MINESH PANDYA
PRINCIPAL
HKA

Cyber resilience for the rail industry during heightened threat levels

As first published in Rail Professional Magazine, May 2022, Page 81

Safety is the priority in the rail industry and the importance of ensuring cyber resilience to help secure control centres, stations, trains and data centres is amplified during elevated threat levels.

Background
Cyberattacks have continued to rise as a result of the Russia-Ukraine conflict. During these times of increased cyber warfare, global governments have issued notices advising their citizens and organisations to remain vigilant and take steps to improve cyber resilience.

Critical infrastructure is under threat. Russian threat actors have a history of launching cyber-attacks against critical infrastructure. Only last month (March 2022) the USA revealed a previously sealed indictment from August 2021 that brought criminal charges against four Russian government officials. Between 2012 and 2018, the USA have alleged that the attackers engaged in two major hacking campaigns that targeted critical infrastructure and affected thousands of computers across 135 countries.

More recently, in February 2022, hacktivists (a group that launches cyber-attack on systems for social or political purposes) claim to have allegedly breached rail traffic controls systems in Belarus, claiming that this was an attempt to disrupt Russian soldiers moving into Ukraine. Hackers were able to render critical systems used for routing and switching inoperable by encrypting the data stored on them (ransomware), causing some trains to be stopped in the cities of Minsk and Orsha, Several Belarus rail websites were also inaccessible as a result of the cyber-attack.

The rail cyber-attack threat is noteworthy because it may represent an advancement in the methods and motivations associated with hacktivists in the past. Hacktivists have previously been seen using basic, widely available tools to launch cyber-attacks using the tactics such as of doxing (leaking confidential information), disruption and defacement. This latest attack represents a higher level of sophistication in tools and a greater effort in intelligence gathering in order to launch the ransomware in a more targeted fashion. The rail industry is on high alert as a result of recent more sophisticated cyber-attacks and a long history of state-sponsored attacks on critical infrastructure.

Addressing cyber risks in the Rail industry
While there are immediate tactical actions that can be taken during heightened threat levels, which we will discuss in the next section, it is prudent to take the opportunity to review overall risk registers to ensure identified risks are treated appropriately. For example, the externally facing business service that hasn't been security patched, or areas of the business with ingress points that aren't strictly access controlled, monitored, and logged. Now is the time to reassess and properly treat these risks in order to reduce the risk of cyber-attack.

From a strategic standpoint, effective risk management and governance, like in other industries, is essential to mitigate cyber security risk. It is critical to escalate cyber security risks that cannot be adequately treated to gain

visibility and sponsorship at the appropriate senior level. The following are some areas that should be reviewed from a risk management perspective for rail in a high-threat situation:

Interfaces and connected systems – As a result of digitisation control centres, trains, stations, signalling, power systems control, trackside monitoring and back-end data centres becoming more connected. Large control centres, for example, now provide an efficient single location for rail network management and monitoring, but system segregation in these locations is vital to protect against external threats from access to the rail network.

These advancements in technology increase the attack surface and, as a result, the points of entry for a potential attacker. To reduce the risk of unauthorised access, it is important to ensure all entry points are strictly controlled, and strong two-factor authentication is used for remote access into the network.

Legacy systems – Legacy systems were traditionally seen as a support function to safety and ticketing systems, they were not refreshed as frequently when compared to other industries, posing real risk to the rail industry. Robust asset management will help identify these systems and ensure they are adequately protected.

Third parties – Rail companies typically outsource their IT capabilities to a third party, it's critical to not only review your contractual agreements to ensure the third party complies with your security policies for protecting systems and data, but also to manage the risk posed by the third party.

"The rail industry is on high alert as a result of recent more sophisticated cyber-attacks and a long history of state-sponsored attacks on critical infrastructure."

Immediate actions to take to improve cyber resilience
The National Cyber Security Centre (NCSC) has published guidance on what organisations should do when the cyber threat level is heightened, which can be found here: https://www.ncsc.gov.uk/guidance/actions-to-take-when-the-cyber-threat-is-heightened It is recommended these items are used as a foundation for a tactical action list, with a goal to immediately address them and ensure that priority is given to resolve these items over other business activities.

Five key considerations and practical tactical measures include:

Review and remediate exposure:

- Vulnerability scan internet facing systems and resolve identified vulnerabilities and unnecessary information disclosure
- Ensure all domains and sub-domains that belong to your organisation are identified and secured, including domain registry data

Protect systems and access:

- Check all systems and devices for the latest vendor patches and firmware
- Review legacy rail systems and disable services that are not necessary
- Ensure unique passwords from staff that are not shared across other non-business systems

- Review and remove unused and old user and service accounts and ensure the principle of least privilege is maintained
- Ensure strong multi-factor authentication for remote access to all business applications

Tune up defences:

- Review logging, monitoring and alerting arrangement to ensure all critical applications and systems are included
- Use threat hunting to actively protect networks against applicable rail specific advanced threats that evade existing security solutions
- Ensure anti-virus is installed, up-to-date and installed on all systems
- Check firewall rules are as strong as possible only allowing necessary port and service specific traffic between only those systems necessary

Prepare to respond:

- Review backup arrangements and ensure offline copies are recent enough to recover from a cyber attack
- Check your incident response plan is up to date, practiced and has all the necessary contact information and escalation points

Communicate and keep up to date:

- Brief your wider organisation and ensure that the heightened threat level is understood so that buy in can be achieved to help undertake the tactical and strategic actions required
- Ensure all staff are aware of the threat of phishing emails and how to report them
- Keep up to date on the latest cyber threat information as threats will rapidly evolve their tactics and techniques during a heighted threat level.

As cyber-attacks become more sophisticated, it is more important than ever to maintain cyber resilience in order to prevent the disruption of safety critical systems.

These tactical items, combined with the previous strategic risk management themes for rail, will help to ensure cyber resilience and, ultimately, customer and employee safety during times of increased threat levels.

If you require any further information, please contact Minesh Pandya at mineshpandya@hka.com.