Task 1

Consider for discussion the overview and key-findings from the UK Government Report of 2023 Cybersecurity Breaches. Take a detailed look at Dealing with breaches or attacks.

What do the incident management statistics indicate about approaches to incident response? Provide 4 issues (bullet points).

Approaches to incident response

- Whilst 40% of organisations would take action(s) following a cyber incident, in reality just over half of those actually have a formalised plan. These findings would indicate that although organisations have an understanding that action is necessary following a cyber incident, there are barriers present that prevent them from formalising those actions into a proactive plan. Reading through the rest of the report provides a couple of possibilities for why this might be, including financial challenges and a lack of appropriate skills and resources.
- There are two sectors in particular that tend to have a more formalised cyber incident response, both of which have responsibility for highly sensitive PII – finance businesses could hold banking or credit card details, health businesses could have details about patient health. This would suggest that the organisations concerned have an appreciation of the sensitivity of the data they are responsible for, and the effects a loss of confidentiality in relation to it would have on their stakeholders. It could also be that the organisations concerned are aware of the magnitude of the action that could be taken against them should a cyber incident put the privacy of the data at risk. Unfortunately there is nothing in the report that specifically explores the reasons behind this trend, though it is stressed throughout the report that both sectors place a higher than average importance on cyber security measures in multiple areas.
- Communication (or lack thereof) has been specifically mentioned as both a shortcoming in incident response and something that has been improved upon following a cyber incident, specifically communications between IT/specialist cyber teams and the wider staff population (including management boards). This would suggest that any incident response that has taken place is either lacking sufficient communication planning or that communications between technical and non-technical staff areas are not being adequately encouraged and supported in the workplace in general. The fact that one of the most common actions to take following a cyber incident was listed as "communications" is an encouraging sign that organisations are seeking to identify shortcomings and improve upon them using lessons learned from the cyber incident.

- The results of the report have demonstrated that incident response measures are more likely to be in place and undertaken by larger organisations than charities or smaller organisations. The report has identified that smaller business and charities are feeling a greater degree of economic pressure in the current climate, and that their prioritisation of cyber security measures is suffering as a result. It might be interesting to conduct further research into this area to try and identify what measures could be taken to support these businesses in their attempts to maintain the CIA triad for the data that they hold as there is indication as to whether the majority of these organisations are downgrading the importance of cyber security because they do not comprehend its importance, and what contingency plans have been put in place now that their defences have been potentially weakened.

Task 2

Conduct an internet search on Disaster Recovery (DR) and Business Continuity (BC) in terms of Information Security. Gather evidence (2/3 examples) for discussion of how UK companies approach DR and BC. Do companies treat both as the same or does it all come under Incident Response?

In his article "Beyond disaster recovery: the benefits of business continuity" from a 2005 edition of the Computer Fraud & Security journal, Ray Stanton argues that whilst awareness of business continuity was increasing in organisations, many of those organisations were still confused about the distinction between Disaster Recovery (DR) and Business Continuity (BC). As per his definitions, DR relates mainly to IT systems, BC is a process that ensures an organisation can continue to operate during and after an incident that serves to interrupt its business. In addition to this, an article from CSG in June 2023 declares that less than 9% of UK organisations have a DR plan, suggesting that not only is the purpose of such a procedure not fully understood, but that organisations simply do not place a high level of priority on the creation and maintenance of these documents.

An example of this flippancy can be evidenced with a 2017 incident suffered by British Airways (BA), caused by a power outage at one of their IT hubs. It has been disclosed that the business had a DR plan, and that it was invoked. Whilst the company did appear to have had a partnering BC plan, it was not practised and consequently several of its elements failed, resulting in the total grounding of all BA flights. This would indicate that the organisation had invested in the development of both DR and BC plans but failed to appreciate that they must be maintained, practiced and revised after creation.

In contrast to this, the NHS (as part of its "Data Security and Protection Toolkit assessment guides" from NHS digital) has made a clear distinction between DR and BC plans, provided a breakdown of what each is used for, how they apply to operational and

strategical IT within the NHS, and a guide of how to create, practice and maintain a BC plan. It is interesting to see that, as with the research produced from the Cyber Security Breaches survey 2023, the NHS has prioritised the formation of a formalised IR plan as a desired organisational component when compared to the approach BA took prior to its 2017 incident.

In my research it was clear that there is still a great deal of confusion about the distinction between the terms "disaster recovery" and "business continuity", as the two terms are often used interchangeably or together to indicate one function. This would suggest that the confusion would continue to permeate to organisations also - it might be argued that finding accurate guidance on this topic could prove very challenging for organisations wishing to develop their IR strategy.

Task 3

What do you consider the difference between CPNI and NCSC in UK. What are international equivalents in Europe and the rest of the world? Give 2 examples.

CPNI - the Centre for the Protection of National Infrastructure:

- Now replaced by the National Protective Security Authority;
- UK authority for protective security;
- Working towards making the nation more resilient to national security threats;
- Part of MI5;
- Provide an advisory service to organisations to help them understand the range, severity and seriousness of all types of threats against the UK.

NCSC - the National Cyber Security Centre:

- Provides practical guidance to organisations and individuals;
- Responds to cyber security incidents with the aim of reducing the harm caused;
- Secures private and public sector networks.

Differences between the two organisations:

- NPSA offers guidance regarding all types of threats (mostly focussed on counter-terrorism), NCSC is focussed on providing guidance for cyber-related threats;
- NPSA advice appears to be aimed towards strategic measures, much of the NCSC guidance is aimed at operational/technical measures;
- Both organisations work with GCHQ.

International equivalents:

- NPSA:
    - Cyber and Infrastructure Security Centre (Australia);
    - European Cybersecurity Competence Centre and Network maintains a list of equivalent organisations in each of the EU member states.
- NCSC:
    - Australian Cyber Security Centre;
    - ENISA (EU).