Griffith and the 2014 G20

IT Security response to the 2014 G20 Summit

Greg Vickers

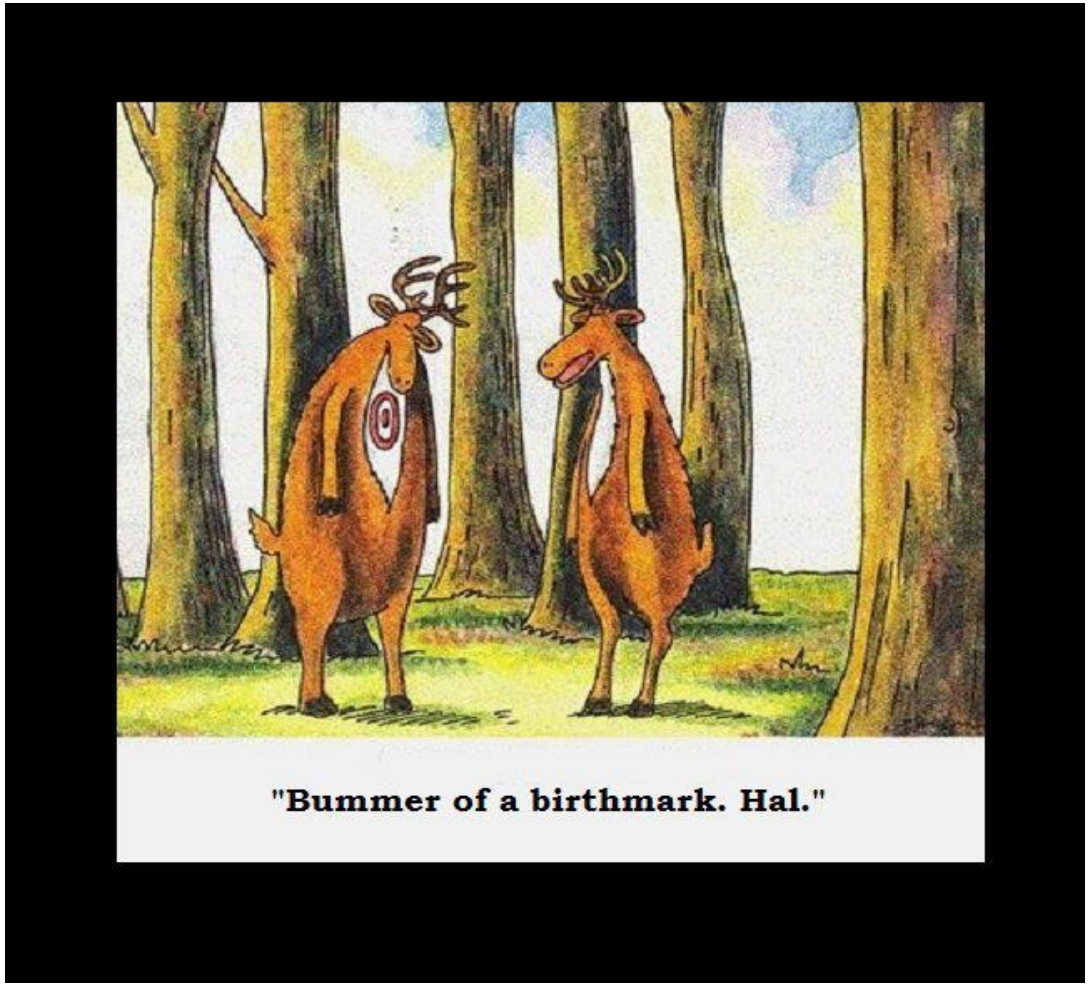
Senior Project Manager

About Griffith

- Closely involved in G20 Summit in Brisbane
- 5 campuses, South Bank campus within a kilometer of the G20 Summit location
  - Some G20 events held at South Bank campus
- ~46,000 students (2014)
- ~10,000 staff (2014)
- lots of endpoints
- 10Gb Internet connection

G20 and Development Conference

Target



Risks

- Risks identified to public and student facing systems
- Breach, defacement, data loss, etc
- Front page of a newspaper or website
- Insider threat

Mitigations

- Managed Security Service (Symantec)
- Cloud-based Application Firewall (Akamai)
- Hosted DDoS protection (Akamai)
- Existing Unified Threat Management system
- 24/7 attention paid to all new and existing mitigation processes during, before and after Summit

Implementation - MSS

- Fairly easy to implement
- Low potential impact on staff/students from required changes
- Point-and-click user interface
- Good graphic views into our data
- Six month engagement

Implementation - Hosted DDoS

- Fairly easy to implement
- Low potential impact on staff/students from required changes
- Point-and-click user interface
- Four month engagement

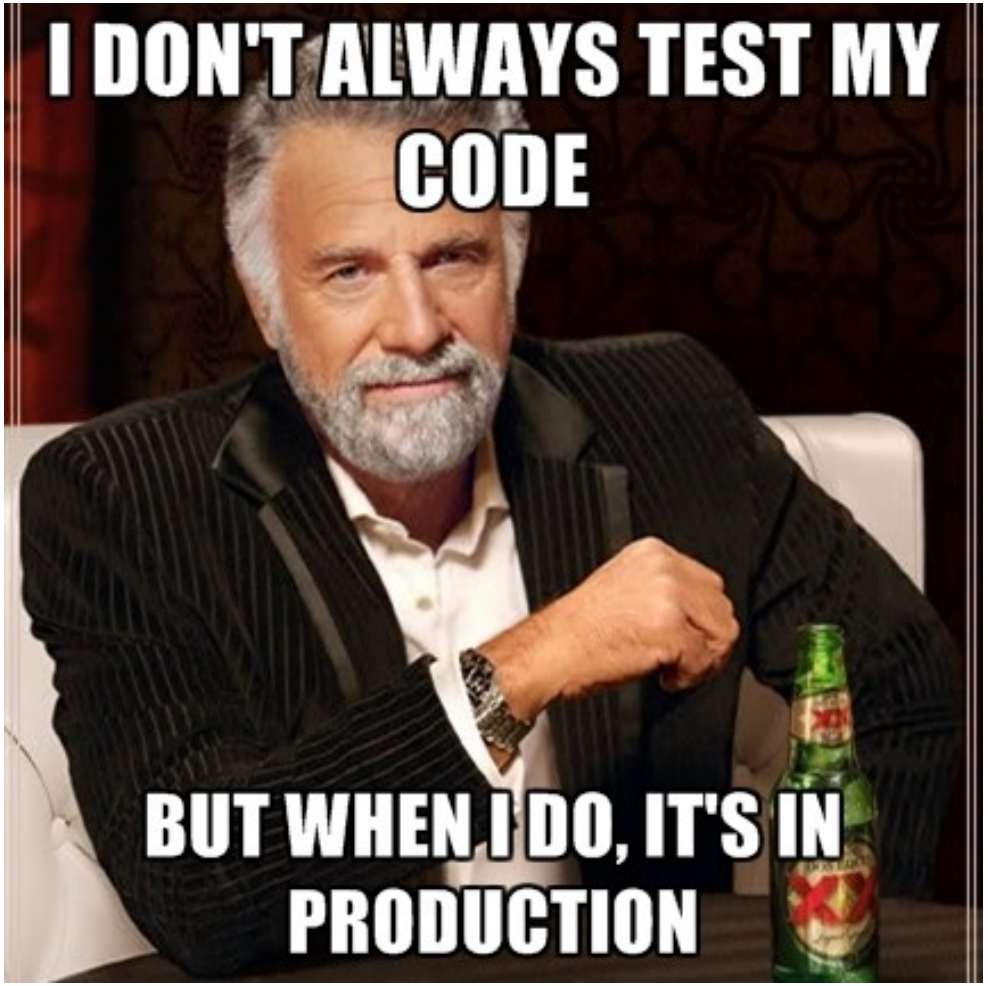
Implementation - Application Firewall

- High difficulty to implement
- High potential impact on staff/students from required changes
- Point-and-click user interface
- Four month engagement

Implementation - Application Firewall

- Pace of project brought scope changes
  - 19 web sites, three months (unheard of)
    - Blackboard
    - CMS/Intranet
    - ERP system
    - SSO, Exams/Timetabling
  - DNS Registrar changes
    - Akamai and Griffith DNS connected at the hip (risk of Akamai DNS failure)

Implementation - Application Firewall



Implementation - Application Firewall

- Testing:
  - Alternate DNS entry created to point at production
  - Web service/site owner engaged to test functionality on their production site/data
  - Internal IT Security specialists worked with owners and vendor technicians on configuration

Implementation - Application Firewall

- Potential Very High impact on staff or student services
- Brought some speed increases to static content
- Web team investigations found delivery delays in Griffith homepage
- Protected against Internet-based attacks
- Decommissioning easy (too easy!)

Implementation - UTM

- Fairly easy to implement, had much attention from networking staff
- Some potential impact on staff/students from required changes, but managed closely
- Familiar user interface
- Ongoing (existing) engagement

Obligatory graph

- Raised profile of Griffith in the international bad guy community

Success!

- No web sites defaced
- No successful attacks detected
- No mass malware outbreak
- No newspapers or web site for the wrong reason

Thank you!

Questions?