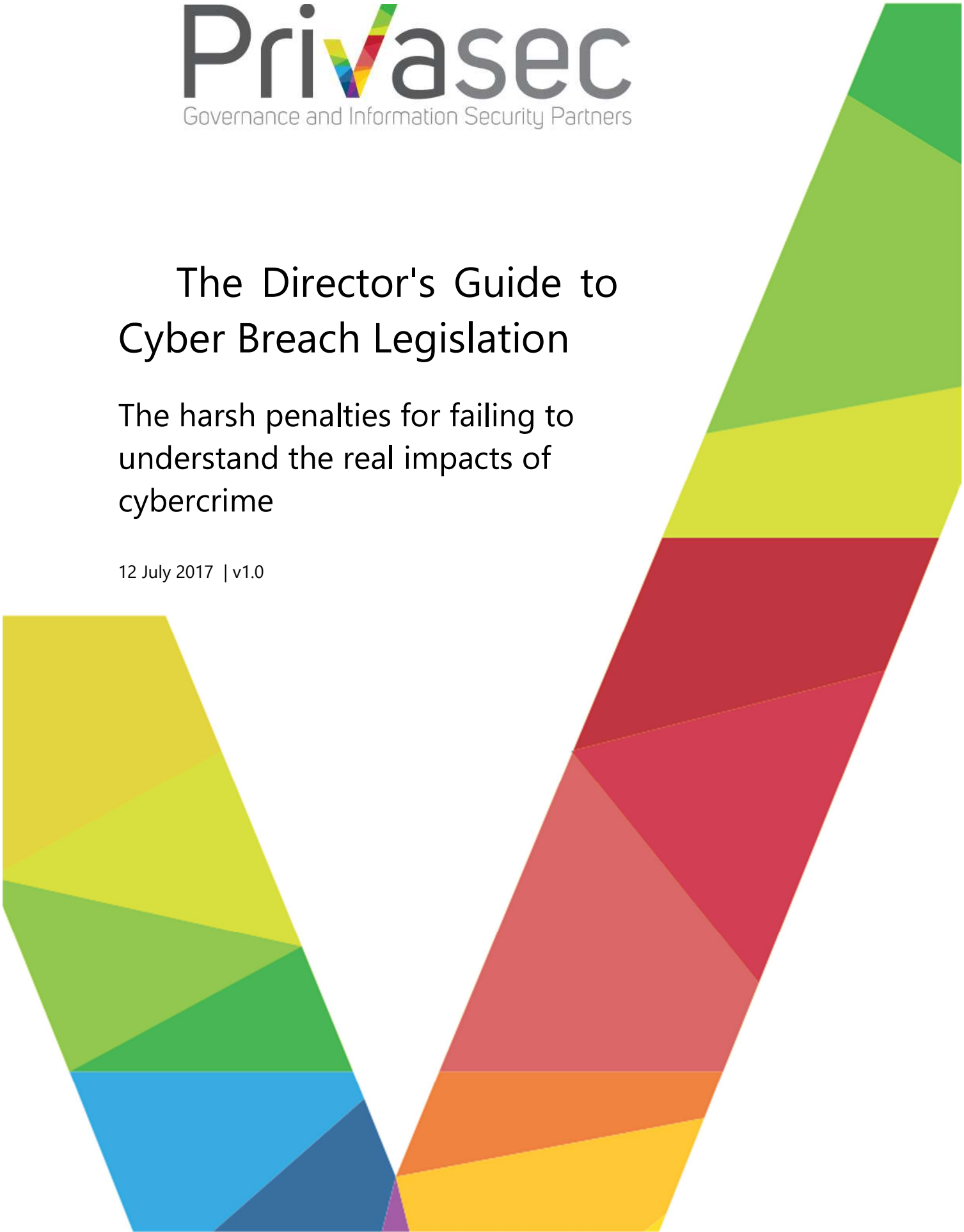
Privasec

Governance and Information Security Partners

The Director's Guide to Cyber Breach Legislation

The harsh penalties for failing to understand the real impacts of cybercrime

12 July 2017 | v1.0



What if tomorrow was your unlucky day and it started with a $1.8 million financial penalty? Imagine if the bottom line of your organisation was reduced by $1.8 million. Now that might not sound like a lot but think about what $1.8 million could represent. It could fund at least ten high profile employees. It might allow you to market the launch of a new product or service. It might be the budget for a project that could move your company to new heights that your competitors simply can't match. We know you can use your imagination here to think about what $1.8 million could buy.

More important than what is why. Why did we ask you this question? Come February 2018, the newly amended privacy act within Australia will come into action with fines to your organisation of up to $1.8 million for failure to disclose a data breach. As we said before, that may not represent a lot of money for an organisation with hundreds of millions of dollars or more in market capitalisation. After all, this may just mean an extra hour or two in generating sales or having each employee work a little longer or a little harder to make up for the loss, but it is just the start of what could be a downward spiral when your organisation faces its next data breach.

Keep in mind that not only are penalties levied at the company level for failure to disclose data breaches, but also at the individual level, which means that executives and directors could also be facing personal losses to the tune of $360,000 per incident.

As an executive or non-executive director, in the same way you need to understand the impacts of competitive and economic threats, it is a necessity, to understand the impacts of cyber threats. There are six kinds of impacts that can occur as the result of cyber threats that progress to attacks and eventually breaches, which are:

1. **Operational impacts** – those impacts which affect the operations of the business. Since operations is usually heavily dependent on people, process, and technology working in tandem, any disruption to the function of one or more of these constitutes an operational impact. Some common operational impacts are technology failures, lost productivity, and incomplete, inaccurate, or outdated processes. When ABS misjudged how many simultaneous users would use the online Census website in August 2016, this create a denial of service and an operational impact.

2. **Physical impacts** – those impacts which impact infrastructure that the business relies upon. Physical damage that may warrant either repair or replacement could come because of environmental disasters, which may be accounted for in business continuity or disaster recovery procedures, but can also come as a result of cyber threats. A frightening example where a cyber threat resulted in physical

damage was in 2011 when Maroochy Shire Council was attacked by an individual whom became frustrated at being overlooked for an IT role. He proceeded to compromise the industrial control systems and cause sewage to flow into clean water.

3. **Personal impacts** – those impacts which impact people that the business relies upon. This could be people such as employees, business partners, customers or shareholders. Each has an important role in the survivability of the business. Personal impacts can include a reduction in one's quality of life through loss of career, illness, injury or in dire circumstances even loss of life. The Ashley Madison attack of 2015, in which the personal data of members was leaked causing panic amongst some high-profile people who were facing accusations of infidelity. In two cases Ashley Madison members committed suicide, demonstrating that the most sinister of personal impacts can result from cyber threats.

4. **Legal impacts** – those impacts which affect the business because of breaches of contract, breaches of regulation, or breaches of law. Many of these can lead to not only financial penalties but also lost productivity due to time and money spent either in or out of court. The Home Depot breach of 2014, is a classic example, of a breach in which it found itself in court and agreed to pay at least $19.5 million to compensate more than 50 million customers whose credit card details had been stolen.

5. **Reputational impacts** – those impacts which affect employee, business partner, customer, or shareholder trust in your brand. In many cases, reputational impact results in loss of customers or shareholders and could also impact future revenue opportunities by causing a lack of trust in prospective customers or shareholders Often, it can result in a slow and painful recovery, if recovery is even possible. The Yahoo breach which made news in late 2016, is one of many examples, highlighting how its perceived value diminished by around $350 million after it suffered a data breach in which more than 500 million records were stolen.

6. **Financial impacts** – those impacts in which money is lost or stolen. Typically, financial impacts result from fraudulent monetary transactions or extortion from ransomware or other types of cyber threats. A recent example was when Fortescue Metals Group chairman, Andrew Forrest, was legitimately transferring $615,000 from one business to another and his online banking session was hijacked with the money being diverted to a bank account belonging to a cybercriminal.

When all impacts are considered, data breaches have far greater ramifications than the $1.8 million organisation and $360,000 personal penalties for a failure to disclose.

In most cases the true cost of cybercrime is often underestimated because not all impacts have been factored in. Target in the US, after its 2013 breach faced a 46% reduction in its profitability throughout the following financial year, and is still paying the price today with costs having amounted to more than $2 billion to date, despite a data breach insurance claim payout. It is essential that costs be attributed to each possible impact to understand the true costs of impact from previous data breaches and to forecast the cost of possible impacts for future data breaches.

It's not all doom and gloom though. Impact and the likelihood of impact are key measures of a good risk management program which is aimed at understanding which risks can be avoided, which can be mitigated, which can be transferred, and finally, which can be accepted.

It all begins by assessing the risk of exposure to cybercrime for your organisation.

Now that you have read the guide, assess how prepared your organisation is for cybercrime by asking your CISO or CIO, face to face, these five questions:

1. How much would it cost the organisation if our three biggest clients decided to go to a competitor because they lost confidence in our brand after a data breach?

2. How confident are you that our security awareness training will stop users from clicking on links in phishing emails?

3. How much would the three most likely cyber threats cost us in terms of potential damage?

4. Do we have a response plan for cybercrime? When was the last time it was updated or tested?

5. What is the ROI of the people, process and technology that have been deployed by the cybersecurity team over the last three years?

Chances are you will not receive the responses you expected, yet these are questions to which having the answers is essential to creating cyber risk strategies and knowing how to best allocate budget to address cybercrime.

Talk to us about developing a solid governance, risk and compliance strategy and we'll work with you to reduce the risk of having the reputation you have spent the best part of your adulthood creating destroyed by cybercriminals in five minutes.

If you would like to speak to a Privasec consultant who can assist you in closing the holes before a breach takes place, rather than having to report it after the fact, please give us a call on 1800 996 001 for a confidential discussion.