
# The Cost of Phishing & Value of Employee Training

## Sponsored by Wombat Security Technologies, Inc.

Independently conducted by Ponemon Institute LLC

Publication Date: August 2015

# The Cost of Phishing and Value of Employee Training

Presented by Ponemon Institute: August 2015

## Introduction

Ponemon Institute is pleased to present the results of the *Cost of Phishing and Value of Employee Training* study sponsored by Wombat Security. The purpose of this research is to understand how training can reduce the financial consequences of phishing in the workplace.

The research reveals the majority of costs caused by successful phishing attacks are the result of the loss of employee productivity. Based on the analysis described later in this report, we extrapolate an average improvement of 64% from six proof of concept training projects. This improvement represents the change in employees who fell prey to phishing scams in the workplace before and after training.

As a result of effective training provided by Wombat, we estimate a cost savings of $1.8 million or $188.4 per employee/user. If companies paid Wombat's standard fee of $3.69 per user for a program for up to 10,000 users, we determine a very substantial net benefit of $184.7 per user – for a remarkable one-year rate of return at 50X.

To determine the cost structure of phishing, we surveyed 377 IT and IT security practitioners in organizations in the United States. Thirty-nine percent of respondents are from organizations with 1,000 or more employees who have access to corporate email systems. The topics covered in this research include the following:

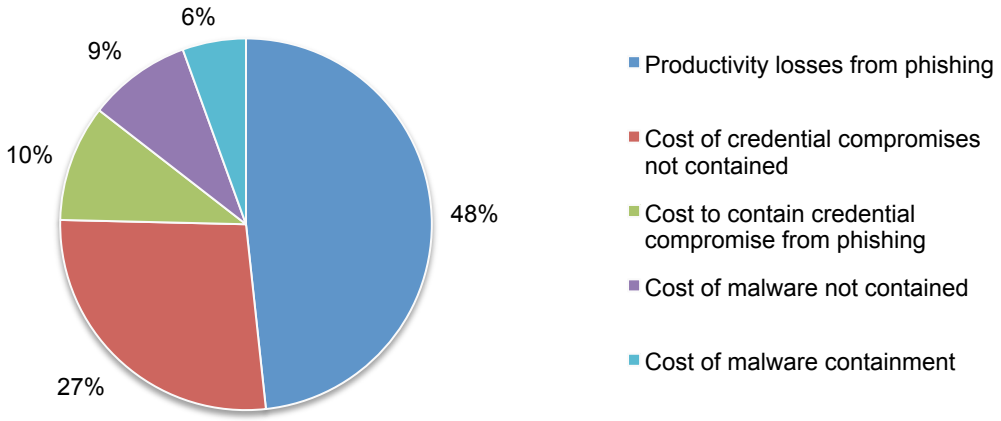
- The financial consequences of phishing scams
- The financial impact of phishing on employee productivity
- The cost to contain malware
- The cost of malware not contained & the likelihood it will cause a material data breach
- The cost of business disruption due to phishing
- The cost to contain credential compromises
- Potential cost savings from employee training

**Phishing scams are costly**. Often overlooked is the potential cost to organizations when employees are victimized by phishing scams. As shown in Table 1, our cost analysis includes the cost to contain malware, the cost not contained, loss of productivity, the cost to contain credential compromises and the cost of credential compromises not contained. Based on these costs, the extrapolated total annual cost of phishing for the average-sized organization in our sample totals $3.77 million.

| **Table 1. Summarized calculus on the cost of phishing** | Estimated cost |
|---|---|
| Part 1. The cost to contain malware | $208,174 |
| Part 2. The cost of malware not contained | $338,098 |
| Part 3. Productivity losses from phishing | $1,819,923 |
| Part 4. The cost to contain credential compromises | $381,920 |
| Part 5. The cost of credential compromises not contained | $1,020,705 |
| Total extrapolated cost | $3,768,820 |

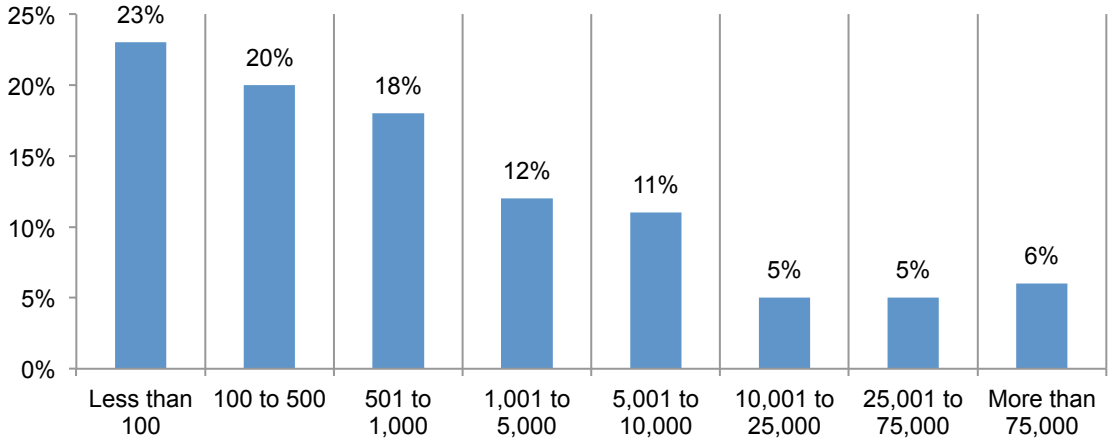
**The majority of costs are caused by loss of employee productivity**. Pie Chart 1 shows the distribution of organizational costs caused by phishing scams. Forty-eight percent of total organizational cost pertains to employee/user productivity losses caused by successful phishing during the workday.

**Pie Chart 1. Percentage distribution of phishing cost categories**




**Headcount in organizations represented in this study range from less than 100 to more than 75,000**. Figure 1 shows the distribution of survey responses based on headcount of employees with access to corporate email systems. In this study, headcount is used as a surrogate for organizational size. The extrapolated average headcount is 9,552 users with email access.

**Figure 1. Average headcount of employees with access to corporate email**
Extrapolated headcount = 9,552



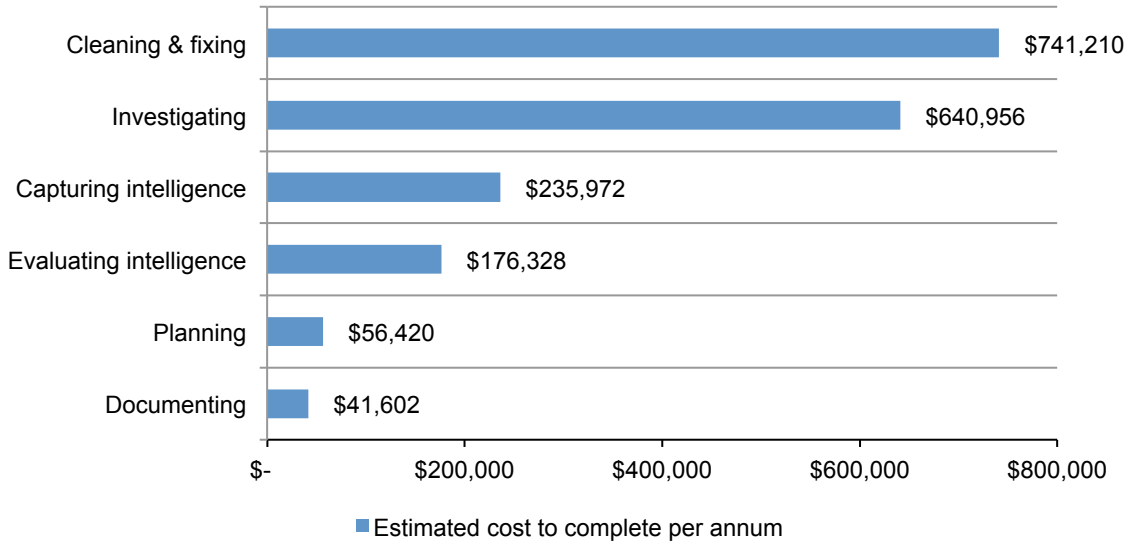
## Part 1. Cost to contain malware

**The average total cost to contain malware annually is $1.9 million.** The first step in understanding the overall cost is to analyze the six tasks to contain malware infections**.** Drawing from the empirical findings of an earlier study, we were able to derive cost estimates relating to six discrete tasks conducted by companies to contain malware infections in networks, enterprise systems and endpoints.[1] Table 2 summarizes the annual hours incurred for six tasks by the average-sized organization on an annual basis. The largest tasks incurred to contain malware involve the cleaning and fixing of infected systems and conducting forensic investigations. Documentation and planning represents the smallest tasks in terms of hours spent each year.

| **Table 2. Six tasks to contain malware infections** | Estimated hours per annum |
|---|---|
| Planning | 910 |
| Capturing intelligence | 3,806 |
| Evaluating intelligence | 2,844 |
| Investigating | 10,338 |
| Cleaning & fixing | 11,955 |
| Documenting | 671 |
| Total hours | 30,524 |

**The annual cost to contain malware is based on the hours to resolve the incident**. Figure 2 shows the cost to contain malware attacks each year for an average-sized organization. These cost estimates are based on a fully loaded average hourly labor rate for US-based IT security practitioners of $62.[2] As can be seen, the extrapolated total cost to contain malware is $1.89 million.

**Figure 2. Annual cost to contain malware for six tasks**
Extrapolated total cost = $1,892,488



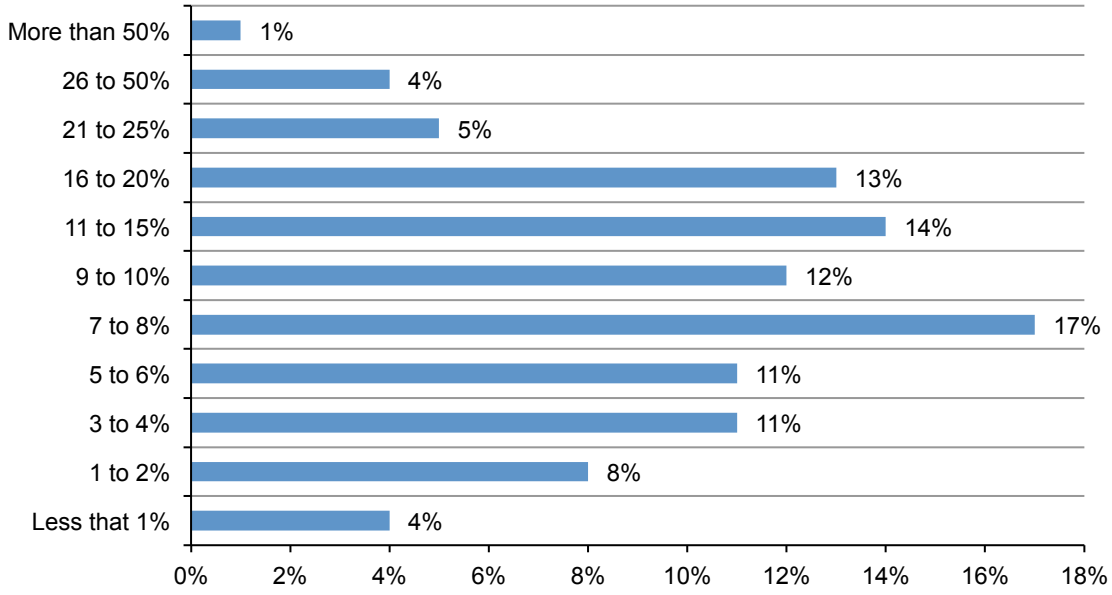

[1]See: The Cost of Malware Containment (sponsored by Damballa). Ponemon Institute, March 2015.
[2]See: Annual IT Security Benchmark Tracking Study. Ponemon Institute. March 2015.

**The adjusted cost of malware containment resulting from phishing scams is $208,174 per annum.** The final step in determining the cost of malware containment attributable to phishing is to calculate the percentage of malware incidents unleashed by successful phishing scams.

Figure 3 shows the percentage distribution of responses to a survey question, "What percent of all malware infections is caused by successful phishing scams?" The percentage rate of malware infections caused by phishing scams was based on our independent survey of IT security practitioners. As can be seen, the estimated range is less than 1 percent to more than 50 percent. The extrapolated average rate is 11 percent.

Drawing from the above analysis, we estimate the cost of malware containment as 11 percent of the previously calculated total cost of $1.9 million.

**Figure 3. Percentage rate of malware infections caused by phishing scams**
Extrapolated rate = 11%



## Part 2. Cost of malware not contained

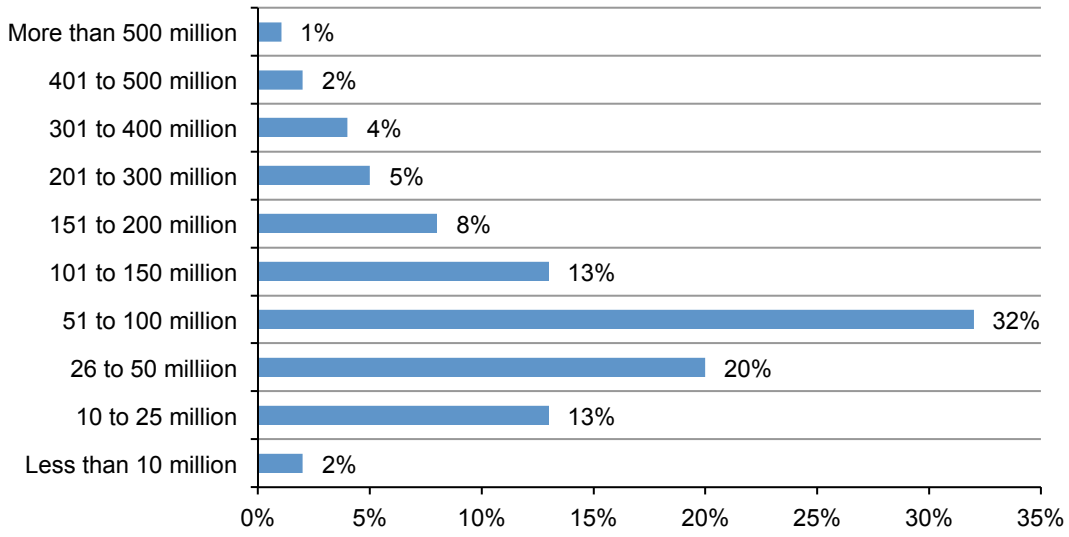
In this section, we estimate the cost of malware not contained at the device level to be $105.9 million. In other words, this cost occurs because malware evaded traditional defenses such as firewalls, anti-malware software and intrusion prevention systems. In this state we assume the malware becomes weaponized for attack.

Following are two attacks caused by weaponized malware: (1) data exfiltration (a.k.a. material data breach) and (2) business disruptions. We determine a most likely cost using an expected cost framework, which is defined as follows:

Expected cost = Probable maximum loss (PML) x Likelihood of occurrence [over a 12-month period].

Respondents in our survey were asked to estimate the probable maximum loss (PML) resulting from a material data breach (i.e., exfiltration) caused by weaponized malware.[3] Figure 4 shows the distribution of maximum losses ranging from less than $10 million to more than $500 million. The extrapolated average PML resulting from data exfiltration is $105.9 million.

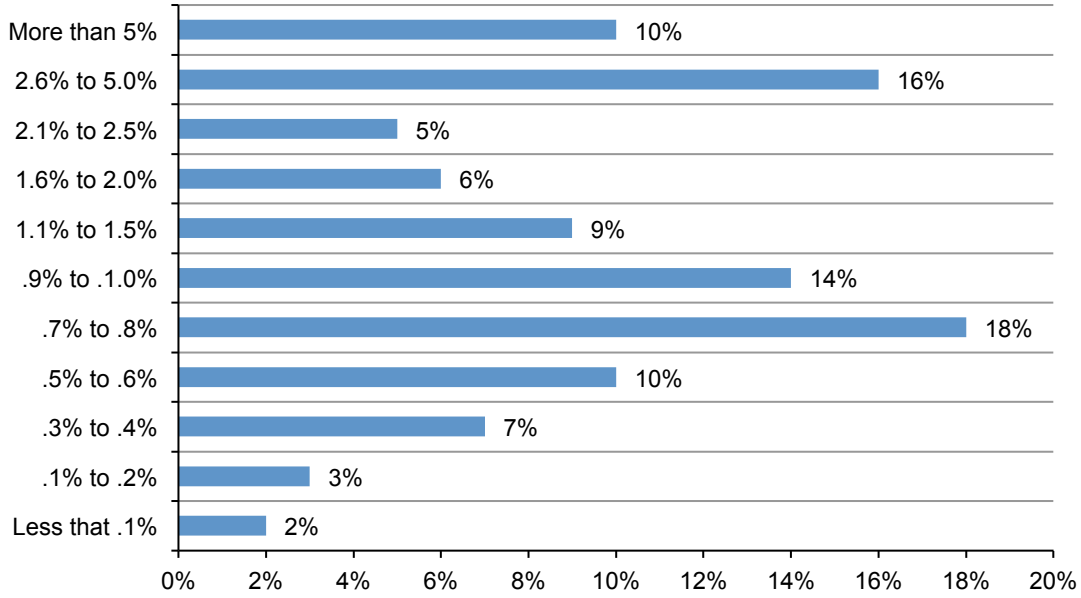
**Figure 4. Maximum loss resulting from data exfiltration caused by weaponized malware**
Extrapolated PML = $105.9 million




[3]Probable Maximum Loss (PML) is defined as the value of the largest loss that could result from cyber attacks, assuming the normal functioning of perimeter controls and other commonly deployed security technologies. Insurance companies frequently use PML to determine risk exposures.

**What is the likelihood of weaponized malware causing a material data breach?** In the context of this research, a material data breach involves the loss or theft of more than 1,000 records**.** Respondents were asked to estimate the likelihood of this occurring. According to Figure 5, the probability distribution ranges from less than .1 percent to more than 5 percent. The extrapolated average likelihood of occurrence is 1.9 percent over a 12-month period.

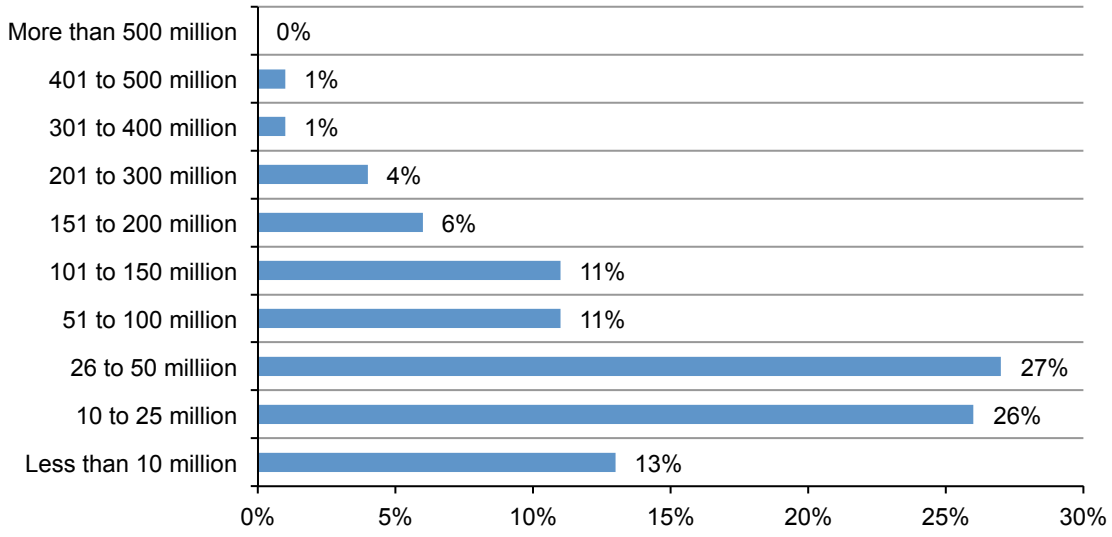
**Figure 5. Likelihood of data exfiltration caused by weaponized malware (over 12 months)**
Extrapolated likelihood of occurrence = 1.9%



**The cost of business disruption due to phishing is $66.9 million.** Respondents were asked to estimate the PML resulting from business disruptions caused by weaponized malware. Business disruptions include denial of services, damage to IT infrastructure and revenue losses. Figure 6 shows the distribution of maximum losses ranging from less than $10 million to $500 million. The extrapolated average PML resulting from data exfiltration is $66.9 million.

**Figure 6. Maximum loss resulting from business disruptions caused by weaponized malware**

Extrapolated PML = $66.9 million



**How likely are business disruptions due to weaponized malware?** Respondents were asked to estimate the likelihood of material business disruptions caused by weaponized malware. Figure 7 shows the probability distribution ranging from less than .1 percent to more than 5 percent. The extrapolated average likelihood of occurrence is 1.6 percent over a 12-month period.

**Figure 7. Likelihood of business disruption caused by weaponized malware (over 12 months)**
Extrapolated likelihood of occurrence = 1.6%

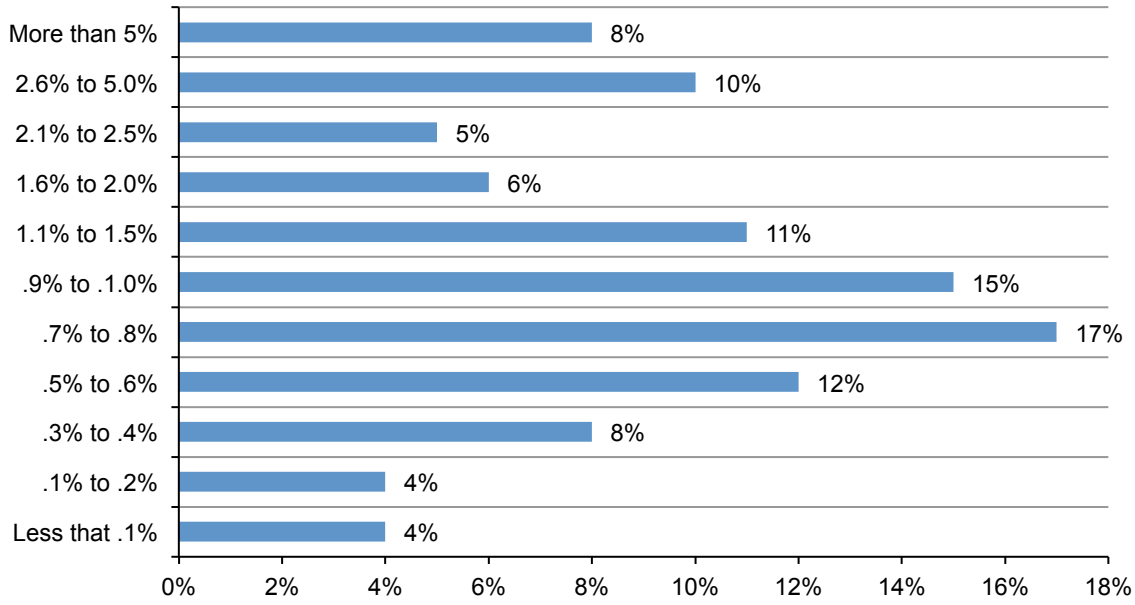



Table 3 reports the expected cost of malware attacks relating to data exfiltration ($2 million) and disruptions to IT and business processes ($1.1 million). The total amount of $3.1 million is adjusted for the 11 percent of malware attacks originating from phishing scams, which yields an estimated cost of $338,098 per annum.

| **Table 3. Recap for the cost of malware not contained** | Calculus |
|---|---|
| Probable maximum loss resulting from data exfiltration | $105,900,000 |
| Likelihood of occurrence over the next 12 months | 1.9% |
| Expected value | $2,012,100 |
| | |
| Probable maximum loss resulting from business disruptions (including denial of services, damage to IT infrastructure and revenue losses) | $66,345,000 |
| Likelihood of occurrence over the next 12 months | 1.6% |
| Expected value | $1,061,520 |
| | |
| Total cost of malware not contained | $3,073,620 |
| | |
| Percentage rate of malware infections caused by phishing scams (see Figure 3) | 11% |
| | |
| Adjusted total cost attributable to phishing scams | $338,098 |

## Part 3. Employee/user productivity losses from phishing

**Employees waste an average of 4.16 hours annually due to phishing scams**. As previously discussed, the majority of costs (52 percent) are due to the decline in employee productivity as a result of being phished. In this section, we estimate the productivity losses associated with phishing scams experienced by employees during the workday. Drawing upon our survey research, we extrapolated the total hours spent each year by employees/users viewing and possibly responding to phishing emails.

Figure 8 reports the distribution of time wasted for the average employee (office worker) due to phishing scams. The range of response is less than 1 hour to more than 25 hours per employee each year.

**Figure 8. Estimated hours per employee each year spent dealing with phishing scams**
Extrapolated hours per year = 4.16

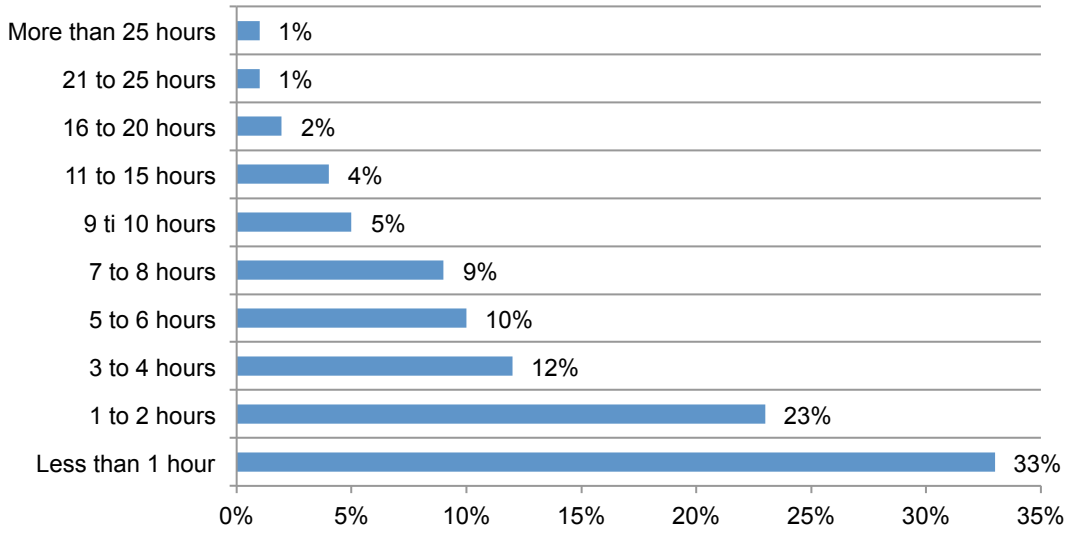



Table 4 reports the calculus used to estimate the productivity losses resulting from phishing scams. Here we assume an average-sized organization with a headcount of 9,552 individuals with user access to corporate email systems. Drawing on an average of 4.16 hours per employee we calculate 39,736 hours wasted because of phishing. Assuming an average labor rate of $45.8 for non-IT employees (users) we calculate a total productivity loss of $1,819,923 per annum.

| **Table 4. Employee/user productivity losses** | Calculus |
|---|---|
| Extrapolated hours per employee each year | 4.16 |
| Average organization headcount (see footnote 1) | 9,552 |
| Extrapolated hours per organization each year | 39,736 |
| Fully loaded average hourly rate for non-IT users* | $45.80 |
| Total productivity loss per year for the average-sized organization | $1,819,923 |

*Source: Annual IT Security Benchmark Tracking Study, Ponemon Institute, March 2015

## Part 4. Cost to contain credential compromises

**What is the cost to respond to a credential compromise?** In this section, we estimate the costs incurred by organizations to contain credential compromises that originated from a successful phishing attack, including the theft of cryptographic keys and certificates. Our first step in this analysis is to estimate the total number of compromises expected to occur over the next 12 months. The range of responses includes zero to more than 10 incidents.

**Figure 9. Distribution of credential compromises caused by phishing scams**
Extrapolated average = 4.0 compromises that originated from phishing over 12 months

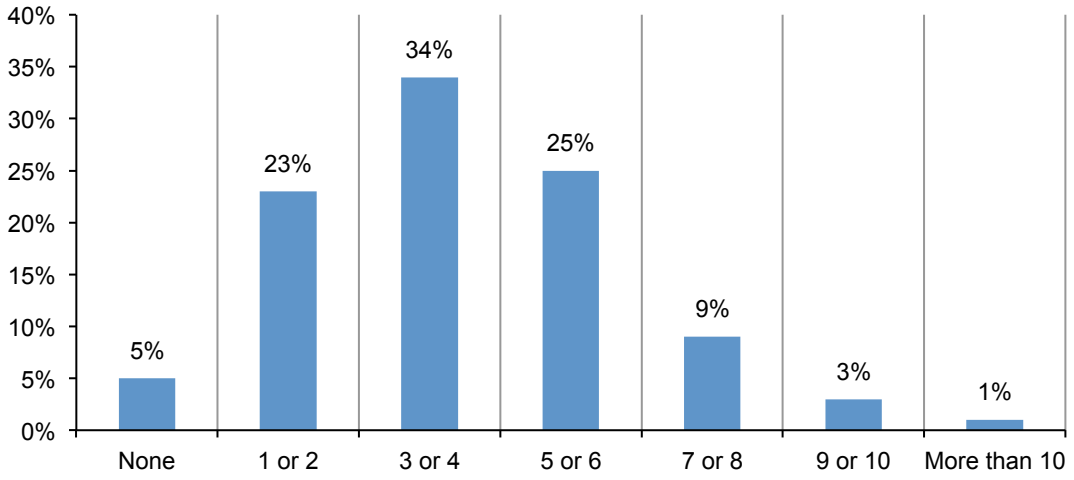



Table 5 summarizes our extrapolated cost. Drawing from an earlier study on the cost of key or credential compromise, we estimate a total of 1,540 hours of tech time investigating and responding to one compromise or 6,160 hours estimated over the next 12 months.[4] Assuming an average annual rate of $62.0 for tech support, we estimate a total cost of $381,920 per annum.

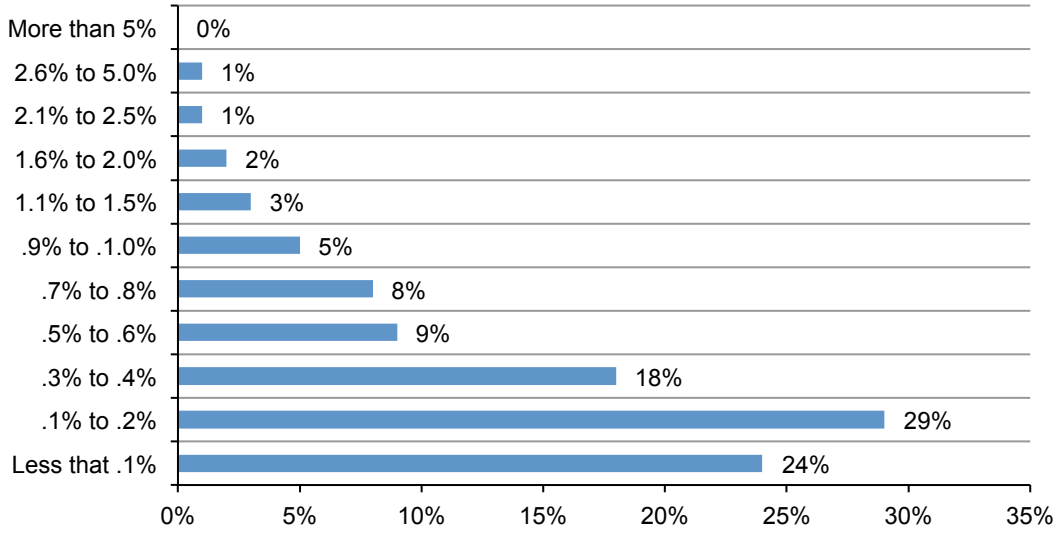
| **Table 5. Cost of credential compromises caused by phishing** | Calculus |
|---|---|
| Estimated number of credential compromises over the next 12 months | 4.0 |
| Tech time investigating and responding to one compromise | 1,540 |
| Tech time investigating and responding to all compromises per year | 6,160 |
| Fully loaded average hourly rate ($) for IT security ops* | $62.0 |
| Total cost of tech time | $381,920 |

[4]See: Annual Cost of Failed Trust Report: Threats and Attacks (sponsored by Venafi), Ponemon Institute February 2013.

## Part 5. Cost of credential compromise not contained

**How likely will a material data breach occur if the credential compromise is not contained?** Respondents were asked to estimate the likelihood of a material data breach caused by credential compromise. Figure 10 shows the probability distribution ranging from less than .1 percent to 5 percent. The extrapolated average likelihood of occurrence is .4 percent over a 12-month period.

**Figure 10. Likelihood of data exfiltration caused by credential compromises (over 12 months)** Extrapolated likelihood of occurrence = .4%



Respondents were asked to estimate the likelihood of material business disruption caused by credential compromise. Figure 11 shows the probability distribution ranging from less than .1 percent to 5 percent. The extrapolated average likelihood of occurrence is .9 percent over a 12-month period.

**Figure 11. Likelihood of business disruptions caused by credential compromises (over 12 months)**
Extrapolated likelihood of occurrence = .9%

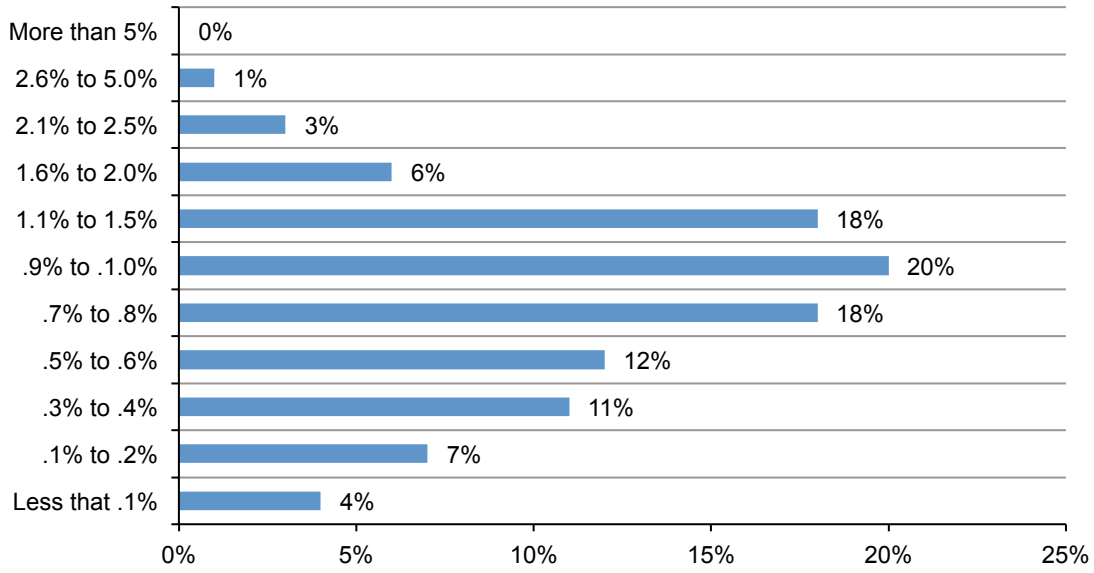



Table 6 reports the expected cost relating to data exfiltration ($423,600) and disruptions to IT and business processes ($597,105), which originated from phishing scams. This yields a total amount of $1,020,750.

| **Table 6. Recap for the cost of credential compromises not contained** | Calculus |
|---|---|
| Probable maximum loss resulting from data exfiltration | $105,900,000 |
| Likelihood of occurrence over the next 12 months | .4% |
| Expected value | $423,600 |

| | |
|---|---|
| Probable maximum loss resulting from business disruptions (including denial of services, damage to IT infrastructure and revenue losses) | $66,345,000 |
| Likelihood of occurrence over the next 12 months | .9% |
| Expected value | $597,105 |

| | |
|---|---|
| Total cost of credential compromises not contained | $1,020,705 |

## Analysis of Wombat's training program

In this section, we estimate the potential cost savings that result from employee education that provides actionable advice and raises awareness about phishing and other related topics. As a starting point to this analysis, we obtained six proof of concept studies completed for six large companies.

These reports provided detailed findings that show the phishing email click rate for employees both before and after training. Table 7 provides the actual improvements experienced by companies, ranging from 26 to 99 percent, respectively. The average improvement for all six companies is 64 percent.

As a result of Wombat's training on phishing that includes mock attacks and follow-up with in-depth training, we estimate a high knowledge retention rate. Based on well-known research, training that focuses on actual practices should result in an average retention rate of approximately 75 percent.[5] Applying this retention rate against the average improvement shown in the six proof of concept studies, we estimate a net long-term improvement in fighting phishing scams of 47.75 percent.

| **Table 7. Proof of concept results** | Improvement |
|---|---|
| Company A | 99% |
| Company B | 72% |
| Company C | 54% |
| Company D | 26% |
| Company E | 62% |
| Company F | 69% |
| Average improvement | 64% |
| Expected diminished learning retention over time (1-75%) | 25% |
| Average net improvement | 47.75% |

Table 8 provides a simple analysis of potential cost savings accruing to organizations that use an effective training approach to mitigating phishing scams. As shown before, we estimate a total cost of phishing for an average-sized organization at $3.77 million.

Assuming a net improvement of 47.75 percent, we estimate a cost savings of $1.80 million or $188.40 per employee/user. At a fee of $3.69 per employee/user, we determine a very substantial net benefit of $184.71 per user – or a one-year rate of return of 50X.

| **Table 8. Calculating net benefit of Wombat training on phishing** | Calculus |
|---|---|
| Total cost of phishing (see Table 1) | $3,768,820 |
| Estimated cost savings assuming net improvement at 47.75 percent | $1,799,612 |
| Extrapolated headcount for the average-sized organization (see Figure 1) | 9,552 |
| Estimated cost savings per employee | $188.40 |
| Estimated fee of Wombat training per user | $3.69 |
| Estimated net benefit of Wombat training per user | $184.71 |
| Estimated one-year rate of return = Net benefit ÷ Fee | 50X |

[5]See: The Learning Pyramid, National Training Laboratories, Bethel, Maine

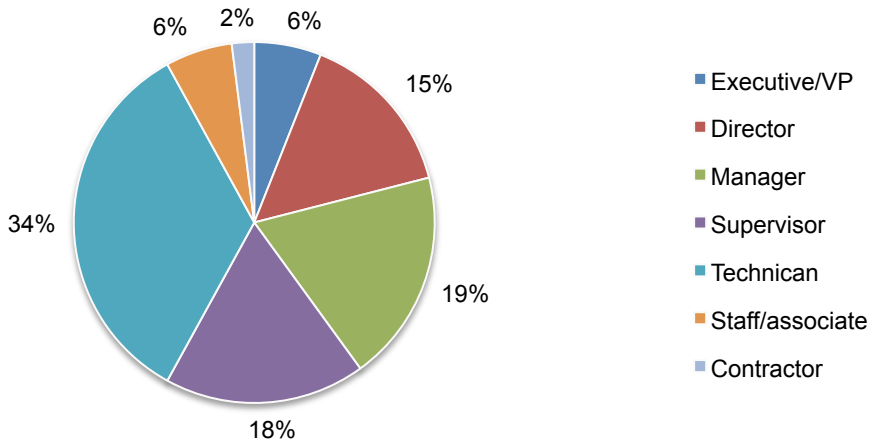
## Methods

Our sampling frame is composed of 12,442 IT and IT security practitioners located in the United States, whose job involves the protection of sensitive or confidential information. As shown in Table 9, 415 respondents completed the survey. Screening removed 38 surveys. The final sample was 377 surveys (or a 3.0 percent response rate).

| **Table 9. Sample response** | Freq |
|---|---|
| Total sampling frame | 12,442 |
| Total returns | 415 |
| Rejected or screened surveys | 38 |
| Final sample | 377 |
| Response rate | 3.0% |

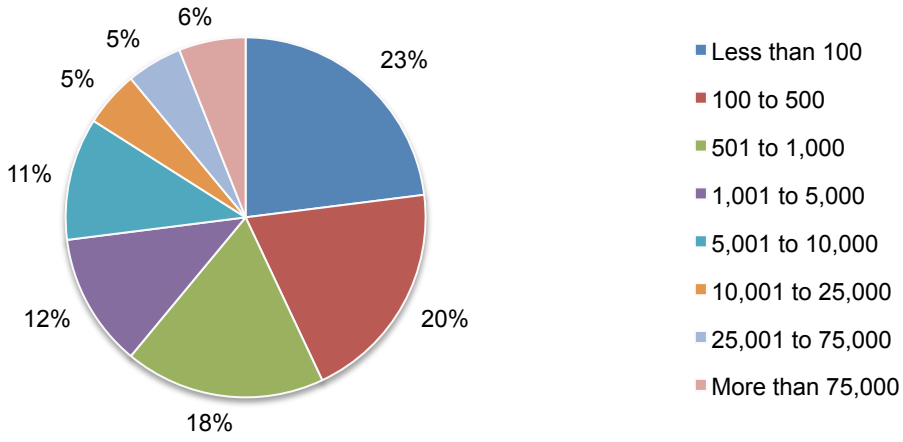
Pie Chart 2 reports the current position or organizational level of the respondents. More than half of respondents reported their current position as supervisory or above.

**Pie Chart 2. Current position within the organization**



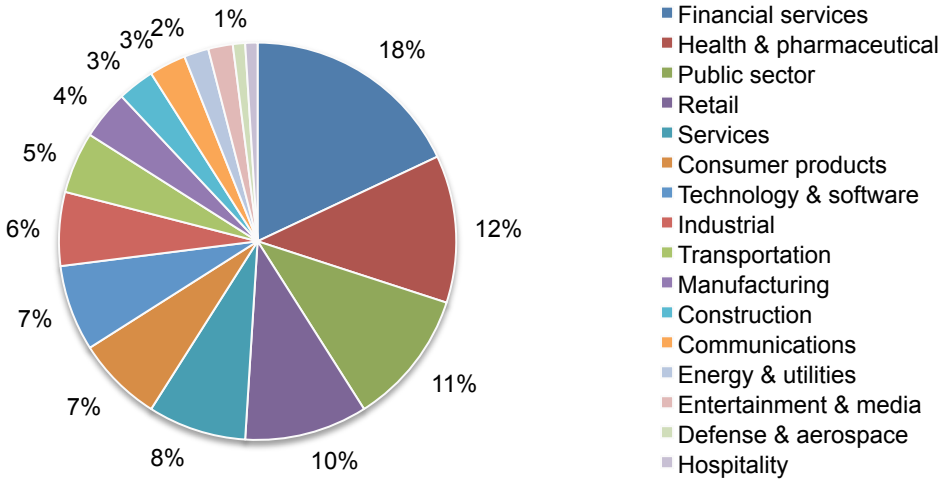

According to Pie Chart 3, 39 percent of the respondents are from organizations with more than 1,000 employees that have access to corporate email systems.

**Pie Chart 3. Full time employees with access to corporate email systems**



Pie Chart 4 reports the primary industry classification of respondents' organizations. This chart identifies financial services (18 percent) as the largest segment, followed by health and pharmaceuticals (12 percent) and public sector (11 percent).

**Pie Chart 4. Primary industry classification**




**Caveats**

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.