

Managing Your Cyber Liability Risks

Cyber and network security breaches have become an increasing liability for businesses. The vast majority of businesses keep sensitive personal information on their computer systems - names, addresses, social security numbers, driver's license numbers and other data that identifies customers or employees. If this sensitive data falls into the wrong hands via a network security breach, it can lead to fraud, identity theft, or similar "cyber" crimes.

With the number of identity theft scams predicted to rise throughout 2010 as a result of the recession*, strict practices should be followed to protect the personal information of employees, prospective employees and customers. Companies could be on the hook to pay damages and claims expenses resulting from network security breaches that result in proprietary information being tampered with.

Insurance can't prevent a security breach from occurring, but it can ease some of the financial burden if the unfortunate occurs. The primary components of Technology Related Coverage or "Cyber Liability" policies are:

- Privacy Liability: Coverage for liability arising out of one's right to privacy
- Network Security: Coverage for liability arising from security breaches
- Technology E&O: Coverage for liability arising from services provided to others
- Media/Content: Coverage for liability arising out of the use/dissemination of media

Simply stated, these third-party liability coverages seek to close many of the gaps created by traditional General Liability policies, which do not intend to fully cover technology and internet exposures. It is recommended that you consult your trusted advisor such as your attorney and insurance broker to determine if you have the appropriate protection for your business.



Tips on How to Manage Your Cyber Liability Risk

- The first step in protecting your company against these risks is to develop and implement an appropriate cyber security policy
- Have a formal process in place to update software, firewalls and anti-virus programs
- Safeguard mobile devices that hold sensitive personal data with encryption codes
- Safeguard personal information within the workplace, segregating pay information and personal details on a separate part of the network and restrict access to staff on a "privilege" basis
- Implement regular staff training on security procedures
- Make sure you have a crisis management plan in place that can be executed as soon as you detect a potential security breach
- Before you outsource any of your business functions – payroll, web hosting, data processing – investigate the company's security practices
- Have an insurance policy in place to cover this type of liability

Source: Identity Theft Resource Center (ITRC), Recession to Cause a Rise in Scams, Thievery and Hacking

Cost Containment Tool: Dependent Eligibility Audit

Reducing overall costs is a top priority in almost every organization and employee healthcare costs are a main focus. With no end in sight to rising healthcare costs and practically every option to curb healthcare spending exhausted, what can employers do? The answer may lie in something as simple as making sure the people you have covered under your health plan are actually eligible for coverage. A dependent eligibility audit may be an option.

Dependent eligibility audits are used to identify ineligible dependents that are enrolled in your benefit plans. Examples include children that have met maximum age or student status, divorced spouses, or children impacted by changes in custody arrangements. Estimates show that 3 to 12 percent of covered dependents are not actually eligible. This can translate into significant cost savings for employers.

When planning an audit, an employer should consider the following:

- Are all plan documents consistent in defining dependents?
- What will the scope of the audit be and who will perform it?
- What documents will satisfy proof of eligibility for various types of dependents?
- What will be the message communicated to employees?
- How will employees perceive an audit? Are there other employee relations issues going on?
- How will privacy issues be addressed?

One of the most essential aspects of a dependent eligibility audit is employee communication. Employees should be told in advance of the coming audit so they can gather the proper documentation. Also, they should be reminded frequently throughout the audit period to ensure the best possible participation rate. Use already established mediums for communicating the message, including your company intranet, e-mails, bulletin board postings, payroll stuffers, etc.

Typically there are two steps to a dependent eligibility audit.

Step One: Employers establish a period of amnesty where employees can voluntarily remove ineligible dependents. Employees are notified by letter, explaining eligibility rules. An employee can then review all covered dependents for status, and no penalty will apply to those dependents removed because they no

longer qualify. Employers generally give employees one month to respond. Ineligible dependents are terminated at the end of the following month.

Step Two: For all remaining dependents after the initial amnesty period, employers should require employees to provide documentation to verify dependent status/relationship. Documents must establish both a dependent relationship and that the relationship still exists. Examples may include:

- Marriage certificate
- Domestic partner affidavit
- Legal documents that establish custody, guardianship or foster care
- Birth certificate
- Tax status form
- Medical documentation of disability
- Adoption papers

If an employee is unable to establish a dependent relationship, employer may impose penalties or seek reimbursement for claims paid for ineligible dependents among other solutions.

Many companies find that hiring an independent audit firm may be desirable as the auditing process can be cumbersome and time-consuming. While an audit of this nature may seem extreme, so is unknowingly paying for healthcare services for people who are not eligible. A dependent eligibility audit provides compelling evidence and helps to preserve the integrity of your corporate benefits package.

For more information on dependent eligibility audits, contact your employee benefits advisor.



At Assurance, we have built our reputation on earning our client's trust and confidence through excellence in every interaction. Independent since our inception in 1961, Assurance is ranked by *Business Insurance* magazine as the 66th largest broker of U.S. business.

For further information, please contact an Assurance representative at 847.797.5700.