Does Your Company Have A Network Breach Plan?

Edward Rhone, CPCU, AIC, Principal, Claims Manager // **Parker, Smith & Feek**

Your I.T. Department has ensured all of the latest updates and patches are in place for your firm's network. Excellent. Your company has even recently purchased "cyber liability" insurance, just in case. Now it's time to sit back and forget about those headlines of security breaches. The insurance coverage has added belt and suspenders to the network, right?

Unfortunately, understanding the firm's network exposure is only the first step. To complete the risk management process, firms should familiarize themselves with network security procedures and insurance, ensure stakeholders are aware of the coverage purchased, and incorporate the correct consultants into a breach response plan.

Historically, network security liability policies have varied widely on the coverage they provide to the policyholder. In recent years, these policies have become increasingly uniform, though may still have unique coverage aspects that need to be reviewed to ensure the best terms for your business.

Most network security liability policies provide first and third party coverage and include some form of self-insured retention (i.e., some contribution by the insured) before the policy will pay for costs incurred.

Possible common first party costs when a security failure or data breach occurs can include:

- Forensic investigation of the breach
- Legal advice to determine notification and regulatory obligations
- Notification costs of communicating the breach to the affected individuals
- Offering credit monitoring to clients/customers/employees as a result of a privacy breach
- Public relations expenses
- Loss of profits and extra expense during the time that your network is down (business interruption)
- Recreation of damaged data
- Regulatory fines
- Payment Card Industry fines
- Extortion demands

Common third-party costs can include:

- Legal defense
- Settlements, damages, and judgments related to the breach
- Liability to banks for re-issuing credit cards
- Cost of responding to regulatory inquiries
- Regulatory fines and penalties

According to Gregor Hodgson, Parker, Smith & Feek's cyber insurance practice leader, "consulting your broker and choosing the best coverage form for your business isn't the end of the risk management process. You want the insurance policy to fully respond and protect the assets of the firm should a breach occur. Specifically, most network security insurers include crisis management coverage, meaning the insurer has contracted with attorney firms and network security professionals who are experienced in hacking events. Often, they will require the insured to immediately notify a crisis hotline upon discovering a breach, and to utilize the insurer's chosen legal, security, and forensic experts. If the policyholder does not use the insurer's team of experts, then the costs incurred may not erode the self-insured retention of the policy and limit the available coverage of the policy. In other words, your company may have purchased a policy, but failed to take advantage of its full coverage."

your company may have purchased a policy, but failed to take advantage of its full coverage.

It is not difficult to imagine how miscommunication could occur following a breach. Often, passing blame is the first course of action taken by the involved parties. Upon discovering the breach, the I.T. Department may attempt to immediately cover their mistakes and not report the breach promptly to senior management. In one case, I.T.'s damage control efforts actually hid the tracks of the intruder, making the cause of the breach much more difficult to identify. I.T. may try to act alone or engage unapproved and uncredited forensic services, due to their desire to fix the situation quickly.

The legal team can also be blindsided. Legal may not have completed due diligence while preparing the breach plan, or may immediately seek outside counsel at exorbitant, non-negotiated rates that the insurer may not agree to pay. Customer service may rashly draft notifications to customers without consulting legal or input from public relations experts. The list of complications associated with pre-loss preparation is endless.

The best practice is to ensure all stakeholders are aware of the network security insurance policy's existence. Those stakeholders should include the I.T., legal, operations, senior management, and customer service departments. If your firm outsources I.T., those vendors should also be updated on the insurance product purchased, and included in creation of breach protocols.

Once the insurance company's experts are identified, they should be included in any breach response plan for your organization. Moreover, if your firm changes network security liability insurers, you will need to repeat this process with the new insurance company. Nevertheless, your organization receives a coordinated breach response with top-notch consultants and erodes any self-insured retention of the policy by using the insurance company's experts. Most importantly, your firm will be fully utilizing the insurance product your company has purchased.

The ever-changing data breach notification requirements in the various states and federal law, increases in the number and severity of cyber-attacks, and escalating federal lawsuit judgments mean companies, large and small, need to address transferring the risk to an insurance company. Partnering with a well-versed risk consultant/broker who understands both the pre and post-cyber breach actions necessary to defend your organization will provide better organizational resiliency if/when your organization is attacked.

Parker, Smith & Feek is a full service brokerage firm providing commercial insurance, risk management, surety, benefits, and personal insurance solutions. Edward Rhone has 30 years of claims advocacy experience and manages Parker, Smith & Feek's claims department. He can be reached at egrhone@psfinc.com.