Cyber Security- incidents and anecdotes from Ireland

1. Introduce myself
2. Outline of talk
3. Travelex
   1. An example of a Ransomware attack
   2. Sodinokibi is the name given by security analyst to the attack
   3. REvil is the name the developers called it – on request
   4. Contacted BBC news and told them about the ransom
   5. They said they would start releasing data in 7 days – more than 7 days ago
   6. So – why didn’t TravelEx fix the vulnerability?
4. Sequence of an attack
   1. Behind scenes companies (like Microsoft) and security companies and individuals work to discover vulnerabilities in software that we all use
   2. Sequence once vulnerability and patch is released
   3. Note – easy to buy, not necessarily on the dark web as malware can be distributed as a “help” to firms and businesses and their security personnel
5. Speed and Spread of an attack
   1. In 2001 a “worm” spread very quickly
6. Check if GIF working
7. Context
8. Graphic
9. Cyber Security in Ireland
   1. Two government sponsored bodies promoting Ireland as place to go for Cyber security
10. In the South –
    1. Strong talent pool (land of saints and scholars)
    2. A nice corporate tax rate
    3. 5 of top 10 worldwide security companies are in Ireland
11. Well-known cyber companies in Ireland
    1. Symantec
    2. IBM
    3. McAfee
    4. Sophos etc
12. Home-grown companies having an impact abroad
13. InvestNI website - I added the red ovals
14. Cyber security companies in NI
    1. CSIT – Centre for Secure Information Technologies, spin-off group from Queen’s University Belfast
    2. Fujitsu – frictionless border technology
    3. SaltDNA – based in Belfast
    4. Titan IC – hardware for cyber security
15. Another example
16. Anecdotes – I asked local ALs and staff for stories (slides 17-22)
17. Impersonation
18. What do you think?
19. What happened next
    1. Note how things have moved on
20. Plagiarism
21. Malware
22. More Malware stories
    1. Variation on ‘the dog ate my homework’
    2. How much malware is out there
23. Interactive Poll
24. Phishing
    1. Note – spear phishing
25. Permission issues
    1. Unexpected 2 factor authentication – we have been told to look out for unexpected emails and events so this was potentially worrying
26. Scary
27. Poll
28. Risks
29. Protection (sensible passwords – 2 or 3 unrelated words, for example objects in a familiar room)
30. Thanks!