THE IPA PRESENTS:

2017 NATIONAL CONGRESS

22 – 24 NOVEMBER

RACV ROYAL PINES, GOLD COAST
Cyber Security and SME’s

Professor Matt Warren,
Deakin University Centre for Cyber Security Research,
Deakin University, Australia.
Structure of Talk

1) SMEs - definition
2) Background
3) Advice
4) Way Forward
Small and Medium-sized Enterprises

The Australian Bureau of Statistics (ABS) defines:

• Micro enterprises have between 1 to 4 employees;
• Small enterprises have between 5 to 19 employees;
• Medium sized enterprises have greater than 20 and fewer than 199 employees.
Small and Medium-sized Enterprises

Why bother?

- Represent 96% of Australian businesses (AIC, 2012);
- Employ 48% of the nation's private workforce in Australia (AIC, 2012);
- Contribute over 33% of Australian GDP (ASMEEA, 2012);
- Definitions of SMEs can vary country to country.
Cyber Crime and Australia - 2015

• 693,053 Cyber Attacks against Australian Organisations in a year.
• Of those attacks 60% were against SMEs.
• StaySmartonline 2015
Average cost per attack

- Denial of service $180,458
- Web-based attacks $79,380
- Malicious insider $177,834
- Malicious code $105,223
- Phishing and social engineering $23,209
- Malware $458
- Stolen devices $13,044
- Virus, worm or trojan $421
- Botnet $867

StaySmartonline 2015
Time to recover per attack

• Average time to resolve an cyber attack is 23 days.
• This time increase to 51 days if the attack was a malicious insider, employee or contractor.
Australian Cyber Security Centre
Threat Report 2017

• The ACSC identified 47,000 major cyber incidents over the past financial year — a 15 per cent increase — and more than half of these were internet scams or fraud. Major Australian businesses were hit by 7,283 of the attacks.

• Defence contractor's SME computer system hacked, files stolen.
What would happen if a SME was a victim of Cyber Crime

- How much immediate business would they lose?
- Could they restore their system and data?
- Could they protect their organisation against future attacks?
- Would customers have confidence in that organisation in the future?
Profile of SME and Cyber Security

In general SMES have the following profiles:

1) Limited budgets and resources;
2) Lack of technical knowledge;
3) Lack of awareness (threats and dependence);
4) Lack of governance processes.
The Unique Role of Accountants

• Many accountant customers would seek advice from their accountants about best practices in terms of cyber security and appropriate security approaches they should implement.

• Accountants have a trusted relationship with their customers.
Accountants have a trusted relationship with their customers, this makes them a potential target.

• An attacker may be after:
  • Information about the Accountant / Clients;
  • Financial Information about Accountant / Clients.
• Stolen data is a financial commodity for attackers.
A SME Cyber Security Case Study
Anonymous

• Anonymous is NOT
  • an organization, a club, a party or even a movement.
  • There is no charter, no manifest, no membership fees.
  • Anonymous has no leaders, no gurus, no ideologists. In fact, it does not even have a fixed ideology.

• Anonymous has no centralized infrastructure but use existing facilities of the Internet, especially social networks.

• “We are ready to hop on to the next one if this one seems compromised, is under attack, or starts to bore us”.

http://www.cyberguerrilla.org
Anonymous Indonesia launched a hacking campaign against Australia after revelations (Snowdon - NSA) of electronic spying from the Australia embassy in Jakarta.

According to Anonymous Indonesia they had hacked 170 Australian websites.

In response to the claims. These sites included Australian government and business sites.

I have identified that five separate hacking groups were involved.
Hacked by ISD_andreas

Stop Spying On Indonesian!!

[#] Indonesian Security Down [#]

justanewbie@isdandreas.org
Hacked By Cyber_Taregh & Jje Incovers

INDONESIAN CYBER ARMY

STOP SPYING ON INDONESIAN...
STOP SPYING ON INDONESIA 😞
GMCNYMOUS For Zombie Event

MR DC - taugeranggetar - VBALZUMEDANG48 - Abdul Mukif - ALL MEMBER HIDDENMOUZ - AL MEMBER INSECT, IPAN
Owned By Malware Vot 10

For Australian Government
Stop All Forms of Tapping Into Indonesia
Or We Will Make Your Internet Network Destroyed
The SME Focus

- Anonymous Indonesia posted the site details of 58 sites that were hacked on Pastebin that were hacked. These 58 sites were all SMEs.
- 4th November, 2013 – The Key Responses Time

<table>
<thead>
<tr>
<th>Time</th>
<th>7am</th>
<th>10am</th>
<th>2pm</th>
<th>5pm</th>
<th>8pm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacked</td>
<td>57</td>
<td>57</td>
<td>50</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>Not hacked</td>
<td>1</td>
<td>1</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
</tbody>
</table>
## The Impact Over Time

<table>
<thead>
<tr>
<th></th>
<th>18th Nov</th>
<th>9th Dec</th>
<th>13th Jan</th>
<th>11th Feb</th>
<th>23rd Mar</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacked</td>
<td>22</td>
<td>21</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Not Functioning</td>
<td>12</td>
<td>13</td>
<td>31</td>
<td>33</td>
<td>35</td>
</tr>
<tr>
<td>Working</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>22</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>58</td>
<td>58</td>
<td>58</td>
<td>58</td>
<td>58</td>
</tr>
</tbody>
</table>
What does the Case Study Show

1) Lack of awareness of being a victim to an attack.
2) Lack of ability to react to a situation
3) Long term disruption of on-line services;
4) Many sites hacked were hosted on third party providers – Gator Web hosting, USA.
Simple Steps to Improve Security

1) Patching Systems – automatic patching of systems;
2) Use strong passwords and 2 stage authentication;
3) Use a cloud based email service and cloud storage;
4) Back up important data;
5) Install Security Software, e.g. anti malware
These four mitigation strategies are more commonly referred to as the ASD TOP 4:

(1) Application whitelisting to ensure that only software that is specified and authorised can run on a system;
(2) Patching third party applications;
(3) Patching operating systems; and
(4) Restricting administrative privileges.
Basic things an SME can do today

1) Patch systems – enable automatic patching;
2) Back up all important data;
3) Use cloud based email system / data storage;
4) Use strong authentication – pass phases, two stage authentication;
5) Set up different accounts, e.g. administrator account, user accounts.
Advanced things an SME can do today

1) Develop a Cyber Security Governance Strategy – ongoing approach;
2) Develop SME policies / best practice approaches;
3) Undertake a Security Risk Analysis review to aware of threats / Risks;
4) Test that the security features in place actually work, e.g. testing back-up approaches;
5) Consider alternatives, e.g. out-sourcing / cyber security insurance.
Issues that’s SMEs face

1) Where to get advice – model of federation – Federal or state?

2) What to do if an SME is a victim?
Cyber Security for Small and Medium Enterprises: Identifying Threats and Preventing Attacks

Discover what common cyber threats and attacks face small and medium enterprises, and what you can do to prevent them.

This course is part of the program IT Security Management, which is one of the building blocks that leads to a Cyber Security degree. Find out more.

https://www.futurelearn.com/courses/cyber-security-business
Conclusion

• SMEs are increasingly dependent on IT system and thus vulnerable to security risks and new emerging security risks.

• The problem is that SMEs may not have the appropriate resources, expertise or understanding of protecting their systems and key data.

• How can SMEs be helped and by whom?
Any questions?

Thank you