Courtesy of
E.B. Cohen

CYBERRISKS&LIABILITIES_

Are You Protected From Insider Attacks?

It is often said in the cyber security world that your employees are your biggest security risk. Workers with access to sensitive information, including contractors that have access to the company's network, may be aware of existing security weaknesses and can exploit them more easily than an outsider. In the case of the 2013 Target data breach that resulted in stolen credit and debit card numbers of more than 40 million people, hackers stole network credentials of one of Target's HVAC subcontractors in order to infiltrate the company. Similarly, three AT&T contractors accessed customers' personal records in April 2014 in order to remove their devices from AT&T's network so they could be resold.

While these two recent examples are of high-profile companies, many more insider attacks go unreported or happen to smaller businesses. Many are the result of negligent employees with no malicious intent. According to the Ponemon Institute, 27% of data breaches are the result of human error, which includes negligent employees or contracts. And according to IBM, human error was a contributing factor in 95% of all recorded cyber incidents.

Insider threats clearly pose a big threat to companies of all sizes, but they don't receive nearly the amount of headlines that external incidents do. A traditional cyber security policy will cover customer notification and litigation costs from the result of external incidents, but what if your business is attacked by an insider?

Why Do Insider Attacks Happen?
There are essentially two types of insider attacks—those with malicious intent and others that occur because of human error:

Malicious insider attacks: There must be a certain level of trust between a company and its employees, but sometimes employees abuse that trust. An employee may steal sensitive data for one of the following reasons:

- To get revenge on a boss or another employee
- To take the company's intellectual property to his or her next job
- To sell the company's proprietary information

Because the employee may already have access to the company's network or devices, an attack can be carried out much more easily from the inside.

Whatever the reason for the attack, companies should be on the lookout for characteristics of insiders who may become a threat, which include the following traits:

- Introversion
- Greed or financial need
- Reduced loyalty
- Inability to assume responsibility for their actions
- Consistent frustration or disappointment

Individuals that exhibit these characteristics may reach a point at which they carry out malicious activity against the organization. One of the best preventive measures is to train employees to recognize and report behavioral indicators exhibited by peers or business partners.

Human error: Whether from negligence or ignorance, human errors that lead to an attack account for a large percentage of insider attacks. As previously mentioned, system misconfiguration, poorly chosen usernames and passwords, and lost business-related devices are all examples of human errors. In addition, the following are ways in which human errors can lead to an inside attack:

- Being tricked into giving a hacker information that leads to an attack. This is called social engineering,

E.B. COHEN
INSURANCE AND RISK MANAGEMENT SINCE 1932

and it includes phishing or scamming.

- Sending sensitive documents to the wrong recipients
- Being undertrained on how to use company software
- Working long, stressful hours that can lead to increased errors or forgetfulness

Insider Attacks as a Cyber Insurance Coverage Gap
Because the cyber insurance market is relatively new and constantly changing, policies may differ widely in terms of whether or not a company is protected from an insider attack, potentially leaving a big coverage gap.

The best way to plug that gap is to know exactly what your policy covers. Some policies may exclude an attack perpetrated by any employee or may only offer coverage if it is carried out by an executive. Others may exclude coverage for an attack when the insider uses or accesses unauthorized devices or systems.

Some industries are also more susceptible to attacks than others are, and that may affect the policy language and certain exclusions. For example, the IBM study notes that companies in the finance, insurance and manufacturing industries carry the highest incident rates and are generally more susceptible to an attack than companies in the retail and public sector industries, so some policies may exclude insider attacks in certain industries.

We Can Help
At E.B. Cohen, we know cyber coverage can be difficult to understand. Let us walk you through getting coverage to make sure your business is protected from an attack.