Gaining Leadership Support - what do we tell them, and how?

Prof. M Angela Sasse RISCS
Geopolitical uncertainty, cyber threats and speed of technological change are top concerns for both CEOs and investors.

**Investors**
- Cyber threats: 1
- Geopolitical uncertainty: 2
- Speed of technological change: 3
- Populism: 4
- Protectionism: 5

**CEOs**
- Over-regulation: 1
- Terrorism: 2
- Geopolitical uncertainty: 3
- Cyber threats: 3
- Availability of key skills: 5
- Speed of technological change: 5

PWC Global Investor Survey, 2018
of corporate board members believe that cyber-related risk is the most challenging risk they are expected to oversee.  
- A 2017-2018 survey by the US National Association of Corporate Directors

80% of all board meetings discuss cybersecurity.

34% of boards are confident about their companies’ ability to defend against a cyberattack.

11% of corporate directors believed their boards possess a high level understanding of cybersecurity risk.  
- A survey by the NYSE Governance Services
Why boards don’t invite cyber professionals

• No confidence in cyber security professionals’ ability
  • to communicate beyond jargon
  • to understand company’s business
  • to articulate how cyber security aligns with it
• Fear
  • that they will be sold something they don’t need
  • of the security issues that will be brought to light

Michael Hill, Infosecurity Magazine
What do we tell boards about security? It’s -
“Never give an order that can’t be obeyed!”

General Douglas MacArthur 1880-1964
Security that takes away too much of staff’s
- Time
- Attention
- Goodwill

Drains employees’ ‘Compliance Budget’

Thanks to Robert Watson
Cambridge University Computer Lab
Phishing your own employees 😞

David Rosenthal @MakeYourselfNrd

Replying to @ajohnsocyber @SwiftOnSecurity

We started doing training a long time ago. Still get phished on occasion like everyone, but now everyone is afraid of any 3rd party link 😞

7:26 am - 17 Aug 2017

David Rosenthal @MakeYourselfNrd - Aug 17

Replying to @MakeYourselfNrd @ajohnsocyber @SwiftOnSecurity

Response rate on some 3rd party survey tools went down drastically after training started. Even with fully branded and well written comms. 😞
"About 50 of you so far marked this message coming from [subcontractor] as phishing” (out of company with around 600 employees).”

Email from HR department that had hired a well-known & expensive supplier to conducting surveys. Employees had been informed, about two weeks in advance, to expect the email.

NCSC guidance on measures to reduce phishing
https://www.ncsc.gov.uk/phishing
Compliance is not enough

Learning from medicine

**Adherence (compliance):** Patient follows the plan set our by professional. Less than half of patients comply.

**Concordance:** Patient and professional agree the most appropriate treatment plan – clarification of goals, joint responsibility. More than half of patients stick to agreed plan.
“Trust and collaboration ... are necessary for effective cybersecurity.”

Security Maturity Levels

Level 5: Champions security to others and challenges breaches in their environment.
Level 4: Has internalised the intent of the policy and adopts good security practices even when not specifically required to.
Level 3: Understands that a policy exists and follows it by rote.
Level 2: Follows security policy only when forced to do so by external controls.
Level 1: Is not engaged with security in any capacity.
ENGAGE

ENGAGE.... ENGAGE!!!
Managing your ‘connections’: an organizational behavior model

An organisational behaviour model designed to assess cyber security culture  Thomas Schlienger 2006
Conclusions: what do we tell boards?

1. Security is an investment, not a grudge sale
2. Don’t worry about your technology skills – your managerial skills are wanted!
3. Make sure your security specialists understand the business and
4. have a “we’re here to help you do that, securely” attitude
5. Bring together different functions and skills to help security specialists
6. Invest in engagement and empowerment