SWETT ALERT

Cyber Storm Warning! Microsoft Discontinues Windows XP Support - Hackers Prepare

On **Tuesday, April 8th**, Microsoft will cease official support of Windows XP. IT Security experts expect a significant influx of cyber attacks targeting current Windows XP users. As Microsoft will no longer offer security patches to the operating system users, experts predict that the hackers will seek to exploit new vulnerabilities in Windows XP. In addition, other software providers may cease continued support for any of their products running on the Window XP platform creating further vulnerabilities to Windows XP users and new opportunities for cyber criminals.

Cyber criminals are expected to ramp up phishing and malware attacks, including the use of self-replicating malware such as the Conflicker worm, which began targeting Windows' users in the fall of 2008. It was designed to create a criminal botnet and was reported to have infected over 15 million machines at its peak. According to Microsoft sources, Ransomware is another malware threat to Windows XP. This type of malware extorts payment from users in return for the unencryption of files the hackers essentially hijacked and encrypted for their nefarious purposes. According to one industry source, cyber criminals are storing up security exploits in the Windows XP operating system to launch these attacks in April.

With over 3,000,000 forms of software viruses, trojans, worms or known malware in the cyber world today and new ones created daily, only a fraction can be detected by most anti-virus software systems. Most small businesses cannot afford many of the latest high tech approaches to protect their systems and may be the last to migrate off the Windows XP platform, creating an enormous opportunity for cyber criminals to exploit the weaknesses in Windows XP going forward. The best solution for all Windows' users is to migrate immediately to the Windows 7 or Windows 8 operating systems to receive continued technical and security support from Microsoft. However, many may not be prepared to do so financially or logistically in such a short time frame, or may discount the threat entirely.

The decision by Microsoft and other software providers to discontinue support escalates the need for Windows XP users to secure cyber liability coverage immediately. It is unknown how underwriters may react to new cyber submissions for existing Windows XP users; some may charge higher premiums or add additional exclusions. Specifically, they may look to secure an exclusion to coverage if an insured's software provider discontinues or withdraws technical and security support. Security notices and patches have certainly been enormously beneficial yet challenging to IT Managers, as they arrive on a nearly constant basis, and their importance can vary from critical to minimal. Yet, under some cyber policies, failing to implement any of these patches on a timely basis,

may void coverage if the failure to implement these security patches was later associated with a cyber claim.

For those companies who have attested to their PCI-DSS compliance within their Merchant Bank agreement, PCS-DSS Requirement 6.1 requires that all security patch releases must be implemented within 30 days of their notice. The withdrawal of technical support to their operating systems or other software programs may affect their PCI compliance, exposing them to potential PCI Fines and Penalties and other costs in the event of a credit card related data breach. We recommend that all companies who accept credit cards payments should contact their Merchant Bank to determine if the withdrawal of Windows XP support may jeopardize their PCI-DSS compliance.

The Microsoft decision will profoundly affect any healthcare entity and their Business Associates (law firms, TPA's, insurance companies, insurance agencies, claims handlers, data processors, data storage companies and other companies who process, store or transmit Patient Health Information) as failure to migrate to the new operating systems will likely be considered a willful neglect of the HIPAA Security and Privacy Rules under the HITECH ACT. In the event the company is subject to an audit or suffers a data breach, this willful neglect to follow these rules may lead to significant regulatory fines or penalties.

Securing the proper cyber coverage can provide the protection critical to clients. To learn more about Cyber Liability insurance, contact AHERN Insurance Brokerage today to speak with a specialist.

Call 1.800.282.9786 or email us at info@aherninsurance.com

AHERN | INSURANCE BROKERAGE

WWW.AHERNINSURANCE.COM

License #0C04825

Thank you to Mark Smith, Director - Swett & Crawford's Professional Services Group for his expert insight.
Mark has been an industry educator and resource for cutting edge issues such as cyber liability, leading Swett & Crawford's Cyber Liability specialty team. In this role, Mark has worked closely with carriers in drafting their cyber policies and has led dozens of cyber focused workshops for retail agents, their clients or industry groups on cyber issues.