COSMOS
Navigate the Compliance Universe

CEP Magazine - August 2020
Is your cyber insurance enough?

By Erich Kron

Erich Kron (erichk@knowbe4.com) is a security awareness advocate at KnowBe4 in Tampa, Florida, USA.

Let's talk for a moment about the exciting world of cyber insurance. Well, I suppose it's not really that exciting until things go wrong, but it does need some discussion given the recent events around the ransomware industry.

Cyber insurance has never been more important in an organization's survival strategy than it is now, but things have potentially changed for the worse in the last few months. Purchasing cyber insurance was finally becoming less difficult as precedents were set and costs were becoming more predictable with respect to ransomware and data disclosure cases. Due to this refinement, it has been far easier to figure out how much coverage was needed to recover from an event, whether it was ransomware or a data breach.

That has all changed with the new trend in ransomware infections: data exfiltration.

The new ransomware landscape

In the past, the ransomware would simply kick down the door and take your data hostage, requiring a payment to gain access again. Initially this caught a lot of organizations off guard. They were not prepared to operate without digital systems, customer lists, past records, or data needed for production of manufactured parts. This triggered a new wave of concentration on data restoration. Organizations that had never felt like they were at risk of a catastrophic failure resulting in data loss suddenly had their eyes opened by the stories about other organizations. Backups were no longer the thing that just happened quietly in the background; they now quickly became a topic in board meetings.

With the increased attention on the ability to restore data quickly and even to operate in the absence of digital systems, the need to pay the attackers when ransomware did raise its ugly head dropped dramatically. This cut into the attackers' wallets, and they have decided to fight back.

Late in 2019, we saw the first real case of ransomware coupled with data exfiltration. Although attackers had been telling victims that they had exfiltrated data and were going to make them public if they decided not to pay, their bluff was called over and over again without consequence. The Maze ransomware strain changed this when hackers released two gigabytes of data (of a claimed 32 gigabytes) said to be exfiltrated during an earlier ransomware attack.[1] This hit the news, and with it, our idea of what to expect during a ransomware attack was fundamentally changed. No longer does the ability to restore data protect us from these cybercriminals; we have to worry about unauthorized data disclosures as well.

To add even more uncertainty to the mix, the COVID-19 pandemic has caused organizations to rapidly move employees to working from home and often have to take shortcuts during the transition due to time and equipment availability constraints. This means many people are connecting to corporate networks through VPNs from their personal computers, and other security measures provided by the corporate network are not operating as initially planned. This is affecting organizations directly as well as entire supply chains, which is why in a

recent Gartner survey, over half of the respondents said that data breaches are the most-increased third-party risk their organizations face.[2] This is setting up organizations to be even more exposed to a potential ransomware infection and the associated recovery.