



Protect our
railway



Take
responsibility



Behave
securely

What is security?

An Infrastructure Manager's Perspective



Darren Hepburn
Network Rail Telecom CISO

UIC "From GSM-R to FRMCS" Conference
Paris, 17-18 of May 2017

Contents

This deck defines the key elements of cyber security, why it matters and what we are doing to mitigate the risk to Network Rail

What do we mean by cybersecurity?

Defining the cyber space

What are the key threats?

Who could attack us and why

What impacts could an attack have?

Defining the risk to our business

What are we doing?

Proactive and reactive controls to manage risk

How does our operating model support cybersecurity?

Strategic and operational factors



Protect our railway



Take responsibility



Behave securely



Protect our
railway



Take
responsibility



Behave
securely

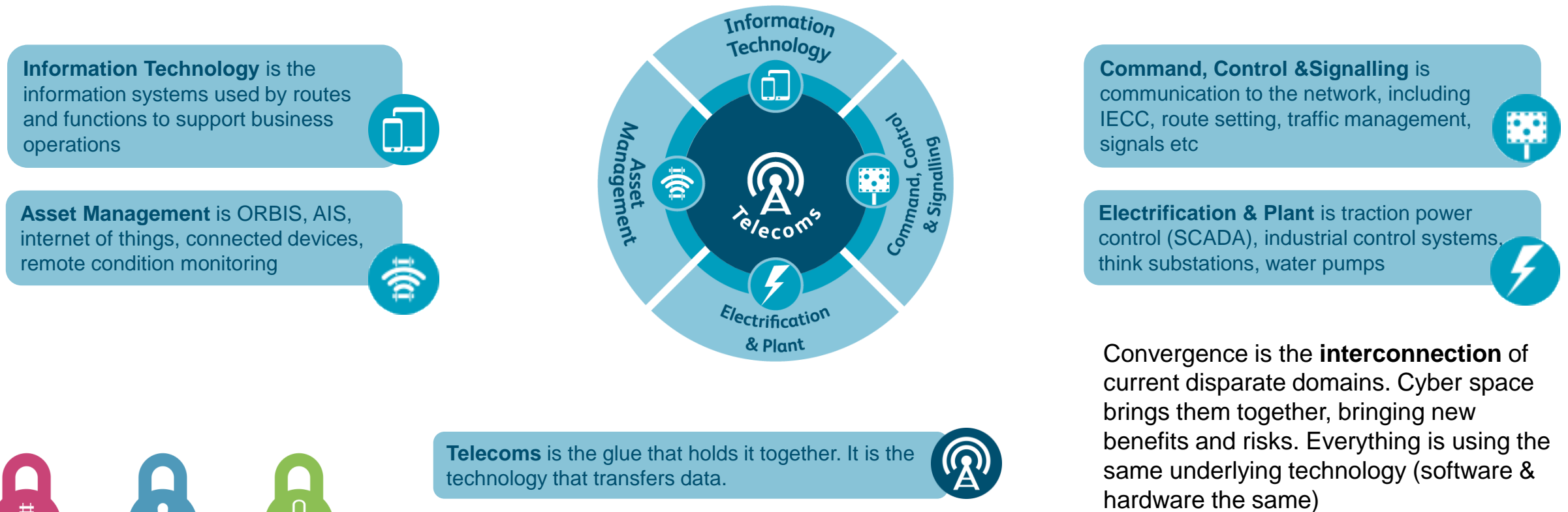
What do we mean by cybersecurity?

Defining the cyber space



Cybersecurity means the protection of cyber space

In Network Rail, **cyber space** is defined by the following technology domains (functional units):



Protect our railway



Take responsibility



Behave securely



Protect our
railway



Take
responsibility



Behave
securely

What are the key threats?
Who could attack us and why



A **threat** is something we need to protect our cyber assets from. We have identified our key **threat actors**:



Threats



Nation State

Network Rail is a part of the Critical National Infrastructure. A successful attack on us could have serious consequences for the country as a whole; hostile **nation states** may wish to exploit this for political ends.



Terrorist

Similarly, **terrorists** could try to compromise safety critical systems to threaten lives or create panic.



Hacker

Hackers may simply want to disrupt our operations or may intend to sell information on the open market for financial gain. Hackers may affect us unintentionally, as part of general activities.



Organised Crime

Organised crime is our most likely threat as there is a greater understanding of the value of information and data.



Activist

Activists may have political or social motivations. Some hackers would also fall into this category.



Rogue Employee

Rogue employees simply want to do the company harm for personal reasons – although they may also intend to benefit financially. This group might work with other groups.



Protect our
railway

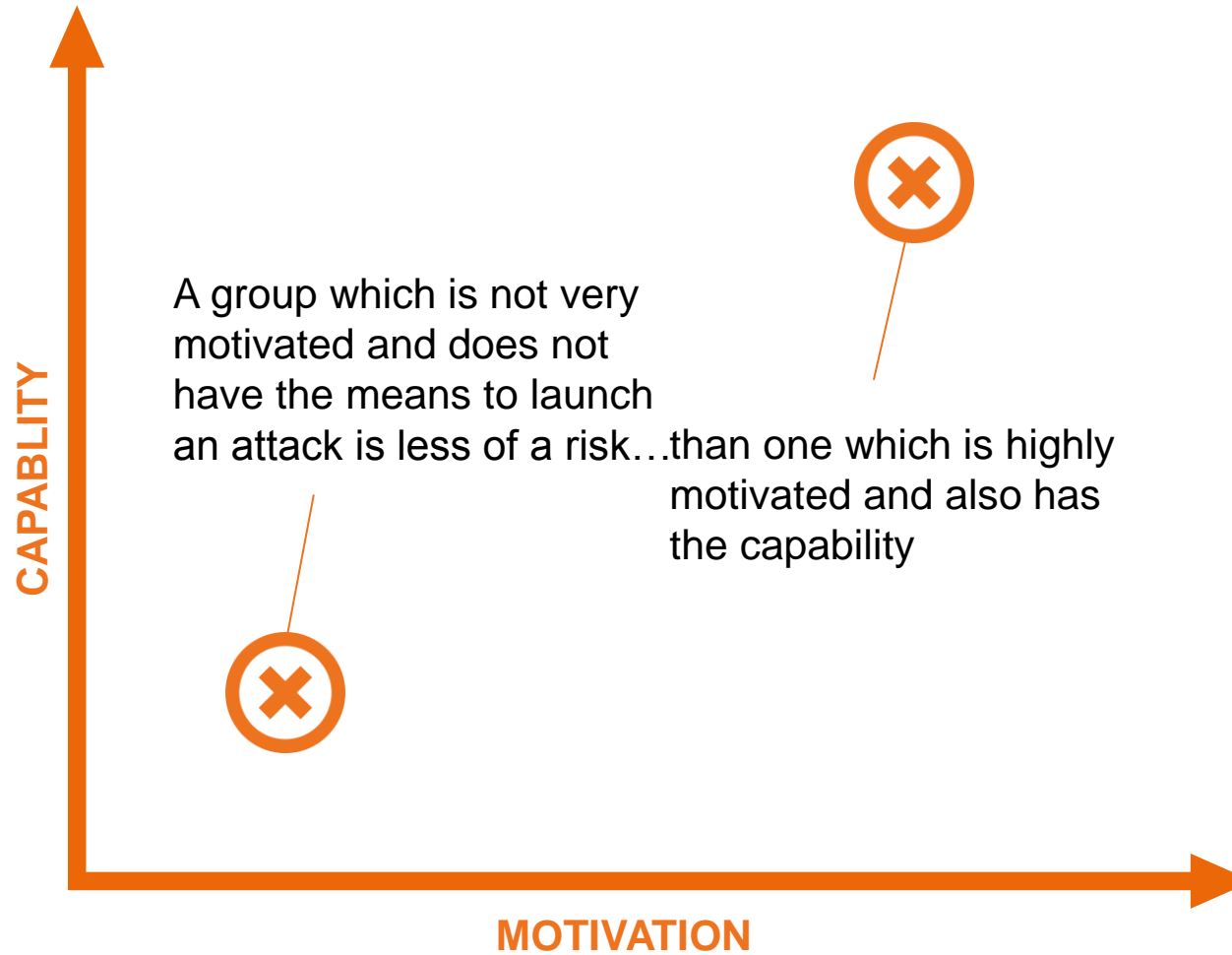


Take
responsibility



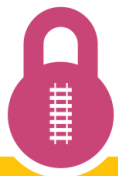
Behave
securely

The **risk** of an attack happening is defined by a combination of the **capability** a group has to carry out an attack and the **motivation** they have to do so.



But these factors may differ according to **type of asset** or **functional unit** – and will also **change over time**...

...so they are all to be **taken seriously and monitored closely** (by Network Rail, National cyber security centre GCHQ and DfT threats team).



Protect our railway



Take responsibility



Behave securely



Protect our
railway



Take
responsibility



Behave
securely

What impacts could an attack have?

Defining the risk to our business



A **impact** is what will happen if an attack is successful. An attack could undermine one or more of the following, all of which are essential components of Network Rail’s strategy:

Impacts

Safety is the protection of people from harm. We have an obligation to keep **our employees, customers and end users safe**. Many cyber assets are safety critical – a successful attack could cause an accident either directly or by causing panic and confusion.

Safety >>>

Reliability is an essential part of our service to our **customers**. Attacks on our systems could cause delays or other disruption which would compromise our ability to provide the service our customers expect.

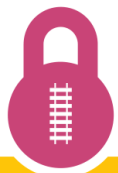
Reliability >>>

Efficiency is about our ability to operate in a commercially viable way and meet our obligations to our **stakeholders**. A cyber attack costs money – not only do we need to tie up resources fixing the problem but in many cases other employees are unable to work while this happens.

Efficiency >>>

Trust relates to our reputation and the perception of our **brand**. A successful attack could expose sensitive or embarrassing information or damage trust by demonstrating our inability to operate securely. This in turn impacts our relationship with customers and suppliers, who may be less confident doing business with Network Rail as a result.

Trust >>>



Protect our railway

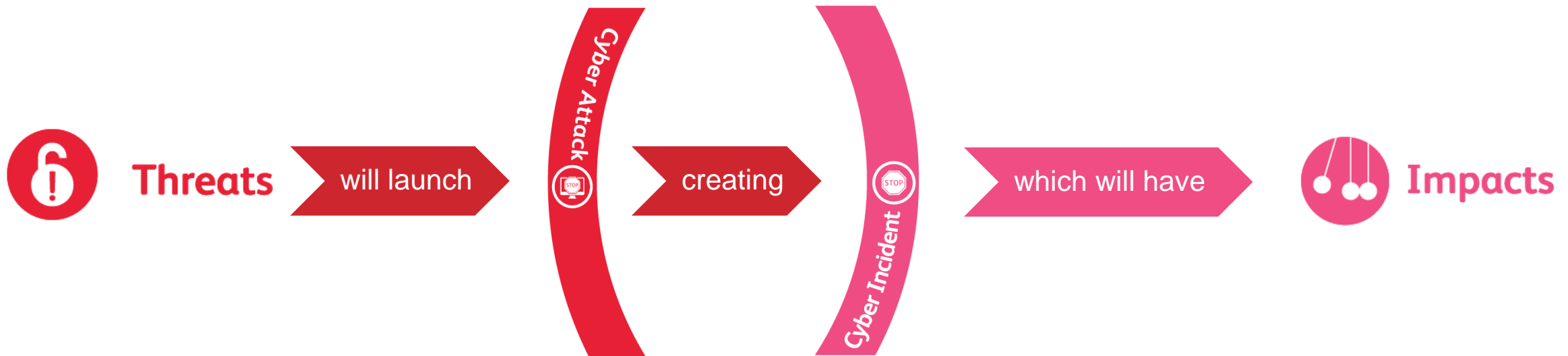


Take responsibility



Behave securely

The **gross risk** is the probability that:



It is not realistic to mitigate cyber risk entirely. One option is to do nothing and accept the risk. At Network Rail this option is unacceptable, so we invest in **bringing the risk down to tolerable levels**. What we define as tolerable is a trade-off between investment and return – ie how much can we reduce the risk within acceptable levels of expenditure.



Protect our railway



Take responsibility



Behave securely



Protect our
railway



Take
responsibility



Behave
securely

What are we doing?

Proactive and reactive controls to manage risk



We reduce risk by imposing **controls**:

PRO-ACTIVE CONTROLS

Deter, prevent, protect are proactive controls – if we get these right there is no potential for loss BUT some attacks need to happen before we know what to do with them (eg viruses)

Deter: First, we act on the intent or motivation, aiming to make an attack less likely in the first place (demonstrating that we are difficult to attack will make it less tempting for e.g. organised crime)

Prevent: Next, we try to make sure that if an attack *is* launched, it will not reach our systems (e.g. by data segmentation or limiting the types of traffic which interface with the internet)

Protect means what we do to systems to make them less vulnerable to attack (e.g. patches, access controls, fixing code defects)

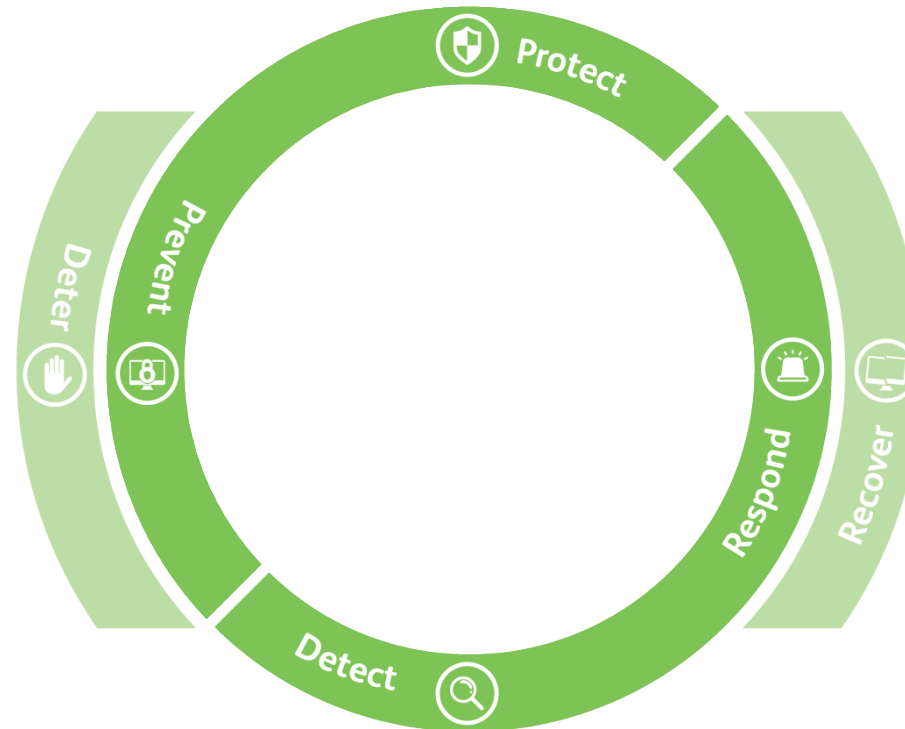


REACTIVE CONTROLS

Detect, respond, recover are reactive controls – what we do to minimise the damage of a successful attack. These are more costly and less effective.

Responding is about limiting the extent of the damage as much possible (e.g. unplug a building or turn off access levels). This may also involve communicating with impacted customers or Mandatory Breach Notification.

Recover means getting back to BAU. It will also include forensic analysis of what went wrong and learning from the incident to try to prevent it happening again.



Detection is about recognising that we have been attacked, that it has been successful and the extent of the damage*



*the global average for the time between an attack happening and victim knowing about it is 6 months.



Protect our railway



Take responsibility



Behave securely



Protect our
railway



Take
responsibility




Behave
securely

*How does our operating
model support cybersecurity?
Strategic and operational factors*




Controls can only be effective if the **operating model** supports them. There are two broad areas where the organisational behaviours interface with security:


Strategic engagement and awareness is about the extent to which cybersecurity is part of the corporate culture at a senior level. It is about understanding the risks and potential consequences and the essential role cybersecurity has in helping Network Rail achieve its strategic and financial goals.




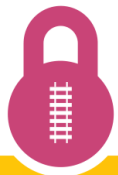
Senior stakeholders can **lead** by defining the company's risk appetite, developing a strategy and generally setting the tone.




Assurance makes sure there are standards and policies in place and that they are being applied correctly. It assesses whether KPIs are being reached and is effectively an audit function.



Governance is about mapping the requirements of the cybersecurity strategy onto the people who will make it happen: who is responsible for which areas, what are the accountabilities, what are the KPIs. Governance may be conducted by boards, steering groups or individuals.

Protect our railway



Take responsibility



Behave securely

Shaping designs specific system and process architecture to make sure that the right controls are defined as requirements at the outset of any new project. For example it might include a standard reference model to allocate particular risks to specific categories.

Building is effectively project delivery – making cybersecurity happen by building the technological systems which will effect the controls detailed above.

Run is what happens when these systems are handed over to BAU. It is the set of activities which will maintain the systems and keep them secure over time. For example, the systems will need to be adapted to cope with new viruses as they are discovered.



Operational engagement and awareness takes place at a more detailed level. It is about situational awareness and what is actually happening.



Protect our railway

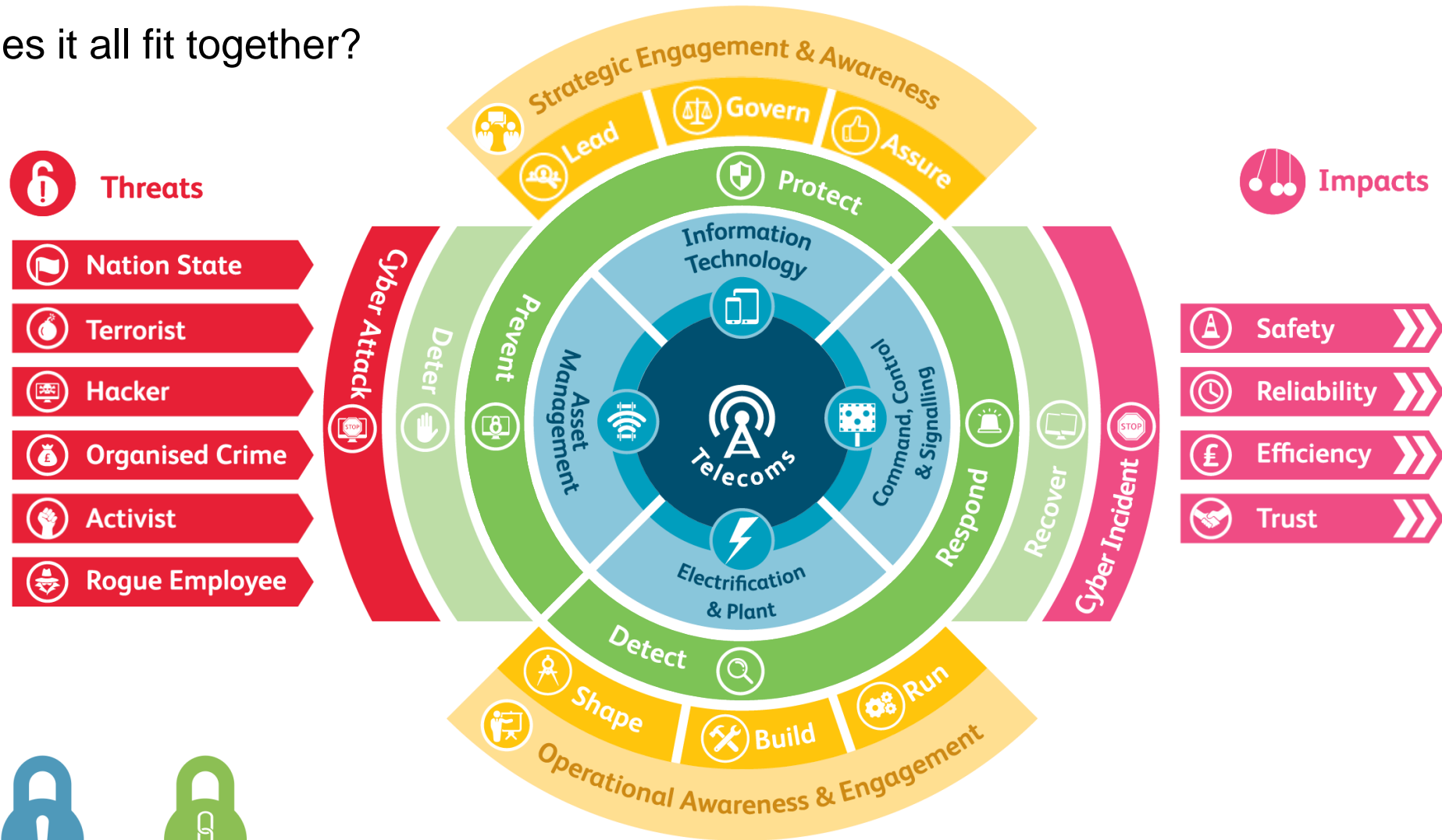


Take responsibility



Behave securely

How does it all fit together?



Protect our railway



Take responsibility



Behave securely



Protect our
railway



Take
responsibility



Behave
securely

Thank You

Questions?

