Barbican
INSURANCE GROUP

2018 A Challenging Year

James Mckinlay / Information Security Officer

Together we rise …

… divided we fall

There is an “asymmetry” between attackers and defenders. Attackers are agile, well researched and not bound by policy, procedure or budget cycles.

Defenders on the other hand …..

Agenda

1. Confidence in our abilities (“Situation Awareness”)
2. Confidence we can stand together against common threats (“Intelligence Sharing”)
3. Confidence in our approach to Cyber Essentials (“Raising the cost to the attackers”)

Background

1. Worked in Financial Services, Travel, Retail, Critical Infrastructure, MSSP
2. ISO27001, PCIDSS, SOC-II, NIST, FCA, T20 Critical Controls, Cyber Essentials
3. Last role managing a 20 seat Security Operations Centre / 150K IP addresses
4. First admin access 1989, first remote access 1996
5. Codes C, Java, bash, ruby, python
6. Believes anything can be automated ☺
7. Always been a defender !

Situation Awareness

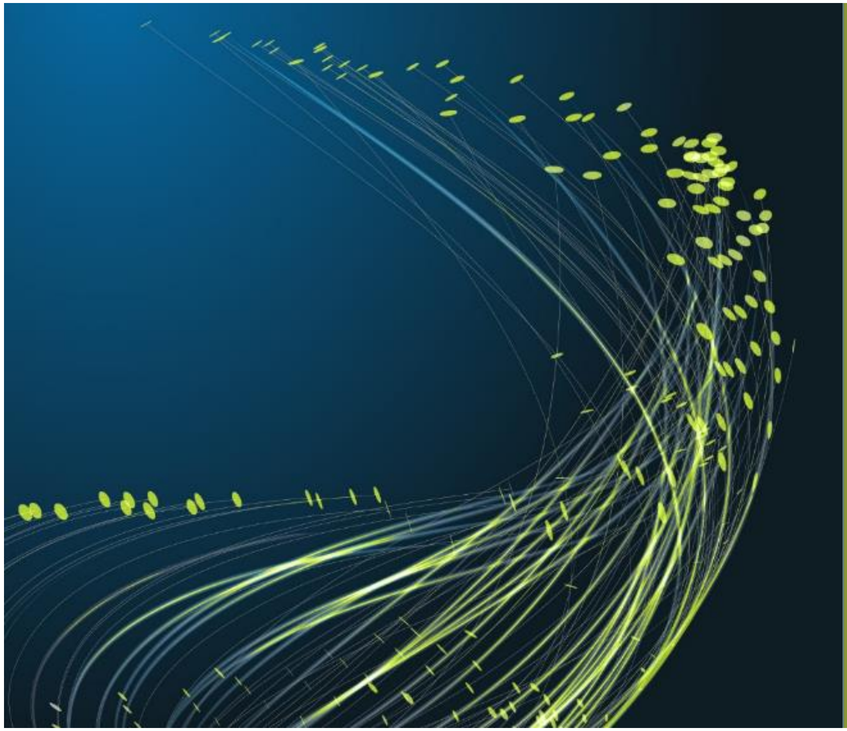
8 Step program

- Manageable Network Plan
- Step 1 – prepare to document
- Step 8 – finish your documentation

Other six steps cover

- Map Network
- Protect Your network
- Hardware assets
- Software assets
- Vulnerability Management
- Secure Configuration

Intelligence Sharing != Cyber Threat Intel Marketing



Intelligence is more than data feeds

https://share.cisp.org.uk/ * social

https://telegram.org * messaging

https://yeti-platform.github.io/ *tooling

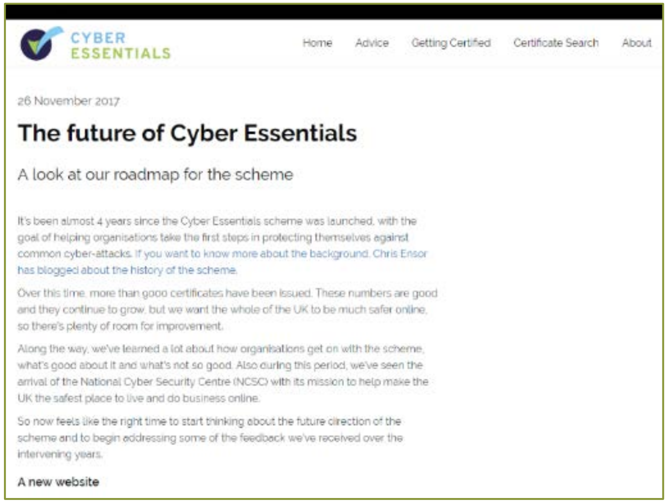
https://www.peerlyst.com/ * social

https://github.com/hslatman/awesome-threat-intelligence * link list

Raising the cost for the attackers

Cyber Essentials (CREST & NCSC)

- Updated November 2017
- Still 5 domains
- Now “*about*” 47 Questions



26 November 2017

The future of Cyber Essentials

A look at our roadmap for the scheme

It's been almost 4 years since the Cyber Essentials scheme was launched, with the goal of helping organisations take the first steps in protecting themselves against common cyber-attacks. If you want to know more about the background, Chris Ensor has blogged about the history of the scheme.

Over this time, more than 9000 certificates have been issued. These numbers are good and they continue to grow, but we want the whole of the UK to be much safer online, so there's plenty of room for improvement.

Along the way, we've learned a lot about how organisations get on with the scheme, what's good about it and what's not so good. Also during this period, we've seen the arrival of the National Cyber Security Centre (NCSC) with its mission to help make the UK the safest place to live and do business online.

So now feels like the right time to start thinking about the future direction of the scheme and to begin addressing some of the feedback we've received over the intervening years.

A new website

Barbican
INSURANCE GROUP

Time is precious,

thank you for yours

james.mckinlay@barbicaninsurance.com