Bridging the divide – nexus of public trust, cyber resilience and risk assessment

A Mimecast Cyber Security, Privacy and Risk Leaders Roundtable

This Issues Paper is the summary of a discussion that took place at the Cyber Security, Privacy and Risk Leaders Roundtable Luncheon, which was co-hosted by cybersecurity provider Mimecast and InnovationAus.com.

The overarching theme of the gathering, titled *'Bridging the divide – nexus of public trust, cyber resilience and risk assessment'*, was the public sector's readiness to build transparency whilst improving information oversight and cyber resilience.

While the discussion did touch upon cutting edge, 'over the horizon' issues, the general consensus was that many of the cybersecurity challenges facing government are already all too familiar; managing complexity, taking a huge, diverse group of people on a journey, and ensuring they have the right approach and attitude towards dealing with cybersecurity issues.

With nine out of 10 Victorian Government agencies experiencing a cyberattack in 2018, email continues to present one of the biggest 'attack surface area' risks.

While one would expect discussions of this nature involving a diverse group of industry stakeholders to throw up a variety of nuanced challenges, there was also a lot of common ground, particularly – and rather worryingly – when it came to workplace fatigue over cyber concerns.

The nuances of records management also prompted some interesting debate over what should be classified as a record and what needs to be protected. It was, however, agreed that how you attach value to something in terms of whether it should be protected is a vital component of information security and needs to be unequivocally laid out to those responsible for records management in the workplace.

How the public sector is working through challenges of making information freely available in the way it's intended under the law, whilst also protecting privacy, was another key talking point. It was agreed that streamlining the Freedom of Information request process – firstly by more clearly defining what constitutes a 'record' – would go a long way to achieving this and improve the public's trust in government transparency (In Australia, access to documents from Australian Government ministers and most Australian Government agencies is regulated by the *Freedom of Information Act 1982* (FOI Act)).

Attendees

Table Hosts

Nick Lennon
Country Manager
ANZ, Mimecast

Christina Van Houten
Chief Strategy Officer,
Mimecast

Corrie McLeod
Moderator/Publisher,
InnovationAus.com

Discussion Participants

Navadeepan Pillai
Acting Director of Service Delivery / General Manager, Design and Development Cenitex

Rohan Davies
Senior Advisor, Cyber Security
Department of Premier and Cabinet, Victoria

Carsten Rudolph
Head of Department for Software Systems and Cybersecurity,
Faculty of IT, Monash University
Director, Oceania Cyber Security Centre

Fadi Alja'fari
Cyber Security and Risk Manager
Deakin University

Alex Nixon
Senior Associate
Kroll

Loris Meadows
CIO
Family Safety Victoria

Michael Trovato
Managing Director, Information Integrity Solutions and Director AISA

Peter Francis
Manager, Standards and Policy
Public Records Office of Victoria

Ken Chee
Applications, Information and Solutions Manager
Victoria Legal Aid

Rachael Leighton
Principal Advisor,
Cyber Strategy & Awareness
Department of Premier & Cabinet

Shannon Dowd
Principle IT Security Advisor
Family Safety Victoria

Simon Naughton
Director,
Infrastructure & Operations,
Information Technology
Swinburne University of Technology

Nick Lennon
Country Manager
Mimecast

Christina Van Houten
Chief Strategy Officer,
Mimecast

Mitra Minai
Head of Technology Specialist Controls, NAB

Corrie McLeod
Publisher
InnovationAus.com

The Key Issues

1. Collaboration

Collaboration is a word and a topic that is used often and its importance frequently highlighted, but while there have been huge strides made in last few years when it comes to state/federal/industry collaboration around cybersecurity, it was generally accepted by the panel that the capacity for far greater sharing of insights across sectors still exists and the scope for improvement in this area is vast.

It's vital to drive resilience and collaboration at a national level. With the Australian Public Service Review submitted for evaluation to the Prime Minister's Department on 20 September 2019, one of its key recommendations was to harness the opportunities technological advances bring.

But overhauling records management and improving access to information can be a costly, difficult and slow process. The importance of collaboration between industry and government, as well as Risk and IT operatives, is critical.

"The key is collaboration and leaning in more to our partners through academia, industry, and international and national government counterparts, because it's a team effort to ensure that cyberspace is a place that we all want to be."

The ongoing skills shortage in cyber-security is proving to be problematic, and the situation is set to worsen. Gartner said that it expects to see a shortfall of 3.5 million cyber security workers by 2022. Forrester added if that was the case, we'd be facing a critical situation.

"There would be huge concerns for society with that dearth of talent in terms of the security risks it presents. There's a responsibility on government, the research community and innovators to solve this issue by looking at levels of automation and integration between different ecosystems."

A representative from ISACA (Information Systems Audit and Control Association) touched upon the work they are doing in this area with the ISO (International Standards Organisation).

"ISACA has been a lead liaison to ISO, working collaboratively with ISO in documenting international standards and frameworks to address cybersecurity concerns, including working with international professional communities to document the governance of artificial intelligence and governance of data standards."

The international collaboration has been effective, with the ISO 27000 information security standard series being updated in recent times. Many of the ISACA and ISO international standards and frameworks are being reviewed and adopted by international regulators, an example being APRA recently updating Prudential Standard CPS 234, which all financial institutions must now comply with.



2. The public sector is a broad church

In government, the challenge exists in convincing the wide variety of people within such organisations into changing their thinking to become part of the solution rather than simply be focused on their own specific roles. From those on the front-line delivering services in the community, to the array of office-based workers, the diversity of roles presents a challenge for government to keep everyone fully engaged in cyber safety.

The diversity and scale of public sector workforces makes the task of cyber-security education even more daunting.

"The Victorian public sector consists of around 311,000 staff and more than 1,800 individual entities that employ different people. We don't have a security person in every entity, which is one of our challenges."

Changing the narrative is preferable to relying on expensive consultants. With the vast majority of organisations, the most harm occurs because the organisation hasn't performed basic cyber processes, such as keeping patching up to date and turning on two-factor authentications.

"It makes no sense to engage a cybersecurity expert who will charge us $350,000 to write a report that tells us what we already know, which then doesn't get actioned because we don't have the money because of the financial outlay on the report."



3. Privacy

Privacy is paramount, but so is transparency within an effective government and democracy when it comes to records management. This is a rapidly-changing area with the proliferation of digital records.

When talking about volume and what needs to be taken into account from a government records management perspective, a balance must be struck between privacy and FOI/transparency. We can't just 'lock everything down', as there's still a role (and in many instances, an obligation) for the government when it comes to sharing information with the public.

If you're protecting something, can you ever look at it in isolation? It usually has to be in context of an email chain. This is challenging when protecting a record: sensitivity is almost always linked to privacy. You're dealing with a set of principles, and then the practical application of them in a very fast-moving environment.

For agencies working with people at risk, a privacy breach can be devastating. This responsibility calls for a balance between communication and client privacy and protection.

Using algorithms to protect the privacy of vulnerable citizens, such as agencies engaged in child protection having a correlation with the Australian Federal Police doing research on child exploitation material, is a prime example.

"There's technology in place that allows us to apply algorithms to data without actually needing to take the risk of accessing the data - but rather just obtaining the research classification."

There is a need to understand what data is being protected. This means security people collaborating with the people in the business that are focused on privacy so they gain a better understanding of what it is they're protecting.

"It makes a huge difference if you can get rid of redundant, obsolete, trivial data, and get the classification down on what the information is and focus, for example, on emails that you want to protect and have available. That's a very different exercise than what I think a lot of security people think about."

4. Freedom of Information

Freedom of Information is a principle, but you can't have effective FOI if the process of finding information is so burdensome.

FOI, and government transparency when it comes to records is almost always about privacy. So how do we define it?

Email is an important part of records management, firstly because there's so much of it, but more importantly, we know from recent Royal Commissions how vital email chains can be in providing evidence of poor conduct and management.

We know email plays an increasing role but where are the grey areas and how do we navigate through them?

Managing the human element appropriately is critical, particularly when it comes to government departments dealing with sensitive information about its citizens, given that those departments often have the responsibility and the power to influence important aspects of their lives.

"For us, it's about that balance between ensuring that information is readily available but also understanding what the implications of that potentially are and how did we as a government not only navigate through a really prickly road to ensure that we meet legislative requirements on FOI, but also ensure that our citizens are safe."

So, what constitutes a record, and how important is classification? Under Victorian legislation, a record is 'Any form of information that's collected or created by an organisation or government'. So, it's a very broad definition, which makes matters easier, because it encompasses email as well as pretty much anything else, including any large data sets a government department or agency might have.

By defining a record, you're giving it a value. You're also giving it certain preservation requirements and the right to maintain its accessibility.

The recent Royal Commission into Aged Care highlighted how emails can become evidence. Email correspondence plays a key role in day-to-day government business, so how it is treated from a records management perspective is critical.

"Any legal investigation will always go through the emails. They won't be too worried about all the documents pushed across the desk at them; emails are often the smoking gun when it comes to intent and knowledge."

Some sections of the community see FOI as an impediment to getting information.

"We know that things can be hard to find if you don't want them to be found. I think it's reasonable that at any given point in time there are good reasons why organisations can't actually find the truth in a reasonable amount of time, but I think it's reasonable that the community expects the tolerance for that should recede over time."

Essentially, if an organisation or government department could not find information it was asked to provide on a previous occasion, the consequences should be dire if they are asked to do so again in the future and they have not put their house in order in the intervening period.




Conclusion

State and Federal Governments have made progress in overturning the perception that information access is opaque and open to risk of cyber threat, corruption and ineffective governance.

The goal is to embed security into people's jobs, enhancing their security awareness and that of their respective company, department or organisation, making it a seamless part of using products and embedding it into processes, rather than just being a box ticking exercise.

Information is key within any organisation, as is the ability to be able to produce it on demand. Government departments and agencies using Mimecast can still recall and access documents at the push of a button, even if a user has deleted them, so any fraudulent or other unlawful or harmful activity can still be identified and dealt with, which is of critical importance.

All attendees demonstrated that they're focused on collaboration. There are huge opportunities to collaborate in this sector and it's of paramount importance that those opportunities are seized upon.

Their roles in the public sector are predominantly about ensuring they keep citizens safe, and getting the balance right between that and the privacy of individuals and organisations. It is a delicate task but one that seems eminently achievable, if the collective views and approach of the event attendees are anything to go by.

Mimecast

Level 3
55 Southbank Boulevard
Southbank Vic 3006
Melbourne, Australia

1300 307 318
+61 3 9017 5101

mimecast.com

mimecast®