Employing Cyber Resilience

Almost two months ago, the Health Service Executive (HSE) of Ireland was hit by a ransomware attack that represented the most significant cybercrime attack on the Irish state to date and understood to be the responsibility of a criminal actors using Conti Ransomware.

Written by Nick Emanuel, Senior Director of Product at Webroot, an OpenText Company

Ambulance services, GP and pharmacy systems were not directly hit but the impact was, and continues to be felt community wide…so the question is what can I do about it, how does it affect a Community Pharmacy?

Given the pandemic and the widespread shifts and disruptions over the past year, we have all been faced with re-evaluating our ability to face unprecedented threats or preventing ransomware attacks.

Some ask if it's even possible to mount a cyber defence with the view that Government has deep pockets and expertise and it still couldn't prevent a devastating and disruptive attack. Still others will say I'm too small to be targeted.

The EU Agency for Cybersecurity (ENISA) regards the health sector as vulnerable to cyber incidents and crises, noting in their 2019 Threat Landscape report that "more than 66% of healthcare organisations experienced a ransomware attack in 2019." The FBI identified at least 16 Conti ransomware attacks targeting U.S. healthcare and first responder networks in the year prior to the attack on the HSE.

Despite the growth in attacks, the National Cyber Security Centre, which advises Government on cyber threats, has an annual budget of just €5 million and no dedicated headquarters nor Director.

Are there practical steps community healthcare providers can take? The good news is yes, you can reduce both risk and impact of an attack by increasing overall cyber awareness as a business, an effect we call 'cyber resilience'

Think of cyber resilience as digital fitness. It's the ability to keep moving forward in the face of adverse cyber threats. Understanding the threat, taking precautions, and layering security will lower the risk to you, and should the worst happen, reduce the disruption, and allow for quicker recovery.

Here are some cyber resilience tips that busy pharmacy and dispensary teams can put in place and improve their digital fitness.

1. **You won't be an expert in a day**, it takes time to reach a healthy level of cyber awareness! There is a lot of help there from vendor guides, government advice and of course bringing in expert help though an IT Security provider.
2. **Deploy the community** - Install reputable cyber-security software that uses real-time threat intelligence gathered from devices all over the globe to protect users by blocking attacks.
3. **School is in!** - training staff about phishing and spam, and common techniques used by criminals is easy with a range of Security Awareness training products. Look for one that specializes in micro-learning (bite size chunks) to help busy pharmacies and staff get trained with minimum disruption.
4. **Make it tougher for the bad guys** - don't share accounts or passwords, not with each other or with other programmes/ software. Reinforce a strong password policy and make multi-factor authentication mandatory wherever possible.
5. **Be cautious of the free tool** - Free email accounts like Hotmail, Gmail or similar can be tempting, but a secure, managed email account from an IT provider with Anti-Spam and Phishing controls will make you less vulnerable to many common attacks.
6. **Upgrade and Patch** - Few treatments are one pill and done, and they need to be taken on time. You PC or device is the same – upgrade to the newest operating system and update/ patch software. Take advantage of the security protection that vendors have rolled into those upgrades to combat new threats.
7. **Back Up** - Shake out and test your data backup plans. Ask yourself: is everyone/every device covered, is the data being successfully backed-up, have you tested recovering your data, are the back-ups secured off site or in the cloud?

Prescriptions are templates with unique additions to tailor treatment to the patient, your digital fitness is similar. By ensuring staff understand they play a critical role in ensuring security, adopting a cyber resilient mind set and taking precautions you can keep safe from a range of common threats and be more cyber resilient!