BAE SYSTEMS

“Patching the Human” -

Projecting the IT Security Message Across the Enterprise

Total Security: from Insider to Cyber, June 2013

Giles England, CISSP,

Head of IT Security - Policy & Risk Management, BAE Systems plc.

Patching the Human – Why ?

"Only amateurs attack machines; professionals hack people"

- 2013 Verizon Data Breach Investigation report:
  - Human element was involved in more than 80% of breaches.
  - "Phishing" is the top human attack method.
  - Senior Managers and Executives are the top attack target "Whaling".

- We deploy traditional defences (AntiVirus and Firewalls) against traditional threats.

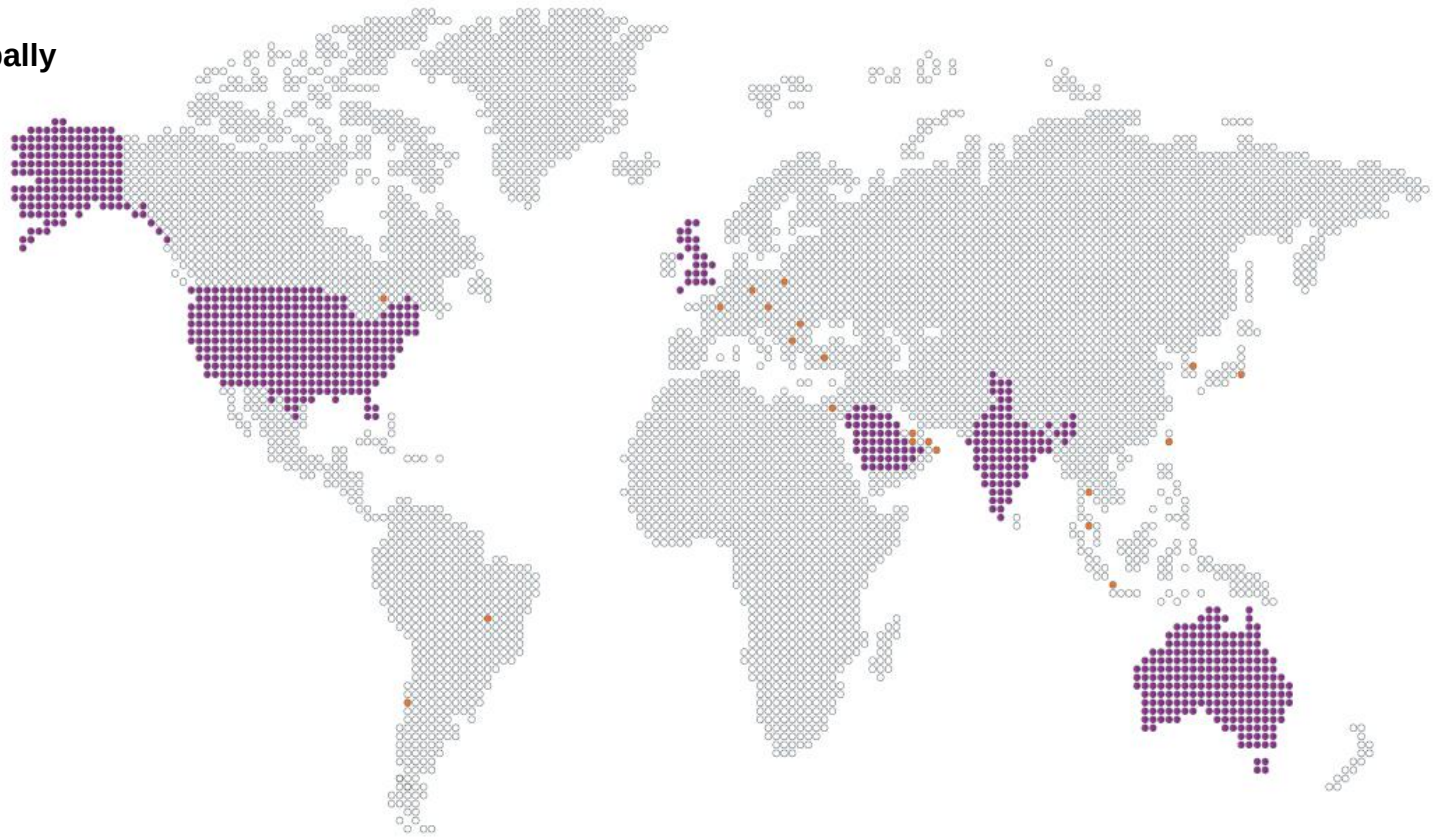
- We can deploy new defences (IPS, IDS, Host Agents) against the cyber threat, but **unless we educate our workforce** on **how to spot** potential attacks, and **how to respond**, we are not protecting ourselves to the best of our ability, or making the most of this investment.

Scope of the Problem….

Global Defence, Aerospace and *Security* Company

c.88,500 employees globally

Operate in over 100 countries



- **BAE Systems Home Markets**

Australia
• circa 5,600 employees

India
• circa 100 employees

Saudi Arabia
• circa 5,800 employees

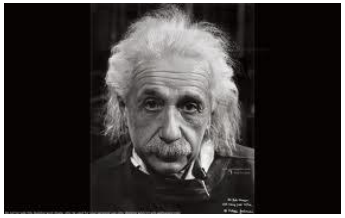
United Kingdom
• circa 34,800 employees

United States
• circa 37,300 employees

- **Global Business Development Offices**

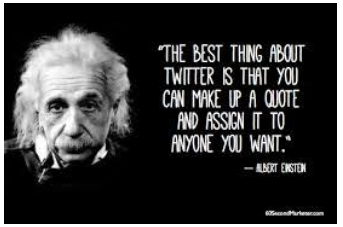
Methodology and Approach

"Any fool can know. The point is to understand."



- Global IM&T Council decided BAE Systems needed a Global approach to IT Security Awareness.

- Initial suggestion of 4 x 15 minute modules, then changed to 12 x 5 minutes modules covering the salient issues.



- Introduction and APT
- Spearphishing
- Working with sensitive emails
- Working securely away from the office
- Social Networking
- IT Security controls – why we have them
- GSOC – global protection
- The Advanced Persistent Threat
- GSOC incident response
- What's the worst that could happen ?
- Cyber-security – is this real ?
- The AUP and you

Methodology and Approach

"Tell me and I forget, teach me and I may remember, involve me and I learn."

- Contracted with 3rd party preferred supplier of eLearning.
- BAE Systems (as SME) generated content and suggested "look and feel" / screen displays of modules.
- 3rd party provided Instructional design, and build.
- Internal Communications function used to ensure "branding" of activity was consistent and to assist with launch publication. (E-cards / posters / webpages etc.)
- Modules launched globally on a monthly drumbeat basis.
- Mandatory training – stretch target of 90% throughput.

BAE SYSTEMS

Lessons Learnt

"Speak softly and carry a big stick. You will go far"

- Get **sponsorship** from the most senior level you can.
  - Ideally Chief Executive, as it is an *Operational* issue.
  - Suggest avoid CIO / CISO, as this brands it a geeky technical issue, not a *human* issue applicable to everyone.
  - Treat as a safety campaign.

- Get sponsor involvement in the launch – and on-going communications, to show how important it is to them.
  - Explain risks to sponsor in business terms, including:
    - *IPR Leakage*
    - *Reputational damage*
    - *Loss of shareholder value.*

BAE SYSTEMS

Lessons Learnt

Q. *"What's the cost of doing this…?"*
*A. "What's the cost of **not** doing this…?"*

- **Business Case –**
  - Hard to quantify savings, however compare the budget required for training with the budget required for technical defences…
  - Became a "no brainer".
  - Senior Sponsor a factor in speedy business case approval….
  - External cost of development for 12 modules – c. $100k.
  - Q. How much do you spend on AV / Firewalls (purchase and run & maintain) that are bypassed by a successful APT attack ?

Lessons Learnt

"You can't over-communicate…"

- Engage your Communications team / function
- Content considerations:
  - Consider use of humour, cartoons, Company logo/branding / sub-branding
    - *However* be mindful of your organisational culture…
  - Support Diversity & Inclusion – ensure actors represent the sexual, geographical and ethnic balance of your organisation
    - *But* don't overdo it...
  - Ensure content is globally-relevant and culturally acceptable.
    - Establish contacts for review / sign-off in major overseas divisions.

BAE SYSTEMS

Lessons Learnt

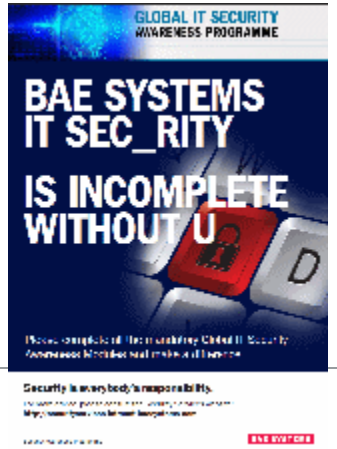
"You can't over-communicate…"

- Content considerations:
  - Consider "dual use" training relevant to home and work
    - E.g. when discussing Social Networking provide guidance on how to secure your child's pages.
  - Use "real life" metrics
    - E.g. how many attacks per day / how many log records are analysed / number of emails to phishing GSOC account etc.).
  - Consider the difficulties some learners may face:
    - Use subtitles
    - Use Cloud-based solutions, to allow access from home.
    - Ensure offline training is available (e.g. via removable media) for remote staff.

Lessons Learnt

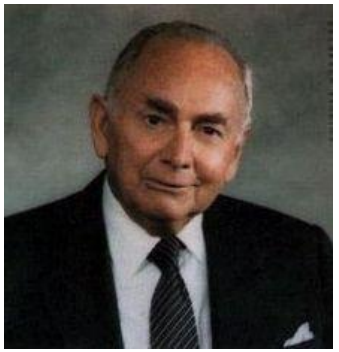
"You can't over-communicate…"

- Additional information:
  - Provide links to further training, or a "landing page" for further information.
  - Provide printable .pdfs with further information:
    - How to report to phishing.
    - "Red Flags" to look for.
    - Consider embedding these links into external email header.
  - Provide downloadable posters / copies of Ecard images for use in local communications campaigns.

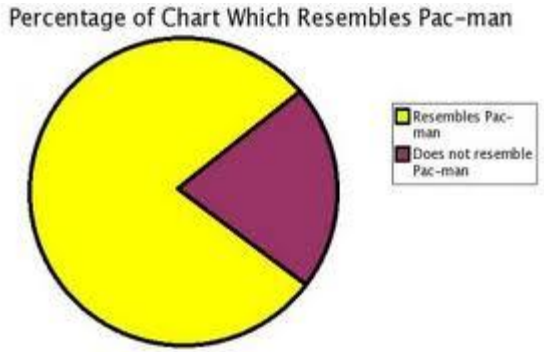


Metrics

"Performance is your reality.
Forget everything else."



- "Scores on the Doors" published regularly to highlight comparative performance across:
  - Home Markets
  - Business Division
  - Business Units
  - Teams
- Engenders a competitive spirit.
- Allows senior focus on areas facing difficulty (e.g. large number of manual workers), or apathy.



- 2012 stretch target of 90% throughput achieved across the Enterprise (90.3%).

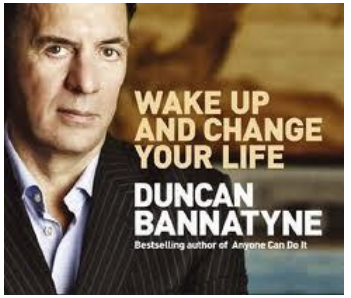
Metrics

"Feedback is the breakfast of champions."

- Measure your programme performance.
  - Use your LMS module scoring / feedback mechanism.
  - Use an online survey tool.
  - Use a scoring system, but also mandate narrative feedback.
  - Follow up on negative comments / scores:
    - Sometimes it's infrastructure or technical problems, rather than poor content.
    - Sometimes someone's having a bad day.
  - Ask for suggestions for future content.

Spearphishing Testing

"Turnover is Vanity. Profit is sanity."



- **<u>Training throughput ≠ Cultural change.</u>**

- Toolsets are available to automate testing of "susceptibility" of email account holders.

- Repeating tests can show the effectiveness (or not !) of your training.

  - Measure susceptibility pre- and post- awareness programme.
  - Provides test-on-test metrics to plot over time.
  - Gives a "Jolt" to those who cruised through training.
  - Identify "repeat offenders" for more targeted training (or *different* training – e.g. face to face).
  - Ability to benchmark with other organisations.
  - Ability to only Phish "High Value Targets" – using open or paid for sources.

BAE SYSTEMS

Once you start, you can't stop…

- IT Security Awareness is not a "once and done" exercise.
- Content needs to be refreshed regularly (at least every 2 years ?)
- New threat vectors are appearing – e.g. watering holes / BYOD.
- Additional requirements:
  - "Induction Module" aimed at new starters with the salient aspects of the 12 modules.
  - Supply chain module.
  - "Quick and Dirty" capability for development of in-house content to provide quick-reaction awareness for newly discovered issues.
    - Can be used post-security incident, to raise level of awareness of the issue.

BAE SYSTEMS

Key takeaways…

- Get sponsorship from the highest level.
- Create engaging content.
- Measure your results.

Thank you