Cyber Attacks

Detecting Breaches Early Reduces Claims: Report

MANY BUSINESSES devote their cyber security dollars to technologies designed to prevent attacks, such as firewalls, virtual private networks and anti-malware applications.

But, an October 2023 report indicates that they might do better to focus both on prevention and detection. Enhanced emphasis on detection could make cyber attacks less severe, resulting in smaller cyber insurance claims and possibly lower future premiums.

.The report from Allianz Commercial found that a tiny fraction of all cyber attacks — 2% — account for the overall amount of cyber insurance losses. Organizations quickly contain 90% or more of other attacks. The dollar loss from most of them is less than the policy deductible; many of these losses are never reported to the insurance carrier.

Cyber attacks are either detected and contained quickly with small dollar losses, or they become full-blown expensive crises. Few fall between these extremes. Detecting an attack in its early stages is the important factor in limiting the damage it causes.

Prevention is not foolproof. If hackers encrypt or steal a company's data, the costs of recovery and downtime skyrocket.

The report's authors found that attacks not caught in the early stages can be more than 1,000 times more expensive than those nipped in the bud. An attack that would cost $10,000 if caught early can end up costing $10 million or more otherwise.

Despite that, the report found that two-thirds of cyber security budgets are spent on prevention. Early detection systems are plentiful, effective and constantly improving, but they get a smaller share of organizations' spending. As a result, only one-third of organizations detect security incidents through their own information technology staff.

WHAT YOU CAN DO

To improve early detection, you may want to consider these steps:

- Regularly assess your business's cyber security risks. Identify potential threats, evaluate how serious they are, and prioritize them to determine which to address first. Perform assessments annually or as the organization's operations and technology change. For example, if your business offers new product lines, a new assessment should be done.
- Devote more resources – equipment, software and personnel – to incident detection.
- Implement policies and procedures for storing data, routinely encrypting sensitive stored information, and securely deleting it when no longer needed.
- Adopt a written incident response plan designed to enable early detection and mitigation of cyber incidents. It should describe the tasks each person involved in the response will perform.
- If your organization is too small to have a dedicated cyber security staff, work with a qualified IT security firm to respond to attacks.

The takeaway

Cyber insurance should be part of every organization's risk management program. Many insurers, in addition to paying recovery costs and business interruption losses, offer forensic specialists to determine how an attack occurred. Ask us about a cyber insurance policy appropriate for your operations.

Even the best defensive line will occasionally give up a big play. Early detection of cyber attacks will help your organization minimize the resulting damage. ❖