PRISMHR

Cybersecurity

Communication Strategies & Talking Points

Communications during difficult times can have long-lasting effects on a company's reputation, both internally and externally. PrismHR wants to help when you need to communicate unexpected incidents to your clients.

During the recent cyber incident, PrismHR engaged communications experts and they provided some great advice. We're also including the talking points developed for PrismHR and are happy for you to use these messages when communicating to your customers.

Communicating in Difficult Situations

1. Difficult situations are not the time to be defensive. Proactively provide customers with accurate and timely information to keep them from guessing, which leads to misinformation.

2. Never lie, hide or spin the truth, or omit details, no matter how unflattering they may be.

3. Acknowledge the emotions of the situations.

4. Never guess or speculate. It's OK to say, "We don't know yet, but we'll share as soon as we do."

5. There will be tough questions. Prepare accordingly.

PrismHR Cybersecurity Talking Points

1. **Cybersecurity issues are a reality for virtually all businesses, and that is why PrismHR takes them so seriously.**

   a. PrismHR employs multiple features to prevent unauthorized access to its system and protect client data, including multi-factor authentication, strict password rules, IP address control and role-based security.

   b. PrismHR's platform is actively monitored 24/7/365 to protect against data breaches and cyberattacks.

   c. Access to the platform requires a secure connection, and all data is encrypted before being sent to or stored in the cloud to prevent it from being captured while in transit or at rest.

2. **PrismHR has maintained SOC 2 compliance since 2018, and they continue to take steps to strengthen security protections and business continuity processes.**

a. SOC 2 compliance means PrismHR has demonstrated to an independent auditor that the PrismHR platform is designed to keep its customers' data secure.

b. PrismHR maintains and regularly tests business continuity, incident response and disaster recovery plans.

c. These processes are designed to detect, resolve, and guide recovery from a security breach and to identify opportunities for improvement.

3. **To safeguard the data of HR service providers and the businesses they support, PrismHR commits to continuously enhancing security practices and protocols.**

a. PrismHR is hosted in a private cloud at a leading enterprise cloud provider, which is subject to regular third-party audits.

b. PrismHR's cloud provider adheres to the latest security, control and performance standards including ISO 27002 and 27001, PCI-DSS, SSAE16, SOC 1, 2 and 3 compliance and Privacy Shield, Content Protection and Security Standard requirements.

c. PrismHR is constantly implementing learnings that increase security beyond its existing high standards, including adding new state-of-the-art security tools and procedures.