CYBER SECURITY UPDATE

As cybercrime is ever on the increase, it has become increasingly important for ALL businesses to be prepared if it were ever to happen to them. In an environment where attacks are more commonplace and attackers are often one step ahead, it's become apparent that the best offence is a good defence. A worrying fact that came out of an Institute of Directors survey was that almost half of UK businesses have no cyber security plans. As a membership organisation, the safety and security of our members' data is first and foremost, and we also want our members to know the basics of being protected.

The results from the survey stated that only 57% of businesses in the UK have a formal cyber security strategy, which is a rather worrying fact considering that cyber security attacks are on the increase, with high profile hacks to Yahoo, Sony and Warner Bros over the last few years. Is your business protected? It tends to be a case of if an attack happens, not when.

The survey, carried out by the IOD and supported by Barclays, shows some concerning results in the event of cyber-crime, with 40% of IOD members not knowing how to react if a cyber-attack hit. Training is also an evident problem, with 49% of companies not having provided awareness or training to their staff. This is a major issue when there are so many phishing scams and malicious emails around. Attackers profit from flaws in browsers and website plugins to gain access to your important information. The latest advice is to concentrate on recovery and backing up your data and being able to recover data from a safe place, as the majority of the time the only way to rebuild your systems is from the ground up. A report from Symantec, who are internet security experts, saw over half a billion personal records lost or stolen in 2015, though this number could potentially be a lot higher, with some companies choosing not to disclose this information.
With different methods of attacks on the increase it's about times companies protected their data and have contingency plans in place should an attack occur? So how do you protect yourselves if you are a small to medium-sized business? The GA would like you to feel safe, so please take a look at our top tips.

1 – UNDERSTAND THE RISKS

This returns to being prepared for an attack and having a complete understanding of the internal and external issues that can occur from an attack. Try to learn how hackers gain entry including methods and motives from phishing to spoofing scams, social engineering, malware, system hacking and everything in between.

2 – DEVELOP A SECURITY POLICY THAT IS INGRAINED IN COMPANY CULTURE

Where there is a risk there is a way. The security policy should be ingrained into every employee when they have a decision to make or process to follow. Your employees are usually the first targets as they are the gatekeepers of the information that hackers want to get their hands on, which also makes them your first line of defence. Educate everyone to understanding what to do to prevent an attack plus what to do if an attack or breach occurs.

3 – PICK UP THE PHONE

Verify financial requests and confirm details by phone, instead of the ever too easy method of email. This will ensure that you have added extra security verification in your process of payments. This will ensure funds go to their correct parties, and will hopefully protect you from loss. Always be wary about information that is already publically available for the hackers to assume identities.

4 – KEEP YOUR SOFTWARE UP TO DATE

Though many of us dislike a software update and waiting for your computers to reboot, it is actually one of the simplest ways of protecting your data. So don't delay in updating antivirus software or other security applications. This will help you guard against the latest threats and keep your business secure. There are some very reliable freeware antivirus and firewall programs, but always make sure you are confident of their credentials before downloading.

5 – HAVE A CONTINGENCY PLAN

Having a plan in place once an attack has happened is crucial, and makes sure your whole company knows if there has been a breach. By having data backed up and having a strong recovery element to this plan is crucial, but don't take it for granted; it requires regular checks to see that data is being recorded as there have been cases where back up tapes are been found to be blank.
We will be having more updates on cyber security which we will pass out to our members, if you have been a victim of a cyber-attack and would like to share your story about how it happened to warn our other members then please get in touch at enquries@ga-uk.org.

Sources.

http://www.cbronline.com/news/cybersecurity/business/nearly-half-uk-business-no-cyber-security-plan/

https://www.symantec.com/en/ca/security-center/threat-report