THE CHALLENGES FOR UK LIFE SCIENCES COMPANIES

Are the UK's life sciences companies doing enough to protect data?

Life sciences companies have intensified their focus on privacy, security and information risk management to avoid regulatory risk and others stealing their information for competitive advantage. But are they doing enough?

A young university spin-out may be more focused on developing its proprietary technology than realising the high importance of protecting its data.

Richard Staynings, Chief Security Strategist at Cylera, a global cyber security company with offices in Cheltenham, says that life sciences organisations have been in the cross-hairs of cyber criminals for nearly two decades.

"Initially this was for the theft and sale of PII (personally identifiable information – any data that could potentially identify a specific individual) and PHI (protected health information) which can fetch high prices on underground marketplaces, but these marketplaces became full of data batches for sale, so prices dropped, and this pastime became less lucrative."

However the market still exists he points out, and a complete personal identity for someone with an excellent credit rating in the right age range and income bracket can fetch thousands of pounds for criminals specialising in identity theft.

"Far more lucrative today appears to be cyber extortion campaigns that steal regulated data and threaten to release it unless a ransom payment is made. Often this is run as a double or triple extortion campaign, where perpetrators approach the organisation and each of the individuals whose data has been obtained to maximise leverage that a payment will be made. The types of attacks are mainly being carried out by organised cyber crime gangs or freelance criminal hackers."

Phil Howe, CTO at Core to Cloud, a cyber solutions company in Cirencester, added: "Failure to protect regulated data such as PII and PHI can result in fines in the millions of pounds or euros, the award of punitive damages and the need to provide credit monitoring services for anyone impacted. Regulators have issued massive fines to the most egregious failures or where inadequate cyber security controls have been put in place to protect non-public regulated data.

> *"Nearly all these cyber espionage attacks have been carried out by the Peoples Republic of China ..."*

"Even more valuable for cyber criminals, and in particular nation-state actors, is the theft of intellectual property including experimental drug and treatment regimes, trial procedures and methodologies, proprietary drug formations, experimental medical devices, more or less any use cases involving AI or machine learning, and anything that helps a healthcare life sciences organisation differentiate itself in the marketplace," added Phil. "This is provided to state owned enterprises which have been told by their autocratic government of the need to surpass western competitors as part of the next five-year central plan."

Richard continued: "Nearly all these cyber espionage attacks have been carried out by the People's Republic of China which is thought to employ close to 100,000 People's Liberation Army cyber warriors engaged in the theft of military-defence, intellectual property, and commercial trade secrets from almost every other nation on the planet."

According to General Keith Alexander, former director of the United State National Security Agency, the Chinese theft of American intellectual property is the "greatest transfer of wealth in history," likely costing the US upwards of $400 billion a year. Britain and Europe have expressed similar sentiments for their respective economies.

"Cyber security company Mandiant first drew mass public attention to the problem of Chinese state-sponsored cyber espionage of commercial trade secrets over 15 years ago," Richard added. "Since then, China has continued to increase its espionage activities. Its theft of commercial trade secrets has been so successful that Chinese companies have been first to patent and launch new products on the global market, based upon ideas and research stolen from others.

"Protecting IP is critical for any innovative company whether long-established or a fledgling start-up. Anyone who doesn't afford comprehensive and holistic cyber security is asking not to be in business for long."