7 infographics from the Cisco 2018 Cyber Security Report explained

In our final part of Cisco’s 68 page 2018 Annual Cyber Security Report, we summarise the key findings and highlight the main takeaways contained in the report.

While most of the information is already known, put in context it gives a thorough view of the changing landscape and importantly identifies some of the steps that Information Security teams could take to mitigate the growing risk.

The reports highlights include;

- Self-propagating ransomware is a growing trend

- Legitimate cloud platforms are increasingly being exploited for cyber attacks
- Cyber attackers are exploiting gaps in security coverage as organisations move to the cloud
- Lack of skilled cyber security staff is a growing problem
- Security is more effective when policies governing technology, processes and people are synced
- Scalable cloud security, advanced endpoint protection and threat intelligence can be deployed to reduce the cyber threat risk

According to the Cisco report, cyber attackers are amassing their techniques and capabilities at an unprecedented scale.

Ransomware is the most profitable form of malware and has evolved into self-propagating network based cryptoworms as witnessed by Nyetya

and WannaCry. These ransomware variants took down whole regions and

sectors of infrastructure such as the Ukraine and the NHS.

Cyber attackers are weaponizing the cloud and using legitimate cloud services from well known vendors such as Google, Amazon, Twitter to host and conduct malware attacks. They are in fact capitalising on the benefits of cloud platforms such as security, agility, scalability and good reputation, oftentimes repurposing their sites before they are detected.

Cyber attackers are exploiting gaps in security coverage including IoT and cloud services especially where the organisation has not extended their security controls to include securing users and data in the cloud. Another growing obstacle to more effective cyber security is lack of skilled cyber security personal and inadequate budgets.

Cisco’s report also provides some essential guidance that organisations

should adopt in order to meet the growing challenge and provide more effective cyber security protection. Some of these measures include;

- Implementing scalable cloud security solutions
- Ensuring alignment of corporate policies for technology, applications and processes
- Implementing network segmentation, advanced endpoint security and incorporating threat intelligence into security monitoring
- Reviewing and practising security response procedures

- Adopting advanced security solutions that include AI and machine learning especially where encryption is used to evade detection

While the security report is essential reading for all personnel responsible for an organisations information assets, in many areas it reiterates what we have been hearing about in the news and trade publications. The essential call to action is really to make a good start by doing the essentials. If you have already done this, then keep testing, refining and improving your cyber security posture.