PGI SME Cyber Digest

18th January 2017

- New Year, New Ransomware
- Company Fined For Data Loss

The SME Challenge

- Prevention Is Cheaper Than Cure
- Insure, You're Covered
- Steps To Cyber-Security Management

CESG Certified Training | CREST | TIGERSCHEME | CHECK IT Health Check Service | PCI DSS COMPLIANT | Cyber supplier to: HM Government

Customer Services
+44 (0) 845 600 4403
pgicyber@pgitl.com

Company Fined For Data Loss

It was announced this week that the Information Commissioners Office (ICO) has issued a £150,000 fine to Royal & Sun Alliance Insurance after the loss of the personal information of nearly 60,000 customers including names, addresses and bank account details. The data was lost after the theft of a hard drive device and the ICO found that appropriate measures were not in place to protect the financial information by preventing the theft from happening at its offices.

Although this incident was initially a physical crime and not cyber-related, it is a timely reminder of the importance of protecting personal information (the data on this hard drive was not even encrypted), especially with the forthcoming EU General Data Protection Regulation which comes into force next year which will carry significantly higher fines where companies are proved to have been negligent.

New Year, New Ransomware

A large number of our reports last year featured regular stories about the threat of Ransomware. Research by Trend Micro, published just before Christmas, found that new ransomware families soared by 400% between January and September in 2016. It was also claimed that 20% of organisations worldwide suffered ransomware-related incidents and 1-in-5 small businesses never received access to their files even after paying the ransom. But, with so many regular reports it can be easy to get 'warning fatigue' and become immune to the threat. Unfortunately, ransomware is expected to continue to rise in 2017 and the rapid growth of the 'ransomware as a service' model, whereby ransomware operators lease their infrastructure to other customers, has also enabled non-technical users to join the fray.

In an attempt to target-harden your business against this threat, one of the most important barriers to attack is improving staff user-awareness and education. Ransomware is spread like any other type of malware and good cyber hygiene is your best chance of minimising infection. The following general considerations can also help mitigate your chances of becoming a victim:

- Be extra vigilant to not click on a suspicious link or attachment. Attachments from strangers are particularly risky, but if you were not expecting a certain attachment from someone you already know, no matter how tempting the name of that link or attachment might be, then you should email or call them to check it's validity first. This may take a small amount of extra time in your working day, but it will still be a lot easier than having to deal with a ransomware infection if the attachment was malicious.

- As with all online systems and programs, make sure they are patched and regularly updated (especially anti-virus systems) to ensure they can detect and repel the latest online threats.

- Backup your important data: The reason ransomware is normally so successful is because individuals or businesses don't have back-ups of the data that has been encrypted by the malware. As a result, their only option to retrieve the data is to pay the ransom (and even doing this doesn't guarantee you actually will get your data back). If your data is appropriately backed-up (on drives that are not connected to your computer to prevent the ransomware scanning for back-ups too), then any ransom demands can be ignored and you can restore your data accordingly.

These steps will still not guarantee 100% protection against ransomware infections, but if your workforce takes these simple steps then it will significantly reduce your chances of becoming a victim in 2017.

The SME Challenge

Insure, You're Covered

Cyber-insurance is increasingly becoming a consideration for many organisations. In many cases it may be necessary to ensure a cyber-insurance policy is integrated into your cybersecurity incident response plan (CSIRP). However, as with many insurance policies, the fine print may reveal criteria that impact the development and efficacy of your plan. For example, some insurance policies have a prescribed list of vendors that organisations must use during the response. Others have requirements that mandate certain industry best practices are followed. Another potential pitfall of cyber-insurance plans are notification requirements. In some cases, insurance companies will not reimburse organisations for money they spend on a breach prior to notifying them of the incident. Even then, the definition of what qualifies as a covered security incident can vary from policy to policy.

Prevention Is Cheaper Than Cure

Experian has recently published a report which states many SME's are unclear about the risks and subsequent costs of a possible breach, suggesting many would not survive an attack. Some 30% of businesses reportedly have no plans to deal with security threats. However, according to government statistics, a data breach costs a small business around £310,000, but SMEs surveyed believed the cost to be £130,000 less, at only £179,990. Given these alarming statistics why are businesses failing to plan? The report offers a number of theories, amongst them is a simple lack of awareness of just how much they are at risk. According to the report, 51% didn't consider a response plan to be a priority, while 39% believed they weren't at risk. However, should a breach occur, it is likely that the time and resource pressures facing many small businesses will only escalate.

Another theory is financial. The report found that 20% of companies didn't have the budget to create a robust mitigation plan. But, the true cost of a breach, whether due to sophisticated cybercrime or basic human error, is far higher than the cost to design and implement a plan. A plan should focus on training employees around cyber awareness and the potential risks and scams they could face. They are effectively the 'first line of defence' for any organisation - over 70% of the time, successful data breaches have been the result of something an employee has inadvertently done. A detailed data breach response plan will reduce the amount of organisational chaos and the time wasted in dealing with an attack. At the same time, preventing significant damage to not only a company's finances, but operations and reputation damage.

STEPS TO CYBER-SECURITY MANAGEMENT

1. Assess the risk to your business;
2. Document your policies and procedures to clearly state how to manage risk;
3. Consider your datasets and what damage could be caused from a security breach;
4. Choose the security measures that are appropriate for your needs;
5. Begin putting the measures in place.

Visit Our Websites

Protection Group International:
www.pgitl.com

Protection Vessels International:
www.pviltd.com

Cyber Services:
www.pgicyber.com

Cyber Academy:
www.pgicyberacademy.com

Intelligence Services:
www.pgi-intelligence.com
www.riskportal.pgitl.com

JTip:
www.jtip.co.uk

Follow us on Social Media:

Customer Services
+44 (0) 845 600 4403
pgicyber@pgitl.com