Cyber Security in the Time of Hybrid Working

Nick Moore

Academic Lecturer

School of Technology

nickmoore@bpp.com

Cyber Security

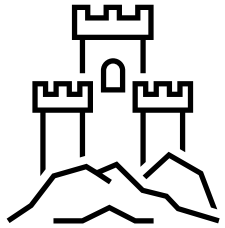
A bilateral relationship

- Employees and employers have key roles to play when ensuring cyber security
  - “The weak point is the user” is an overly **simplistic** and **inaccurate** slogan
- “Blame culture” is rarely conducive to a strong and trusting relationship
  - Mistakes are made to be learned from
- Both sides need appropriate **incentives**
  - Not just sticks – carrots work too!

Hybrid working

Akin to face-to-face and home working, yet distinct from both

- Hybrid working **combines** threat environs
  - F2F often relies on “perimeter security”
  - Home working often uses home security assumptions



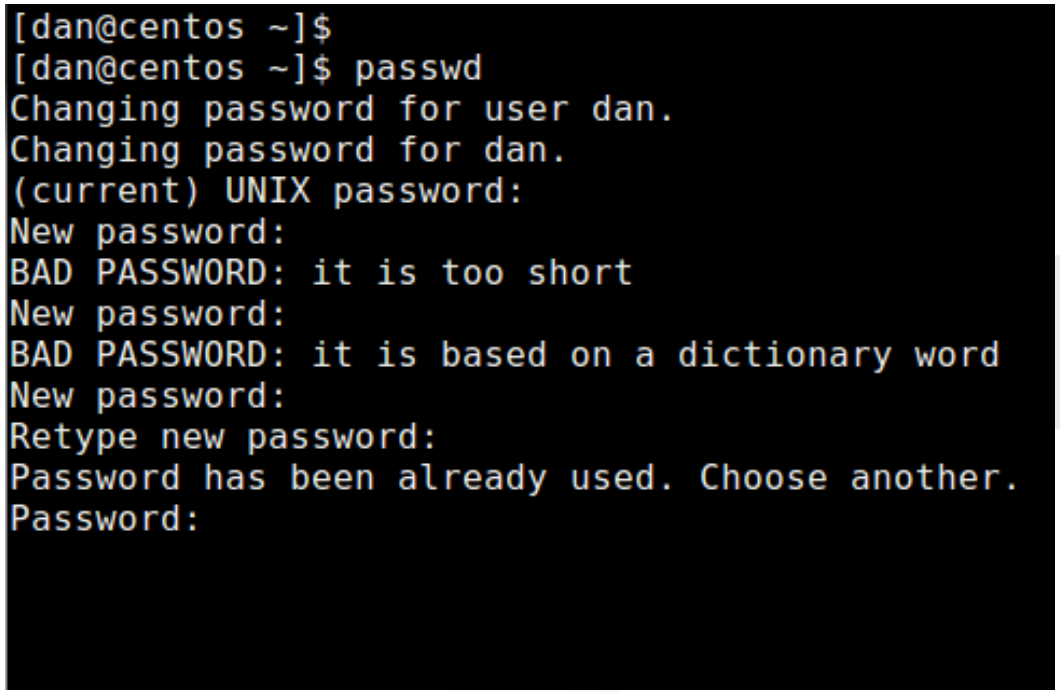
- **Travelling** and use of coworking spaces
  - People and devices going back-and-forth
  - Using more diverse and **less trusted** infrastructure

- This may **increase** the likelihood of certain attacks
  - E.g., attackers with physical access to sensitive devices becomes more plausible

Authentication

Ensuring users are who they say they are is vital for hybrid working

- User authentication remains a **core** element
  - But many have not moved beyond passwords
  - Widespread enforcement of discredited practices
- What **should** organisations do?
  - Encourage use of **multi-factor authentication**
    - Something you know, something you have
  - Minimise **unnecessary** cognitive overhead
- What are password **don't**s?
  - Frequent enforced **unnecessary** password changes can lead to bad practices
  - Avoid **discouraging** good practices with arbitrary rules



Monitoring

What you don’t know CAN hurt you!

- **Moving away** from perimeter monitoring
  - Hybrid working = reduced perimeter control
  - Each **device** needs to monitor itself for risks and intrusions
  - **Users** can play their part too, if you let them!

- What should we be looking for?
  - **Patching**, patching, patching!
  - Anomalous behaviour may indicate **intrusions**

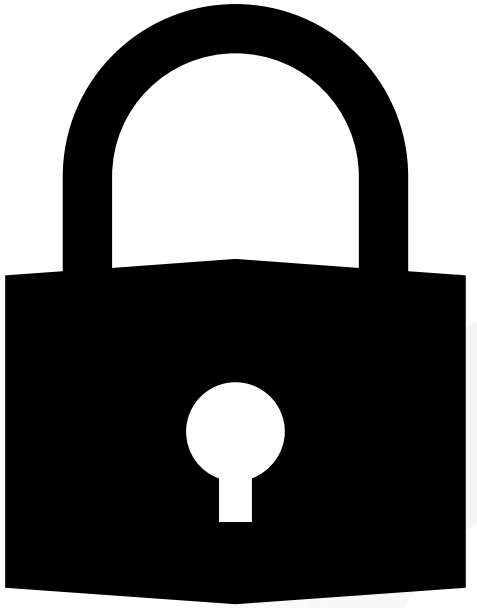
- Potential **ethical** considerations
  - Hybrid working can blur device usage boundaries

Cryptography

An important part of cyber defence, but not a panacea

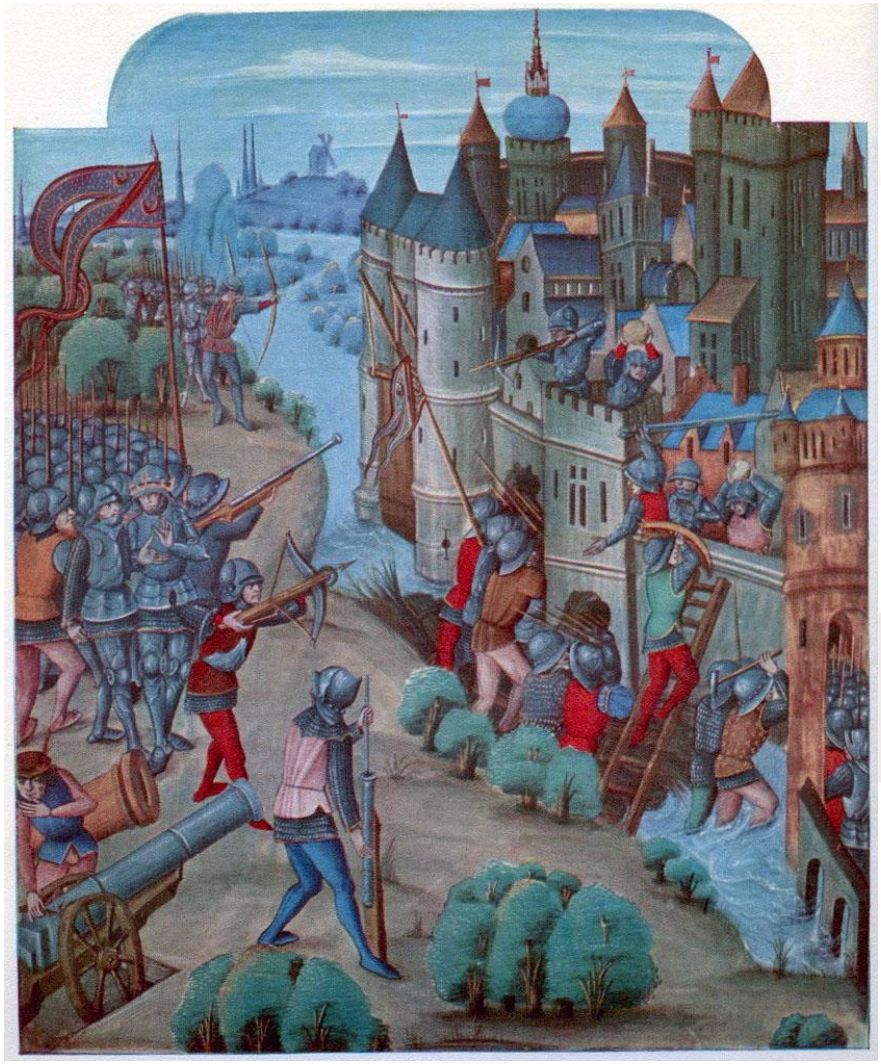
- Many organisations use **encryption** for remote security 👍
  - Widespread home working led to increased use of
    - virtual private networks (**VPNs**)
    - encrypted websites (**HTTPS**)
  - **Device/disk encryption** becomes more important with regular travel
  - Encryption does have associated **costs**

- Encryption can lead to a **false** sense of security
  - E.g., VPNs rarely protect **all** device network traffic
  - None of the above will necessarily **prevent** exploitation of a software vulnerability



Conclusions

- Perimeter approaches for cyber security are not as **effective** in a hybrid working world
  - Combining threats of face-to-face and home working
  - Travel and shared workspaces add additional risks
- Hybrid working **needs** technological solutions that are user-friendly and comprehensible
  - “Computer says no” inevitably leads to workarounds or non-compliance
- Cyber security can be **collaborative**
  - “Us vs. them” dichotomy is unhelpful



Thanks for your participation!

Nick Moore

Academic Lecturer

School of Technology

nickmoore@bpp.com

Contact us

UK Head Office
BPP, Aldine Place, 142-144 Uxbridge Road, London, W12 8AW

Hong Kong
Level 54 Hopewell Centre, 183 Queens Road East, Hong Kong

Malaysia
Unit 30-01, Level 30, Tower A, Vertical Business Suite, Avenue 3, Bangsar South,
No.8 Jalan Kerinchi, 59200 Kuala Lumpur, Malaysia

Singapore
80 Robinson Road #02-00, Singapore 068898

Image Credits

- Slide 2: https://bestpicko.com/ (Creative Commons CC BY 2.0)
- Side 4: http://xmodulo.com/ (Creative Commons CC BY 2.0)
- Slide 5: https://flic.kr/p/dXiKrW (Creative Commons CC BY 2.0)
- Slide 7: https://commons.wikimedia.org/wiki/File:15jh_castle_siege.jpg (public domain)
- All others taken from Microsoft Office icons collection, with the exception of the BPP logo