35 Parkwood Drive, Suite 200
Hopkinton, MA 01748

April 21, 2021

On February 28, 2021, PrismHR experienced a security incident that affected the availability of our HR, payroll, and benefits software. In accordance with our information security policies and procedures, we immediately disabled access to certain systems within the PrismHR network to help protect customer data and employed a cybersecurity firm to conduct a forensic investigation.

PrismHR teams worked around the clock to securely bring our systems back online. While customer systems were restored throughout the week, full functionality for all customers was restored by Sunday, March 7.

Over the past six weeks, we have been working closely with our cybersecurity firm on a comprehensive forensic investigation.

The investigation has concluded and determined there was no evidence of unauthorized access, misuse, or theft of data contained on the PrismHR servers.

The cybersecurity firm reached this conclusion after a comprehensive examination based on practices they've honed from investigating thousands of cyber incidents.

PrismHR is committed to continuous improvements and implementing learnings that increase our security posture beyond our existing high standard. That includes adding enhanced security tools and procedures.

Managed Endpoint Detection and Response (EDR)

EDR solutions detect and investigate suspicious activity across all endpoints (i.e., devices that connect to a network such as laptops, desktops, or servers).

Based on counsel from cybersecurity experts, we upgraded the endpoint monitoring solution that we previously had in place.

The EDR solution we now use leverages artificial intelligence (AI) to look for irregular behavior in the PrismHR system and quickly locks down any suspicious activity. System administrators can also control user access and add authentication steps as part of a zero trust approach to identity verification.

Our EDR also includes 24/7 managed response by a team of cyber defense experts. That means a specialist with years of experience detecting and remediating cyber threats is continuously monitoring the PrismHR system and responding instantly to suspicious activity.

This combination of sophisticated software with human oversight is designed to address a constantly evolving landscape of cyber threats.

Zero Trust Strategy

PrismHR will move further toward a zero trust approach—a leading cybersecurity methodology—to reduce risk and ensure users across the system have the appropriate level of access. Strengthening the perimeter of the network is critical to preventing unauthorized users from getting in, but with zero trust, security doesn't end at the entrance.

Zero trust incorporates what users (including authorized ones) are doing inside the system and authenticates users as they move through the system based on access level and behavior patterns. This approach leverages advanced technologies such as multi-factor authentication, identity and access management, and endpoint security to verify the user's identity and maintain system security.

Under a zero trust approach:

- Users have only the level of access they need to do their jobs
- Requests for additional privileges will trigger a process to authenticate the user's identity and/or validate the need for access
- Access to certain areas of the system may only be turned on temporarily for a user
- Validating a user's identity may use a combination of login credentials, multi-factor authentication, IP verification, and behavior

Zero trust will be woven into everything we do to make the system—and its users—more secure.

Improved Cyber Disaster Recovery

We are bolstering our disaster recovery with processes and technology that allow us to restore system access more quickly from a cyber incident.

First, we are adding failover environments that are disconnected from production which will shield them from being impacted. Second, we are limiting how often failover environments connect to the internet (e.g., periodically for backups) instead of keeping them constantly online. This provides an additional layer of protection which will allow us to recover far more quickly from an incident.

The actions outlined above are part of a continuous effort to safeguard our system and your data from cyber threats. We appreciate your continued patience and support.

Thank you,

Gary Noke
President and CEO
PrismHR