**Current Synveta cyber security team:**

* Cyber security analyst: generalist, responds to cyber incidents as they come. Reports

to Synveta’s IT manager.

* Network engineer: manages the firewalls. Reports to the Network Team Leader.
* Cyber Security Consultant: my role at Synveta. Initially to report to the IT

manager.

**Synveta Current Cyber Security Controls:**

• Organizational governance:

o CEO has a clear business strategy for the business. However, roles and responsibilities for cyber security haven’t been defined. They’re assigned to the IT team. There is no cyber security strategy.

• Asset Management:

o The IT team has a Excel spreadsheet with serial numbers of laptops.

o The Excel spreadsheet includes the model of each machine and details about the warranty.

o Synveta uses Microsoft Office 365 and relies exclusively on Software-as-a-Service applications from various vendors (not only from the Microsoft ecosystem, but there are also others). No software development in-house.

o All data is in Microsoft Azure cloud

o The IT team uses a Secure Operating Environment (SOE) to image all their laptops with the latest Windows desktop version

• Business Continuity and Disaster Recovery:

o The IT team conducts regular disaster recovery testing

o The IT team has clear and documented business continuity plans

o The IT team takes regular backups. Backups get tested periodically

• Vulnerability management:

o Synveta have purchased Qualys vulnerability scanner.

o The IT team uses Qualys on an ad-hoc basis.

o There is no formal vulnerability management program in place.

o Large number of high and severe vulnerabilities reported by Qualys

• Risk management:

o Synveta has a risk team but they perform financial risk activities only.

o There is no technology or cyber risk process at Synveta.

• Third Party Risk Management:

o Synveta doesn’t perform any third-party risk management.

o Contracts are reviewed by procurement and finance, not IT.

• Identity and Access Management:

o Synveta uses Microsoft Active Directory to manage users and groups

o There is no privileged access management solution in place

o Admin account password is shared with a few senior members of the IT team

o Access to resources is granted upon request

o The organization does not use two-factor authentication for login

o Complex login passwords are used

o Employees use a VPN solution to login remotely when required

• Network security:

o The organization has Palo Alto Next Gen firewalls.

o The firewalls have been configured by the network

o The firewalls get audited every year by the network team

o The firewalls get regular updates

o The IT team have up to date network diagrams. The diagrams include the

cloud the environment.

o The network is segmented using VLANs.

• Physical Security:

o Synveta is a highly secure facility, with state-of-the-art CCTV cameras

everywhere

o Synveta takes physical security very seriously

o They do extensive vetting for all their employees

o The have a 24/7 monitoring for their research labs and physical facilities

• Data Security:

o Synveta doesn’t have a DLP solution

o All data resides in Microsoft Azure cloud and Microsoft Office 365

o Key critical application is a SaaS service from a startup called Horizon Labs.

• Policy:

o There is one generic IT policy in place

o No formal information security policy

o There are no data governance policies or information classification

• Cyber Security detection and response:

o There is no detection or response capability

o The IT team responds to alerts from the anti-virus (Microsoft Defender)

o No SIEM in place

• Security Education and Awareness:

o All employees are required to do an introduction web training module. The module includes basic instructions about cyber security.