CYBER THREAT TO TRANSPORT

Cyber Threat To Transport

26 Jun 2017 by: Philip Ingram

75,000 people stranded and a reported up to £150 Million compensation for what has been described as an engineer allegedly failing to follow proper procedures at an IT centre in Heathrow. His re-booting of computer servers led to ‘catastrophic physical damage’ to other servers across the world. Now, this has not been described as a cyber-attack, but it has highlighted the vulnerability of interconnected systems in our transport sector. How big is the cyber risk? Philip Ingram looks for the UK Security Expo.

According to a 2016 EU Transport sector economic analysis report, transport plays an important role in today's economy and society and has a large impact on growth and employment. The transport industry directly employs around 10 million people and accounts for about 5% of gross domestic product (GDP). Effective transport systems are fundamental for European companies' ability to compete in the world economy. Logistics, such as transport and storage, account for 10–15% of the cost of a finished product for European companies. The quality of transport services has a major impact on people's quality of life. On average 13.2% of every household's budget is spent on transport goods and services. Like many industries, transport is reliant on interconnectivity through cyber space. The BA outage highlights just how fragile elements of the cyber infrastructure is. Andy Blackwell of Blackwell Security Consulting says of the threat to the transport sector, “It’s not just physical attacks that the industry has to concern itself with. The aviation sector faces increasing vulnerability to cyber-attacks as technologies such as WI-FI become more widespread. Recent initiatives by the International Civil Aviation Organisation (ICAO) and the European Aviation Safety Agency (EASA) provide us with an indication of the increasing

risk to the sector's cyber security due to increased connectivity." The accidental insider remains one of the greatest risks as shown by the recent BA outage. Procedures, training and a culture of enablement is what deals with these. The cultural cure to accidental insiders is probably one of the strongest preventative measures. Deliberate insiders are probably the most concerning and therefore at airports vetting for those with "airside" passes are particularly important but we don't see the same vetting applied to Road, Rail and Maritime transport sectors. This could be an area for discussion in the rounds at the UK Security Expo at the end of November. Transport networks are becoming increasingly digitised, connecting physical networks with virtual networks through a wide variety of modern but often legacy control mechanisms. It is these legacy items that create the greatest vulnerabilities for transport systems to cyber exploitations. Add in an increasing number of IoT enabled capabilities utilising increased Wi-Fi connectivity and the potential attack surfaces are growing massively. Of note, the Willis Towers Watson 2016 Transportation Risk Index highlighted that for air the most critical risk identified was failure of critical IT systems and in the maritime and land environments it was Increased security threat from cyber and data privacy breaches. The report goes on to say, "Cyber is the primary risk when an aggregate rating is taken across the five regions, and across the 12 transportation subsectors. Through that lens, the threat of cyberattacks is the top perceived risk for companies operating in such diverse business arenas as space, rail freight and third-party logistics." As part of its summary it adds, "Business crises tend to have broad technical, financial, operational and reputational consequences, so risk mitigation strategies have to be formed in the boardroom, where the full spectrum of possibility is recognised. The responsibility for digital risk management no longer belongs in the IT suite, where technical solutions take priority over any business-continuity response. Not only is it costly to construct a technical response to a cyberattack or critical systems failure, there are simply more effective ways to limit their commercial and reputational impact." The BA outage reinforced this message. Commenting on ways to improve cyber security in the sector, Andy Blackwell said, "an integrated approach to security will help improve resilience. The UK's Security Management System (SeMS) Framework, developed with industry by the DfT and CAA , if implemented correctly, will provide corporate assurance that ALL known security risks are being managed. Collaborative approaches between industry, government and key stakeholders are vital, particularly with regards to the sharing of information and best practices." These are clearly issues that will be examined in detail through the 2 days of the UK Security Expo at Olympia on the 30 and 31 November, just one of the reasons to ensure you have registered to attend.