PARKER | SMITH | FEEK

COMMERCIAL INSURANCE
EMPLOYEE BENEFITS
PERSONAL INSURANCE
RISK MANAGEMENT
SURETY

MARCH 2016

DOES YOUR FIRM HAVE A NETWORK BREACH PLAN?

Ed Rhone | Principal, Claims Manager

Your IT Department has assured the latest updates and patches are in place for your firm's network and your technology consultants are confident the system is set to prevent a hacking attack. But, just in case, your firm has recently purchased "cyber liability" insurance. It is time to sit back and forget about those headlines of security breaches that occur for other professional services firms. Belt and suspenders have now been added to the network with insurance, right? Unfortunately, understanding the firm's network exposure is only the beginning of the risk management process – you're still at step 1. To complete the risk management process, professional services 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.

Insurance coverage for a network breach is often referred to as Privacy Breach or Network Security and Privacy Liability Coverage. Historically, these policies have varied widely as to the coverage they provide to the policyholder. In recent years, network security liability policies have become more uniform, though each may still have unique coverage aspects that need to be reviewed to ensure the best terms for your firm.

Most network security liability policies provide first and third party coverage and include some form of self-insured retention, or 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 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 client/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

continued >

Common third-party costs 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

However, consultation with your broker and choosing the best coverage form for your business is not the end of the risk management process. You want the insurance policy to fully respond to protect the assets of the firm should a breach occur. Specifically, most network security insurers include crisis management coverage. The insurer has contracted with attorney firms and network security professionals who are experienced in hacking events and the best remedies following a breach. The insurers will often require the insured to immediately notify the crisis hotline upon discovery of a breach, and to utilize the insurer chosen legal team, 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 tap into its full coverage.

We have seen CFOs who purchase the network security policy, but fail to advise others in the organization of the policy's existence. Without knowledge of the network security policy, the IT and legal departments act to resolve the breach, without consideration of the reimbursement of costs available by the insurance product. The organization goes into a crisis response, but may not recognize an insurance policy is available to pay for the costs incurred, leaving the firm exposed to the high cost of that breach.

It is not difficult to imagine how miscommunication could occur following a breach. Often, the blame game is the first course of action by the involved parties. The IT department, on discovering the breach, may wish to immediately cover their mistakes, and not report the breach promptly to senior management. In one case, IT's forensic work actually hid the tracks of the intruder, making the determination of how the breach occurred much more difficult. IT may try to go at it alone or engage forensic services that have not been vetted for their technical expertise, or approved through proper channels within the organization, due to the desire to fix the situation quickly.

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

The best practice is to ensure all stakeholders in an organization become aware of the existence of the network security insurance policy. Those stakeholders should include the technology, legal, operations, senior management, and customer service departments. Note, experienced insurance companies have managed

continued >

thousands of breaches and they are an excellent resource to help you manage the crisis. If your firm outsources IT services, those vendors should also be updated regarding the insurance product purchased and included in creation of breach protocols.

In conjunction with the insurance broker, the insurance company's underwriter should be involved to determine the breach response team assembled within the insurance company's crisis response group, including legal, public relations, and forensic experts, for both network security as well as the potential loss of income of the insured organization. An underwriter may be willing to add your firm's favorite experts to the insurer's approved panel, but adding experts is usually reserved for the largest of insureds.

Once the insurance company's experts are determined, those experts should be included in any breach response plan for your organization. Moreover, should your firm change network security liability insurers, this process will need to be repeated with the new insurance company and their list of legal and panel experts. However, by using the insurance company's experts, your organization receives a coordinated breach response with top-notch consultants, as well as eroding any self-insured retention of the policy. Nevertheless and most importantly, your firm will be fully utilizing the insurance product your company has purchased.

The ever-changing requirements in data breach notification requirements within the various state authorities and the federal law, increase in the number and severity of cyber-attacks, and escalating federal lawsuit judgments make transferring the risk to an insurance company an important topic that needs to be addressed by professional services organizations, both large and small. 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 when your organization is attacked.