CyBOK Funded Outreach Workshop Notes

Proposal Outline

The CyBOK team are looking to encourage greater awareness and adoption of the CyBOK amongst a wider community, including public sector, education and industry. This workshop has been put together by ITSUS Consulting specifically for use with Local Government, Authorities, and Education teams.

Aims and Objectives:

The workshop aims to:

- Establish the extent to which CyBOK is known in Local Authorities / Education teams;
- Disseminate information about CyBOK and how it relates to the public sector;
- Run through a scenario which maps to four key Knowledge Areas, demonstrating their importance and relevance to the discussions.

Scenario and CyBOK areas

The target audience for the workshops is Local Authority and Education providers, with the main focus being on IT teams (as opposed to front line staff, office staff or strategic leadership teams). As such, a scenario will be presented around a disgruntled employee facilitating a ransomware attack on the organisation. Four areas of CyBOK are used as a basis for discussions: Malware & Attack Technologies, Security Operations & Incident Management, Human Factors, and Adversarial Behaviours. Other areas should be mentioned as appropriate. Linking the scenario and follow up discussions to each of these knowledge areas is detailed in the PowerPoint presentation, and there are notes and discussion points listed in this guide.

Run time:

2-2.5 hours, plus time for refreshments

Resources required:

- CyBOK / ITSUS Local Authority slide deck
- Scenario print outs on four cards per team
- Flip chart paper or equivalent
- Pens

Preparation:

At the start of the event (or via a form beforehand), you may wish to ask your attendees what they know about CyBOK and the four Knowledge Areas that will be covered. Consider collecting demographic data too.

Workshop

The workshop starts with a group introduction (slides 1-5). You may wish to replace slide 1 with your own organisational information. This includes an introduction to the facilitators and their organisation, followed by an introduction to CyBOK and the four specific KAs that will be focused on during the session.

Following this, attendees should be split into group of 4-5. Discussions will take place within these groups for each part of the scenario before feeding back to the main group as a whole.

For each stage of the scenario, read the slide to the attendees. Provide a copy of the relevant stage of the scenario on a card for groups to scrutinise as some will prefer to read from the card than the screen. Ask each group to consider the key concerns of the scenario as detailed on the slide / card and make some brief notes.

Allow 15 minutes or so for groups to discuss. You may find it useful to wander amongst the groups asking questions or re-steering discussions if they go off track and some suggested discussion points are provided below.

Revisit the scenario stage as a whole group, asking each smaller group to highlight the key points they have made.

Repeat for each stage.

Notes for facilitators:

The first stage (Scenario 1.1, Slide 6) links to the Adversarial Behaviours Knowledge Area**. Valuable areas to consider in linking the KA to the scenario include:**

- **Cyber Enabled v Cyber Dependent Crime**
- **Sabotage**
- **Infection vectors**
- **Specialised services (Exploit Kits)**
- **Attack trees**
- **Kill chains**
- **Environmental criminology**

Discussions can be encouraged around:

- Consider the people side of things. Why has Helen reached a tipping point?
- Could this have been prevented and if so, how?
- Helen has become an adversary
- Some security measures suggested (e.g. USB blocking) can be a barrier to efficient working and as such individuals may find work-arounds.
- Humans are prone to take actions when disgruntled.
- Highlighting the importance of having people-focused processes to prevent staff from reaching this point.
- Physical security may have been useful (e.g. surveillance cameras to detect the adversary).

Main controls suggested (to share following group feedback if not mentioned by the groups):

- Policy for blocking USBs or read only policy
- Policy for reacting to USBs (firewall etc.)
- Training and awareness raising
- Data loss prevention
- Removable media controls
- Application controls
- Monitoring controls

Question – where does the human element sit, who is responsible?

The second stage (Scenario 1.2, Slide 8) links to the Human Factors Knowledge Area**. Valuable areas to consider in linking the KA to the scenario include:**

- Human capabilities and limitations

- Fitting the task to the human
- Social context
- Human error
- Cyber Security education and awareness
- Positive security
- Stakeholder engagement

Discuss with the groups why Evan acts as he does:

- Vulnerable, fearful for future, curious about what is on the USB
- Feels there are no consequences as he has finished his probation
- Is he an adversary? No malicious intent but possibly
- Actioned something he knows is wrong
- Maybe lacks loyalty as has only been with the organisation for 6 months
- Untrained or lacks training

General discussions around:

- Culture of uncertainty – stems from management
- Communications with staff can be dictatorial, meaning that people don't respond well to them (in response to directives not to plug in unknown devices for example)
- Question as to whether human factor has been considered in organisation's strategic plan
- Tendency to focus on external adversaries rather than potential internal ones
- There *should* be a policy to cover this
- Design of policy could be improved, to make it easier to digest for individuals (e.g. could be delivered via interactive training / videos etc)
- Lack of inter-departmental discussion (e.g. legal teams, IT, management etc), siloing is not helpful
- Importance of continual education / training

The third stage (Scenario 1.3, Slides 10 & 11) links to the Malware and Attack Technologies Knowledge Area**.**
Valuable areas to consider in linking the KA to the scenario include:

- Types of malware
- Kill chains
- Confidentiality, Integrity and Availability
- Malware detection
- Monitoring
- Analysis
- Counter measures

Consider the following discussion points with groups:

- Delay doesn't help
- Has Caroline done the right thing? (NCSC Ransomware timeline guidance is useful here)
- Should Evan admit / report his actions?
- Machine not disconnected
- Culture of fear of repercussions if Evan comes clean?
- Fear of fines from IPO may act as a greater incentive than anything else to data privacy breaches
- Understanding the implications of an attack (e.g. refuse collections disrupted) can be more meaningful to staff on the importance of good cyber security practices
- Incident response plans need to be tested and evaluated prior to an attack

The final stage (Scenario 1.4, Slide 13) links to the Security Operations and Incident Management Knowledge Area**. Valuable areas to consider in linking the KA to the scenario include:**

- MAPE-K (Monitor, Analyse, Plan, Execute – Knowledge)
- Architectural principles
- Monitoring
- Detection
- Analysis
- Anomaly detection
- SIEM (Security Incident & Event Management)
- SOC (Security Operations Centre)
- IPS / IDS (Intrusion Prevention / Detection Systems)
- SOAR (Security Orchestration, Automation and Response)

Discussions can be encouraged around:

- Levels – Do organisations use High, Medium and Low or some other metric?
- Are these levels understood by everyone involved?
- Security Analyst chooses the level in this scenario
- Cyber Incident Response Team needed
- Security monitoring used – SIEM / SOC
- Technical controls
    - USB Controls
    - Malware protection
    - Controls to prevent propagation
    - Admin privileges
- CyBOK – Prepare, Handle, Follow up

It should be noted that all stages will cross over into other KAs and these can be discussed throughout.

The incident timeline is then provided and discussed, either in groups or collectively, and reference made to the NCSC resource detailed on the slide notes.

The Cyber Kill Chain is discussed, as this draws together the various elements of the incident and raises awareness of the process that underpins most cyber security incidents. Attendees can be asked to map the scenario stages to the Cyber Kill Chain.

Finally, the relevant Knowledge Areas can be summarised and any remaining discussion points covered.

You may wish to adapt slide 19 onwards for your own delivery.

Summary

The workshop can be run in person or online, although the in-person may generate more lively discussions and sharing of best practice.

The Human Factors Body of Knowledge may be an area that has not been given much consideration by attendees, depending on their job role. There can be a tendency to focus on technical controls and to miss the psychological aspects of various events within an organisation and the impact these can have on individuals.

It is helpful to encourage attendees to go back and read their own Cyber Action Plans more thoroughly or review their own processes and incident response plans.

Post Workshop

If you asked your attendees to complete a pre-workshop survey on their knowledge of CyBOK, you could ask them to complete a similar post-workshop survey to measure distance travelled.