Have you got the cyber blues?

Looking at the cyber security liability application, requirements that our clients – and our agencies –must meet to just get a quote is incredible. A few years ago, every carrier was writing cyber; today the insurance marketplace realities have hit. Markets are dwindling, losses are showing no sign of slowing and requirements to get a quote are increasing as fast as a new application comes in for coverage. Coverage limits and covered losses are becoming more and more restricted, while premiums have skyrocketed. I've stopped trying to "guess" what a new policy might cost, much less the daily question, "How much do I budget for our cyber renewal?"

Comparing policies so we can sell the best coverage we can find, there is very little consistency. Consider the fact that every carrier has a different definition for cyber/data breach/network security event. Definitions and exclusions matter. Policy forms must be read along with a careful review of the carrier proposal. Does the carrier proposal give the insured first-party protection such as loss of the actual digital assets, business income, extortion, crime, terrorism and security events costs? Did you even know that the insured must hire a computer forensics company after a loss to determine how their system was invaded? Any idea of that cost?

What about protection for others – those third parties who were hurt because the insured was attacked? What about the notifications required after a claim? How many years of credit reports is the insured required to provide to the injured parties? What about their monetary and reputation loss? And the list grows from there.

Social engineering – is that covered? We've seen several claims where hackers diverted emails and money from our insured's bank account to the hackers. Does the policy cover this social engineering? Some carriers will add an endorsement with a social engineering sub-limit.

On renewals, if the carrier will stay on the risk, the renewal quote comes in last minute and there are hoops to jump through to get it issued. Premiums are up since last year, and let's hope the insured didn't have a claim.

Let's talk statistics. The average cost of a cyber security incident in 2021 according to Willis Towers Watson was $9.05 million. The same article indicated that "according to IBM and Ponemon 2021 Cost of a Data Breach Report, the average breach cost was $1.07 million higher in breaches where remote work was a factor." Pocket change, right? Not for our agency and I'm sure it's not for yours either.

So, how do we protect our own agency and our clients? This list is what my agency has done internally and what we use to guide our clients:

- Reputable managed service provider (MSP) with 3rd party oversight
- Annual penetration tests and vulnerability assessment
- Data risk mapping
- Updated software and timely patches
- Firewalls and anti-virus protection
- Multi-factor authentication (MFA) and "zero trust tokens"
- Cyber security awareness and training
- Established IT policy and accountability

Many of these protections are required to obtain a quote and/or renew a policy. Carriers are refusing to write or renew over a lack of strong enough IT security. Agents are left with a mess of an upset client and no market.

What can you do as the agent? Keep your clients as informed as possible on the issues when renewing cyber coverage. Start working on these policies very early in the renewal process. You might find it helpful if you provide a list of resources for security services (our office offers our clients the same resources we are using). This is no different than the list we provide if they are looking for an annual fire extinguisher inspection provider. As agents, we guide our clients and prospects so that they can keep/get this valuable insurance coverage.

Coverage matters and in today's world strong IT security is 100% necessary to get that cyber security coverage!

Deena James, CIC
MAIA coverage advisory committee, Cowell James Forge Insurance Group, Kansas City

If you encounter any issues with policy forms, coverage gaps or problematic language, please report them to MAIA's Coverage Advisory Committee so they can work on getting them corrected through their discussions with ISO, NCCI and ACORD.