IT Security K - 12

Not just a technical issue. It is also behavioural one.
Australian National University 'hit by Chinese hackers'

ANU has spent several months fighting off a threat to its systems, which some reports say can be traced to China.

Australia's top-ranked university says it has spent several months fighting off a threat to its computer systems, which some media reports say have been compromised by Chinese hackers.
The Southport School – IT Team

- Team of 4 supporting two campuses around 1610 students, 250 staff, 310 boarders, and residential families
  - Richard Humphreys – IT Manager
  - Brent Buckley – Network & Systems Administrator
  - Stephen Robinson – IT Support Officer
  - Bryce Murphy – IT Support Officer
The Southport School – Network Environment

• BYOD for years 5 – 12
• Approximately 1200 school owned devices
• 235 HP Aruba access points
• HP Aruba Clearpass
• 2x 1000mbps (1gbps) internet connections
• 2x Palo Alto 3020 firewalls
• 90 switches (HP Procurve / Aruba)
The Southport School – IT Info

• 8 Physical servers hosting 100 virtual servers
• 2.8TB of memory
• 2x HP 3Par storage array replicating between production and disaster recovery
• Avigilon surveillance camera system
• 40kva uninterrupted power supply with est 2.5hr runtime
• Veeam Backup with HP StoreOnce backup appliance
1. Current Threats for Education
2. International Standards & Government Support
3. Technical Best Practices & Solutions
4. User Education
5. Live attack demo (if the demo gods are kind)
Current threats for Education

Ransomware

• TSS has been the victim of 3 ransomware attacks since 2015
• Attacks were infected files delivered to a TSS Mailbox and a Gmail Mailbox
• Alternative delivery methods including – online advertising, infected websites, and local file delivery
Current threats for Education

Privacy
- Data Breach Notification Law
- Cloud storage

Malicious
- Denial of service attacks
- Compromised systems
- Credential Stuffing (same password for everything)
- Social Engineering
Current threats for Education

Credential Stuffing

Breaches — 505 emails found

<table>
<thead>
<tr>
<th>Email</th>
<th>Pwned sites</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:101992@tss.qld.edu.au">101992@tss.qld.edu.au</a></td>
<td>tumblr</td>
</tr>
<tr>
<td><a href="mailto:10580panya.reidler@tss.qld.edu.au">10580panya.reidler@tss.qld.edu.au</a></td>
<td>OnlineSpambot</td>
</tr>
<tr>
<td><a href="mailto:105814@tss.qld.edu.au">105814@tss.qld.edu.au</a></td>
<td>Shatbow</td>
</tr>
<tr>
<td><a href="mailto:106148@tss.qld.edu.au">106148@tss.qld.edu.au</a></td>
<td>Edmodo</td>
</tr>
<tr>
<td><a href="mailto:106719@tss.qld.edu.au">106719@tss.qld.edu.au</a></td>
<td>OnlineSpambot</td>
</tr>
<tr>
<td><a href="mailto:106787@tss.qld.edu.au">106787@tss.qld.edu.au</a></td>
<td>Adobe</td>
</tr>
<tr>
<td><a href="mailto:108467@tss.qld.edu.au">108467@tss.qld.edu.au</a></td>
<td>Lifeboat</td>
</tr>
<tr>
<td><a href="mailto:108865student@tss.qld.edu.au">108865student@tss.qld.edu.au</a></td>
<td>Evony</td>
</tr>
<tr>
<td><a href="mailto:110954@tss.qld.edu.au">110954@tss.qld.edu.au</a></td>
<td>Edmodo</td>
</tr>
<tr>
<td><a href="mailto:14345.student@tss.qld.edu.au">14345.student@tss.qld.edu.au</a></td>
<td>OnlineSpambot</td>
</tr>
<tr>
<td>56008gttss.qld.edu.au</td>
<td>OnlineSpambot</td>
</tr>
<tr>
<td><a href="mailto:tss@tss.qld.edu.au">tss@tss.qld.edu.au</a></td>
<td>OnlineSpambot</td>
</tr>
</tbody>
</table>
Insurance

Cyber Insurance Policy
• Third party claims – compensation
• Business Interruption – loss of income
• Remediation – forensic, and data restoration
Laws, Standards, and Government Support

- We are required to adhere to Australian Law, and Queensland Law
- AUS/NZ ISO 38500 Corporate governance of Information Technology
- NIST /ASD Cyber Security Frameworks
- ACSC - Australian Cyber Security Centre (cyber security incident)
- Office of the eSafety Commissioner (Cyberbullying, illegal content, image-based abuse, and education resources)
- CERT Australia
Technical Best Practices & Solutions

- Apply security patches
- Antivirus / antimalware applications
- Network access controls and segregation
- Password complexity and lockout policies (Microsoft LAPS)
- Full disk encryption (Microsoft Bitlocker)
- Backup
  - 3 – 2 – 1 rule. 3 copies of data, on 2 media types, with 1 remote copy off site
  - Shadow copies for file servers
  - Manual recovery verification
Technical Best Practices & Solutions

• Edge firewall technology
  • Palo Alto Networks, Checkpoint Technologies, Fortinet are all Gartner Magic Quadrant Leaders 2017
• Log analysis
• Integration with user directory
• SSL Decryption
• Cloud based threat analysis (collaboration)
Aruba have published a tech note titled "ClearPass Policy Manager 6.x - Palo Alto Networks Integration with CPPM". This document is used to describe how the Palo Alto firewalls can leverage the Identity tracking features provided by ClearPass. ClearPass integrates with the Palo Alto firewalls as illustrated in Figure 3.
Technical Best Practices & Solutions

- BYOD Device Management
  - Mobile Data Filtering
  - Non TSS network including hot spot Filtering
  - Family Zone & Avrio Mobile Device Management
  - Malwarebytes Endpoint Protection
User Education

• Training Sessions / Presentations
• Phishing Campaigns
• Penetration Testing
• Security and Vulnerability Assessments
Phishing Campaign

- November 2018
  - 64 leaked credentials
- June 2019
  - 15 leaked credentials
Hi Richard,

The Enterprise Bargaining Agreement has undergone a further revision prior to release.

You will have received an encrypted mail titled, “2017 Enterprise Bargaining Agreement”, from Human Resources.

You can view the updated policy in secure mail by clicking on the following link:

Login to Secure Mail

Regards,

Robyn Baker-Wright
Human Resources Manager | The Southport School
Winchester Street | Southport Qld 4215 | Australia
P +61 7 5531 9950 | E +61 7 5531 9977 | www.tss.qld.edu.au
Hi Richard,

Someone recently used your password to try to sign in to your TSS Account richard.humphreys@tss.qld.edu.au.

We prevented the sign-in attempt in case this was a hijacker trying to access your account. Please review the details of the sign-in attempt:

**Date:** Wednesday June 06, 2018 15:25:04 PM AEST  
**IP Address:** 68.80.81.79 (c-68-80-81-79.telstra.com.au)  
**Location:** Southport, QLD, AU

If you do not recognize this sign-in attempt, someone else might be trying to access your account. You should sign in to your account to confirm your identity.

[Review Suspicious Logins](#)

Sincerely,

TSS IT Department
Live Demo