**HRTec Blog Posts**

**Articles 7 and 8**

**Ian Mabon**

**Article 7: Insurers Predict $33bn Bill for Catastrophic "Cyber Event"**

Insurers are predicting a massive “once in 200 years” loss in the cyber-insurance industry due to a cataclysmic “cyber-event” that could happen in the next few years. Using three types of modeling software being fed data from millions of cyber policies, analysts in this industry say losses can amount to “$15.6bn to $33.4bn, covering three potential scenarios: a cloud outage, data theft and ransomware/malware.” These scenarios would disrupt any type of business that uses cloud computing or stores personal information, leading to insurance companies paying billions of dollars to repair the damages of these harmful attacks or malfunctions. However, all models agree that a ransomware attack would be the most harmful and costly to businesses, leading to around 30 billion dollars insurers would have to pay to their policyholders. The premium of these policies have reached 9 billion dollars, despite only being 2.6 billion dollars in 2019. Despite the alarming figures and potential impact, the report suggests that the cyber-insurance industry has the resilience to withstand significant losses from a catastrophic cyber event. As quoted by the article: “Industry leaders and insurance entrepreneurs recognize this [potential event] and spy opportunities for continued growth and performance in this sector.”

**Article 8: Accelerating Our Economy Through Better Security: Helping America’s Small Businesses Address Cyber Threats**

This article written by the Cybersecurity and Infrastructure Security Agency (CISA) describes the steps that small and medium enterprises should take to secure their private data from cyber attacks. In the article, the CSIA states that small businesses are “three times more likely to be targeted by cybercriminals than larger companies and total cost of cybercrimes to small businesses reached $2.4 billion in 2021.” To counteract the impact this has on businesses, there are a few steps these businesses can take to reduce their risk of being attacked by malicious hackers. First, total company awareness of this risk is key for success. Staff should be regularly updated on security protocols and reminded to take the necessary steps to secure the data they use during the workday. Second, analogue data such as physical mail and filing cabinets should be uploaded to a secure service that protects data from cyber attacks and where onsite security doesn’t need to be involved in protecting important data. This might sound like the opposite of securing data from hackers by putting it online, but using a trusted service is much more secure than a filing cabinet that anyone can have access to in the office. Third, using Multi Factor Authentication to confirm the right person is accessing the appropriate data is one of the most effective ways to stop cyber attacks. Sending a SMS to an employee’s phone or an email to their work email stops hackers from easily accessing data. Lastly, regularly communicating with a CSIA cybersecurity advisor to keep up to date with security protocols and methods of securing data helps a business stay on top of security threats. To quote the article, taking these steps in a small to medium sized business is “a recipe for a sustainable future, and one in which we all have a stake.”