# 2016 STATE OF PRIVACY AND SECURITY AWARENESS REPORT

MEDIAPRO

Adaptive. Integrated. Proven.

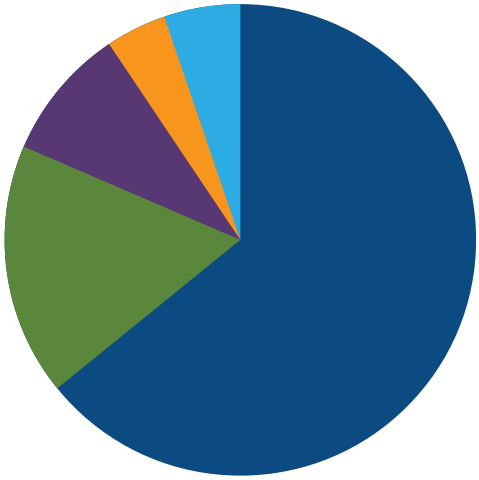
# State of Privacy and Security Awareness

MediaPro surveyed more than 1,000 employees and members of the general public over a one-month period in late 2016 to gather a baseline of security and privacy awareness across a slice of the general population.

We tested survey-takers' knowledge across eight different risk areas. We then assigned them one of three different risk profiles, which indicate the survey-taker's privacy and security awareness IQ. The three risk profiles—Risk, Novice, and Hero—are based on the number of proper behaviors correctly identified. The more correct behaviors an employee can identify, the less of a privacy and security risk they represent.

## Who Were the Survey Participants?

About how many employees work at your organization?



| | |
|---|---|
| 0 - 1,000 | 64.3% |
| 1,001 - 5,000 | 17.1% |
| 5,001 - 20,000 | 9.2% |
| 20,001 - 50,000 | 4.1% |
| Above 50,000 | 5.3% |

What industry does your organization belong to?

| VALUE | PERCENT |
|---|---|
| Other | 18.8% |
| Technology | 18.3% |
| Retail | 14.2% |
| Professional Services | 13.9 % |
| Healthcare | 12.3% |
| Finance | 9.6% |
| Education | 8.9% |
| Government | 3.9% |

## Findings in 8 Key Risk Areas:

The numbers below represent the percentage of survey respondents who showed risky behaviors in each of the eight risk areas that were surveyed.

| VALUE | PERCENT | |
|---|---|---|
| Incident Reporting | 26% |  |
| Working Remotely | 20% |  |
| Access Controls | 19% |  |
| Identifying Personal Information | 19% |  |
| Identifying Malware Warning Signs | 18% |  |
| Cloud Computing | 15% |  |
| Social Media | 14% |  |
| Identifying Phishing Attempts | 13% |  |

The danger of sensitive client or customer data compromised by a data breach threatens organizations of all sizes and industries. Year after year, massive breaches affecting millions of people continue to make headlines. Reports of lost revenue, lost customers, and lost reputation often follow.

And more often than not, the culprit remains the same: the risky behavior of employees. Often-cited cybersecurity reports like Verizon Enterprises' annual Data Breach Investigation Report continue to bear this out.

The 2016 edition, for example, found that 30% of phishing emails were opened in 2015; up from 24% the year before. And falling for scam emails is just a sampling of the dangers posed by employees lacking security or privacy awareness.

When risky behavior goes unchecked, employees continue to—intentionally or unintentionally—jeopardize your organization and the information that it promises to protect.

# INCIDENT REPORTING

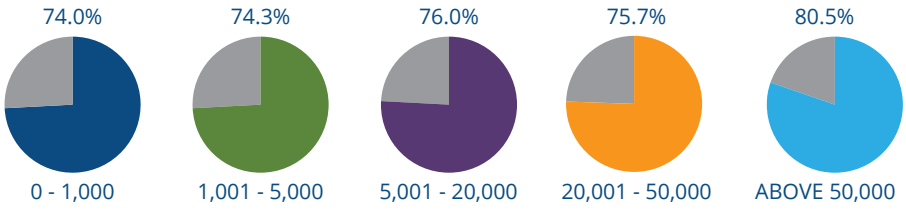
Overall, **26%** of employees failed to report a variety of potential security or privacy incidents, including unsecured personnel files or confidential product information and potentially infected computers.

**Key Takeaway:** Letting security incidents go unreported is like rolling the dice with an organization's data. The risk of letting such an incident go unreported could result in a critical data breach, not to mention creating a culture of ignorance that lets incidents happen again and again.

**30% of employees failed to report an unsecured file cabinet containing sensitive personnel files.**

**SOURCE:** State of Privacy & Security Awareness Report, 2016 (MediaPro)

## AVG. SCORE BY COMPANY SIZE




# WORKING REMOTELY

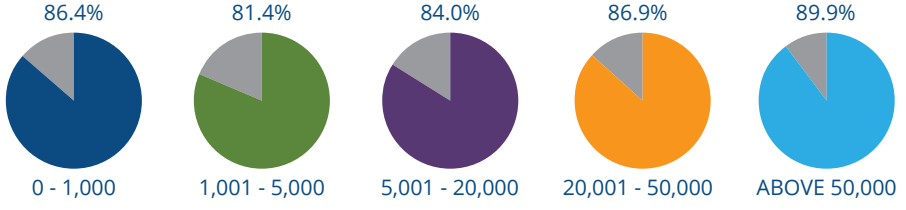
**20%** of employees didn't see a risk logging in to a public Wi-Fi to complete work.

**Key Takeaway:** Public Wi-Fi networks lack security features, making it easy for hackers to intercept communications or spread malware.

**According to a 2016 Symantec survey, only half of U.S. consumers think that they are responsible for protecting their personal information when using public Wi-Fi, while only 18% protect themselves by using a VPN.**

**SOURCE:** Internet Security Threat Report, 2016 (Symantec)

## AVG. SCORE BY COMPANY SIZE



# ACCESS CONTROLS

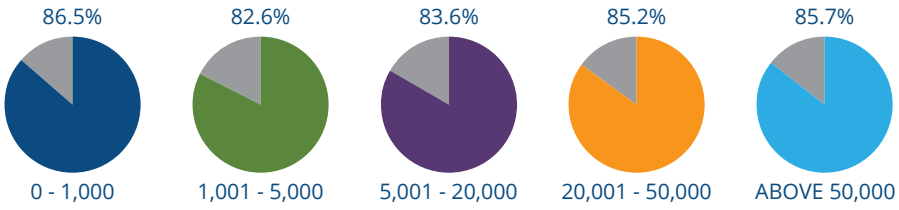
**19%** of employees couldn't identify best practices for controlling access to their organization's building.

**Key Takeaway:** Security awareness begins at the front door. If an employee can't keep threats out of the office, think how many mistakes they're going to make throughout the day.

**"Tailgating is the easiest way for an outsider to gain entry to secure facilities. 18% of surveyed employees said they'd hold the door open for someone, even if they lacked identification."**

**SOURCE:** State of Privacy & Security Awareness Report, 2016 (MediaPro)

## AVG. SCORE BY COMPANY SIZE




# IDENTIFYING PERSONAL INFORMATION

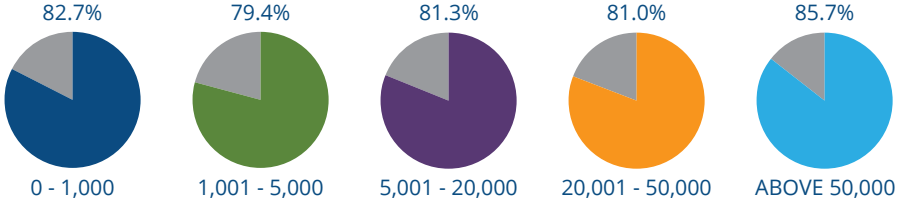
**19%** of employees made mistakes in classifying and identifying documents containing personal information.

**Key Takeaway:** Failing to correctly handle and safeguard personal information isn't just a sloppy business practice, it poses a risk to the employees whose data is exposed, and puts your organization in violation of privacy regulations.

**Violating some privacy regulations, like the European Union's General Data Protection Regulation, or GDPR, can attract fines of up to 4% of an organization's total global annual turnover.**

**SOURCE:** Preparing for the GDPR, 2016 (MediaPro)

## AVG. SCORE BY COMPANY SIZE



# IDENTIFYING MALWARE WARNING SIGNS

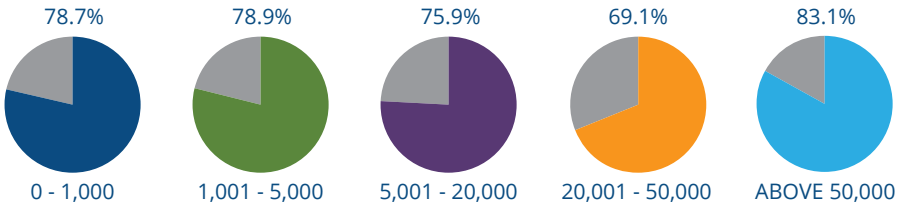
**18%** of employees couldn't identify the warning signs of malware that had infected their computer.

**Key Takeaway:** Signs of malware, such as a sluggish computer and anti-virus software mysteriously switching off, should not go unreported. Catching an infected computer early could save an organization valuable time and resources.

**31% of data incidents result from malware. Ransomware attacks, a specific type of malware, increased 119% from 2015 to 2016.**

**SOURCE 1:** Data Security Incident Response Monitor, 2016 (BakerHostetler)
**SOURCE 2**: Malware Infections Drop, 2016 (www.networkworld.com)

## AVG. SCORE BY COMPANY SIZE




# CLOUD COMPUTING

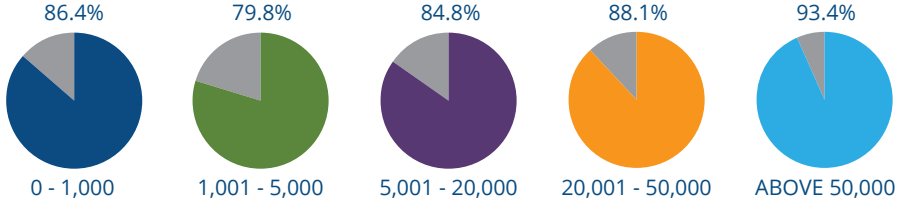
**15%** of employees inappropriately send company data using their personal email or save it via personal cloud-based storage.

**Key Takeaway:** Using public email and cloud services is not only a breach of privacy obligations, but also dangerous. Public networks lack the defenses of an enterprise security system, putting secure information at risk.

**In August 2016, Dropbox suffered a data breach hack that revealed more than 60 million passwords.**

**SOURCE:** Dropbox Hack, 2016 (www.independent.co.uk)

## AVG. SCORE BY COMPANY SIZE



# SOCIAL MEDIA

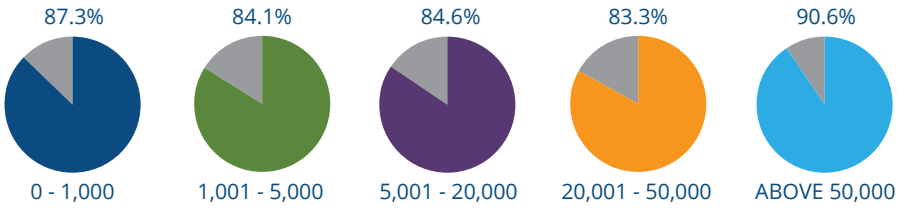
**14%** of employees thought it was acceptable to post to their personal social media account on behalf of the company.

**Key Takeaway:** Posting about company matters on social media can lead to a damaged reputation or violate an organization's code of conduct.

92% of information systems professionals believe that social network use increases likelihood of a successful advanced persistent threat attack.

**SOURCE:** Advanced Persistent Threat Awareness Report, 2016 (ISACA)

## AVG. SCORE BY COMPANY SIZE




# IDENTIFYING PHISHING ATTEMPTS

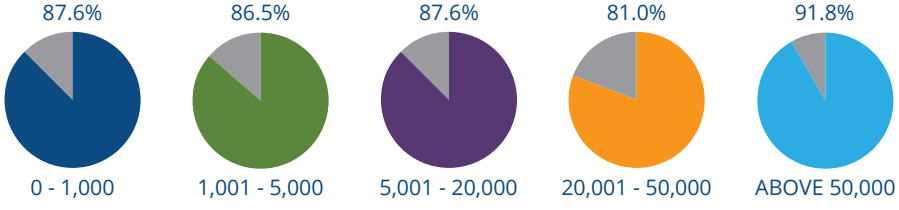
**SOURCE:** FBI Warning on Business E-Mail Scams, 2016 (www.fbi.gov)

**25%** of employees failed to spot a phishing attempt coming from a suspicious email address.

**Key Takeaway:** Exploiting human error is one of the easiest ways to steal information or infect a company's systems with malware, and spear-phishing techniques makes this method harder to spot all the time.

Business email compromise scams, which include those where cybercriminals pose as CEOs requesting fund transfers, victimized 17,000 people between October 2013 and February 2016, according to the FBI. This amounted to more than $2.3 billion in losses.

## AVG. SCORE BY COMPANY SIZE



## Conclusion

Just like in the real world, privacy and security decisions sometimes exist in a gray area. A decision you make might not be wrong, per se, but it may not be the best decision. This survey was purposefully designed to be very challenging--not every question had a clear right or wrong answer.

So how can you and your employees differentiate between a good decision and the best decision? Don't overlook the details. Those personnel files were labeled appropriately and kept from prying eyes, but were they kept under lock and key? The lady outside was nice enough, but was she checked for an ID badge before she was let into the office?

Good privacy and security practices are often common sense—but ensuring that this common sense is applied consistently and rigorously makes all the difference in the world. In a truly risk-aware organization, employees combine policy know-how, common sense, and a keen eye for detail as they regularly align their actions with your organizations security and privacy principles. How will you ensure that you've got such a culture?

## About MediaPro

MediaPro offers all the tools and services you need to run a comprehensive awareness program: phishing simulation, knowledge assessments, and an extensive library of varied training content. More than 500 of the world's most risk-aware organizations have trusted MediaPro to provide comprehensive, expertly-crafted employee awareness programs based on proven adult learning principles.

***Contact Us Today***