CONNER
STRONG &
BUCKELEW

Ransomware Readiness: Developing Your Risk Management Strategy

OCTOBER 2017

TERRENCE J. TRACY, CPA | MANAGING DIRECTOR AND EXECUTIVE VICE PRESIDENT | CONNER STRONG & BUCKELEW

For today's data-driven businesses, a ransomware attack can be the stuff of nightmares: a hacker breaches a company's computers, locks out the users and holds the firm's data hostage until a ransom is paid.

Once a company has been breached, there are a host of issues to manage: the threat of losing all of the data; the risk of the data being released publically; the potentially costly interruption of business. In many cases, while management is in a standoff with the hackers, workers and work itself comes to a standstill.

In recent years, because ransomware attacks have become easier for hackers to execute, the number of breaches has skyrocketed. Organizations looking to head off this threat must take stock of their vulnerabilities and develop a plan to defend their data, manage a potential crisis and ultimately finance the repercussions of a breach – if it comes to that.

Getting all departments aligned on a strategy is the first step. An effective ransomware risk management plan will address three critical elements:

The Human Element

Every stage of a ransomware attack is designed to play on the psychological vulnerabilities of its victims, starting at its inception. Most ransomware is distributed through phishing emails, which are intended to catch employees in moments of distraction or fatigue (for example, by disguising as a LinkedIn email), create a sense of fear (for example, by telling victims an unauthorized payment has been made from their account) or play on curiosity (for example, by attaching a file supposedly containing employee salary information).

Once the ransomware encrypts a company's files, it presents employees with a page outlining the hackers' demands. Hackers use a variety of manipulative tactics to create a sense of urgency and panic, such as counting down to a set deadline for payment, disguising the page as an FBI alert or threatening to release files to the public.

> "Hackers use a variety of manipulative tactics to create a sense of urgency and panic, such as counting down to a set deadline for payment, disguising the page as an FBI alert or threatening to release files to the public."

This kind of attack can elicit powerful emotional responses from the recipient, ranging from anxiety and anger to guilt and embarrassment. Therefore, an effective risk management plan must be created with the understanding that in the heat of an attack, judgment at the employee and management level may be clouded.

The plan should clearly define the company's policies on ransom and include an effective reporting structure, not only to the firm's management and board but also to the appropriate industry regulators and authorities. It also should provide guidance on creating and distributing statements for customers, partners and the media.

As part of this effort, companies should ensure employee trainings on phishing threats are reflective of the most up-to-date, manipulative tactics and use embedded drills to ensure ongoing understanding and compliance, and a clear, easy-to-follow plan for employees to follow if an attack does penetrate firewalls.

The Data Security Element

ISACA's 2017 State of Cyber Security Study paints a clear picture of the IT function at many organizations: under-resourced and overwhelmed by the complexity and volume of threats. The study found that while 80 percent of IT governance professionals believe they're likely to experience a cyber attack this year, just over half have a formal process in place to deal with a ransomware threat.

Developing a plan comes down to the first rule of risk management: no one can operate in a vacuum. It's only through the ongoing collaboration of IT and risk managers that organizations can properly prepare their systems, management and employees for an attack.

Together, IT leaders and the management team should outline a strategy for:

- **Data backup** – Conducting regular backups of mission-critical files to the cloud, remote servers or external hard drives, keeping in mind that some ransomware can also infect and encrypt backed-up copies.

- **System updates** – Continually updating company software to reflect the latest security patches. The WannaCry attack in early 2017 exploited a vulnerability in the Microsoft Server Message Block (SMB); though a patch was available, many companies failed to install it.

- **Disaster recovery testing** – Running ongoing simulations of business interruptions to identify vulnerabilities and resource gaps.

The Insurance Element

In addition to managing defense and response strategies, risk managers should ensure their insurance coverages reflect the current threat landscape. Too often, organizations overlook the significant financial, regulatory and reputational risks that can be transferred to an insurance policy.

Cyber insurance was created so that organizations who experience a breach could recover the cost of business interruptions and data restoration, and ransomware is commonly covered in these policies.

Risk managers may be aware that ransoms demanded in these attacks are relatively low. In the WannaCry attack, which infected over 200,000 computers around the world, hackers demanded just $300 – likely much less than most deductibles. However, when an attack results in significant lost profits from business interruption, legal liability and follow-up communications, tapping into coverage makes sense.

In recent years, some ransomware victims that did not have cyber coverage – or could not meet their deductables – turned to the kidnap and ransom (K&R) sections of their policies to recover damages. K&R coverage was not designed to cover ransomware; it was intended to protect physical threats to company executives and employees, especially those traveling to volatile areas of the world. Thus, the payouts from these claims are often significantly lower. With the recent uptick of ransomware attacks, it's also likely that insurers will limit K&R coverage for ransomware attacks.

While insurers continue to update their coverages to keep pace with cyber threats, a knowledgeable broker can help risk managers minimize their vulnerabilities and prepare their team for the worst