We are seeing, as a result of this crisis, increasing Cyber threats against a variety of targets, including Critical National Infrastructure and the health sector.

We have all seen the impact such an attack can have, particularly on the NHS, and recognise the impact a major cyber incident would have at this time.

The existing wider, high volume of sophisticated ransomware attacks, which can cripple an organisation and put it out of business, is also a growing threat. The current "business as usual" level of attacks may have more impact in this period as businesses themselves, their IT companies and wider cyber security industry may have less capacity to respond, through sickness and self-isolation.

The following are high risk areas:

1 Ransomware
2 Phishing
3 Home working
4 Wider online fraud

With the increasing stress on organisations, especially those at the front line of the fight against Covid19, there is an even greater imperative that existing protocols are adhered to.

As people are not always expected to be in their current routine this creates further opportunities for socially engineering intrusions and data exfiltration.

Any attempts to circumvent the normal rules and procedures could leave an organisation wide open to cyber criminals and others to take advantage.

If you require any further information, assistance or guidance please do not hesitate to contact your EMSOU Prepare/Protect team

Ian Hickling *Cyber Security Advisor/Protect Officer* *Regional Cyber Crime Unit* *East Midlands Special Operations Unit* ***Tel**: 01623 608169 **Mob**: 07866 942793* ***E:** Ian.Hickling@leicestershire.pnn.police.uk*	Shevani Raichura *Cybercrime PREVENT/PROTECT Officer* *Regional Cyber Crime Unit* *East Midlands Special Operations Unit* ***Mob**: 07966277893* ***E:** Shevani.Raichura@leicestershire.pnn.police.uk*