

IT SECURITY THREATS

Over the last decade, security has become a bigger issue for IT admins. It's hard work staying up to date with real attacks and the occasional hoax. Whether you're running windows or on a MAC OS, the threats are out there.

What does this mean to our business?

The key issues are resources. Time to manage the threats, time to sort out issues after viruses and malware have accidentally been downloaded, time to recover lost data, time to do the day job and time to ensure the organisation is productive. Financially companies can struggle if key files or folders are corrupted, damaged or destroyed.

- Remember downloading the Christmas e-Card that contained a Trojan horse and sent out masses of spam from your PC which meant the internet service providers blocked your email address which mean that you could no longer send emails to clients?
- And what about the emails offering discounts on medications that looked like you sent them but were as a result of a colleague accidentally launching an executable link in their email?
- And did you find the critical files that you haven't needed for 2 years that had become corrupted?

We have all heard different stories about how IT security has an impact on our businesses. Hacking was seen by some as fun but today these threats have become more sophisticated. It's no longer just spyware, Trojans, worms, rootkits, bots and polymorphic viruses, but phishing scams seeking your personal and financial information, and the increased appearance of rogue malware protection (real people are paying real money for anti-virus and malware protection that does nothing) making programmers work harder on their code to evade security defences.

Chris Roche, Managing Director at Acutec Limited commented "it's all very well ensuring the senior team are aware of the implications, in business today, all staff use a computer, all staff use email plus the internet and all staff can download items that can critically damage the business."

"The average cost in repairing a cyber attack is £5,000. Time is needed to identify the damage, repair the systems, reinstall uncorrupted software, reinstate the users and identify whether critical data has been leaked."



Endpoint security

To protect your systems, Endpoint security has developed. This is software that includes

- Firewall
- Anti-virus
- Anti-spam
- Anti-spyware
- Anti-phishing
- Network Access Control

Many companies economise by selecting one element of endpoint security rather than a multilayered defence system which offers real protection. When selecting endpoint security systems, IT admins need to consider

- Holistic solution that protects the organisation against the very latest attacks
- System that performs and doesn't slow the organisation down when managing issues
- Accurate catch rates so that any attacks are correctly and promptly managed
- Real time reporting to enable instant responses
- Solutions that integrate into your existing systems
- Easy to use system that requires minimal input from IT admins

In the last 31 days alone the Acutec virus system detected hundreds of viruses across all systems. Added to which, malware (malicious software) is a new tool used by organised crime worldwide. If you do one thing today, make sure your endpoint security is switched on and is protecting your organisation.

Acutec provides Endpoint Security Solutions that protect over 5,000 users from viruses, spam, spyware, phishing and Network Access Control. We help companies stay better protected from unwanted attacks.