How safe is your Member Data and what’s around the corner

Paul Ramsbottom
Managing Director, ASI Asia-Pacific
Agenda

• Common Threats
• Top 12 Security Best Practices
• Your Association Exec Role
• Q&A

The information contained in this presentation (the “Content”) is provided for informational purposes only, and should not be construed as legal advice on any subject matter. You should not act or refrain from acting on the basis of the Content without seeking legal or other professional advice. The Content is general information only and may not reflect current legal developments or address your situation. We disclaim all liability for actions you take or fail to take based on any Content.
Notifiable Data Breaches
Scheme 12-month
Insights Report

www.oaic.gov.au
12 Month Summary

- 964 notifications
- 35% human error
- 60% malicious or criminal attacks
- 5% system faults
Human Error Data Breaches

- PI sent to wrong recipient (fax): 4
- Insecure disposal: 8
- Unauthorised disclosure (verbal): 11
- Other: 12
- PI sent to wrong recipient (other): 17
- Unauthorised disclosure (failure to redact): 17
- Failure to use BCC when sending email: 24
- PI sent to wrong recipient (mail): 42
- Loss of paperwork/data storage device: 46
- Unauthorised disclosure (unintended release or...): 62
- PI sent to wrong recipient (email): 97

Number of data breaches
Malicious/Criminal Data Breaches

- Phishing (compromised credentials): 153
-Compromised or stolen credentials (method unknown): 112
-Brute-force attack (compromised credentials): 39
-Hacking: 24
-Ransomware: 24
-Malware: 24
-Hacking (other means): 10
-Unknown: 5
-Other: 3
Type of Personal Information Disclosed

- Other sensitive information: 86
- Tax file number: 184
- Health information: 249
- Identity information: 328
- Financial details: 433
- Contact information: 833

Number of notifications
85% of Organisations struggle because their data is captured and stored in disparate, disconnected systems - Silos of Doubt  (According to Research by the Aberdeen Group)
17-31% Brand Value Drop After a Breach

Source: Ponemon Institute
“Monday's share price slump was another blow to the company, whose shares have halved since the first data breach ... in January ...”

"put the cost ... at around $7 million"
Data Loss (Typically) Not Covered Under Corporate Insurance ...
Not-for-Profits ARE at Risk!

- Hacktivists
- Increasing Regulation
- Growing IT Complexity
- More Online Transactions
- Perceived “Easy Target”
ACTE members’ data stolen by hackers

Hackers have stolen data of all members of the Association of Corporate Travel Executives (ACTE).

ACTE’s executive director, Breck Koch said that there had been a “malicious theft” yesterday (August 11) of members’ names and email addresses, although no other data such as credit card details or addresses acquired by the hackers.

Members of the US-based association who receive a “questionable email” from an ACTE email address are being asked to forward it on to info@acte.org.

“The authorities have been notified and tighter security measures have been put in place,” added Koch.

“In the past year, major credit card companies, government agencies, and retailers have all been the target of hackers. As such, we are always reviewing our own data security processes.”

ACTE said that it would not ask members for credit card information or password confirmations through email “until further notice”.

“I regret any inconvenience this situation may have caused,” said Koch.

UK Scouts database 'flaws' raise concerns

System holds records of ALL scouts in the country

23 Jan 2015 at 11:21, Kat Hall
ANU data breach stretching back 19 years detected

The Australian National University has been hit by a massive data hack, with unauthorised access to significant amounts of personal details dating back 19 years.

A sophisticated operator accessed the ANU’s systems illegally in late 2018 but the breach was only detected two weeks ago, the university said in a statement.

Based on student numbers over that time, as well as staff turnover, the university has estimated approximately 200,000 people were affected by the breach.

"We believe there was unauthorised access to significant amounts of personal staff, student and visitor data extending back 19 years," ANU vice-chancellor Brian Schmidt said.
LandMark White under pressure as industry body hits back

By Carolyn Cummins
June 3, 2019 — 6.37pm

The Australian Property Institute has hit back at LandMark White, saying the firm's latest data leak is an internal corporate failure and not an industry-wide issue, as two major banks again suspended the valuer.

On Thursday, LandMark White revealed it had been hit with another data breach and claimed it was the victim of a sabouter bent on destroying the company.
Top 12 Security and Privacy Best Practices
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>• Enforce effective password management policies</td>
</tr>
<tr>
<td>2</td>
<td>• Least privileged user access (LUA)</td>
</tr>
<tr>
<td>3</td>
<td>• Harden client devices by deploying multi-layered firewall protections</td>
</tr>
<tr>
<td>4</td>
<td>• Conduct regular penetration tests and vulnerability scans</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>5</td>
<td>• Require email authentication of all inbound and outbound mail streams</td>
</tr>
<tr>
<td>6</td>
<td>• Implement a mobile device management program</td>
</tr>
<tr>
<td>7</td>
<td>• Continuously monitor in real time the security of your organisation’s infrastructure</td>
</tr>
<tr>
<td>8</td>
<td>• Deploy web application firewalls to detect/prevent common web attacks</td>
</tr>
</tbody>
</table>
9. Permit only authorised wireless devices to connect to your network

10. Implement always on secure socket layer (AOSSL)

11. Review server certificates for vulnerabilities and risks of your domains being hijacked

12. Develop, test, and continually refine a security assurance plan
Understanding PCI Compliance
What is PCI Compliance?

“The PCI [Payment Card Industry] Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including the:

- **Data Security Standard (PCI DSS)** and

- **Payment Application Data Security Standard (PA-DSS)** requirements.”
PCI DSS
• Payment Card Industry Data Security Standard
• Overall Security Standard (Site and Applications)

PA-DSS
• Payment Application Data Security Standard
• Application Specific Standard

Self-Assessed:
Organisation assesses their own compliance

3rd Party Validated:
Organisation hires accredited assessor to complete compliance evaluation

Compliant vs. Validated
✓ PCI DSS Validation + PA-DSS Validation = Maximum Security

✓ PCI DSS + PA-DSS = Proxy for All Data Security
Association
Executive Role
Consider Cyber Liability Insurance
Train Yourself & Staff

- Detect and report email-based threats (phishing)
- Basic account security (secure passwords)
- Protecting devices
- Data handling practices
- Data breach response plan

- Dedicated training / e-learning
  - Regular exercises & simulations
- Consider wider workforce - Volunteers, committees
- Review & minimise unnecessary data holdings
Questions?

Download:
ASI’s Data Security Best Practices & Strategies Whitepaper

www.advsol.com/AuSAENews