MEDIAPRO
Adaptive. Integrated. Proven.

EMPLOYEE AWARENESS IN FINANCIAL SERVICES 2017

809 EMPLOYEES in financial services were tested on their cybersecurity and data privacy know-how in eight key risk areas vital to an organization's overall risk posture, offering a rare snapshot of employee behavioral risk in the financial sector.

In conducting the survey, MediaPro sought to answer the following questions:

1. How risk-aware are financial services employees relative to the general population?
2. In which risk areas are financial services employees most vulnerable to privacy and security threats?
3. What can be done in 2017 to better address the changing threat and regulatory landscape?

HERE'S WHAT WE FOUND:

80% have awareness deficiencies that put their organizations at risk of a privacy or security incident.

26% demonstrated potentially fatal behaviors seen in several of the risk areas.

20% fall into our "hero" risk profile, capable of dealing with a variety of threat vectors.

Risk Awareness in Financial Services

Using the skills test from the inaugural State of Privacy & Security Awareness report, financial services employees were categorized into one of three profiles — risk, novice, or hero. The numbers represented below indicate the percentage of financial services employees that tested into each respective risk profile.

RISK	26%
NOVICE	54%
HERO	20%

Risk (00.0%-74.2%)
These individuals put their organizations at serious risk for a privacy or security incident.

Novice (77.4%-90.3%)
Novices have a good understanding of the basics, but could stand to learn more.

Hero (93.5%-100%)
These individuals know their stuff, and are adept in keeping information secure.

AVERAGE SCORE

FINANCIAL SERVICES	ALL INDUSTRIES
83.6%	83.9%

Our 2016 survey revealed that 88% of employees in all industries lack the awareness to stop preventable privacy & security incidents.[1]

LEARN MORE

Financial Services Risk Areas

Below we call out the average score for each risk area, compared to a variety of other industry sectors, such as education, retail, and healthcare.

CLOUD COMPUTING

FINANCIAL SERVICES	ALL INDUSTRIES
81%	84%

Industry Leader: Government (93%)

WORKING REMOTELY

FINANCIAL SERVICES	ALL INDUSTRIES
83%	84%

Industry Leader: Technology (87%)

RECOGNIZING MALWARE

FINANCIAL SERVICES	ALL INDUSTRIES
84%	85%

Industry Leader: Retail (87%)

IDENTIFYING PHISHING

FINANCIAL SERVICES	ALL INDUSTRIES
89%	90%

Industry Leader: Education (93%)

IDENTIFYING PERSONAL INFORMATION

FINANCIAL SERVICES	ALL INDUSTRIES
81%	82%

Industry Leader: Professional Services (84%)

ACCESS CONTROLS

FINANCIAL SERVICES	ALL INDUSTRIES
84%	85%

Industry Leader: Government (93%)

INCIDENT REPORTING

FINANCIAL SERVICES	ALL INDUSTRIES
81%	80%

Industry Leader: Government (93%)

SOCIAL MEDIA

FINANCIAL SERVICES	ALL INDUSTRIES
85%	86%

Industry Leader: Government (90%)

ARE YOU AN AWARENESS RISK, NOVICE OR HERO?

TAKE THE SURVEY NOW!

2017 Outlook for Employee Awareness in Financial Services

In the wake of increasing cyber threats, financial services firms are spending an unprecedented amount of money to bolster their cybersecurity defenses.

In 2017, **86% of firms** plan to spend **more time and resources on cybersecurity** than they did in 2016.[4]

But are the right investments being made when **more than 50%** of these firms cite **regulatory and compliance requirements** as the reason for increasing those investments?[5]

Especially when **1 in 1,918 emails** sent to financial services employees were classified as **phishing attempts**,[3] and over **90% of breaches** cite **phishing** as a main cause?[7]

Organizations that focus only on compliance training are engaged in a race to the bottom that leaves employees ill-prepared for the dynamic threats that a static approach to cybersecurity simply can't address.

When firewalls fail to pick up on these threats, an employee's ability to identify a phishy email is all that stands in the way of a potentially backbreaking news headline.

This is exactly why employee awareness and training need to be viewed as exercises in risk mitigation — not just a means of fulfilling once-a-year compliance requirements.

BUT THERE'S MORE TO EMPLOYEE AWARENESS THAN RECOGNIZING A PHISHING ATTEMPT

Financial services firms are increasingly putting sensitive data and work processes into the cloud, using third-party software that runs marketing and sales, customer service and operations, a trend that puts customer data at risk.

CONSIDER THE FOLLOWING:

60% of financial services firms say they'll run IT services **in the cloud.**[2]

48% entrust **finance functions** to cloud providers.[2]

60% use or intend to use **managed security services.**[2]

This brings into question not only the ability of third-party vendors to protect this data, but also the ability of employees accessing these services to properly secure and protect it. Customers expect and demand it.

CONSIDER THAT:

In 2016, **22%** of companies reported **losing current customers** because of a breach.[7]

Of those that did lose customers, **39%** stated they **lost 20% of their customers** or more.[7]

So, it should come as no surprise that **50% of IT professionals** in finance express concern about **potential for theft or loss of control** of the company's customer or client records.[6]

These concerns are warranted given that **3,554,225 identities** were reported as **stolen through the financial services sector in 2016.**[3]

And **39.2%** of all information lost in breaches, was **personal financial information** – including debit card details or banking financial records.[3]

In 2018, the **General Data Protection Regulation (GDPR)** will go into effect and require financial services organizations with data points in the European Union to comply or be subject to hefty fines.

Along with rapidly changing customer demands, it's clear that 2017 needs to be a year that financial organizations consider a data protection strategy and how to keep privacy top-of-mind for all employees.

Put yourself ahead of the rapidly evolving threat and regulatory landscape with MediaPro's adaptive and comprehensive approach to employee privacy and security awareness education.

CLICK HERE TO LEARN MORE

120+ AWARDS

1K+ SUCCESSFUL PROJECTS | 12M+ LEARNERS TRAINED

2016 2015 2014 SECURITY AWARENESS
NAMED A LEADER IN GARTNER'S MAGIC QUADRANT

MEDIAPRO
Adaptive. Integrated. Proven.

SOURCES

1. State of Privacy & Security Awareness, MediaPro, 2016
2. PWC Global State of Information Security Survey, 2017
3. Symantec Internet Security Threat Report, 2017
4. Survey of Financial Service Firms, Duff & Phelps, 2016
5. Cybersecurity in Financial Institutions, Kaspersky, 2017
6. Travelers Risk Index, Travelers.com, 2016
7. Verizon Data Breach Investigations Report, 2017