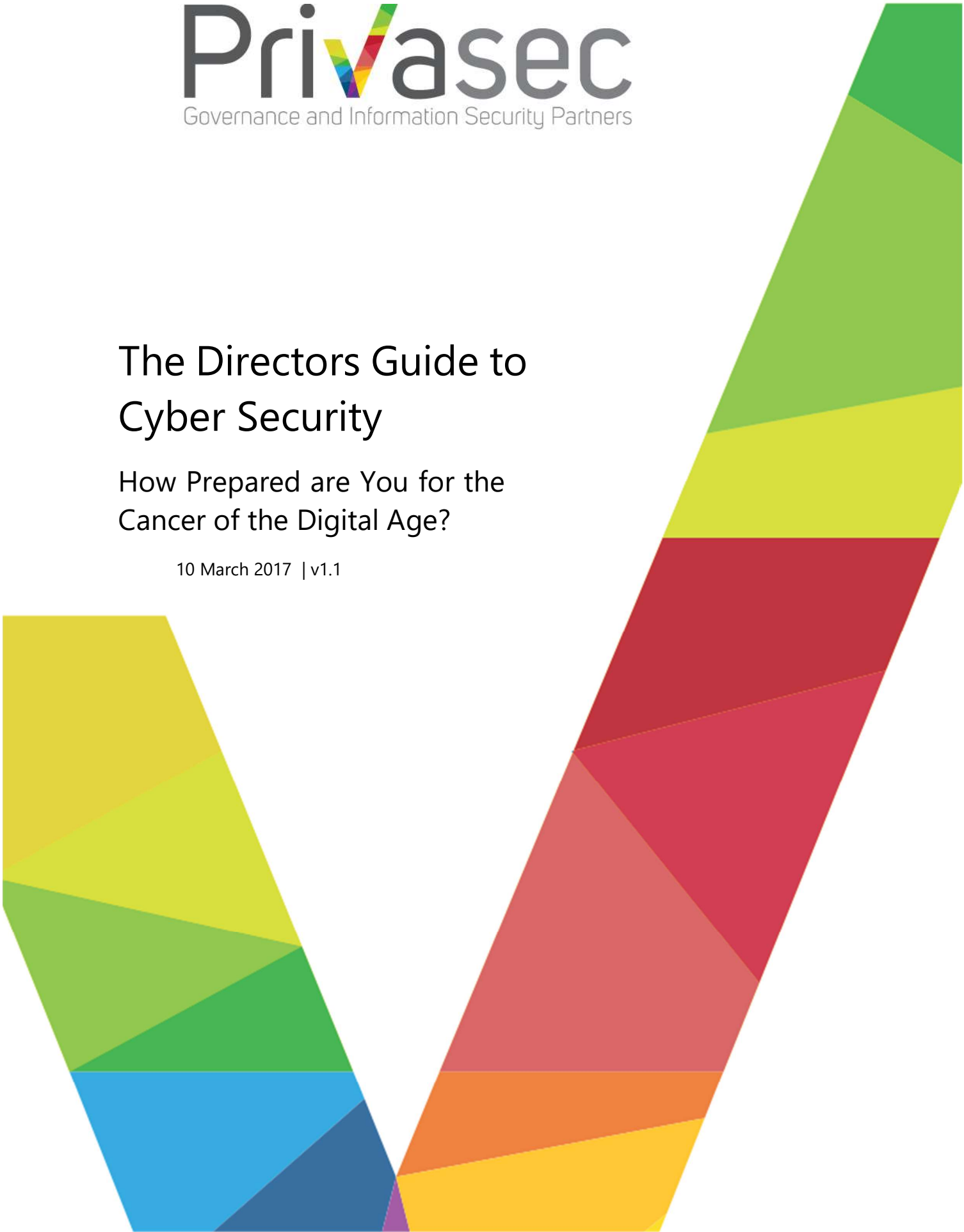
Privasec

Governance and Information Security Partners

The Directors Guide to Cyber Security

How Prepared are You for the Cancer of the Digital Age?

10 March 2017 | v1.1



You have a firewall, anti-virus installed on each computer, security policies, and the best IT security operations people taking care of your organisation's cyber security. Everything is under control, right?

Think again. Sony Pictures, The Office of Personnel Management, Ashley Madison, and Target also had all of these, yet each was vulnerable to cyber-attacks so damning that the CEOs were forced to resign. Having to replace a CEO whilst in crisis mode is a challenge for any board, but it gets worse, much worse.

Consider if you were on the board of a company that had suffered a $252 million loss as the result of a cyber-attack. How do you imagine shareholders and customers would react to that kind of loss? What impact would that have on your conscience? That's the loss that Target faced, resulting in shareholders ousting the board of directors. Imagine waking one morning to discovering your unblemished record of career excellence tarnished by a cyber-attack.

What each of these companies failed to have, which could have reduced the risk of cyber-attack to within the organisation's risk appetite, was a board that was engaged and playing a small, but necessary role in combating cyber-attacks.

To date, most boards have been passive with respect to cyber security simply due to a lack of awareness and understanding of the full impact that cyber-attacks can have on their organisation. A lack of awareness and understanding has put you in a state of fear, uncertainty and doubt which prevents you from being empowered with the best information with which to make informed decisions. Consequently, as the threat of new cyber-attacks increases each day, this puts, not only your organisation, but your tenure as a board member in jeopardy.

With IT, having held the accountability reigns already for so long, it has put your organisation in grave danger of being the next Sony Pictures or Target. Here are some of the problems that have unfolded because IT was made accountable:

1. IT has done what they do best – solve problems with the use of technology. Whilst technology has the benefits of being optimised to perform repetitive tasks over and over 24 hours a day, technology struggles to keep up to date with the rapid pace at which the cyber adversaries are adapting and changing their attack methodologies. This leaves your organisation exposed to newer threats.

2. The use of technology so prevalently by IT has skewed the balance of the arsenal required to achieve an optimal strategy predicated on people, process and technology.

3. The overreliance upon technology marketed as cyber-attack prevention solutions has created a false perception that cyber-attacks can be prevented. The truth is, that eradicating cyber-attacks is no more achievable than eradicating Malaria and Small Pox. Whilst these diseases still exist, these are under control. This is the best we can hope to achieve with cyber-attacks. This means there is a powerful need to be ever vigilant rather than assuming there is some magic solution that can make the entire problem go away.

4. The increasing failure of prevention technologies has left your IT department, or perhaps an outsourced equivalent, scrambling to react spontaneously doing the best they can to detect, respond, and recover from a cyber breach rather than having a well thought out strategic plan that has considered the most likely assets that will be targeted, the most likely vulnerabilities that will be exploited, the most likely threat vectors to exploit those attacks, and the impacts of those attacks.

5. IT's skillset is centred around understanding and mitigating the possible operational impacts to the organisation should technology fail or be compromised in a cyber-attack. More often than not, these days cyber-attacks have resulted in physical, personal, legal, reputational, and financial impacts, all of which IT does not have the capacity to fully comprehend, nor is equipped to deal with.

Directors who take these precautions lightly, and fail to appreciate the significance of these problems will undoubtedly encounter the wrath of the new legislation and amendment to the Privacy Act, that has been passed, making the disclosure of cyber breaches to regulators and shareholders mandatory. The penalty for a breach can be up to $1.8 million for organisations and $360,000 for each board member. Simply put, ignorance and failure to act will not suffice as valid excuses in court.

Change is required if boards want to govern organisations that not only survive but thrive in the digital age we now live in. It is imperative that the change begins right now with the first step being to recognise that IT is not accountable for cyber security, the board must take on that accountability itself.

Next, the board must recognise that cyber-attacks are inevitable and no matter how good your IT department is, or how good your outsourced IT specialists may be, your organisation is being tested each day against the wits and ingenuity of advanced cyber adversaries. If it hasn't been already, it is simply a matter of time before your organisation falls victim to a newsworthy cyber-attack.

The only real defence is to implement a customised cyber security strategy that aligns with the organisational strategy to ensure that people, process, and technology are all leveraged to the full extent to create the best weapon of defence against these cyber adversaries. A downloaded set of policies from the internet is simply not sufficient, it provides a mere illusion of due diligence. Each organisation's cyber security strategy is unique and should focus on the why, what, and how to address any gaps in preparedness for cyber-attacks in your organisation.

Cyber-attacks, are the silent and invisible threats to the inner workings of your organisation. Like a digital cancer, by the time you discover how little prepared you and your organisation really are, it will be too late. Why not contact Privasec now to schedule your security health check and avoid reading about your company in the news. Call 1800 996 001 for a confidential discussion.