INDUSTRY INSIGHTS: HEALTHCARE

STATE OF PRIVACY AND SECURITY AWARENESS

Almost double the amount of healthcare employees showed less knowledge of security and privacy best practices, compared to the respondents in our general population.

Here are five key findings from our survey that every security leader at a healthcare organization should be aware of:

1. **RISK**
   - 22% of healthcare employees knew the importance of sound security principles. Such a state comes from multi-faceted and integrated awareness programs, not just training. This is the path to a preparedness culture within healthcare organizations.

2. **IDENTIFYING MALWARE WARNING SIGNS**
   - 23% of respondents failed to recognize common signs of malware, compared to the respondents in our general population.

3. **IDENTIFYING PHISHING ATTEMPTS**
   - 30% of employees said they'd take potentially risky actions when presented with scenarios involving storing company data or files on personal cloud-based storage or sending work documents via personal email.

4. **ACCEPTABLE USE OF SOCIAL MEDIA**
   - In the "Risk" category, nearly three times more employees at healthcare organizations took unnecessary risks compared to their non-physician counterparts.

5. **INCIDENT REPORTING**
   - Almost a quarter of employees (24%) chose risky options when asked about mobile computing or working remotely.

Security Awareness report.

The 2017 DBIR also found that human mistakes accounted for 80% of the malware incidents impacting the healthcare industry involved ransomware.

Verizon Enterprises Data Breach Investigations Report (DBIR) found that 72% of breaches in the healthcare industry involved ransomware.

Doctors were among the most at-risk employees. Three times worse at identifying phishing emails, nearly double the amount of physicians showed a lack of preparedness (scoring 0% - 74.2%) compared to 8% of their non-physician counterparts, such as insurance providers or pharmacy personnel.

Hospitals and other healthcare organizations have proven nearly irresistible to cybercriminals in recent years. Think of a clinic or hospital through the eyes of a cybercriminal. All that patient data - medical history, Social Security numbers, Social Security numbers, Social Security numbers - just sitting there, waiting to be swiped and resold on the dark web.

MediaPro offers an awareness report that is designed to be deployed among an employee population. We used the survey that underpinned our 2017 State of Privacy and Security report.

The key takeaway is that healthcare organizations of all sizes need a comprehensive approach to awareness education that includes HIPAA courses often do not include information on how to stay cyber-secure in an increasingly interconnected world. Keeping within HIPAA regulations, while vital, is not enough. Understanding the risks and implementing a plan to address them is critical.

CONCLUSION

Healthcare organizations need to prioritize security awareness programs that go beyond mere compliance. Being prepared for a security breach or incident is more important than ever, and it's not just a matter of protecting patient information. It's about protecting the reputation, financial and consumer trust of the organization.