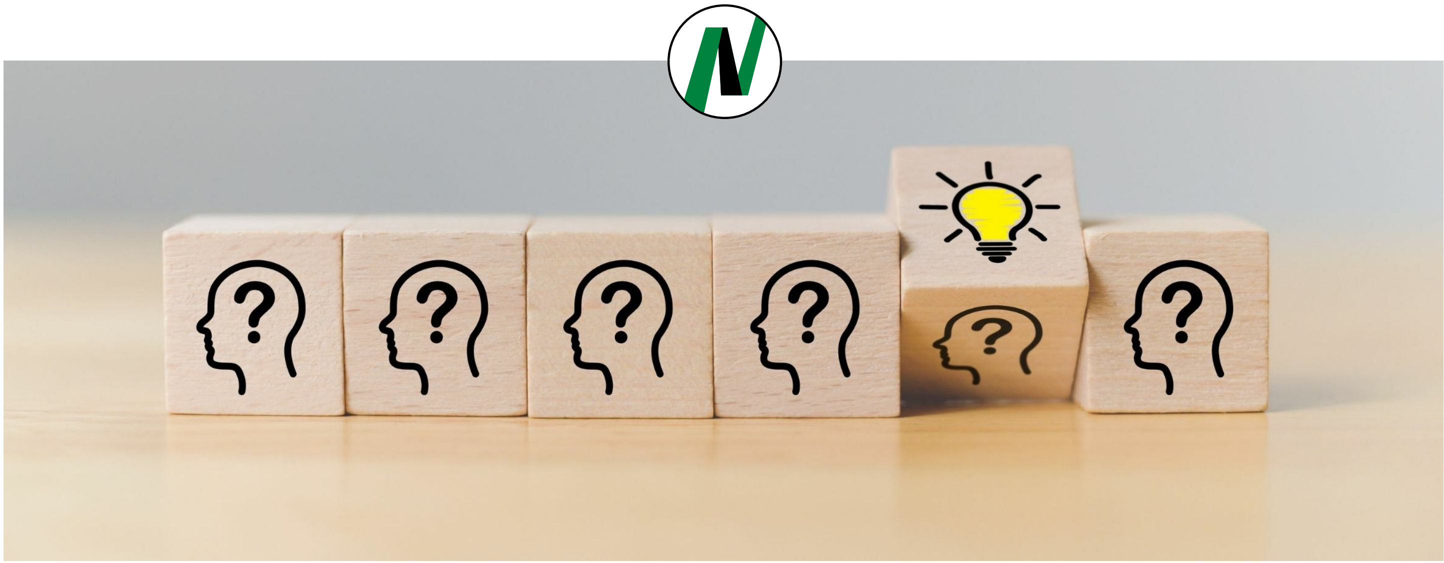

Beazley Report Details Increase in Ransomware Attacks

11.02.2016 | By James H. Vorhis

A report issued last week by Beazley, one of the prominent insurance companies in the cyber field, revealed what industry experts predicted earlier in the year – ransomware is an increasingly prevalent menace. That report is a reminder to everyone that there is no time like the present to review backup and incident response plans, and to take a close look at your insurance policies.

Beazley has been a prominent cyber insurance player since the inception of that specialized coverage. As an early presence in this area, Beazley started its data breach response unit in 2009. During that time, it has been tracking its incident response figures based on claims from its policyholders. And the early reports from 2016 reveal ransomware to be a growing threat. While the percentage of ransomware attacks as part of the broader data breach universe stayed proportional to the figures seen in 2015, there was a huge uptick in the total number of ransomware incidents. As Beazley noted, cyber thieves have apparently determined that it is easier to get payment in bitcoins via ransomware than selling information on the dark web.

But all is not lost in this grim report. There are easy lessons to take away that can help prevent or minimize the risk or damage from a potential ransomware attack.

- First, ensure you have robust backup practices. A thief stealing your company's data is a bad outcome. But Ransomware can cripple a company. Backup processes are no sure solution, but the absence of a solid backup plan will certainly result in catastrophic results because the ransomware will leave you at the mercy of the attackers.
- Second, prepare or update your incident response plan. Whatever that plan may be, you do not want an actual data breach attack to be the first time you have practiced your plan.
- Third, educate your employees. Over 80% of data attacks resulted from human error – when your employee opens the wrong attachment, it is utterly meaningless if you have the Fort Knox of cyber defenses.

- Finally, review your insurance portfolio. Ransomware is somewhat unique in its mode of attack, and the damage that it does to your system. Does it actually do damage your data? Your computers? Insurers will certainly argue to the contrary. An important takeaway is that you should understand where your potential cyber coverage might lie, and determine if you need additional coverage. Cyber insurance may or may not be cost effective for your company, but you need to understand your insurance portfolio to better evaluate your risk profile.