Cybersecurity in the healthcare sector is a crucial piece of infrastructure, to ensure the safety and stability of healthcare providers. Through the research conducted during our investigation, I was surprised at the huge amount and variety of cybersecurity risks in healthcare. Data breaches expose the personal, sensitive information of millions, leading to identity fraud and a concerningly expansive amount of other negative outcomes. Social engineering to take advantage of unaware employees to gain access to a healthcare provider's network can bring the most secure companies to their knees, and result in intellectual property theft, further data breaches, and put medical devices at risk of being exploited. If there is anything I realised through the research on cybersecurity risks in healthcare, it is that the ways in which hacks can take place are ever-increasing. With every kind of device now becoming connected to the internet and increasingly technologically complex, potential points of exploitation are popping up everywhere.

With such far-reaching and devastating consequences that can occur as a result of cybercrime, an equal opportunity is posed for greater education and understanding of cybersecurity to take place. People are often the weakest link when it comes to the security of technology and can be easily tricked into assisting bad actors. One example I came across was a phishing attack in which an employee at Premera Blue, an insurance company, was sent an email containing a zip file. When the file inside the zip was opened, the company's internal systems were breached. Further, the breach went unnoticed for 8 months. This revealed both a flaw in the strength of Premera Blue's cybersecurity systems and the competency of the staff managing their security. It is a great example of how basic education can help put a stop to many cybersecurity attacks. If the unaware employee who opened the zip file had known not to touch it, the breach would have never occurred. The same exploit provides an opportunity for new cybersecurity technologies to be invented and implemented, to stop similar social engineering attacks from ever making it to employees in the first place. Advanced email filtering and systems to monitor employee interactions with the internet could also help to act as a barrier between the unsuspecting person and the intrusion. With every risk posed by cybercrime, there is an abundance of opportunities for education and innovation to patch vulnerabilities.

Despite the opportunities being simply beneficial to the industry, there are still some ethical implications that could slow the speed at which cyber safety is improved. Because systems to monitor technology have to be hyper-aware of every aspect of a system, in order to stop any kind of breach, they require access to every aspect of a network. It could be said that such an invasive system is unethical and allowing it to essentially spy on the activities of employees could be unethical, and overreaching. At what point does cybersecurity encroach on a person's right to privacy? I wouldn't feel too comfortable knowing every single action I took was being monitored and assessed. Because of this, there has to be a reasonable middle ground between the absolute protection of a network and the respected privacy of people. However, for every 'step back' that cyber protection takes, in order to respect boundaries, the vulnerabilities for an attack increase.

The current state of cybersecurity in companies might argue against the idea of a reasonable middle ground. It could be said that when using company devices which are connected to a company network, monitoring is justified. Using the device shows an understanding by the employee that they will be monitored, and by using it they are agreeing to whatever measures a company instils to protect their cyberinfrastructure. Generally, that is the framework by which the ethics of cybersecurity protection are handled in society at the moment. An employee is using a device they do not own, accessing a network, and information all owned by the company they work for. And in doing so, their forfeit the right to privacy in the interest of cyber safety. If they believe it to be invasive, they have the choice to resign, if the issue was ever significant enough to them.

Cybersecurity in the healthcare sector can be a slippery slope between invading privacy and allowing technological weaknesses to exist. There are an ever-increasing number of risks and parallel to that, an equal amount of opportunities to protect against such risks. The healthcare sector deals with the wellbeing of people and there cannot be any room for failure when dealing with human lives. As technology becomes an increasingly vital aspect of every kind of device, cybersecurity has no other option than to evolve in strength, scope, and sophistication.