Shelston IP Lawyers

itnews

SC MAGAZINE FOR IT SECURITY PROFESSIONALS

Understanding Australia's new Privacy Act

An IT systems and policy response to compliance

Authors **Mark Vincent,** Partner, Shelston IP

Brett Winterford, Group Editor, iTnews.com.au

January 2014

Table of Contents

With thanks to our sponsors

blancco IMPERVA splunk>

FOREWORD

By March 2014, Australian organisations with annual revenues of over $3 million will need to comply with an amended Privacy Act.

Broadly speaking, the new laws sharpen existing requirements under the current Privacy Act. As Mark Vincent, co-author of this report has often stated, compliance with the existing Act probably gets you 95 percent of the way to complying with the amendments.

But neither Mark nor I are convinced that most organisations are compliant with the existing Act. That hasn't been too much of a problem in the face of a Privacy Commissioner that lacked the sole authority to name, shame and fine organisations found to have breached the Act; not to mention the absence of Data Breach Disclosure laws that would have compelled organisations to make these breaches public.

The Privacy Act amendments give a series of powers to the Privacy Commissioner to audit, to accept enforceable undertakings and to apply to the Court for an order that an organisation pay a penalty for breaches of the act. This, above all else, should be a primary driver for IT and InfoSec professionals to revisit compliance efforts.

There are also some subtle nuances organisations need to get a handle on with regards to the obtaining of consent and the due diligence Australian companies need to complete before sending customer data offshore.

IT departments have found it difficult to gain access to Australia's Privacy Commissioner to have vagaries in the amended Act clarified as his office is inundated in the lead-up to the Act coming into law. While the Office of the Australian Information Commissioner has not vetted this report, we expect it will provide some of those answers.

In a recent survey of CIOs conducted by *iTnews*, around a quarter said the amendments were not even on the radar just yet. The same number felt compliance was a high priority that required urgent attention.

We hope this guide is a good start.

-- Brett Winterford

Shelston ip Lawyers

itnews SC MAGAZINE FOR IT SECURITY PROFESSIONALS

AMENDMENTS TO AUSTRALIA'S PRIVACY ACT

A legal overview

- Amendments made to the Privacy Act 1988 by the *Privacy Amendment (Enhancing Privacy Protection)* Act 2012 come into force on 12 March 2014.
- The Australian Privacy Principles (APPs) will replace the current National Privacy Principles (NPPs).
- There are a number of changes, including a general obligation to implement compliant privacy practices, new privacy policy requirements, new procedures for dealing with unsolicited personal information and new requirements for direct marketing.

Specific Changes

Who must be compliant?

- The new APPs are a single set of privacy principles applicable to "APP entities": government agencies and *"organisations".*
- There is no change to definition of *"organisation",* which continues to mean any individual, body corporate, partnership, unincorporated association or trust that is not a small business operator (a small business generally has less than $3 million annual turnover).

What information must be protected?

- The definition of *"personal information"* remains substantially the same. As amended, *"personal information"* means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not.
- The emphasis remains whether the information, together with any other information the organisation may reasonably be able to access, allows the organisation to identify the individual.
- The amendments apply to all personal information you hold – even if it was collected prior to 12 March 2014.

General obligation to implement privacy practices

- APP 1.2 introduces a new general obligation on organisations to take reasonable steps *"to implement practices, procedures and systems"* to ensure compliance with the APPs and allow them to respond to privacy inquiries and complaints.

Privacy policy requirements

- APPs 1.3 to 1.6 impose new requirements for privacy policies. Under APPs 1.3 and 1.4, an organisation must have a clearly expressed and up-to-date policy about its management of personal information, including:

  - the kinds of personal information it collects;

  - how it collects and holds personal information;

  - the purposes for which it collects, holds, uses and discloses personal information;

  - how an individual can complain about a breach of the APPs and how the organisation will deal with such a complaint;

  - whether the organisation is likely to disclose the personal information to overseas recipients; and

  - the countries in which overseas recipients are likely to be located.

Under APP 1.5, the privacy policy should be available free of charge and in an appropriate form.

Unsolicited personal information

- APP 4 introduces new procedures for dealing with unsolicited personal information. Unsolicited personal information is personal information received by the organisation that it has not requested. Where an organisation receives unsolicited personal information, it must determine whether it could have collected the information under APP 3 if it had solicited the information.

- If the organisation determines that it could not have collected the information, and if the information is not contained in a Commonwealth record, the organisation must destroy or de-identify the information, if it is lawful or reasonable to do so.

Direct marketing

- APP 7 introduces new requirements for direct marketing. An organisation must not use or disclose personal information for the purpose of direct marketing, unless it meets the requirements of APP 7.2 or 7.3.

- APP 7.2 applies where the organisation collected the personal information from the individual and the individual would reasonably expect the organisation to use or disclose the information for direct marketing. In those circumstances, an organisation may use or disclose personal information if the organisation has provided a simple means to opt-out of direct marketing and the individual has not opted-out.

- APP 7.3 applies where the organisation collected the personal information from a person other than the individual or where the individual would not reasonably expect the organisation to use or disclose the information for direct marketing. In those circumstances, an organisation may use or disclose personal information if the individual consents or it would be impracticable to obtain consent, and the organisation has provided a simple means to opt-out of direct marketing and the individual has not opted out.

Cross-border disclosure

- APP 8 introduces new requirements for cross-border disclosures of personal information. Under APP 8.1, before an organisation discloses personal information to an overseas recipient, the organisation must take reasonable steps to ensure that the overseas recipient does not breach the APPs. New section 16C deems a breach of the APPs by an overseas recipient to be a breach by the organisation.

- APP 8.1 does not apply if the overseas recipient is subject to a law or binding scheme that has the overall effect of protecting personal information in a substantially similar way to the APPs or if the organisation has expressly informed the individual and the individual consents to the disclosure after being informed.

Access and correction

- Under APPs 12.4 and 13.5, organisations are now required to respond to requests for access to personal information and requests to correct personal information within a reasonable time.

Pseudonymity

- Under APP 2, individuals must have the option of dealing with an organisation anonymously or pseudonymously, unless identification is required by law or where it is impracticable to deal with the individual anonymously or pseudonymously.

Commissioner's enforcement powers

The changes also give the Commissioner a new set of enforcement powers.

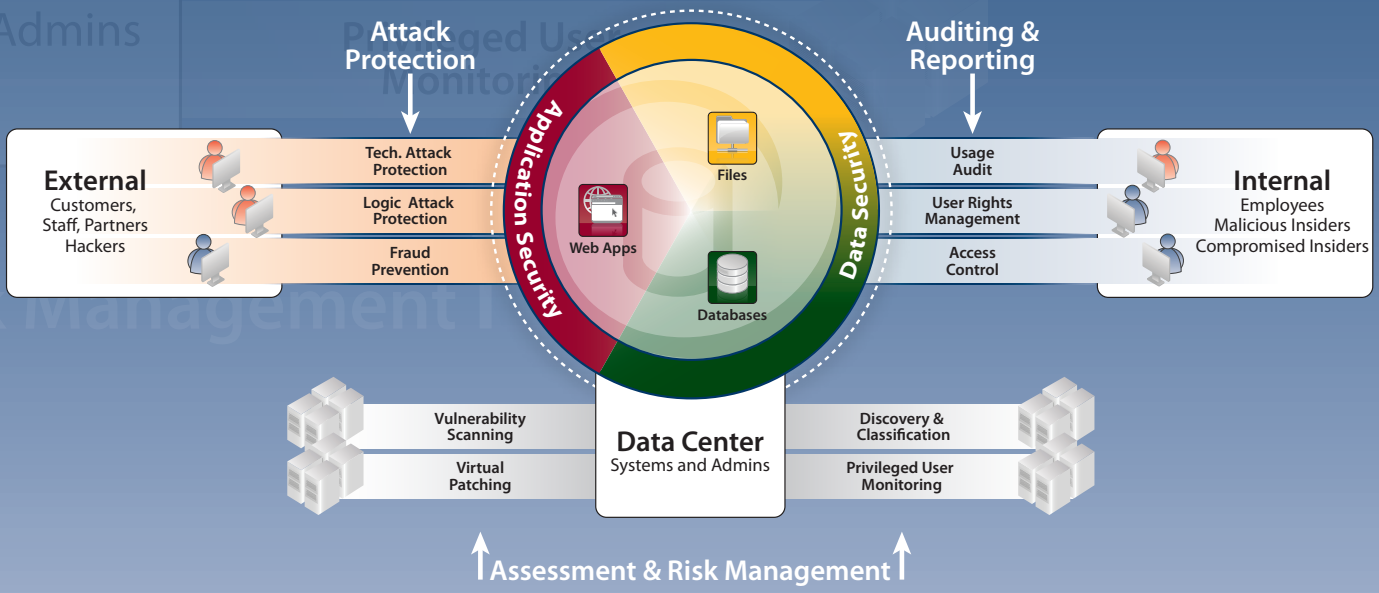
- A breach of the APPs is deemed to be an interference with the privacy of an individual: s.13(1). Where an organisation engages in a serious interference or repeatedly engages in interferences, the Commissioner may apply to the Federal Court or Federal Circuit Court for a civil penalty order against the organisation of up to $1.7 million.

- The Commissioner has the power to accept and enforce written undertakings: ss.33E and 33F.

- The Commissioner may investigate interferences with the privacy of an individual, whether as a result of a complaint or on his own initiative. After investigating, the Commissioner may make a determination requiring the organisation to take certain steps. The Commissioner may commence court proceedings to enforce the determination.

MEETING SECURITY AND DATA PRIVACY REQUIREMENTS

Imperva, pioneering the third pillar of enterprise security, fills the gaps in endpoint and network security by directly protecting high-value applications and data assets in physical and virtual data centres. With an integrated security platform built specifically for modern threats, Imperva data centre security provides the visibility and control needed to neutralize attack, theft, and fraud from inside and outside; to mitigate risk; and to streamline compliance – all without adding complexity or slowing down your business



Meet Australian data privacy requirements for data stored in databases and files with tools specifically designed for the task. Imperva SecureSphere provides a solution that resides in the data centre itself. This comprehensive data audit and protection solution:

» Automates monitoring and controls for databases and files
» Prevents data theft for your most private information
» Audits sensitive data and privileged users
» Strengthens data privacy, and manages user access rights

With Imperva SecureSphere you can streamline your process and meet the mandates of data privacy regulatory compliance – and still ensure information confidentiality, integrity and availability.

Imperva Australia
Level 20, Tower 2 Darling Park | 201 Sussex St | Sydney, NSW 2000 | Australia | Tel: +61 2 8916 6260

Key issues for IT and Infosec professionals

Managing consent in the age of big data

The amended Privacy Act should be studied in detail by any organisation intending to engage in 'big data' - the hoovering up of large unstructured datasets for long-term storage on commodity hardware for later analysis.

The amended Act requires the organisation to notify a user of the intended purpose of collecting the information at the point that personal information is collected. Consent must also be kept up-to-date - customers should be informed of when their data may be used for a different purpose to what was communicated when it was collected.

This is a clear point of tension in the big data era - organisations are storing more data than ever, much of it unstructured (often machine data). The price point to capture data (using social networks or machine data logs), to store it (using commodity file storage and file clustering software such as Hadoop) and to analyse it (using query tools like MapReduce) has encouraged organisations to retain data for far longer periods of time.

The intention is for this data to later be analysed to improve products and services to the benefit of the customer and ultimately the profitability of the collector. But often the collector of the data won't fully comprehend what questions will be asked of it at the point of collection.

Organisations will thus be tempted to seek broad and open-ended consent from users before they sign up to a service or offer their personal data. The Privacy Commissioner has made clear that this will be frowned upon in any audit, as would an organisation coupling consent with permission to use the service or bundling consent up with a large number of other terms and conditions in a long and arduous agreement few users would be likely to read.

Further, the Act requires organisations to destroy or de-identify data once it has been used for the purpose it was collected, which complicates not only big data strategies but mobility strategies (is data stored on client devices?), CRM systems (do you have a single customer record?) and business continuity (is your data replicated across clusters or data centres in the name of redundancy and disaster recovery?).

It does not, however, override existing regulations that seek for organisations to retain data (for audit or discovery purposes, for example).

See recommendation 3 on page 14 for how we propose organisations approach these issues.

The Privacy Act's view of offshore clouds

Australia's new Privacy Act will come into effect during a period of tremendous turbulence in the technology sector, owing to a surge in subscriptions to cloud computing services.

Organisations looking to public cloud computing services that are hosted offshore will need to consider Australia's amended Privacy Act in detail. The new Australian Privacy Principles (APPs) deal with transborder data flow slightly differently to the current legislation (see APP 8.1 on page 7).

From March 12, if data is disclosed offshore to a third party provider, your organisation can be held vicariously liable for any breach by that third party. If there is a breach at your cloud computing provider, it is treated as your breach.

It is important for CIOs to consider two exceptions to this rule.

The first is if — in the case of a breach — an organisation can prove that they are disclosing the data to a jurisdiction with the same privacy rigours as Australia, or have otherwise contractually bound their third party provider to provide protections that would meet APP standards.

These assurances are unlikely to be found within the generic contract an organisation would sign with a global provider of commodity cloud computing services (Amazon Web Services, Google, Microsoft, Rackspace etc), and require an organisation to consider additional due diligence, bespoke contract negotiations with cloud providers or the use of additional security controls.

The other exception for those organisations considering subscribing to offshore cloud services, call centres or direct marketers is to first gain the consent of affected individuals before the data is transferred.

As previously described, this consent must be timely, specific and 'informed' - not buried within a unwieldy set of terms and conditions.

Protect valuable company data with Blancco.

Don't damage your brand with unsafe privacy protection procedures.

Blancco securely erases data to give you the peace of mind that your data breach plan is in place prior to Australia's new Privacy Act to avoid a potential $1.1 million fine.

Be confident your data has been permanently erased with Blancco.

Blancco Australasia
karl.gaines@blancco.com
Australia +61 7 3303 0175
New Zealand +64 9 889 1030
www.blancco.com

blancco
CERTIFIED DATA ERASURE

Recommendations

It is the view of the authors that compliance with the amended Privacy Act is most likely to impact the following areas:

- Privacy policies and direct marketing strategies
- System design of e-commerce and Point of Sale systems
- System design of CRM and customer contact systems
- Audit processes
- Data storage and analysis
- Perimeter security (firewalls, intrusion detection and prevention) and SIEM (security incident event monitoring) systems.

Our recommendations:

1. Assume all customer information is PII

RECOMMENDATION 1.1: Assume all data you collect about an individual is personally identifiable information (PII) and thus caught by the Act.

The most important aspect of the revised Act to consider is that the definition of PII isn't defined narrowly, and could feasibly be applied at the Privacy Commissioner's whim - the same individual that has the authority to levy fines and other penalties against you.

The most basic principle is that it includes all data that could identify an individual - either alone or in concert with other data. The safest path is to assume all customer data is PII.

RECOMMENDATION 1.2: De-identify PII data once the primary reason you collected it has been satisfied.

The amended Act seeks for PII data to be destroyed or de-identified once it has outlived the stated purpose for which it was collected.

If your organisation still feels this data to be of value, consider 'stripping' or 'masking' the data such that a customer record cannot directly identify an individual.

The metadata that remains may still be of value for future analysis.

RECOMMENDATION 1.3: When de-identifying data, use the 'Google Test' as the bare minimum standard for ensuring data can't be re-identified.

The wording of the Act states that PII includes all data about an individual, even if it requires matching with other publicly available data to identify the individual.

It is thus important to ask yourself whether the data that remains after a record is 'de-identified' could be used in combination with a simple web search to ascertain the identity of an individual. If you can infer from this data the identity of an individual, you would be hard-pressed to say it wasn't PII.

Clearly data scientists (and hackers) have superior tools at their disposal for re-identification, the key questions becomes whether their efforts are likely to stretch beyond what the OAIC considers a 'reasonable' level of protection for data.

For that reason, we posit that the 'Google test' might - in the short term - be enough to satisfy the Commissioner.

2. Revisit your privacy policies

RECOMMENDATION 2.1: Update your privacy policy, clearly communicating how personal information is managed and the purpose for which it was collected.

Organisations with annual revenues exceeding $3 million must maintain an up-to-date library of privacy documentation, if only as evidence in the face of an audit that the organisation has taken the Privacy Act seriously. An organisation's privacy policy must communicate the purpose for which data is collected and any plans your organisation has in the immediate future to "disclose" (send or store) that data offshore.

It is advisable for larger organisations to also produce a Privacy Impact Assessment and a Data Spill/Breach policy. While the latter isn't compulsory (data breach notifications are not mandatory by law), the Privacy Commissioner would undoubtedly look favourably on a policy that states what level of notification would be provided to affected customers and the OAIC in the case of a breach.

RECOMMENDATION 2.2: Plan for the unlikely event of a privacy audit.

From March 12, The Privacy Commissioner has an arbitrary right to audit organisations and to seek penalties for non-compliance.

Large organisations should make sure there is responsibility for privacy compliance at the "C" level and consider the appointment of a Privacy Officer to keep privacy and information management policies up-to-date and manage ongoing privacy issues. A Privacy Officer would prepare a plan to cope with a breach or audit and train staff on new privacy practices, procedures and systems.

Smaller organisations should consider starting with the standard/template privacy policies prepared by your law firm.

RECOMMENDATION 2.3: Ensure your privacy policy takes into account the life cycle of customer data.

While your Privacy Policy should ideally be refreshed at regular intervals, consider the tricky issue of consent for future use of PII data within each update. What happens to a customer's data after it is collected? Where is it stored initially, and in what form? How is it transformed (de-identified) in the future? Explain to the user the concept of metadata if that is material to your big data future.

3. Focus on consent

RECOMMENDATION 3.1: The best way to obtain "express, informed consent" is a prominent, plain english, easy to understand summary of how you intend to use personal information at the point of capture, linked through to a larger privacy policy on the web site.

This is perhaps the most important recommendation for compliance with the revised Act.

Organisations are obliged to do more than offer a large clickwrap set of terms and conditions and an 'I agree' button.

We would advise you provide customers a simple, brief description on what you do with their data, linked to the more detailed privacy policy and terms and conditions. It would otherwise be hard to say you have consent that is both 'informed' and 'express'.

While this is relatively simple for online services, it is more difficult out at physical point-of-sale or in the field. Under those circumstances, consider the capturing of consent data using electronic signatures, or promote further reading of your privacy policy by publishing a link to a simplified URL from the receipts handed to a customer.

RECOMMENDATION 3.2: List a legitimate, primary purpose for the collection of PII data, and consider listing a secondary use at the point of collection.

The requirement to be specific about your intentions for use of personal data needs to be balanced against legitimate future uses.

The challenge is to provide a broad enough consent that doesn't wind up as an exhaustive list of purposes for which the data might be used.

We recommend stating a primary and secondary purpose for obtaining consent to cater for future uses of the data.

There is no silver bullet describing how this should be structured, and no case law to rely on (yet).

Consult your legal counsel as to how to structure the communication of a secondary use to ensure you strike the right balance.

RECOMMENDATION 3.3: Automate the capture and storage of consent data obtained from users into an audit-friendly system.

Capturing consent data in a format that is searchable will ensure you are best prepared for a privacy audit.

We recommend that you not only record consent information but develop a process that auto-generates triggers for when consent ought to be revisited with a given individual.

4. Invest in adequate IT security

RECOMMENDATION 4.1: Benchmark your organisation against the IT security investments of similar-sized organisations.

The new APP 1.2 introduces a new general obligation on organisations to take reasonable steps *"to implement practices, procedures and systems"* to ensure compliance with the APPs. In addition, the new APP11 requires organisations to take reasonable steps to ensure PII data is protected from interference and unauthorised access, modification and disclosure.

The definition of "reasonable steps" is at the Privacy Commissioner's discretion, by way of ensuring the Act remains relevant over time. We can thus assume the standard of IT security required to meet the Commissioner's expectations will be a moving feast.

For the purposes of initial compliance, revisit your IT security systems and ask yourself:

- How up-to-date are your perimeter security systems (firewalls, IPS, IDS)?
- Are these and your customer records systems patched?
- How regularly have you reviewed staff access rights to customer data?
- Have you documented IT security upgrades and updates to IT security policies?

RECOMMENDATION 4.2: Apply security controls according to the sensitivity of personal data.

Name and address data would, by the OAIC's reckoning, be far less damaging in the case of a breach than credit card numbers, an individual's political affiliation or sexual orientation. While there is little to distinguish sensitive from non-sensitive PII data under the law (it is all protected), the steps you will need to take to protect sensitive information that can cause harm are more onerous. Assume sensitive data requires a higher level of protection and invest accordingly.

RECOMMENDATION 4.3: Monitor, monitor, monitor.

Compliance is not a point in time exercise. It needs to be ongoing for the life of any given system.

The Privacy Commissioner has stated that 'checkbox compliance' with the amended Act isn't enough of a defence in the case of a breach. Organisations need to not only invest in IT security tools, but configure them to best practice and, most importantly, *staff* them. Employ analysts armed with Security Incident Event Monitoring (SIEM) systems to monitor your logs for suspicious behaviour, or seek a trusted third party to conduct this activity on your behalf.

RECOMMENDATION 4.4: Where practical, encrypt PII data

Well-resourced organisations should consider use of data encryption technologies, especially when sending data offshore. Test and document the relationship between the level of security afforded a data set via the use of encryption and the performance and cost overhead such a process incurs before choosing a technology.

5. Build a single version of the truth

RECOMMENDATION 5.1: Consolidate customer records

The Privacy Act requires organisations to be able to provide customers the ability to review and seek the modification or deletion of personal information held about them.

Best practice in this regard would be to attempt to build a single view of the customer that allows for customer contact agents to meet these requests with minimal disruption.

RECOMMENDATION 5.2: Check on conflicting regulations before destroying customer data

The Privacy Act insists upon a range of occasions in which a customer's PII data must be deleted - at their request, for example, or once it has outlived the stated purpose for which it was collected.

Stakeholders should first consider whether there is a conflicting regulation that insists upon this data being retained - for audit or discovery purposes, for example. These regulations will vary industry to industry. It is safe to assume that these regulations will trump compliance with the Privacy Act if push came to shove.

6. Push for a better deal on offshore clouds

RECOMMENDATION 6.1: Conduct thorough due diligence on both the security posture of any third party provider and the Privacy Laws in their chosen jurisdiction.

Consider the range of global security certifications (such as ISO27001) a cloud service provider may adhere to, and how far up their infrastructure stack responsibility for security reverts to the user. Document the due diligence done on a chosen provider for consideration in the unlikely event of a Privacy Audit. The *iTnews*' 'Cloud Cover' report may prove useful.

RECOMMENDATION 6.2: Use competitive tension in the cloud services market to seek security assurances that would meet APP guidelines or for access rights for audit.

Numerous large Australian organisations have managed to convince large commodity cloud providers to allow them audit rights or to provide additional security guarantees beyond the standard cloud contract.

Use the threat of choosing competing services (of which there are plenty in every category) to overcome hesitation on the part of your supplier to negotiate on these terms.

Organisations that do not have the scale to negotiate bespoke agreements with these providers should consider the use of additional safeguards to fill any gaps in the cloud provider's security posture, such as encryption and de-identification.

RECOMMENDATION 6.3: Obtain consent from customers for any transborder data flow (use of offshore cloud or contact centre services, for example).

Be transparent with your customers if you intend to use offshore services, and use this transparency to cover off future possibilities for how you might use the data.

Conclusion

There are a range of obligations all organisations need to consider under the amended Privacy Act.

The requirements are both complex for large organisations and onerous for SMEs.

We don't expect all organisations to be compliant come March 12, 2014. But neither do we expect the Privacy Commissioner to be geared up to regulate the many industries caught by the Act.

We expect, as one of our working group so colourfully put it, the Commissioner to "come out firing, and make his point in the marketplace.

"He will pick on a couple of different sectors, drag them through the mire, publicly name shame and penalise to make the point and set the benchmark."

If history is any guide, the OAIC won't brave a fight with one of Australia's largest organisations first off the bat - there is always the risk that the legal resources at their disposal could make a mockery of the Commissioner's newfound powers. Nor will the OAIC pick a business that barely makes the $3 million threshold, only to be accused of being heavy-handed on small business.

If your organisation falls somewhere between, take heart in two comments that resonated at our workshop.

The first, from co-author Mark Vincent, is that the Privacy Commissioner's definition of "reasonable steps to secure information" isn't prescriptive and should be viewed as a sliding scale. More investment in compliance is likely to be expected of large organisations, less of smaller.

The other was from a CIO of a financial services organisation, who recommended organisations consider Privacy Act compliance a journey as much as a destination:

"It's unrealistic to change all systems overnight. The important thing is to have a plan for compliance which details the steps you'll take to get there.

"I don't think there is a panacea for compliance and I also don't think, come March 12, that we are all going to be on the front page of the news. It might be instead that you have a policy which defines a target state, perhaps right now you're only at Level 1 and you want to get to Level 3. Perhaps that's ok.

"But to have done nothing is a brave move."