Article from https://www.cbsit.co.uk

Types of Cyber Security Breach

1. Viruses, spyware and malware. Statistically speaking, these account for a massive 68% of breaches and cause the most disruption to businesses. Viruses and malware are introduced by being bundled into other downloaded applications and can easily be allowed to enter a system by simple human error, tricking the user into downloading something unnecessary. Once in, a virus will react just as a biological virus, embedding itself and then multiplying and spreading throughout the system. They can be almost impossible to remove, often providing no uninstall option. Such an attack can result in loss of data, hardware failure, or it can entirely shut down a network.

2. Impersonation of an organization accounts for 32% of all reported breaches, significantly lower than viruses and malware, but still a third of all cases. Businesses in the finance and insurance sectors are more vulnerable to this type of attack, as these types of attackers are likely to be looking for financial gain. They may send you a false invoice, or claim that your bank account has been hacked and that you need to verify some details, for example.

3. Denial of service attacks are the third in line, accounting for 15% of reported breaches. This type of attack attempts to prevent customers and clients from accessing services. One high profile example of this was the attack on the BBC at the end of 2015, which put the BBC out of action for a number of hours.

Below these, hacking and money stolen electronically come a close fourth place at 13% each, while theft of intellectual property accounts for just 1%.

The Aftermath

The government survey has shown that the main impact that a cyber security breach can have on a business is, surprisingly, not based on reputation or financial losses. Instead, the impact is felt on the time and manpower required to clean up the mess and implement new measures to protect from future attacks. There are often financial implications with regards to repair costs and the possibility of having to invest in new or updated security software. The average financial cost of a breach is reportedly £3480.

Preventing an Attack

Above all, it is important to be able to identify a breach when it happens, and to identify the weaknesses that allowed for the breach. Breaches could be spotted by an employee – this is more likely if the employee is well-trained in this area. A breach could manifest as a disruption to business activities or website take-downs. In ideal situations, a good antivirus software will identify a potential threat before it attacks, or a business could receive an alert from an external IT provider.

The government provides information on how to protect against common internet threats with their Cyber Essentials Scheme. The simplest ways of mitigating an attack include installing, changing or updating antivirus or malware software – this should be done regularly, but should also be combined with a good firewall system and additional staff training and communications. This is especially important, since the survey reports that human error is the single biggest cause of cyber security breaches. It is also important to have in place security policies and procedures which are regularly vetted and updated.