(In)secure services
CYBER SECURITY

HI

Increased connectivity has increased the need for cyber security. Once everything is networked, small groups and individuals working remotely can launch covert attacks, stealing (for example) personal information from customer databases, distributing and activating malware or carrying out botnet distributed denial of service (DDoS) attacks. Organisations may come under cyber attack from individuals, criminal groups or hostile nation states. It is now accepted that all future conflicts will have a cyber element and that some may be fought entirely in cyberspace.

The cost of some types of cyber attack is simple. In the US, 1.4 million Jeep Cherokees were recalled in 2015 after a vehicle was hijacked by hackers taking control of the car's air-conditioning, radio, and windscreen wipers before removing control of the accelerator and brakes from the driver. The hackers were ten miles away from the car at the time they took control of it; and it was an experiment.

What does this mean for the future of cybersecurity? Simply put, that companies with no experience of the information security industry - toymakers, carmakers, financial institutions and more - should not work alone on products which require a connection to the interneT but should work with experts.

No surprise then that demand for cyber security skills is expected to surge; but tackling the issue will also require all workers to become cyber aware – and, governments and business to maintain up to date security software.

Implications for Gwent

This is an issue that faces Gwent directly as well as requiring Gwent to advise business.

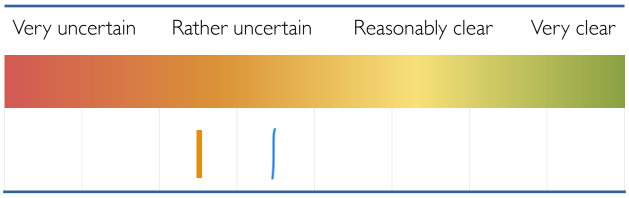
Research published by Invotra at the end of 2017 highlights that the majority of senior IT managers working in the public sector view data and system security as their 'biggest priority'. 79% of IT managers saw security as their main priority while 60% said high profile cyber attacks had prompted more scrutiny of their systems.

Just over a quarter (26%) said the attacks made people within their organisation 'fearful', which negatively impacted productivity. A further 23% described high profile hacks as 'demotivating'.

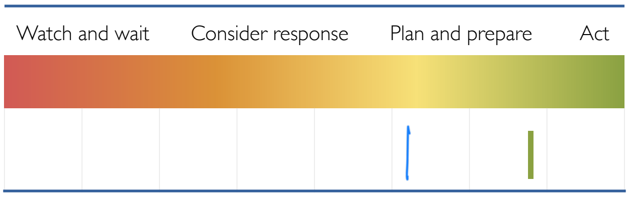
When asked about the progress made towards the Government's 'digital by default' standard, 44% described digital transformation as 'an important focus', but said the public sector is 'way behind' the private sector. Almost a third (32%) feel too little is invested in technology to achieve digital transformation goals, and 29% believe a lack of skills is a barrier. The survey found that, even when investment has been made in technology, just over half of respondents did not believe there was sufficient training in new systems.

Perhaps Wales should follow the US in launching cyber security badges for Girl Scouts. Or perhaps it should launch a Welsh version of the badge for local government staff. Gwent could suggest and pilot the scheme.

How might the issue impact on Gwent in the future



How might Gwent public services respond?


Watch and wait
Consider response
Plan and prepare
Act