Exercise 1, based on Presentation #1 submitted by a fellow student

Identify and example of supply chain attack. Give details on the attack, how the attackers achieved their aim, what was exploited, and what affect the attack had on the overall supply chain.

★ Not Petya

External research:

Arguably one of the most well-known examples of a supply chain attack is that of the 2017 attack against Ukrainian critical national infrastructure that made use of the Not Petya malware. The virus was distributed through an infected update to a tax accounting program called MeDoc, which was widely used by Ukrainian companies and made use of the EternalBlue exploit that was also responsible for the Wannacry attack of the same year. The update had been infected by the use of a backdoor installed on servers housing the updater service belonging to MeDoc. The attack crippled the nation, rendering government ministries, banks, transport systems and other state-owned enterprises unable to operate as large volumes of data were overwritten and permanently damaged. The update was launched on the eve of a Ukrainian public holiday, allowing the virus to spread without interference and therefore increasing the amount of damage it caused. Whilst approximately 80% of the affected businesses resided in Ukraine, the attack also managed to spread to companies in other countries where those companies had regional offices based in Ukraine.

Exercise 2

Using the example for exercise 1, give some examples of how the 12 principles could have been applied to prevent the attack happening.

★ Principle 2 - know who your suppliers are and build an understanding of what their security looks like.

★ Principle 3 - understand the security risk posed by your security chain.
The owners of MeDoc had previously been warned about the lax security on the servers by anti-virus companies but had not taken steps to improve matters. Had the organisations utilising the MeDoc software been aware of this, it's possible they might have chosen an alternative supplier or been able to carry out a risk analysis treatment programme.

★ Principle 4 - communicate your view of security needs to your suppliers.

★ Principle 5 - set and communicate minimum security requirements for your suppliers.

If organisations utilising the MeDoc software had communicated their security requirements to the supplier, the supplier might have implemented better security measures (for both monitoring and defensive measures), particularly if there was a risk of lost business if those security requirements were not met.

★ Principle 9 - provide support for security incidents.

Had the affected organisations taken an active security monitoring posture, it's possible that the attack could have been prevented from establishing itself from within individual organisations. Given the automated nature of the Not Petya attack this is unlikely, however earlier intervention could have slowed the spread of the attack across the nation and into other nations. Earlier detection would also have resulted in a shorter system interruption.

★ Principle 10 - build activities into your supply chain management.
If organisations issued risk transference statements to MeDoc on the basic of software update integrity, it's possible that the owners of the MeDoc software might have conducted more thorough testing of its updates before deploying them to customers.

Identify other examples of policy guidance or best practice. Compare them to the 12 NCSC principles discussed (NIST is a good place to start). Discuss any key differences and how comprehensive the alternative is.

★ NIST SP 800-161r1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

External research:

This 326-page document aims to provide "guidance to organizations on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of their organizations". The authors of the document have sought to develop "a systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures". It centres around 11 "dimensions" of cybersecurity supply chain risk management (C-SCRM) that the authors argue should be considered by enterprises in line with their C-SCRM, and these are brought together in the formation of 7 interlinking C-SCRM documents. The authors also discuss how C-SCRM should fit in with other elements of enterprise risk management. An appendix of security control "families" is provided with guidance on what security controls should be considered when undertaking an C-SCRM programme. The document is very comprehensive and draws upon a number of other NIST SPs to inform the guidance.

As a contrast, the 12 Pillars of the NCSC have refined much of the guidance contained within the NIST documentation into self-reflective questions an organisation can ask of itself and its supply chain relationships, arguably provided more concise guidance that is easier to apply to real-world scenarios.

Exercise 2, based on Presentation #2 submitted by a fellow student

Question 1

Which service could I buy from Microsoft so my work network will be considered zero trust?

Microsoft Security, which consists of the following product families:

- Microsoft Defender;
- Microsoft Sentinel;
- Microsoft Entra;
- Microsoft Priva;
- Microsoft Purview;
- Microsoft Intune.

Question 2

Why is it important to understand the business while working on implementing zero trust?

Remembering that each company has unique requirements, the following elements need to be considered in order to align zero trust with the corporate values held by the business:

- How does the business make money?
- How do business transactions flow through the business network?
- How do stakeholders interact with business transactions?
- What is the appetite for risk held by the company?
- What organisational assets, applications, and data need to be secured?
- How is sensitive data utilised across the organisation?

Only once these points (among others) have been considered can a zero trust architecture be deemed as appropriate to the individual needs of the business.