# INTERVIEW PREPARATION

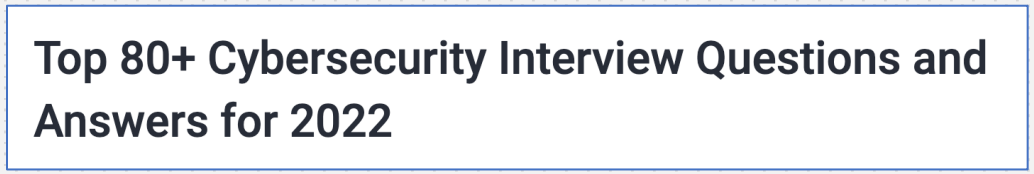
## UPSKILL IN CYBER // JOHN CORCORAN // AUGUST 2022

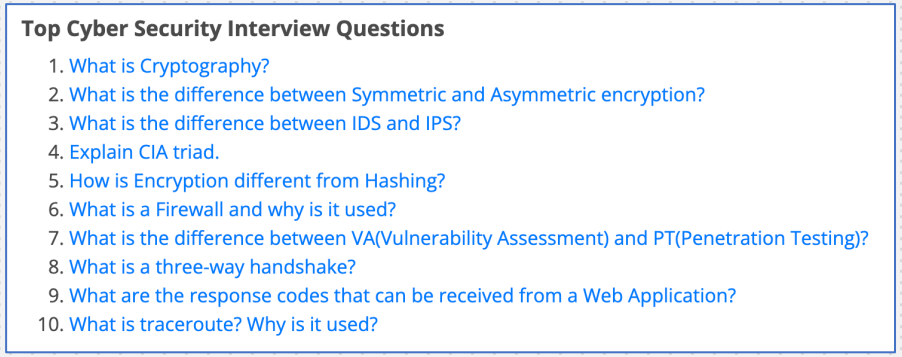
# Hello

- John Corcoran
- Working in cyber since 2009:
  - Currently: cyber security data science, public sector.
  - Previously: incident response / digital forensics / cyber research, private sector.
- Opinions are my own and do not reflect those of current / former employers:
  - I have recruited, but am not a recruiter.

# Context

- Searching ‘preparing for cyber security interview’ seems to get you either lists of tech questions, or basic personability advice.
- I’ve tried to avoid too much generic interview advice in this session – but it all applies!

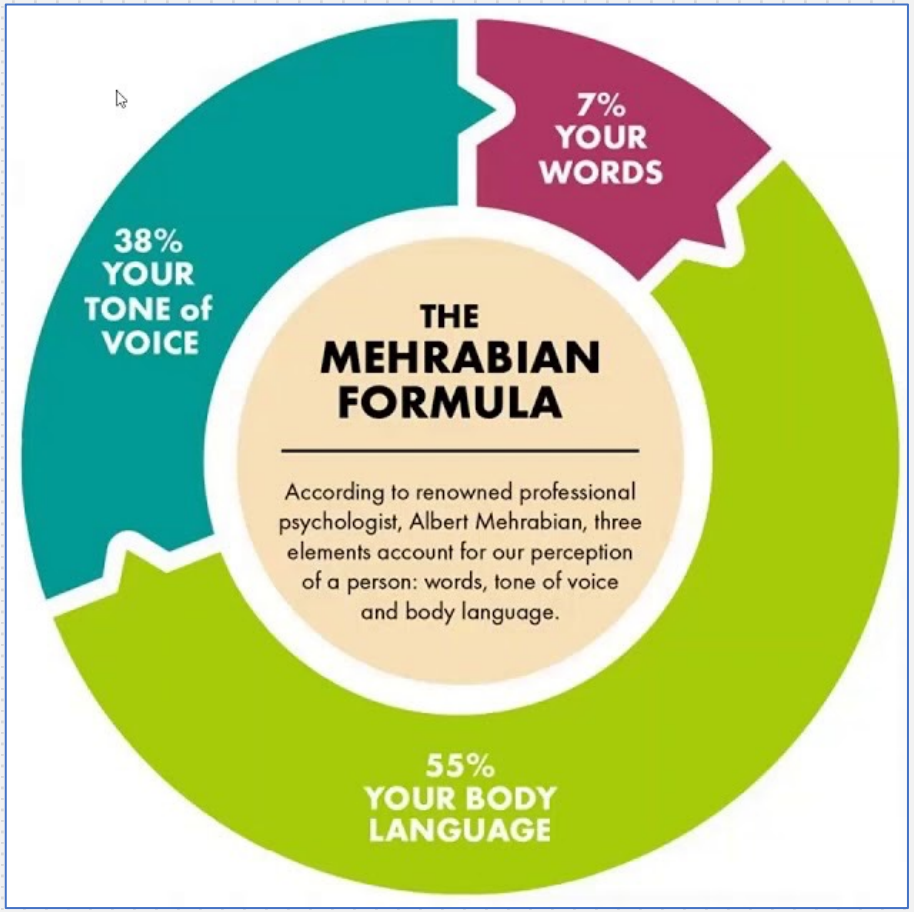




# *Main message for this session*

- Expectations are (usually) realistic for early career recruitment.
- Interviewers are (usually) accommodating, decent human beings: they want you to succeed.
- Being nervous is OK!
- **Enthusiasm, personability and aptitude are the main qualities that interviewers are looking for.**



# *Preparing for interview*

1. Understand where the role sits.
2. Employer recruitment strategies.
3. Employer recruitment frameworks.

# *Preparing for interview*

## 1. Understand where the role sits

MAJOR OVERSIMPLIFICATION WARNING

| | Product/service delivery | Advisory, policy and programme |
|---|---|---|
| **Externally-facing** | **Sells* cyber security 'things' to clients/customers.**<br><br>**Example:** professional services firm holds SOC and incident response retainer agreements with multiple clients.<br><br>**Example question:** how do you scale the service during periods of increased client demand (e.g. new wide-reaching zero day published)? | **Sells* cyber security 'thinking' to clients/customers.**<br><br>**Example:** professional services firm provides crisis management procedure development to individual clients.<br><br>**Example question:** how have client concerns changed over the last few years? |
| **Internally-facing** | **Delivers cyber security 'things' within the organisation.**<br><br>**Example:** internal SOC and threat intelligence service to identify and contain cyber threats on the organisation's network.<br><br>**Example questions:** how have attacks against your network changed over time? | **Delivers cyber security 'thinking' within the organisation.**<br><br>**Example:** developing policies and procedures for reporting phishing attacks within an organisation.<br><br>**Example question:** how do you measure improvement in user responses to phishing exercises? |

# *Preparing for interview*

## 2. Employer recruitment strategies

- Larger firms with sizeable apprentice / graduate yearly recruitment tend to seek generalists: enthusiasm/personability/aptitude beats in-depth tech knowledge.
- Tailor approach based on nature of advert and during interview.
- Possible question:
  - "Is there any cross-skilling / movement between teams for new starters?"

# *Preparing for interview*

## 3. Employer recruitment frameworks

- Recruitment frameworks provide a templated approach for employers to base recruitment and interviews around.
- Most commonly found in public sector – but methodologies are useful for any interview.
- Methodologies:
  - STAR: Situation, Task, Actions, Results
  - CAR: Context, Action, Result
  - Further info: search “Civil Service success profiles”


# *Delivery / format of interview*

1. Quantity and delivery format.
2. Exercises and presentations.
3. Questions you may be asked.

# *Delivery / format of interview*

## 1. Quantity and delivery format

# Potential number of interviews is highly variable: could be anything from one interview through to four+, irrespective of experience levels.

# In-person preferable, but may (still) be over video call:

## Over video, worth an early expectation setting about not meaning to inadvertently speak over someone (if interviewer doesn't do this already), or inability to see questions if presenting material.

# *Delivery / format of interview*

## 2. Exercises and presentations

- Take-home exercises less common for early careers: but could take the form of a file to analyse (e.g. memory/disk image, or log file).
- Standard in-person technical exercise advice applies:
  - Show thinking if you don't know the actual answer; pseudo/broken code is fine!
- Presentations more common: depending on the ask, content only tangential to cyber may be fine.
  - Confirm whether time windows given for presentations are strict limits, or flexible.

# *Delivery / format of interview*

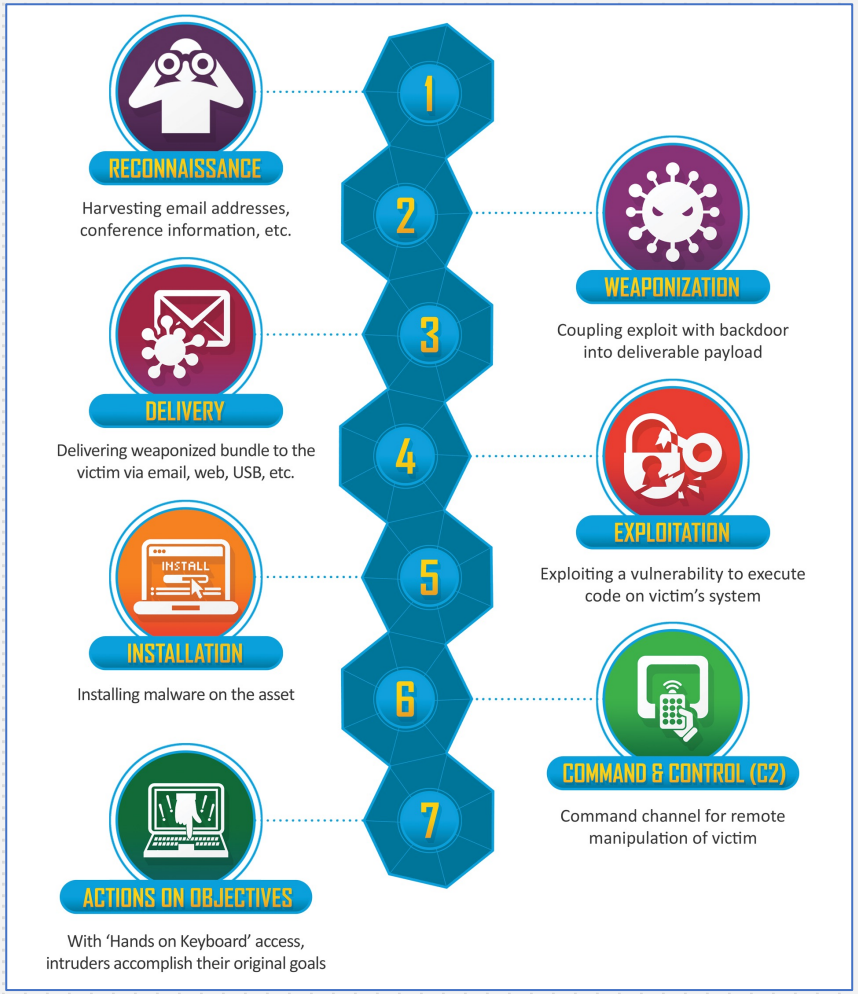
## 3. Questions you may be asked

1. What is your understanding of how a cyber attack begins and progresses?

    # Cite: kill chains (e.g. Lockheed Martin), MITRE ATT&CK framework.

2. What do you think are the main cyber risks our organisation faces?

    # Cite: sector research on cyber threats, any recent incidents in that sector (or if not, whatever the most recent major newsworthy vulnerability and exploitation was).

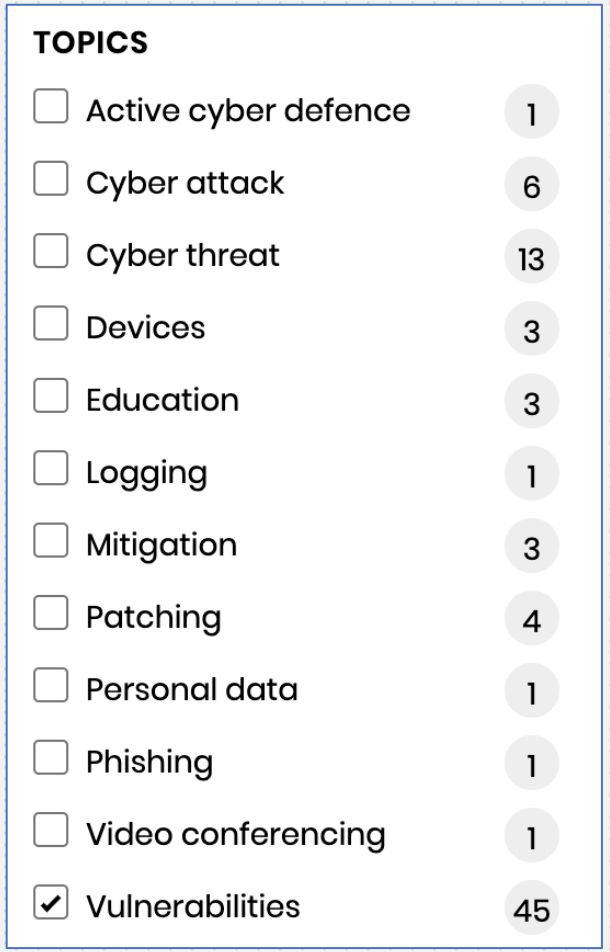


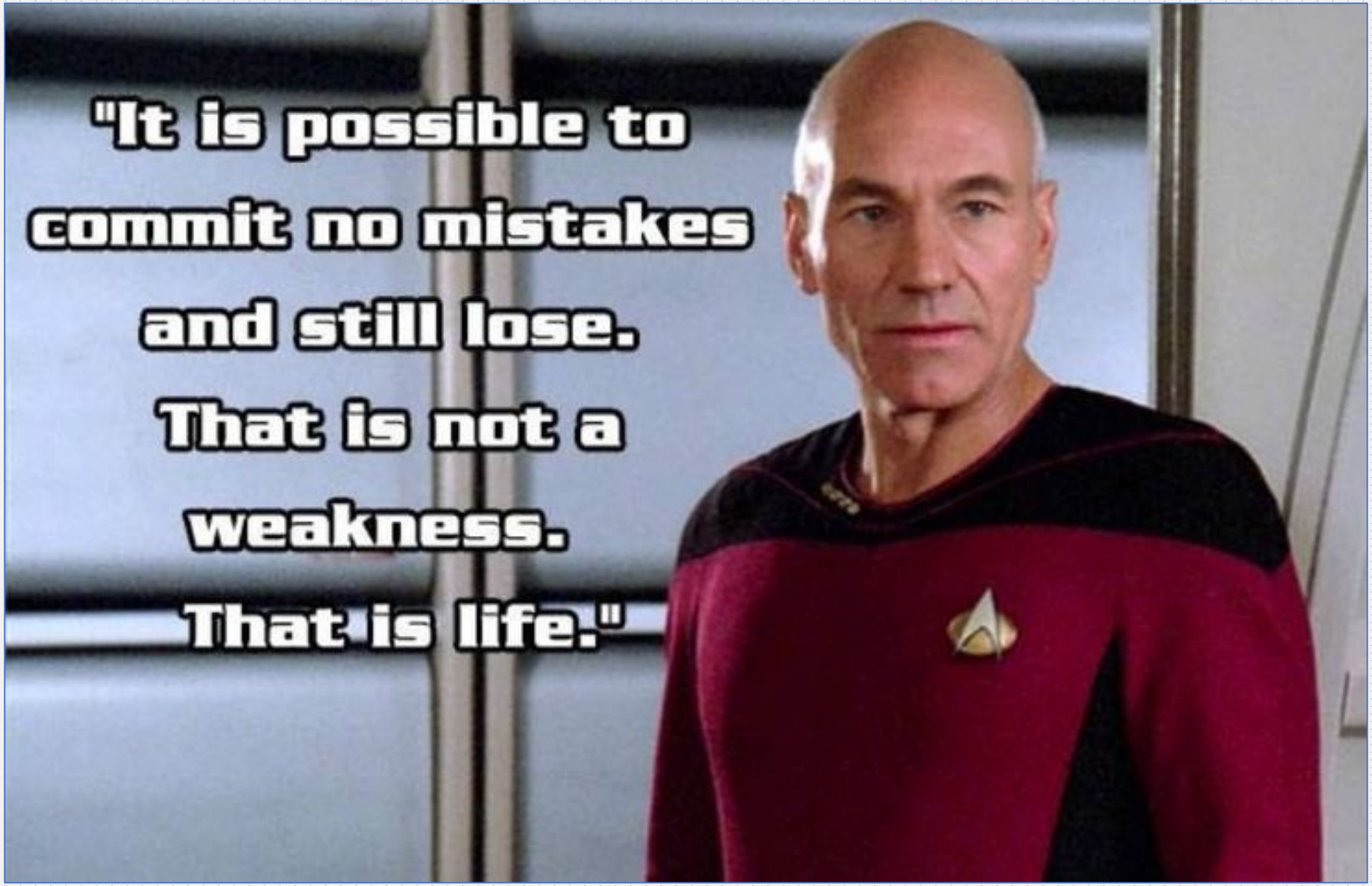
# Highlighting strengths and enthusiasm

- SANS is recognised across industry as the gold standard for technical training: having two certifications is an excellent position to be in!
- Outside of standard personability advice, highlight enthusiasm by:
  - Researching a couple of recent, high profile cyber incidents, vulnerabilities, or threat groups that are likely relevant to the organisation.
  - Any open source tools or techniques that you've used in SANS or during your own research.
- If opportunities to mention them don't come up organically, can mention during questions (i.e. expand 'questions' to give a quick talk on your interest in the domain, citing research you've done).

# Useful open source resources

- News:
  - NCSC: https://www.ncsc.gov.uk/news – filter to 'Vulnerabilities' – read latest advisory summary report / posts for latest high profile vulnerabilities: cyber teams will have been working recently to resolve these, so an excellent talking point.
  - Twitter
- Tools / techniques:
  - https://attack.mitre.org/
  - https://www.sans.org/posters/
  - https://awesomedfir.com/
  - https://github.com/meirwah/awesome-incident-response
  - https://github.com/hslatman/awesome-threat-intelligence




"It is possible to
commit no mistakes
and still lose.
That is not a
weakness.
That is life."

# *Thanks for your time!*

## Any questions?