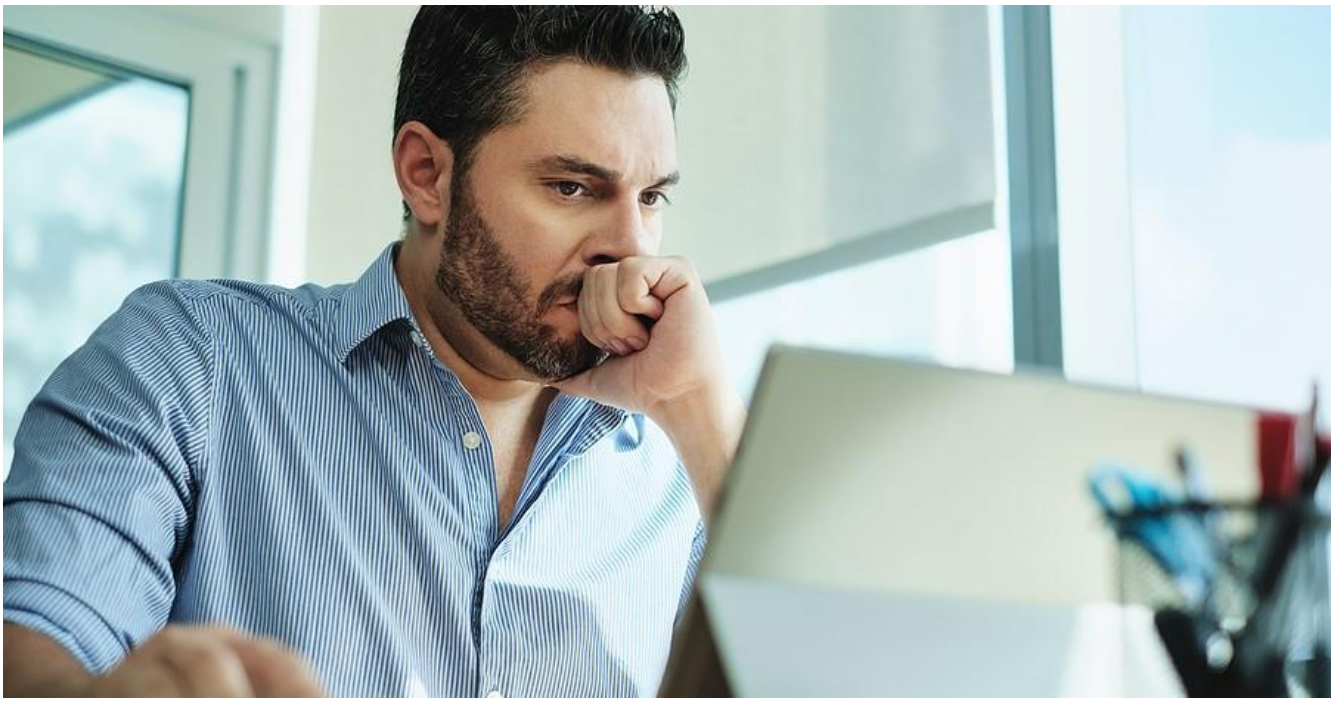
Ransomware Insurance Coverage Disappearing, Not Enough for Robust Cybersecurity



On May 9, European insurance giant AXA announced it will no longer provide support for ransom payments made to hackers. While AXA appears to be the first insurer to deny ransom payments, the move could signal an impending shift in ransomware insurance coverage.

The AXA announcement comes as ransomware attacks prove an increasingly lucrative business model. For instance, victims paid an estimated $350 million in ransom payments in 2020, over 300 percent more than in 2019. In recent high-profile cases, Colonial Pipeline paid attackers $4.4 million, and CNA Financial Corporation paid a whopping $40 million.

Meanwhile, cyber criminals continue to attack organizations across critical sectors. While the FBI and other security experts warn against paying ransoms, companies face devastating losses and even interruptions to critical care. Cybersecurity best practices, combined with following recommended steps when an attack does occur, may provide the best protection.

Ransomware Insurance Coverage Primer

Cyber insurance has become a hot topic as organizations scramble to protect themselves against losses resulting from cyber-attacks. In addition to ransom negotiations and payments, typical policies also cover legal costs, as well as costs for forensic analysis, data restoration and communications related to the breach.

However, even before the AXA announcement, many cyber insurance companies had begun to ask more from the companies they insure. For instance, some insurers require policy holders to complete certain basic security steps. Others have begun to charge a coinsurance or limit payment to a percentage of the loss incurred.

To Pay or Not to Pay

This evolution in cyber insurance reflects more than a move by insurers to manage their own risk. The FBI and other government agencies, as well as many cybersecurity experts, warn against paying ransoms. Researchers at cybersecurity provider Kaspersky explain that paying a ransom provides no guarantee that organizations will recover their data intact.

More importantly, paying the ransom encourages attackers to carry out more attacks. And some experts suggest that carrying cyber insurance actually makes organizations more attractive targets. Clearly, companies cannot depend on insurers to continue to shoulder the bulk of the cyber risk.

Best Practices to Protect Against Ransomware Attack

While cyber insurance still provides significant benefits, organizations must focus on cybersecurity best practices to defend against ransomware. Some of those best practices include:

- Regular backups – Conduct regular data backups, including system images. Keep multiple copies of the backups, including a copy not connected to the network. And make sure to test the backups.
- Keep systems and software up to date – Apply security updates to software, firmware and operating systems when they become available. This includes antivirus and other security solutions.

- Develop and review an incident response plan – Having a detailed plan in place before a security incident occurs greatly increases the chance of a successful outcome.
- Conduct regular cybersecurity training – While organizations can, and should, implement technology solutions, employees remain a key line of defense against cyber-attacks. Make sure users know how to recognize phishing attempts, share files safely and secure home offices.
- Address third party risks – Look into the security practices of the vendors with which you do business to ensure they do not put your company at further risk.
- Carefully regulate access controls – Give users only the access they need to the services and data necessary to perform their jobs. This proves even more important in a remote work environment.

Steps to Take if Ransomware Attack Occurs

Even the best cybersecurity measures cannot provide complete protection against ransomware. But an effective response can help to reduce the damage from a ransomware attack when it does occur.

At the first indication of a ransomware attack, isolate impacted systems to contain the incident. Then perform a root cause analysis and begin to eradicate the infection and rebuild systems, giving priority to critical areas. Ensure effective communication throughout the process. This will include both internal and external teams and law enforcement.

Ransomware in the Cloud Hot Topic at New York State Cyber Security Conference

Carl Mazzanti, President and Co-founder of eMazzanti Technologies, a specialist in cybersecurity, will address the New York State Cyber Security Conference on the topic of Ransomware in the Cloud. His virtual presentation runs from 12:30 – 1:30 pm, June 8, 2021. Interested parties may register here.

2015 | 2013 | 2012 Microsoft Partner of the Year
WatchGuard 5x WatchGuard Partner of the Year
Inc. 500 | 5000 2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010
hp Partner of the Year
ShoreTel Sky Partner of the Year

Ransomware attacks continue at alarming rates because it's profitable for cyber-criminals. Every business of every size is a target, even in the cloud, but small businesses are least prepared. In his presentation, Mazzanti will discuss the essential facts about ransomware, including:

- How ransomware attacks happen in the cloud
- How cyber-criminals continue to get away with it
- Costs to recover double for companies paying the ransom
- How to protect your business for a small investment

Safeguard Your Organization with Cybersecurity Partnership

Ransomware attacks will continue, and organizations cannot depend on cyber insurance to provide adequate protection. Instead, the best protection also includes implementing cybersecurity best practices and building a solid incident response plan. The data security experts at eMazzanti help business leaders prepare for inevitable ransomware attacks.

2015 | 2013 | 2012 Microsoft Partner of the Year
WatchGuard 5x WatchGuard Partner of the Year
Inc. 5000 | 5000 2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010
Partner of the Year
ShoreTel Sky Partner of the Year