Submission to Australian Government Discussion Paper

Strengthening Australia's cyber security regulations and incentives

From: Mimecast Australia Pty Ltd

About Mimecast

Mimecast (NASDAQ: MIME) was born in 2003 with a focus on delivering relentless protection. Each day, we take on cyber disruption for our tens of thousands of customers around the globe; always putting them first, and never giving up on tackling their biggest security challenges together. We are the company that built an intentional and scalable design ideology that solves the number one cyberattack vector – email. We continuously invest to thoughtfully integrate brand protection, security awareness training, web security, compliance and other essential capabilities. Mimecast is here to help protect large and small organizations from malicious activity, human error and technology failure; and to lead the movement toward building a more resilient world. Learn more about us at www.mimecast.com.

We opened our first office in Australia, in Melbourne, in 2013 and now we also have an office in Sydney and two Australian data centres. We employ over 110 people in Australia and serve more than 2,000 customers.

Overview of submission

Rather than address all questions raised in the discussion paper, our submission focuses on those which we believe to be the highest priority and likely to be most effective in achieving the government's goal as set out in the discussion paper: "to make Australia's digital economy more resilient to cyber security threats, by uplifting the cyber security of all digitally enabled businesses."

We would note that the distinction of a "digitally enabled business" is largely superfluous: almost every business would, as a minimum, have an internet connection, browse the web and use email, and therefore be at risk of disruption from cyberattack. Such disruption could in turn disrupt the operations of other larger and truly "digitally enabled" enterprises, depending on the role of the compromised entity in the larger enterprise's supply chain.

Therefore, we believe the goal should be to improve the cyber security of all Australian businesses and public sector organisations who are also focusing on hardening their own cyber security postures.

Improving cyber resilience is likely to be particularly difficult for some of the least digitally enabled businesses.

Our submission addresses the following questions raised in the discussion paper.

Chapter 2: Why should government take action?

1 What are the factors preventing the adoption of cyber security best practice in Australia?

2 Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?

Chapter 4: Governance standards for large businesses

5 What is the best approach to strengthening corporate governance of cyber security risk? Why?

Chapter 8: Responsible disclosure policies

22 Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?

Chapter 9: Health checks for small businesses

23 Would a cyber security health check program improve Australia's cyber security? If not, what other approach could be taken to improve supply chain management for small businesses?

24 Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?

25 Is there anything else we should consider in the design of a health check program?

Chapter 11: Other issues

Our views on these questions are as follows

Chapter 2: Why should government take action?

1 What are the factors preventing the adoption of cyber security best practice in Australia?

Mimecast view: There has been much discussion around mandating reporting of ransomware attacks and payment demands, to the point where a private members bill has been submitted that will make this mandatory. We believe businesses need some external pressure to fully acknowledge the risk of ransomware, to take appropriate steps to protect against it, to report ransomware and avoid payment.

Australian results from Mimecast's State of Email Security 2021 report show ransomware to be having a massive, and growing, impact on Australian businesses, and many to be ill-prepared to defend themselves.

Looking at key insights from Australian businesses involved in the report:

- 64% experienced business disruption from ransomware, a massive increase from 48% in 2020.
- 54% paid the ransom, but only 76% of these recovered their data after paying.
- Only 51% of businesses surveyed have a cyber resilience strategy in place.
- 76% of companies surveyed were hurt by their lack of cyber preparedness. This is up from 62% in 2020.

An argument can be made that in the absence of regulation - such as mandatory reporting - a business impacted by ransomware will make fiduciary decisions that represent the best outcome and best value for shareholders. This may not be in the best interests of its supply chain, its customers, or the community at large, because secrecy about ransomware disclosures hides the true extent and cost of the problem and limits greater understanding of the techniques and perpetrators. This lack of understanding significantly compromises efforts to thwart and deal effectively with future ransomware attacks.

More broadly, there is a great need for better training and awareness of cyber threats and risks across all workers – in the private and public sector – that have access to the Internet in their workplace or even remotely, given the current geographically scattered nature of many organisations. The training that is provided is, in many cases, ineffective, because the lessons are soon forgotten. The organisations that display best practice in employee cyber awareness training share a common trait: they all adopt continuous learning and reinforcement as part of their approach. Importantly, these organisations focus on changing security behaviours with their awareness and training, rather than simply treating it as a compliance exercise.

Mimecast's State of Email Security 2021 survey found only 25% of companies practice ongoing cyber awareness training, and 45% delivered training only quarterly, or even less frequently. This is despite employee deception being one of the most common attack vectors. Sixty-nine per cent of respondents had been hit by an attack initiated by compromising a user, and 69% believe risky employee behaviour is putting their company at risk.

By far the most common means of compromising employees is via email deception, and this has surged during the pandemic, with 66% of

Australian organisations seeing an increase in the volume of email-related attacks involving phishing with malicious links or attachments. Even so, 19% of respondents had no email security system at all, leaving them wide open to such attacks. This a bone-chilling state of affairs.

6 *What cyber security support, if any, should be provided to directors of small and medium companies?*

7 *Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?*

Mimecast view: There is certainly a need to raise awareness and understanding of cyber issues and cyber risk among senior business leaders. There are no mandatory requirements in Australia for company directors to hold any certification to prove their cybersecurity competence. However, certifications from the Australian Institute of Company Directors (AICD) are available, highly regarded and highly sought after. They include a course that focuses on the board's role in cybersecurity.

In today's world, knowledge and understanding of cyber issues and cyber risk are as fundamental to business as understanding finance and financial risk. So there needs to be some means for senior business leaders to gain, and be recognised as having, a level of understanding of cyber issues. Recognition of their knowledge of cyber would need to rank equal in importance to understanding of more traditional aspects of a director's role. This is especially true when viewed through the risk lens of a director.

However, such training is unlikely to raise the level of cyber awareness and expertise in smaller organisations that typically do not have AICD qualified directors, only ones qualified by experience. They are unlikely to see the merit in dedicating time to gaining such qualifications. Many are time-poor and already swamped as they navigate changing business conditions and the elevated threat landscape caused by the pandemic. The government should consider initiatives that increase the profile and prominence of programs and materials available that deal with cyber issues and cyber risk for SMEs. If such consideration is not given, a true resilient supply chain will not be achieved.

Chapter 8: Responsible disclosure policies

22 Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?

By and large software vendors have an increasing focus on security by design, but this can sometimes unwittingly be compromised in the quest to release new products and features quickly. That's because speed to market usually trumps the cost to slow down and build secure software. Vendors are moving rapidly to fix vulnerabilities once discovered of their own accord or by third parties. This thirst to find and fix vulnerabilities is evidenced by some vendors offering bounties to third parties who can proactively find and report vulnerabilities.

Voluntary disclosure can and does work when the vendor has the right ethics and approach in place. Even so, with the pace at which malicious attacks, including ransomware, are increasing, speed of disclosure is just as critical as the act of disclosing and fixing vulnerabilities.

With this in mind, mandatory vulnerability disclosure, similar to mandatory ransomware reporting, could be of benefit in creating a consistent approach to cybersecurity regulation and attitudes across industries, from those creating software to those using it. In short, while voluntary disclosure could work, given the tsunami of cyberattacks currently being experienced, mandatory will get us closer to where we need to be, faster.

Chapter 9: Health checks for small businesses

2 *Would a cyber security health check program improve Australia's cyber security? If not, what other approach could be taken to improve supply chain management for small businesses?*

24 *Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?*

25 *If there anything else we should consider in the design of a health check program?*

Mimecast strongly supports, in principle, the introduction of a cybersecurity health check program for small business. We believe this could be very powerful in raising the cybersecurity posture of individual businesses, while also raising awareness of the importance of good cybersecurity practices in small businesses. Small businesses that lack cyber expertise are increasingly becoming the weak link in supply chains that can extend to organisations responsible for critical infrastructure.

Widespread uptake and awareness of such a scheme could result in small businesses that were 'health checked' being looked upon more favourably

when seeking contracts with larger organisations. This would further drive uptake and lift Australia's overall cybersecurity posture.

When considering such a scheme, it would need to be structured and implemented in such a way so as to not to deter small businesses from participating through fear of having failures shown up and on the record, as these could potentially come to light in the aftermath of any future cybersecurity incidents.

Questions that would need to be addressed include:
- Who would administer the scheme?
- How would it be funded? If businesses are expected to pay, they would need to be convinced of the scheme's merits: both through increased cyber resilience and the cachet of gaining certification.
- How could SMEs be assisted to become more 'cyber healthy': ie strengthen their cybersecurity posture? With many SMEs time and cash poor, any health check initiative needs to be combined with a health and fitness program for those businesses found wanting as a result of the health check.

A cybersecurity health and fitness program could be similar to healthcare provided to varying degrees by different countries. Looking at this as an SMB Cyber Health Program, there is a huge opportunity here for a partnership between the private, public and tertiary sectors to offer a service that is free for the first period of engagement. This will allow SMBs to have their cyber health diagnosed, gaps identified and measures put in place for them to achieve a certain standard of SMB Cyber Health without having to make an upfront investment.

To maintain their accreditation after the first year, SMBs could buy the ongoing SMB Cyber Health service at a competitive cost. This would support education and provide real world experience for students, uplift the cybersecurity posture at scale across SMBs and provide a sustainable way for SMBs to maintain their accreditation.

Ultimately, this initiative would help harden supply chains and reduce risk.

This is a very indicative overview of a practical scheme that could have a real and positive impact across all manner of industries, and requires deep consultation and investigation to build the right structure around. But it is one example of a practical pathway that can be created to deliver the necessary baseline accreditation needed for SMBs to achieve satisfactory cybersecurity standards. Furthermore, businesses that are time and cash-poor - especially in the current business climate – won't need to pay an upfront cost.

Chapter 11: Other issues

Cyber dangers are now a constant, mainstream threat to the business and personal lives of all Australians, with very real and damaging consequences. Avoiding and dealing with real world dangers have been the subject of extensive, and successful, government awareness raising campaigns in the past. Two prime examples include: the 'slip slop slap' campaign which began in the 1980s to encourage skin cancer protection; and Melbourne Metro Trains' iconic "Dumb Ways to Die" campaign to encourage safety around its trains and stations.

We believe a similarly broad, educational and engaging campaign that puts responsible cybersecurity practices on the mainstream agenda is long overdue. Its primary target should be consumers and small businesses with minimal or no IT skills, to raise awareness and educate them on practical steps they can take to protect themselves against cyberattacks, and the actions to take if they are attacked.

This will have a flow-on effect into larger businesses and public sector departments by the very nature of the campaign's mainstream messaging and communication channels, if created and executed effectively.

By far the biggest cyber danger is ransomware. Available statistics show that more needs to be done to arm organisations with the right defence against agile and enterprising attackers.

As stated earlier, Mimecast's State of Email Security 2021 Report found 64% of respondents had experienced business disruption from ransomware, a massive increase from 48% in 2020. And of the 54% that paid the ransom, only 76% recovered their data after paying.

However, these figures reveal neither the full extent nor the true cost of the problem, given that the commonly-held wisdom is that many organisations pay ransoms, don't report it, hope that their data is unlocked and therefore unwittingly perpetuate the problem.

To combat ransomware effectively it is necessary to have better knowledge of its scale, the perpetrators and their techniques. Such information can only be gained if organisations report details of attacks to a central body.

We believe reporting of ransomware attacks and payment should be mandatory, but first the government must clarify the situation regarding the legality of such payments, which its March 2021 report *Locked Out: Tackling Australia's ransomware threat* clearly stated could in some cases be illegal.

The discussion paper acknowledges ransomware as "pos[ing] the highest cyber security threat as it requires minimal technical expertise, is low cost and can result in significant impacts to a business," (page 6) and says, "Cyber security costs to society include ransom payments," (page 8). Yet the discussion paper makes no other request for input on how ransomware should be combated.

Mandatory reporting – if implemented – must be done so in such a way that it does not inadvertently push the problem underground and undermine its intent. Alongside this, the insurance industry will need to be consulted to achieve clarity on what will and won't be covered if reporting is made mandatory. For example, if mandatory reporting was introduced, would insurance cover some or all of the following aspects: ransomware payments; remediation; recovery; and reputation and ongoing financial damage.

It is our view that the recent increased focus on ransomware in media and political discussion needs to morph into clear, actionable regulations that give businesses and public sector organisations clear guidance and reporting requirements. If left up to individual organisations, short-focused actions will invariably result, reporting will be sometimes non-existent or at times painstaking (as seen recently) and no real long-term gains will be made. On the flipside, clear parameters, education and measurement will drive tangible outcomes.

Yours sincerely,

Nicholas Lennon
Country Manager ANZ
Mimecast