PrismHR Cybersecurity Event Report

Overview

On Sunday February 28, 2021, PrismHR, the largest provider of payroll processing services to the PEO industry, learned that critical systems were encrypted by a team of hackers who has commonly used this type of exploit to extort money from organizations. Over the next 48 hours PrismHR worked to make a decision on paying the ransom, while also working on how to recover the use of their systems. The resulting outage impacted hundreds of PEO's who stepped up with their best efforts to deliver payroll services to their customers in any way they could. Within a week, all PrismHR services were returned to normal. Unfortunately, many PrismHR customers, and their worksite employees, were impacted by the outage.

Future Point of View (FPOV) and the PEO Coalition

FPOV – www.fpov.com – is a digital strategy firm that has worked in the PEO industry for many years. Our services include cybersecurity risk analysis, digital event management, and vendor negotiations when clients end up in disputes with vendors. This put FPOV in a unique position to help the PEO's hold PrismHR accountable for the results of the February cybersecurity event, and more importantly, the security improvements that need to be done to assure there is not a second event in the future. On March 5th FPOV was hired by a Coalition of PEO's – including your PEO – to provide 3rd party verification of the causes and impacts of the cybersecurity based outage.

Forensics on the Digital Event

- **Security Firms Involved** – PrismHR hired three different security firms to advise them on different aspects of the event. One to help with the extortion itself, one to give general security advice and do the forensics, and another to help with security infrastructure improvements. The vendors engaged are high end and appropriate for the size of organization and risk level of the data handled.
- **Data Access** – One of the most important questions that needs to be answered in a digital security event is the possibility that data was stolen. The firm that did the forensics over a thirty-day period post-event has delivered an opinion that **no data** was stolen. FPOV has reviewed all the information available, and we agree that the likelihood that customer or worksite employee data was stolen is

miniscule. PrismHR has agreed to do dark web monitoring for a year just to be sure that no data was stolen.

The Improvement Model

- **Immediate improvements** – PrismHR moved quickly to make infrastructure improvements and did a good job hiring multiple security firms to advise them. FPOV feels positive about the investments they made in the first thirty days to assure a second event would not happen.
    - *Infrastructure* – PrismHR moved immediately to find ways to provide payroll data to their PEO customers during the event. They quickly identified new methods for creating multiple stores of data in order to provide better defenses in the future.
    - *Security systems* – PrismHR implemented new security software systems within two weeks of the events. They are now using one of the top security tools providers in the market and are investigating additional vendors to harden their defenses.
- **Current Improvements** –
    - *New endpoint policies* – PrismHR is dramatically improving endpoint security in order to assure that digital criminals do not have easy ingress into their systems. They are moving to a Zero Trust model that when implemented will improve their ability to stop hackers from using many of the more common techniques to breach their system.
    - *Further abstracting of platforms* – They are moving to a model where backup systems and data are abstracted from the core system. This provides a more resilient model where the core system could be breached but there would be back up systems that are not connected that could be used by the PEO's until the primary system is healed.
- **Future improvements** –
    - *Improved digital event response playbooks* – PrismHR will be creating much more professional digital event response playbooks. Hopefully they will never be needed, but if there is another event, their ability to neutralize and recover will be much improved.

- *Cybersecurity council* – The company is creating a PEO customer security advisory council that will help hold the company accountable to maintain higher levels of security from now on.
- *Additional security systems* – PrismHR is now committed to spending whatever is needed to continue to improve their systems to assure they are very difficult to successfully attack.

Future Security Risk

There is simply no ability to be 100% secure. The first goal is to be hard enough to attack successfully that the benefits are not worth the level of work to penetrate the organization. The second goal is to be resilient enough that if there is a successful attack, the company can still provide services to their PEO customers. While we believe there is always cyber risk for an organization, PrismHR will now manage the risks in a much better way. This means their downstream customers are much safer from business interruption than they were in February.