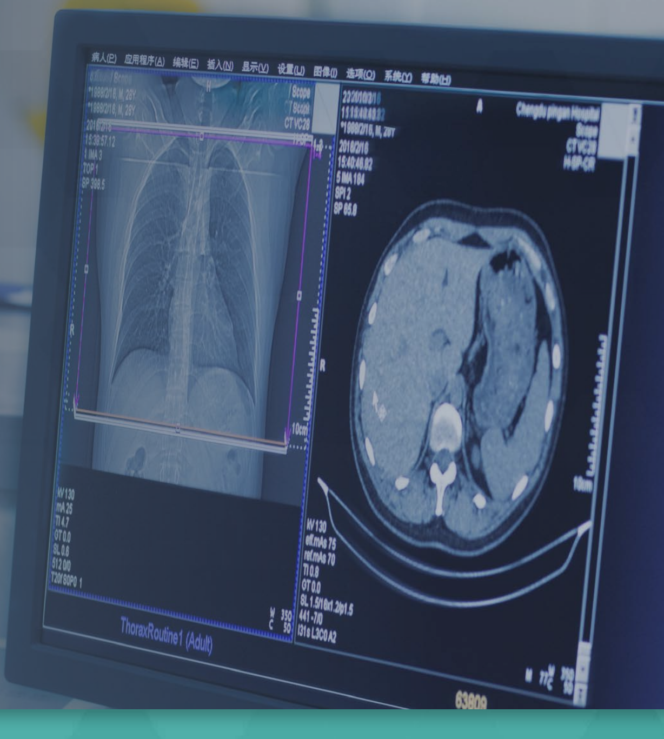
# STATE OF PRIVACY AND SECURITY AWARENESS
## INDUSTRY INSIGHTS: HEALTHCARE



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 personal information just sitting there, waiting to be swiped and resold on the black market. Not to mention the money that could be squeezed out of a healthcare facility by holding its network hostage with ransomware. The 2017 Verizon Enterprises Data Breach Investigations Report (DBIR) found that 72% of malware incidents impacting the healthcare industry involved ransomware.

The 2017 DBIR also found that human mistakes accounted for 80% of the breaches in the healthcare industry. We think a deeper understanding of the average healthcare employee's knowledge of cybersecurity and data privacy best practices is warranted, given that it's real, live humans making sure patient protected health information (PHI) and other sensitive data is kept secure.

## HEALTHCARE INDUSTRY KEY FINDINGS

We used the survey that underpinned our 2017 State of Privacy and Security Awareness report to gauge the privacy and security awareness of healthcare sector employees. We surveyed **1,009 healthcare employees** in the U.S. and compared these results against the broader sample of employed adults in our larger report.

**VIEW THE 2017 REPORT**

Overall, **78% OF HEALTHCARE EMPLOYEES** showed at least some lack of preparedness (scoring "Risks" or "Novices") to handle the common privacy and security threat scenarios that were presented, compared to the 70% of employees sampled across all industries, per our 2017 report.

## KEY TAKEAWAYS

Here are five key findings from our survey that every security leader at a hospital, clinic, or other healthcare institution needs to know:

### HEALTHCARE WORKERS SHOWED LESS KNOWLEDGE

about security and privacy best practices than the general population represented in our larger 2017 State of Privacy and Security Awareness report.

### 24% OF PHYSICIANS

and other types of direct healthcare providers showed a lack of awareness toward phishing emails, compared to 8% of their non-provider counterparts, such as office workers.

### HALF OF PHYSICIANS SCORED IN THE "RISK" CATEGORY,

meaning their actions could put their organizations at serious threat of a privacy or security incident.

### ALMOST DOUBLE THE AMOUNT OF HEALTHCARE EMPLOYEES

(24%) had trouble identifying a handful of common signs of malware, compared to the respondents in our general population survey (12%).

### 22% OF HEALTHCARE EMPLOYEES OVERALL

scored into the "Hero" category, meaning they showed a strong understanding of security and privacy best practices.

## HEALTHCARE RISK PROFILES

37%

**RISK**

| | SURVEY SCORE RANGE | PERCENT RANGE |
|---|---|---|
| **RISK** | 0 - 23 | 0% - 74.2% |

These individuals put their organizations at serious risk for a privacy or security incident. Such incidents can mean big trouble for an organization, including loss of consumer trust, financial and reputation damages, and more.

41%

**NOVICE**

| | SURVEY SCORE RANGE | PERCENT RANGE |
|---|---|---|
| **NOVICE** | 24 - 28 | 77.4% - 90.3% |

Novices have a good understanding of the basics, but could stand to learn more. They should remember that even one wrong decision or mistake can lead to a security and/or privacy incident.

22%

**HERO**

| | SURVEY SCORE RANGE | PERCENT RANGE |
|---|---|---|
| **HERO** | 29 - 31 | 93.5% - 100% |

These individuals know their stuff, including how to identify and properly dispose of personal information, recognize phishing attempts and malware, and keep information safe while working remotely.

## HEALTHCARE INDUSTRY THREAT VECTORS

The numbers below represent the percentage of respondents who chose incorrect or risky behaviors when answering questions in each of the eight threat vectors, compared to the general population surveyed in our 2017 State of Privacy and Security Awareness Report:

### INCIDENT REPORTING

| HEALTHCARE SECTOR | GENERAL POPULATION |
|---|---|
| 23% | 19% |

Overall, 23% of respondents failed to report a variety of potential security or privacy incidents, including unsecured personnel files and potentially malware-infected computers.

### IDENTIFYING PERSONAL INFORMATION

| HEALTHCARE SECTOR | GENERAL POPULATION |
|---|---|
| 21% | 19% |

21% of respondents failed to recognize some forms of personally identifiable information, or PII. Doctors and other care providers showed riskier behaviors in this category than did their non-physician coworkers.

### PHYSICAL SECURITY

| HEALTHCARE SECTOR | GENERAL POPULATION |
|---|---|
| 30% | 24% |

Overall, 30% of respondents took unnecessary risks in scenarios related to allowing others access to their office buildings. Specifically, a quarter of respondents said they would simply hold their office door open for a maintenance worker asking for access rather than telling him to wait while his identity was confirmed.

### IDENTIFYING PHISHING ATTEMPTS

| HEALTHCARE SECTOR | GENERAL POPULATION |
|---|---|
| 18% | 8% |

Overall, 18% of employees identified phishing emails as legitimate ones. The most mis-identified email of the four examples presented was an email from a suspicious "from" address containing an image attachment. **Doctors were three times worse at identifying phishing emails** than their non-physician counterparts.

### IDENTIFYING MALWARE WARNING SIGNS

| HEALTHCARE SECTOR | GENERAL POPULATION |
|---|---|
| 23% | 12% |

23% of respondents failed to recognize common signs of a malware-infected computer. For example, 19% of employees failed to recognize that their internet browser repeatedly sending them to the same site, no matter which URL was entered, is likely a sign of malware.

### WORKING REMOTELY

| HEALTHCARE SECTOR | GENERAL POPULATION |
|---|---|
| 24% | 19% |

Almost a quarter of employees (24%) chose risky options when asked about mobile computing or working remotely. Specifically, 26% of respondents chose to log on to an unprotected, public Wi-Fi network to complete work tasks, despite the danger it presents.

### CLOUD COMPUTING

| HEALTHCARE SECTOR | GENERAL POPULATION |
|---|---|
| 18% | 11% |

Overall, 18% of respondents chose risky actions when presented with scenarios involving storing company data or files on personal cloud-based storage or sending work documents via personal email.

### ACCEPTABLE USE OF SOCIAL MEDIA

| HEALTHCARE SECTOR | GENERAL POPULATION |
|---|---|
| 30% | 20% |

30% of employees said they'd take potentially risky actions related to their company on social media, such as re-posting a coworker's inappropriate social post about a competitor.

## CONCLUSION

Healthcare sector employees are a vital safeguard against data breaches, fines, and reputational damage. Beyond training geared toward HIPAA compliance, healthcare employees need a comprehensive approach to awareness education that includes security and privacy awareness.

The results of our survey show that more work needs to be done in this regard. HIPAA courses often do not include information on how to stay cyber-secure in an increasingly interconnected world. Keeping within HIPAA regulations, while vital, does not educate users on how to spot a phishing attack, for example. Additionally, mere compliance does not equate to a fully security-aware culture. In our experience, organizations of all types are best served when their whole employee population knows 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 risk-aware culture within healthcare organizations of all sizes.

An important part of a comprehensive program is the ability to assess risk among the employee population and plan an awareness initiative accordingly. MediaPro offers a risk assessment tool based on the survey we used in our State of Privacy and Security Awareness report that is designed to be deployed among an employee population.

**LEARN MORE ABOUT OUR RISK ASSESSMENT**

**MEDIAPRO**
Adaptive. Integrated. Proven.