An OWASP Top 10 for Managers

Presenters: Shahn Harris and Dean Carter
Date: 31st August 2012
Company: Lateral Security (IT) Services Limited
Company Overview

- **Company**
  - Lateral Security (IT) Services Limited
  - Founded in April 2008 by Nick von Dadelszen and Ratu Mason (Both Directors)
  - Staff - AKL - 6 people, WGTN - 7 people, Hong Kong - 1 person

- **Services**
  - Security testing (design & architecture, penetration testing, configuration, code reviews, security devices & controls, mobile apps)
  - Security advisory (Lifecycle compliance & audit – ISO, PCI-DSS, NZISM, policy process development, threat modelling and risk assessment)
  - Regular ongoing technical testing and assurance programs

- **Differentiators**
  - True vendor independence
  - Security testing and advisory are our niche specialties
  - Highly experienced and skilled staff
Who are these guys?

- **Shahn**
  - Security Consultant for Lateral Auckland
  - Ex ISP, Finance and Local Government sector (sorry about the rates)
  - Convinced an ex-QSA to wear a fur suit at a hacker con…

- **Dean**
  - Security Consulting Manager for Lateral Auckland
  - Ex ISP, Finance, Telco and Media sectors
  - Recovering ex-QSA
  - Appeared at Kiwicon dressed in blue fun fur…. ‘nuff said
Objectives

- This contents of this presso seemed blindingly obvious to us... but...

  - These 10 aspects of a solution delivery lifecycle are often neglected or ignored in projects

  - As a result security is considered a roadblock

- We want you to embrace security within your project lifecycle without delaying delivery

- As a result your developers can deliver on the technical “bits” (using OWASP of course!)
Sacrebleu!

- **Point solutions are like the Maginot Line**
  - They protect on a single front
  - Exposing every other flank
Holistic security

- Our Top 10 is hand picked by Lateral Security
- This will help project planning and budgets
- Reduce delays by removing roadblocks!
- Allows your Developers to weave their magic
Our Top 10...

1. Data
2. Laws and Regulations and Standards
3. Access Controls
4. Technology Stack
5. Security
6. 3<sup>rd</sup> Parties
7. End State
8. Maintenance
9. Risk
10. Reputational Damage
Data

- **Identify the data you will be touching**
  - PII (Personal Identifiable Information)
  - PCI (Payment Card Industry)
  - Corporate
  - Customer Data
  - Your Customer’s Customer’s Data

- **Classify the data**
  - Classification dictates handling rules
  - Yes, you’ll need a policy
  - May require legal and HR input
    - May not be solely a security or project issue
Laws and Regulations

- Which laws and regulations apply?
  - Privacy Act, local Government etc

- Which compliance requirements apply?
  - PCI DSS, PA-DSS etc

- What are the relevant (internal) policies and standards that apply?

- Where is your data being stored
  - Are you really sure?

- What about data jurisdiction?

- Is it on Megaupload?
Access Controls

☐ Does access need to be restricted? Clue: YES!
   ☐ By IP, MAC, username, other?

☐ Who will have access?
   ☐ Customers, Service Desk, Third Parties etc

☐ Do they really need admin access? No, REALLY?

☐ Is all access authenticated?
   ☐ Level of auth should reflect risks
   ☐ How many different roles exist?
Technology Stack

- Are you innovating or replacing “like for like”?
- Is it technology that your organisation is prepared / able to support?
- Does it fit your IT strategy?
- Do you have enough staff to support it?
- Are your staff appropriately trained / skilled?
- Consider the future
  - Are you an SMB who could be the next TradeMe?
Security

☐ Is it a consideration for every project?
☐ When does the engagement with the security team take place?
  ☐ Start early… keep in touch!
☐ Does the investment in security match the project risks?
  ☐ Internal Wiki?
  ☐ Online Share Trading?
  ☐ Remote access?
☐ Future enhancements could drastically change the security posture
Third Parties

- Makes sense if you don’t have internal skills
- What standards do you require of your 3\(^{rd}\) parties?
  - OWASP, PCI etc
- Do you check their references?
- Do you buy on price alone?
- Do YOUR 3\(^{rd}\) parties outsource?
- CONTRACT – talk to legal and procurement early
  - Right to audit
  - SLAs
  - Code fixes and upgrades
  - Change control
End Environment

- Is it internal or external facing?
  - Access controls! (refer earlier slide)
- Is it transactional?
  - Could it be in the future?
- Type of data?
- Value of data?
  - What is the value to your Organisation?
  - What is the value to your Customers?
  - What is the value to an attacker?
- What is the worst that can happen?
Maintenance

- You’ve built it…. It’s gone live...
- **Who maintains it?**
  - Internal / External?
  - SLAs
  - Do they understand the tech stack?
  - Are they up to date with threats and vulnerabilities?
- **You need to maintain your investment**
  - New threats evolve
  - It is cheaper to maintain than rebuild
- **Operational security processes**
  - Change Control
  - Vulnerability scanning,
  - Patching
  - Log review
Risk

- There is no such thing as 100% secure
- Understand your risks
  - Communicate them with the Business
- Start simple if you have nothing
  - Track risks on a risk register
- Use risk register to drive remediation budget
- Do you understand the real implications of the risks you are signing off
- Again… ask yourself and others…. What is the WORST thing that could happen?
  - The concept here, is not to spread fear, but to get team buy-in
Reputational Damage

- Ask your CEO how he/she would feel
  - To be on the front page of the NZ Herald
  - To be the feature story on the News at 6
  - Be on the Register for emailing out passwords to your conference

- Rebuilding a server is easier than rebuilding your reputation
  - Keeping it patched is even easier

- Marketing have great ideas
  - Balance them with your Security Pessimist!
Parting Thoughts

- Make an attempt to bridge the gap between tech and management
- Balance the security controls
  - Prevent – Detect – Correct
- Point solutions are like the Maginot Line
- Laws and regulations are your friends
  - Use them to improve security awareness and drive budgets
- These 10 tips are just a tiny part of the security puzzle
Contact Details

Lateral Security (IT) Services Limited

Wellington

38-42 Waring Taylor Street (level 7, Petherick Tower)
PO Box 8093, Wellington 6143, New Zealand
Phone: +64 4 4999 756
Email: sas@lateralsecurity.com

Auckland

187 Queen Street (level 8, Landmark House)
PO Box 7706, Auckland, New Zealand
Phone: +64 9 3770 700
Email: sas@lateralsecurity.com