We are based in the Hunter Valley, Australia, the home of the worlds best coal, finest red wine and biggest mosquito, the mighty Hexham Grey. To visit our website click on the logo below.

brass razoo