NSW Office of Sport

Cyber Security

Adam Irwin | Managing Partner

Carl Millington | Business Advisory

February 2022

Important information

Pitcher Partners

This presentation ('Presentation') has been produced by Pitcher Partners and has been prepared for informational and discussion purposes only. The information provided in this document is of a general nature and has been prepared without taking into account your objectives, circumstances, financial situation or particular needs. This Presentation does not constitute personal advice.

This Presentation has been prepared by us in the ordinary course of our profession. In providing this Presentation, we are not purporting to act as solicitors or provide legal advice. Appropriate advice should be sought prior to acting on anything contained in this Presentation or implementing any transaction or arrangement that may be referred to in this Presentation.

Information contained within this Presentation is based on the relevant law and its interpretations by relevant authorities as it stands at the time the information is provided. Any changes or modifications to the law and/or its interpretation after this time could affect the information we have provided.

This Presentation, or any part thereof, must not be distributed, copied, used, or relied on by any person, without our prior written consent.

To the maximum extent permitted by law, Pitcher Partners will not be liable for any loss, damage, liability or claim whatsoever suffered or incurred by an person arising directly or indirectly out of the use or reliance on the information contained within this Presentation.

Pitcher Partners is an independent member of Baker Tilly International. Baker Tilly International Limited is an English company. Baker Tilly International provides no professional services to clients. Each member firm is a separate and independent legal entity, and each describes itself as such. Pitcher Partners is not Baker Tilly International's agent and does not have the authority to bind Baker Tilly International or act on Baker Tilly's behalf. None of Baker Tilly International, Pitcher Partners, not any of the other member firms of Baker Tilly International have any liability for each other's acts or omissions. The name Baker Tilly and its associated logo is used under license from Baker Tilly International Limited.

Pitcher Partners is an association of independent firms.

Any trademarks, logos, and service marks contained herein may be the registered and unregistered trademarks of their respective owners. Nothing contained herein should be construed as granting by implication, or otherwise, any license or right to use any trademark displayed without the written permission of the owner.

Liability limited by a scheme approved under Professional Standards Legislation.

PITCHER PARTNERS

Opening Comments

Context

- In 2020, customer personally identifiable information was the most common type of record lost and featured in 44% of breaches
- For each lost customer record in 2021, businesses incurred an average cost of $180, up 10% on 2020
- More than half of the attacks in 2020 were triggered by malicious action - either outside or inside the business
- The average loss per successful email compromise event in financial year 2020-2021 increased to more than $50,600
- In 2020 two-thirds of Australian businesses reported a ransomware attack. In the UK it was estimated that at least 70% of sports organisations experienced a cyber incident or breach
- The mean amount paid in ransomware payments in Q2 2021 was US$136,576, and the average downtime caused by a ransomware attack was 23 days
- In the 2021 financial year to 30 June 2021, Australian businesses self-reported losses in excess of $33b
- According to the ACCC, compromised email accounts were responsible for losses of $13.5m through sending or accepting fake invoices
- Cyber security is constantly evolving in response to ever increasing cyber risks. You cannot adopt a “set and forget” approach

Q&A

Q&A

Q1. Bearing in Mind that the majority of SSOs are small organisations with limited resources, is this really necessary for them to worry about this issue as it seems that it only affects the big organisations?

- In most cases, attacks are not targeted specifically at sport organisations, they just happen to be victims of mass campaigns using commonly available tools and techniques which don't need a lot of technical knowledge to be effective.
- It would be unwise to think that there is little risk because it is only a small operation. How many SSOs have the following:
    - Email addresses for your SSO, its employees or volunteers
    - Bank accounts and making payments online
    - Accounts or pages on social sites
    - A website or blog
    - Personal information about your athletes, employees, volunteers, other participants
    - Internal online business systems (e.g. cloud based accounting systems)
    - A system or database with confidential medical or performance data for players or athletes
    - Non-work approved personal devices (mobile phones, tablets, laptops etc.)
    - Work approved personal devices

Q&A

- The increasing frequency of cybercriminal activity is compounded by the increased complexity and sophistication of their operations. The accessibility of cybercrime services – such as ransomware-as-a-service (RaaS) – via the dark web increasingly opens the market to a growing number of malicious actors without significant technical expertise and without significant financial investment.

- In its report for the 2020–2021 financial year, the Australian Cyber Security Centre identified the following key cyber security threats and trends in the 2020–2021 financial year:

  - **Exploitation of the pandemic environment**
    - COVID Related phishing
    - Superannuation scams
    - Online shopping scams / Australia Post / Courier
  - Disruption of essential services and critical infrastructure
  - **Ransomware**
  - Rapid exploitation of security vulnerabilities
  - Supply chains
  - **Business email compromise (BEC)**
    - Average loss $50,600 – 1 ½ times more than previous financial year

Q&A

Q2. How well do you think most employees / volunteers understand the risks posed by cyber security?

- Line between personal / organisation become blurred especially with COVID 19.
    - Human firewall – The path of least resistance
    - Ransomware
    - Business email compromise
    - Personal emails / activities not delimitated from those of the organisations

Q&A

Q3. We titled this session "Are your Crown Jewels safe". What does that mean as it applies to data?

- Are Information assets of greatest value and would cause major business impact if compromised.
- You need to know what value it has, not just for your organisation and customers but also the value to those who may wish to steal it.
- All data has value to someone.

Your most valuable and confidential data (your crown jewels) might include:

- Data assets – such as the information on a CRM database
- Business-critical documents including strategic plans and agreements
- Documents or information that are subject to regulations
- Intellectual property (IP), such as product designs and technical specs
- Personal information – for instance employees' details.

Q&A

Q4. What basic steps can a SSO take to assess the extent of cyber risks it may face, and to determine how it might best protect its 'Crown Jewels" with limited resources?

5 knows of Cyber Security

1. Know the **value** of your data
2. Know who has **access** to the data, e.g.
   - volunteers,
   - 3rd parties,
   - people no longer involved with the organisation
3. Know **where** your data is (especially if it is sitting with someone else)
4. Know who is **protecting** your data
5. Know **how well** it is protected.

Q&A

Three key areas that SSOs should review at a minimum are:

1. Change the culture within the organisation

    a. Awareness training
    b. Simulation testing
    c. Regular board event
    d. Incident response planning

2. Low hanging fruit

    a. Multi-factor
    b. Keep patching and the like up to date
    c. Vendor assessment
    d. Payment processing

3. Protect the crown jewels

    a. Inventory of devices
    b. Inventory of data and where it is kept
    c. Stay on top of those who have access

Q&A

Q5. How can State Sporting Organisations raise awareness within their organisation about cyber security and the risks that exist?

- Formalise staff awareness training, simulation testing etc.
- Repetition is the mother of all learning
- Repeat topics (at least those most important to your organisation) often to ensure buy in
- Be conscious this is harder in a virtual environment
- Stay front of mind

Q&A

Q6. What are some of the key components of an effective cybersecurity management program?

1. Focus on increasing maturity
2. Change culture – not a tick the box exercise, make it front and centre at management level
3. Understand your data, where it is held and who has access to it
4. Catalogue the devices that have access to your data
5. Educate and re-educate your team / staff / volunteers alike
6. Implement MFA

Q&A

Q7. What resources are available for SSOs to help them manage cyber risks?

- Australian Cyber Security Centre - https://www.cyber.gov.au
- Your internet provider; your third party IT provider
- Cyber Aware - Security Awareness Training - cyberaware.com
- Pitcher Partners
  - **Adam Irwin**, Managing Partner, Sydney - Adam Irwin - Pitcher Partners
  - Cyber security article Part 1 - Cyber security – the numbers you need to know Part 1 - Pitcher Partners
  - Cyber security article Part 2 - Cyber security – the numbers you need to know Part 2 - Pitcher Partners
  - Cyber security article Part 3 - Cyber security – the numbers you need to know Part 3 - Pitcher Partners
- Welsh Sports Association – Cyber Security for Sports Organisations

Questions

Pitcher Partners

Contact us

Adam Irwin
Managing Partner
+61 2 8236 7738
adam.Irwin@pitcher.com.au

Carl Millington
Consultant – Business Advisory
+61 2 9228 2249
Carl.millington@pitcher.com.au

PITCHER PARTNERS

Get in touch with us

Visit us
Level 16, Tower 2 Darling Park
201 Sussex Street
Sydney NSW 2000

Email
sydneypartners@pitcher.com.au

Phone
+61 2 9221 2099

Website
www.pitcher.com.au

Thank you