Cyonic

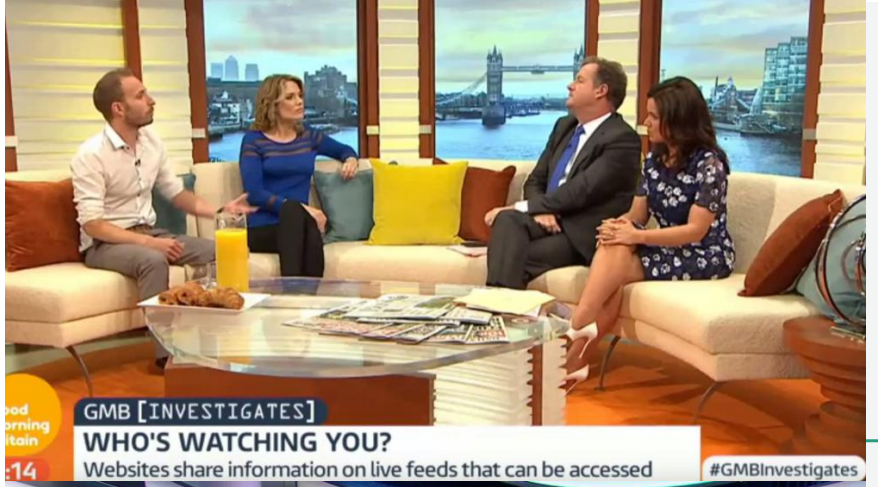
How to Hack Any Company

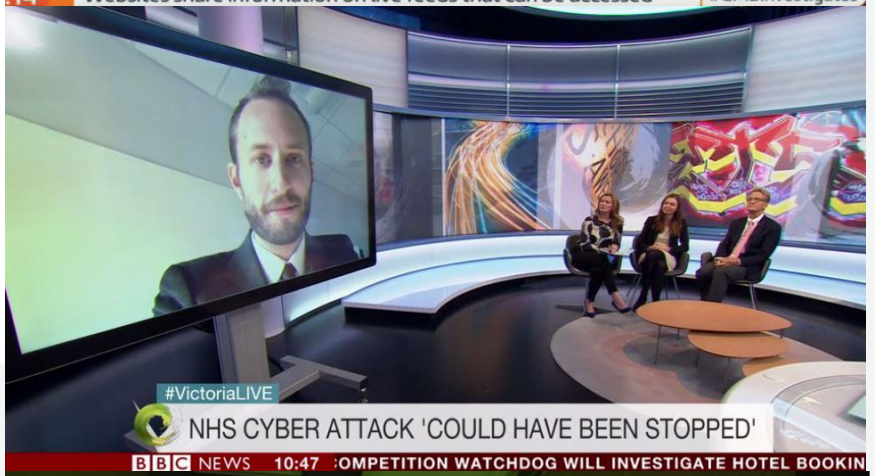
Rob Shapland, Ethical Hacker & Director

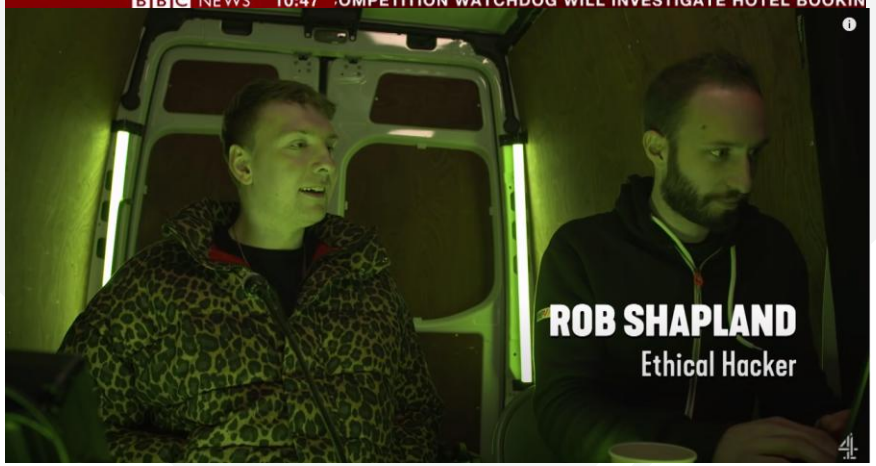
Cyonic Cyber

Rob Shapland

- Ethical Hacker and Founder of Cyonic Cyber
- Cyber Security adviser for BBC, ITV, Channel 4 and Sky News
- Designed and executed attacks against hundreds of companies, from SMEs up to large multinationals
- Physical intrusions of hundreds of different locations worldwide







Open-Source Intelligence Gathering (OSINT)

The first stage of an attack is to find out as much information as possible about the target company.

- 15 offices in UK, reviewed on Google maps and Street View
- Main website plus some SaaS services
- Office 365 for remote email access
- LinkedIn used to identify employees and deduce their email addresses

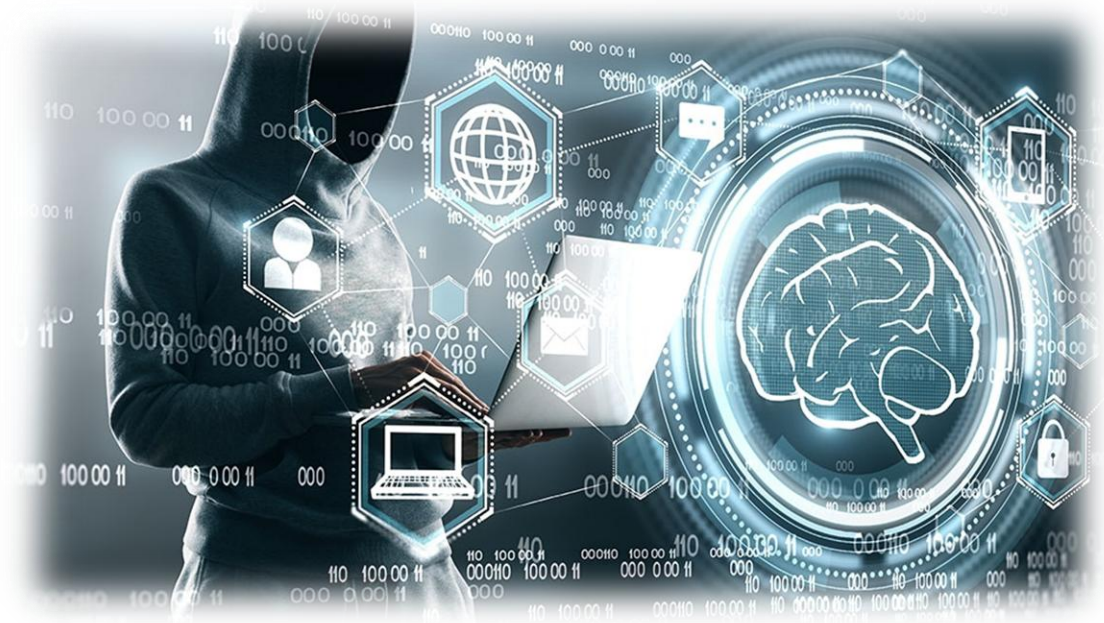
Breaching the Defences

Objective 1: Gain access to email and SharePoint of the CEO or CFO.

- Email addresses and phone numbers are listed on the company's website
- IT employee's LinkedIn profile mentions experience of implementing Microsoft Authenticator MFA
- Dark web searches reveal several staff members have had their credentials compromised, including the CFO

Deepfake Vishing

- We have the CFO's credentials through the dark web search and will attempt these on the Office 365 login page for the target company.
- Likely this will trigger a Microsoft MFA prompt
- Therefore may need to combine the attack with social engineering by pretending to be an IT employee
- Clone the voice of the IT staff member, using a YouTube video as the sample audio
- Called the CFO pretending to be the IT employee and tricked them into authenticating through Microsoft Authenticator



Spotting Deepfake Audio

- The voice and speech patter is usually slightly different – odd intonation and pauses
- Always focus on the request - think about what the person is asking you to do – is it unusual?
- How to protect your staff: **training**, preferably face-to-face live sessions
  - ✓ Educate staff about more advanced phishing techniques
  - ✓ Teach them to recognise the differences in deepfake calls
  - ✓ Make it interesting and engaging through storytelling

Objective 2 – Physical Intrusion

Branch office:

- High street premises, no guards
- Small reception, one receptionist
- Door intercom
- Information used to plan on-site attack

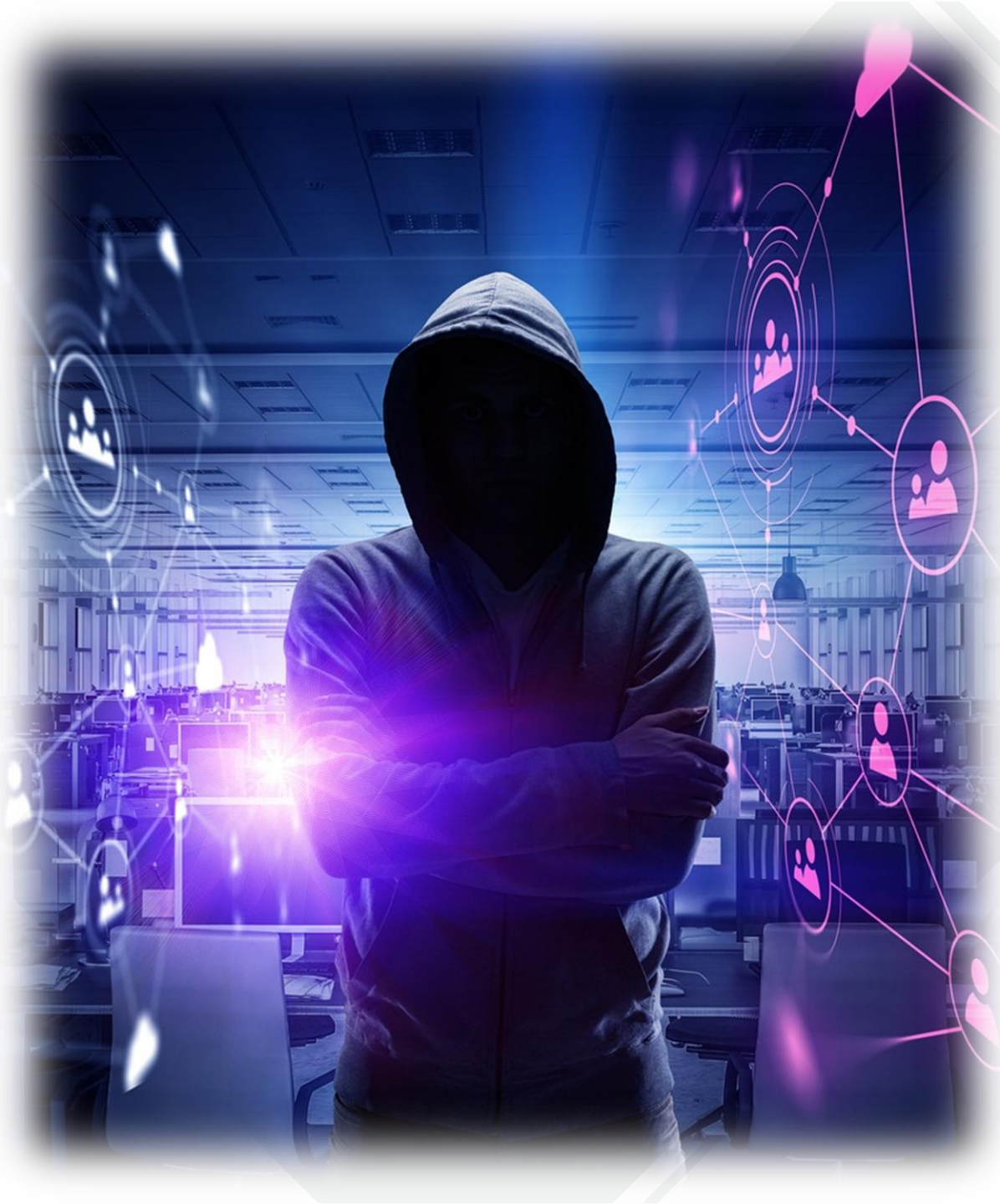
Head office:

- Razor-wire fences, perimeter guards with dogs
- External CCTV
- Main reception manned and controlled
- Goods entrance well controlled
- No other access

Developing a Pretext

Based on the information gathered from our OSINT and hostile recce, we decide on how we are going to break in - who we will dress up as and how we will act. An example of some pre-texts criminals use:

- Employee
- Cleaner
- Security guard
- BT Engineer
- Fire Alarm technician



How to Defend

- **Technical Defences.**
  EDR / Detection systems (MDR/XDR) / Secure email gateways / Strong Passwords / MFA everywhere
- **Your staff are your most important defensive layer.**
  Security awareness training is key – help staff understand the threats they face both at home and at work in an entertaining way**. Don't rely on e-learning.**
- **Have a plan for when it goes wrong.**
  Panicking is not a plan. Nor is quitting and moving to Barbados.
- **Backups.**
  Almost every company that is breached has their backups breached too. Make sure you airgap your backups completely, and test restoring them.

rob.shapland@cyonic-cyber.co.uk

linkedin.com/rshapland