» CYBERWORLD

Financially Protected

Keeping pace with changes in cyberinsurance coverages

By Cheryl Winokur Munk

Many community banks no doubt realize the importance of a strong cyber-insurance policy, but the intricacies of what proper protection means can be, well, tricky.

Financial attorneys say there is no such thing as a standard policy and possible coverage runs the gamut. With new cyber-risks emerging every day, insurance carriers continue to refine their coverage, and community banks should keep pace.

"This is one of those areas where there are lots of traps for the unwary," says Kevin L. Petrasic, a partner in the New York law firm White & Case LLP.

Commercial insurance policies typically offer liability coverage for damages caused during and after a cyberattack or data breach. Cyber-insurance policies are purchased separately from property and casualty policies. Their terms and conditions vary by issuer, attorneys say.

Cyberinsurance coverage commonly falls into two categories: first-party coverage and third-party coverage (or liability insuring agreements).

First-party insurance coverage generally provides compensation expenses related to a breach response, business interruption and cyberextortion. Those cyberattack costs, for which banks should consider obtaining insurance coverage, include:

- Security breach mediation for costs associated with notification and forensics in response to a breach and credit monitoring;
- Crisis management for public relations response to mitigate reputational risk;
- E-business interruption for lost revenue and expenses; and
- Network extortion for damages paid to a third party or for expenses to prevent an extortion event from occurring.

Third-party insurance coverage typically protects again litigation and regulatory defense costs. For cyberinsurance policies, third-party coverage to consider includes:

- Regulatory coverage for costs associated with a regulatory investigation;
- Communications and media liability for claims arising from copyright infringement, libel, slander, etc., in electronic content; and
- Network liability for claims against a bank, including the legal costs and settlements that result from a breach in network security.

Cyberextortion, which happens when hackers send an email laced with ransomware, is one area where community banks need to check their insurance coverage, attorneys say. A few years ago, insurance carriers didn't routinely cover damages from these types of attacks. They also generally didn't cover cyberterrorism—the politically motivated use of computers and information technology to cause severe disruption or widespread fear in society.

"There was a lot of confusion in the past whether these acts were covered. Some policies are vague or silent. Some expressly cover it," says Paul Ferrillo, a cybersecurity lawyer with the New York law firm Weil, Gotshal & Manges LLP.

Community banks also should ensure that their insurance policy's "act of war" exclusion is clearly defined, lawyers advise. Defining this coverage well became a more pressing issue after Sony Pictures Entertainment was hacked in 2014 and North Korea was named the likely culprit—blurring the lines between cyber-risk and terrorism, Ferrillo says.

Careful attention also should be paid to coverage limits and sublimits. Banks may buy a policy with a $6 million aggregate limit, but the overall policy aggregate limits often are not available for every type of loss covered by the policy, says Erica Dominitz, a partner with the Atlanta law firm of Kilpatrick Townsend & Stockton LLP.

David Cox, a partner at the same firm who works closely with Dominitz, gives the example of a community bank client that purchased a primary cyberinsurance policy worth several million dollars. The bank also bought an excess policy to gain an additional few million dollars of coverage. However, before a legal review, the bank was not aware that coverage under the excess policy was narrower than the primary coverage, so the bank was not as protected as it had thought, Cox says.

Community banks often rely on only one insurance broker for their facilities and staff general liability policies, but banks should check to make sure they're obtaining the special cyberinsurance coverage they want and need, attorneys say. IB

Cheryl Winokur Munk is a freelance financial writer in New Jersey.

Bottom Line: Review the details of your community bank's cyberinsurance coverage.