Cyberinsurance – Is your company ready?

The single biggest challenge faced by insurance companies today is the lack of actuarial data on cyber-attacks which makes pricing these cyber insurance policies very difficult. As a result, insurance companies are increasingly resorting to other methods to assist them in more accurately pricing these policies which is good news for them but which will result in a number of challenges for businesses.

Assessments will become standard - Insurance companies will increasingly rely on "security readiness" assessments to determine the amount of potential risk a company carries. This will then be measured against a "best practices" list that will evolve and change as new tools and techniques are introduced into the market.

Incident response plans will become a requirement - Insurers will demand that companies develop and document incident response plans. These plans are designed to spell out the exact steps a company must follow in the aftermath of an attack or data breach.

Security "FICO scores" will emerge - Score providers will grade a company's security posture based on publicly available information combined with ongoing analysis of externally visible behavior. Companies will be forced to continually monitor their scores and will also need to alter their behavior to ensure that their rating does not get negatively impacted.

Monitoring tools will be required - These monitoring tools will provide insurers a way to reduce their risk through the real-time collection and analysis of data.

Information sharing will become the norm - Cyber insurers will be actively working together to share information so long-term profiles can be created. For companies, this ultimately means that information related to their cyber security readiness and exposure will no longer be kept out of view.

Disclosure mandates will be implemented - Cyber insurers will increasingly force companies to find ways of mitigating the impact of these breaches. Already, 47 states have enacted legislation requiring companies to notify individuals of security breaches of information involving personally identifiable information.

Businesses shelled out $2 billion in cyber insurance premiums in 2015 but current projections show that astronomical growth rates will result in a market of over $20 billion by 2025. Companies should proactively focus not just on protecting their most critical assets, but also on developing notification protocols that can be rapidly implemented once breaches have been identified.

For more information on this subject or to schedule a network assessment, please contact us today!