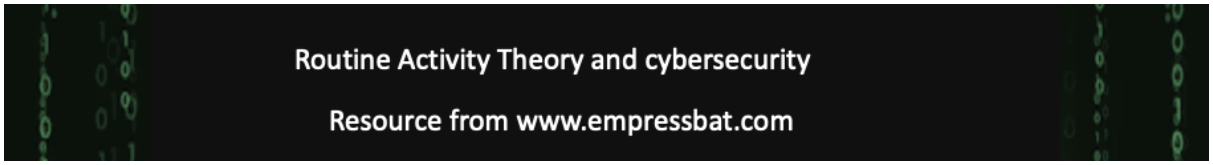

Criminology theories are just as applicable to cybercrime as they are to crime in physical space. For example, **Routine Activity Theory** is a criminological theory that seeks to explain the occurrence of crime based on the everyday activities and routines of individuals within a society. This theory was developed by Marcus Felson and Lawrence E. Cohen in 1979, and it posits that for a crime to occur, three elements must converge.

- motivated offenders
- suitable targets
- absence of capable guardianship

Routine Activity Theory can be applied in a cybersecurity context to cybercrime occurs when there are motivated attackers, vulnerable systems or networks (suitable targets), and inadequate security measures (absence of capable guardianship).

The motivated offenders could be nation state sponsored threats, financially motivated criminals, or hacktivists.

The suitable target from a cybersecurity perspective could be individuals or organisations with weak email security protocols or employees who are not adequately trained to recognise suspicious emails such as phishing attempts.

The absence of capable guardianship might refer to the lack of effective email filtering systems or cybersecurity awareness training programs within the targeted organisation.

By applying Routine Activity Theory to cybersecurity, operational cybersecurity analysts, cybersecurity risk assessors, and those involved in awareness and security culture programmes, can better understand the conditions that contribute to cybercrime and develop strategies to help mitigate risks by addressing the factors related to motivated offenders, suitable targets, and guardianship.