How to keep your Vice Chancellor out of Jail

Dr Nick Tate

9th May 2017
CYBERSECURITY
GOVERNANCE

Did I need to know about that?
What is Cybersecurity and why should you care?

**Cybersecurity**, also referred to as information technology security, is a set of processes, practices and technology solutions which are designed to protect IT infrastructure, (such as computers, smartphones, networks and communication links) together with software programs and confidential or personal data, from unauthorised access, use or destruction.
What could possibly go wrong?

A short summary
US Office of Personnel Management (OPM) – Data Breach

Estimated 21.5m records accessed

Suggested that the stolen data contained 5.6 million fingerprints

OPM had been warned multiple times about their security vulnerabilities

Source: https://www.afge.org/article/victims-of-personnel-records-breach-must-reapply-for-protection/
What happened after the OPM data breach?

OPM Director, Katherine Archuleta resigned on 10th July 2015 shortly after visiting President Obama in the White House.

OPM CIO, Donna Seymour resigned on 22nd February 2016, two days before she was due to testify before a house panel.

A $1 Billion class action lawsuit has been filed.

In July 2015, personal data from the Ashley Madison extramarital affairs website were stolen and subsequently posted to the internet.

Although making people pay to have their accounts deleted, it appears that they were not deleted.

Source: https://www.theguardian.com/technology/2015/aug/20/ashley-madison-hack-your-questions-answered
What happened after the Ashley Madison Data Breach?

- C$760 million lawsuit
- CEO stood down
- Some suicides attributed to the breach

Organised crime

Example values of credentials

- 1,000 stolen email addresses $0.50 to $10
- Credit card details $0.5 to $20
- Scans of real passports $1 to $2
- Custom malware $12 to $3,500
- Stolen cloud accounts $7 to $8
- One million verified email spam mailouts $70 to $150
Data Breaches are just one type of cyber risk
Data Breaches are just one type of cyber risk. Source: Ponemon Institute – Security Beyond the Traditional Perimeter
Couldn’t we just leave this to the CIO?
The right governance can protect the University
What is the right Governance?

Adopt a framework based approach

(1) Clearly determine the current state of cybersecurity across the university through a risk based assessment of all systems, infrastructure, policies and procedures (*possibly using external help*)

(2) Identify short term (12 month) goals for management or mitigation based on an assessment of risk and cost

(3) Similarly identify longer term (1-5 year) goals
Lloyds of London

Cyberisk insurance in the top five
Which framework?

A framework is used to structure the measurement of current and future states.

Several to choose from

NIST Cybersecurity Framework used here as an example.
### NIST Cybersecurity Framework

<table>
<thead>
<tr>
<th>Functions</th>
<th>Categories</th>
<th>Subcategories</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROTECT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DETECT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RESPOND</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RECOVER</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CYBERSECURITY FRAMEWORK CORE

IDENTIFY
- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy

PROTECT
- Access control
- Awareness and training
- Data security
- Information protection and procedures
- Maintenance
- Protective technology

DETECT
- Anomalies and events
- Security continuous monitoring
- Detection process

RESPOND
- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER
- Recover planning
- Improvements
- Communications

OPPORTUNITY FOR FUTURE IMPROVEMENT

Source: https://www.praetorian.com/blog/nist-cybersecurity-framework-vs-nist-special-publication-800-53
## Implementation Tiers

<table>
<thead>
<tr>
<th>Tier</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Partial</td>
<td>Risk management is Ad-hoc with limited awareness of risks and no collaboration with others.</td>
</tr>
<tr>
<td>1</td>
<td>Risk Informed</td>
<td>Risk management processes and programme are in place but are not integrated university-wide; collaboration is understood but university lacks formal capabilities.</td>
</tr>
<tr>
<td>2</td>
<td>Repeatable</td>
<td>Formal policies for risk management processes and programmes are in place enterprise-wide, with partial external collaboration.</td>
</tr>
<tr>
<td>3</td>
<td>Adaptive</td>
<td>Risk management processes and programmes are based on lessons learned and embedded in culture, with pro-active collaboration.</td>
</tr>
</tbody>
</table>
CYBERSECURITY FRAMEWORK PROFILE AND TARGET

Source: https://www.praetorian.com/blog/nist-cybersecurity-framework-vs-nist-special-publication-800-53
How could this Governance be implemented?

1) Agree the framework and approach to be adopted
2) Arrange for a current state security review to be undertaken
3) Assess the outcomes of the review and determine current risk profile
4) Agree the university’s desired risk profiles for short, medium and long terms
5) Develop and implement a plan to go from current to the agreed future profiles
6) Undertake regular monitoring and status reporting
What do you do if nobody is listening?
What do you do if nobody is listening?

1) Institute your own review of the current state of Cybersecurity
2) Use external monitoring such as Bitsight for additional evidence
3) Undertake regular monitoring and status reporting
4) Report your findings through your own Governance channels
5) Clearly document your recommendations and present them through your Governance channels
THE BITSIGHT SECURITY RATING PLATFORM

The BitSight Security Rating Platform generates objective, outside-in ratings on companies’ security performance. Using evidence of security outcomes from networks around the world, BitSight applies sophisticated algorithms to produce daily security ratings.

The BitSight Security Ratings Platform gathers terabytes of data on security outcomes from sensors deployed across the globe. From our data, we see indicators of compromise, infected machines, improper configuration, poor security hygiene and potentially harmful user behaviors. BitSight’s sophisticated algorithms analyze the data for severity, frequency, duration, and confidence and then map it to a company’s known networks, creating an overall rating of that organization’s security performance. These objective ratings, based on externally accessible data, give visibility into a company’s security posture over time.

Source: https://www.bitsighttech.com/security-ratings
Contact and Further Information

Contact details:

Dr Nick Tate

Email: n.tate@uq.edu.au

Phone +61 412 674010