Risk Management Considerations

Q. Why should you purchase cyber coverage? A. Heartbleed

It's been around for the last 2 years without being widely known. We felt safe using a website with the little lock icon. Little did we know that the security protocol called open-source Secure Socket Layers (Open SSL) had an encryption flaw called the Heartbleed bug. We learned about the flaw last week when researchers at Codenomicon discovered it with Google Security engineer Neel Mehta and published the exploit. This exploit allows an outsider to steal usernames, passwords, emails and documents from a site without leaving a trace.

You try to do everything right, such as update your antivirus software; have secure configurations for your network devices – firewalls, routers and switches; use strong authentication and encryption. You have security policies and procedures and train your employees in your security protocols. You make your employees change their passwords every 28 days and instruct them to never share their passwords. And you feel comfortable. Then you learned about Heartbleed, the bug that revealed that much of the web has been insecure for the last 2 years.

The first step in the risk management process is to identify risk. Yet for the last 2 years an unidentified encryption flaw existed in the software used by most of our trusted websites. What else is out there? In light of Heartbleed the question becomes – can you realistically identify all of your risks? And if you can't identify all of the risks, how can you measure your financing exposure?

Maybe today's "new normal" in cyber risk management lies in the following steps.

1. Do everything you can to secure your systems and critical data within your existing resources.
2. Have an independent security firm work with your IT professionals to review your security protocols and to determine what vulnerabilities still exist and which should be fixed first.
3. Have Municipal Council or Your Executive Board adopt your policies & procedures.
4. Develop and have your Municipal Council or Executive Board adopt a risk appetite statement that is used to guide all measures you take (IT; Legal & Insurance).
5. Transfer your financing exposures to an insurer rather than gambling with your own capital.

Frank Cowan Company has developed a cyber risk policy. We have also entered into a partnership with Emerging Technologies Group for network security assessments and negotiated a special rate for Frank Cowan Company clients.

Start protecting yourself today against tomorrow's threats. We know there are more out there. We just don't know what they are; when they will surface and how much they will cost.

Call your Frank Cowan Company marketing representative for more information today.