Ponemon INSTITUTE


# The 2021 Cost of Phishing Study

## Sponsored by Proofpoint

Independently conducted by Ponemon Institute LLC

Publication Date: June 2021

# The 2021 Cost of Phishing Study

Presented by Ponemon Institute: June 2021

## Part 1. Introduction

Ponemon Institute is pleased to present the results of *The 2021 Cost of Phishing Study* sponsored by Proofpoint. Initially conducted in 2015, the purpose of this research is to understand the risk and financial consequences of phishing. For the first time in this year's study we look at the threats and costs created by business email compromise (BEC), identity credentialing and ransomware in the workplace.

The key takeaway from this research is that the costs have increased significantly since 2015. Moreover, with the difficulty many organizations have in securing a growing remote workforce due to COVID-19, successful phishing attacks are expected to increase.

We surveyed 591 IT and IT security practitioners in organizations in the United States. Forty-four percent of respondents are from organizations with 1,000 or more employees who have access to corporate email systems.

The following findings reveal that phishing attacks are having a significant impact on organizations not only because of the financial consequences but also because these attacks increase the likelihood of a data breach, decrease employee productivity and increase the likelihood of a business disruption.

**The cost of phishing more than tripled since 2015.** The average annual cost of phishing has increased from $3.8 million in 2015 to $14.8 million in 2021.The most time-consuming tasks to resolve attacks are the cleaning and fixing of infected systems and conducting forensic investigations. Documentation and planning represent the least time-consuming tasks.

**Loss of employee productivity represents a significant component of the cost of phishing.** Employee productivity losses are among the costliest to organizations and have increased significantly from an average of $1.8 million in 2015 to $3.2 million in 2021. Employees are spending more time dealing with the consequences of phishing scams. We estimate the productivity losses based on hours spent each year by employees/users viewing and possibly responding to phishing emails averages 7 hours annually, an increase from 4 hours in 2015.

**The cost of resolving malware infections has doubled total cost of phishing.** The average total cost to resolve malware attacks is $807,506 in 2021, an increase from $338,098. Costs due to the inability to contain malware have more than doubled from an average of $3.1 million to $5.3 million.

**Credential compromises increased dramatically. As a result, organizations are spending more to respond to these attacks**. The average cost to contain phishing-based credential compromises increased from $381,920 in 2015 to $692,531 in 2021. Organizations are experiencing an average of 5.3 compromises over the past 12-month period.

**Credential compromises not contained have more than doubled.** The average total cost of credential compromised not contained is $2.1 million and has increased significantly from $1 million in 2015.

**BEC is a security exploit in which the attacker targets employees who have access to an organization's funds or data.** The average total cost of BEC's exploits was $5.96 million (see Table 1a). Based on the findings, the extrapolated average maximum loss resulting from a BEC attack is $8.12 million. The average total amount paid to BEC attackers was $1.17 million.

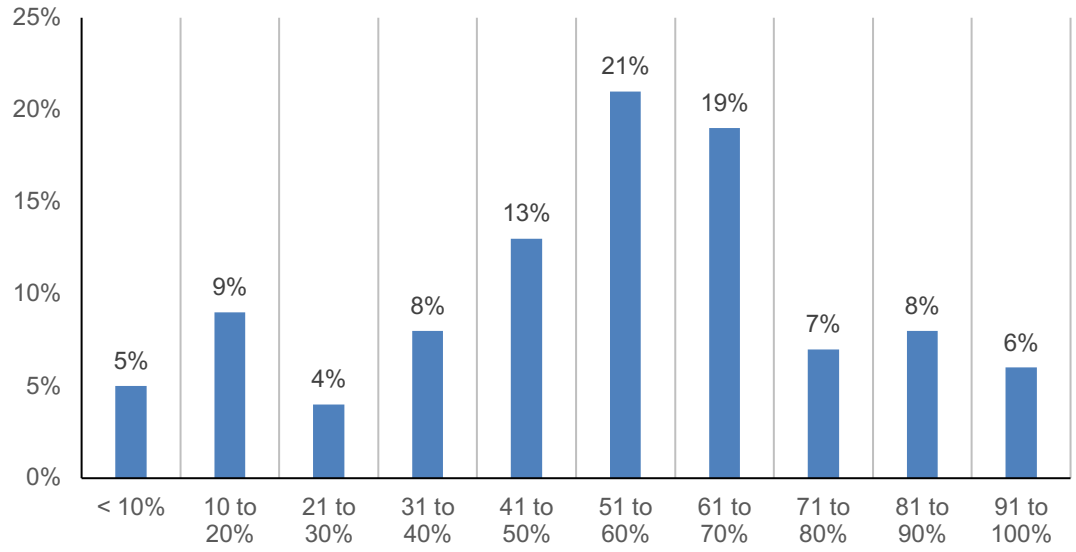
**What is the cost of business disruption due to ransomware? Ransomware is a sophisticated piece of malware that blocks the victim's access to his/her files.** The average total cost of ransomware last year was $5.66 million (see Table 1a), and the average percentage rate of ransomware attacks from phishing was 17.6 percent.

**Employee training and awareness programs on the prevention of phishing attacks can reduce costs.** Phishing attacks are costing organizations millions of dollars. According to the research, the average annual cost of phishing scams is $14.8 million, an increase from $3.8 million in 2015.

Respondents were asked to estimate what percentage of phishing costs that could be reduced through training and awareness programs that specifically address the risks of phishing attacks targeting the workforce. As shown in Figure 1, the cost can be reduced by an average of more than half (53 percent) if training is conducted.

**Figure 1. Percentage decrease in the cost of phishing attacks as a result of employee training interventions**

Extrapolated value = 53%



## Part 2. Key findings

In this section, we provide an analysis of the research findings. The complete audited findings are presented in the Appendix of this report. The report is organized according to the following topics.

- The cost of phishing scams and impact on employee productivity
- The cost of malware contained and not contained
- The cost of business disruption due to phishing
- The cost to contain and not contain credential compromises
- The cost of business email compromise (BEC)
- The cost of ransomware

### The cost of phishing scams and impact on employee productivity

**Loss of employee productivity represents a significant component of the cost of phishing.** Table 1a presents the costs related to different types of phishing attacks.

The average annual cost of phishing has increased from $3.8 million in FY2015 to $14.83 million in 2021. As shown, productivity losses have increased significantly from $1.8 million in 2015 to $3.2 million in FY2021. Please note that information about BEC and ransomware was not available in FY2015. In the current study, we estimate an annual cost of phishing for BEC at $5.97 million and ransomware at $996 thousand.

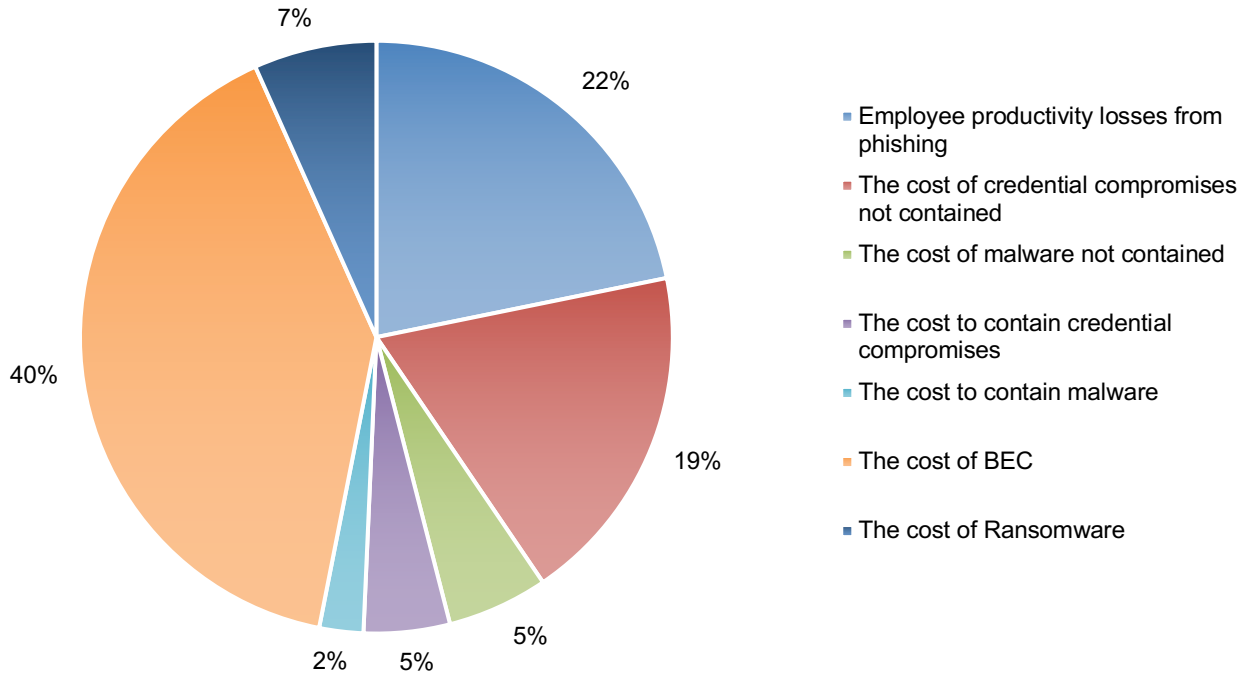
| **Table 1a. Phishing cost components** | Estimated cost FY2015 | Estimated cost FY2021 |
|---|---|---|
| The cost to contain malware | $208,174 | $353,582 |
| The cost of malware not contained | $338,098 | $807,506 |
| Productivity losses from phishing | $1,819,923 | $3,234,459 |
| The cost to contain credential compromises | $381,920 | $692,531 |
| The cost of credential compromises not contained | $1,020,705 | $2,776,340 |
| **Total original phishing cost components** | $3,768,820 | $7,864,418 |
| Total cost of BEC | | $5,965,534 |
| Total cost of ransomware from phishing | | $ 996,265 |
| **Extrapolated total cost of phishing** | | $14,826,217 |

Table 2 summarizes the annual hours incurred for six tasks by the average-sized organization on an annual basis. The most time-consuming tasks to resolve phishing scams are the cleaning and fixing of infected systems and conducting forensic investigations. Documentation and planning represent the least time-consuming tasks.

| **Table 2. Six tasks to resolve attacks** | Malware infections | Business email compromise | Ransomware | Credential theft |
|---|---|---|---|---|
| Planning | 1,248 | 1,019 | 967 | 885 |
| Capturing intelligence | 4,892 | 4,450 | 3,889 | 3,630 |
| Evaluating intelligence | 4,282 | 5,001 | 4,200 | 5,411 |
| Investigating | 12,045 | 12,336 | 11,901 | 12,884 |
| Cleaning & fixing | 13,215 | 14,395 | 13,415 | 11,950 |
| Documenting | 951 | 1,075 | 913 | 1,002 |
| Total hours | 36,633 | 38,276 | 35,285 | 35,762 |

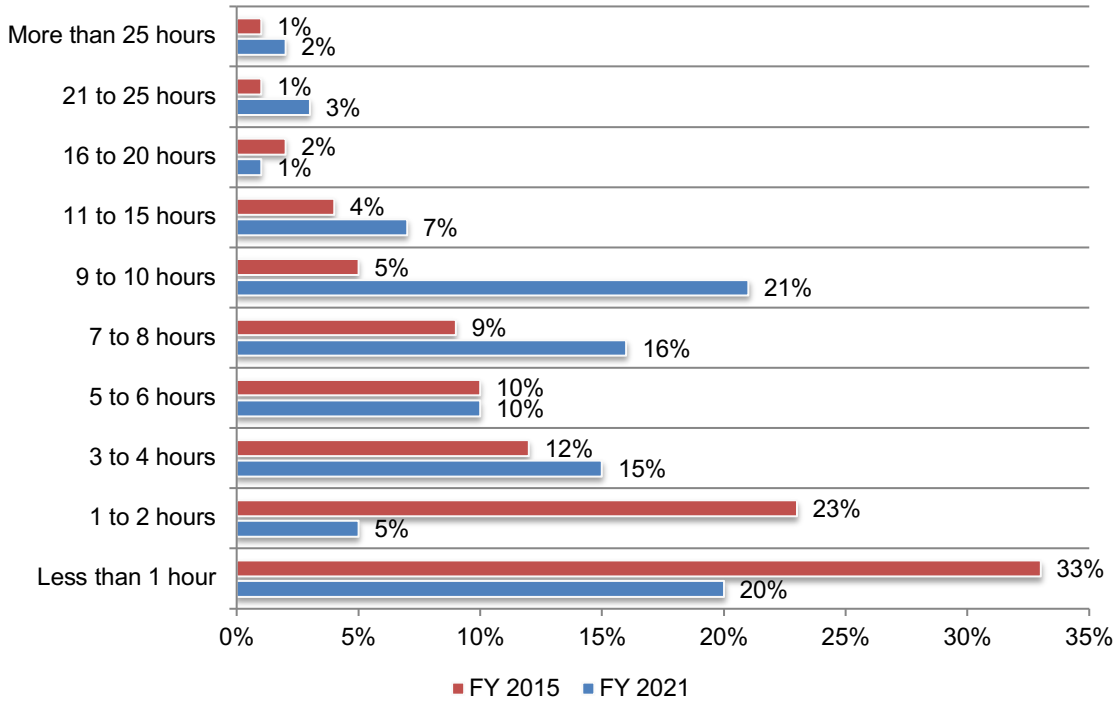
Pie Chart 1 shows the distribution of organizational costs caused by phishing scams (excluding BEC and ransomware). The top two cost categories are

**Pie Chart 1. Percentage distribution of phishing cost categories** (as shown in Table 1)



**Employees are spending more time dealing with the consequences of phishing scams.** Figure 2 reports the distribution of time wasted for the average employee (office worker) due to phishing scams. The range of hours is less than 1 to more than 25 hours per employee each year. We estimate the productivity losses based on hours spent each year by employees/users viewing and possibly responding to phishing emails. As shown, each employee wastes an average of 7 hours annually due to phishing scams, an increase from 4 hours in 2015.

**Figure 2. Estimated hours per employee each year spent dealing with phishing scams**
Extrapolated hours per year in FY 2021 = 6.83
Extrapolated hours per year in FY 2015 = 4.16




**As discussed, the costliest consequence of a successful phishing attack is employees' diminished productivity.** Table 3 reports the calculus used to estimate the productivity losses. Here we assume an average-sized organization with a headcount of 9,567 individuals with user access to corporate email systems. Based on an average of 7 hours per employee we calculate 65,343 hours wasted because of phishing. Assuming an average labor rate of $49.5 for non-IT employees (users) we calculate a total productivity loss of $3.2 million annually, an increase from $1.8 million in 2015.

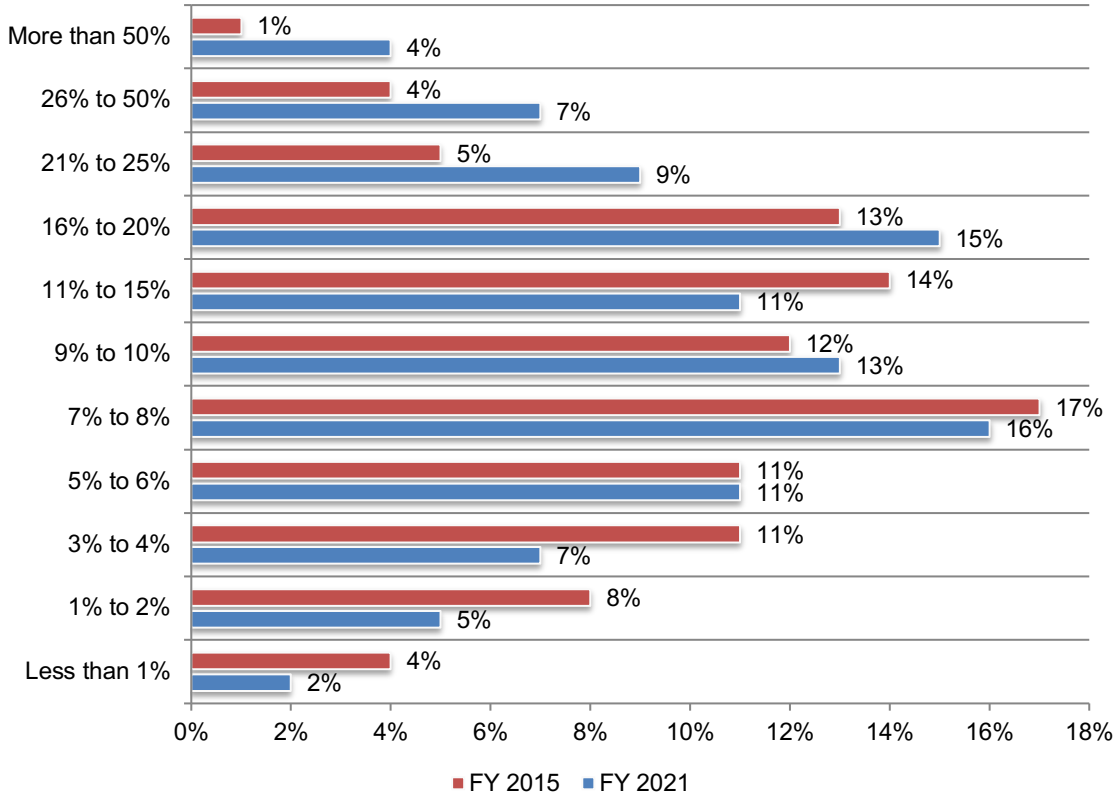
| **Table 3. Employee/user productivity losses** | Calculus FY 2015 | Calculus FY 2021 |
|---|---|---|
| Extrapolated hours per employee each year | 4.16 | 6.83 |
| Average organization headcount (see Part 3) | 9,552 | 9,567 |
| Extrapolated hours per organization each year | 39,736 | 65,343 |
| Fully loaded average hourly rate for non-IT users* | $45.80 | $49.50 |
| Total productivity loss per year for the average-sized organization | $1,819,923 | $3,234,459 |

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

**The cost of malware and malware not contained**

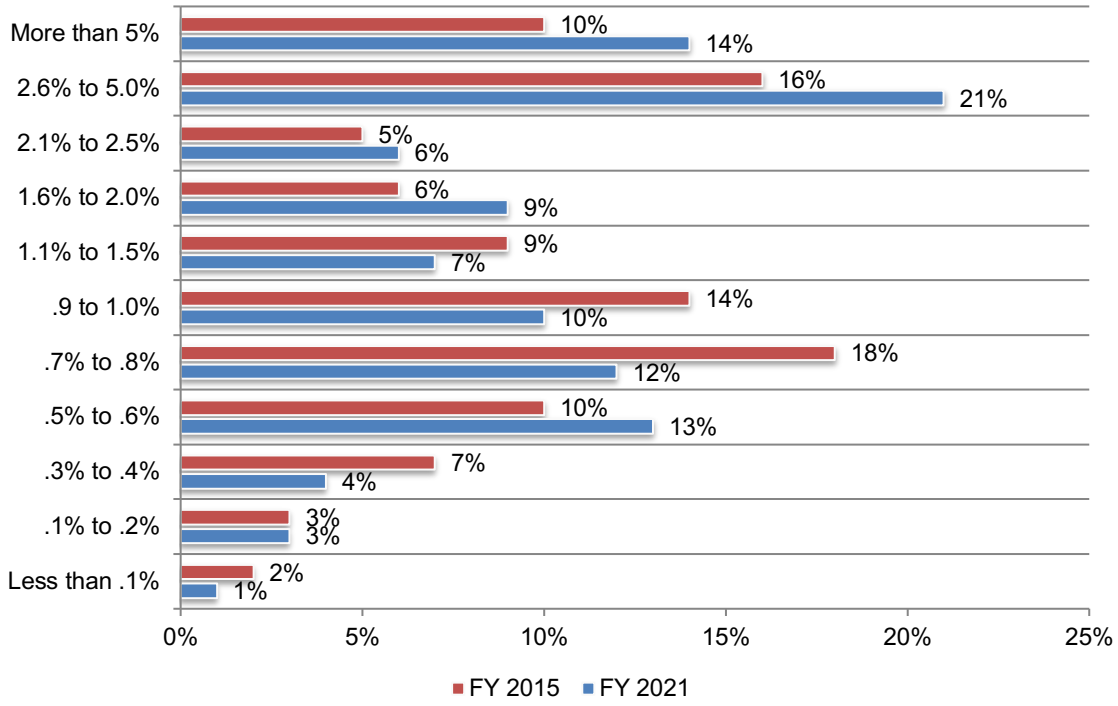
**An average of 15 percent of an organization's malware infections are caused by phishing scams.** Respondents were asked to estimate the percentage of malware infections caused by phishing scams. As shown in Figure 3, the estimated range is less than 1 percent to more than 50 percent. The extrapolated average rate is 15 percent. As discussed above, the cost to contain malware is estimated to be $353,582 (see Table 1).

**Figure 3. Percentage rate of malware infections caused by phishing scams**
Extrapolated rate FY 2021 = 15%
Extrapolated rate FY 2015 = 11%



**The likelihood of a malware attack causing a material data breach due to data exfiltration has increased since 2015.** 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 4, the probability distribution ranged from less than .1 percent to more than 5 percent. The extrapolated average likelihood of occurrence is 2.3 percent over a 12-month period, an increase from 1.9 percent.

**Figure 4. Likelihood of data exfiltration caused by a malware attack (over 12 months)**
Extrapolated likelihood of occurrence in FY 2021 = 2.3%
Extrapolated likelihood of occurrence in FY 2015 = 1.9%



**The total cost attributable to malware attacks caused by phishing scams more than doubles.** Table 3 reports the expected cost of malware attacks relating to data exfiltration at $3.2 million and disruptions to IT and business processes at $2.2 million. The total cost to resolve malware attacks is $807,506 in 2021, an increase from $338,098 in 2015.

| **Table 3. The expected cost of malware attacks** | Calculus FY 2015 | Calculus FY 2021 |
|---|---|---|
| Probable maximum loss resulting from data exfiltration | $105,900,000 | $137,170,000 |
| Likelihood of occurrence over the next 12 months | 1.9% | 2.3% |
| Expected value | $2,012,100 | $3,154,910 |
| | | |
| Probable maximum loss resulting from business disruptions (including denial of services, damage to IT infrastructure and revenue losses) | $66,345,000 | $117,300,000 |
| Likelihood of occurrence over the next 12 months | 1.6% | 2.1% |
| Expected value | $1,061,520 | $2,157,630 |
| | | |
| Percentage rate of malware infections caused by phishing scams (see Figure 3) | 11.0% | 15.2% |
| Average cost of malware attacks | $338,098 | $807,506 |

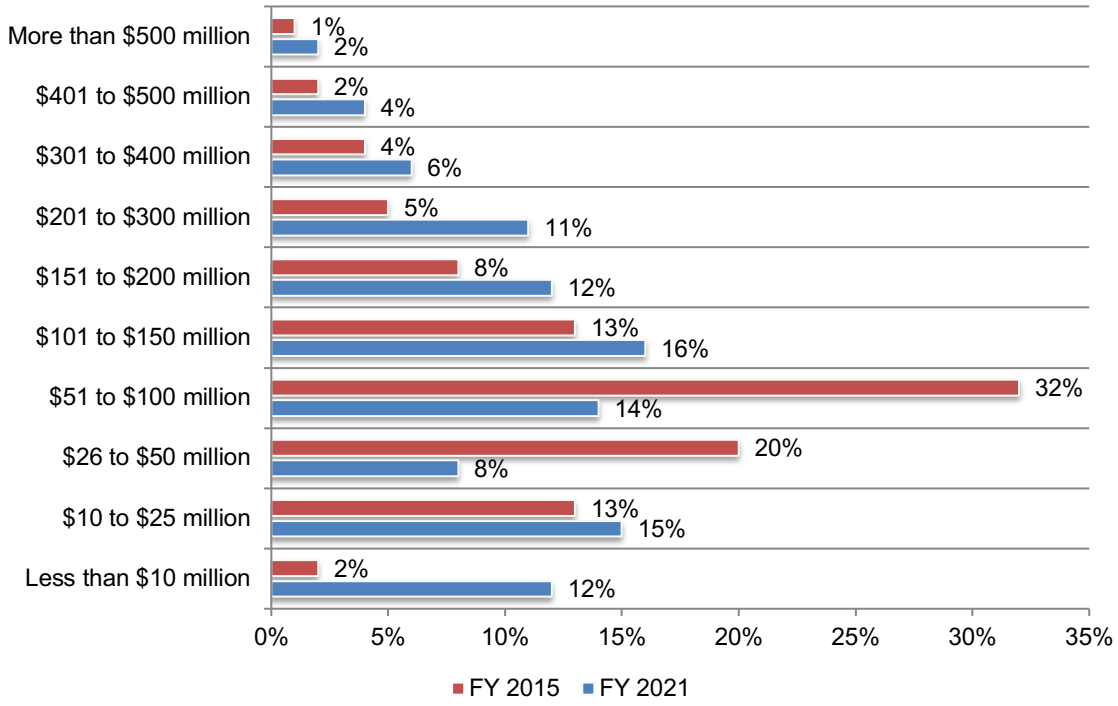
**Phishing costs due to the inability to contain malware have more than doubled (see Table 1) and represents 11 percent of the total cost of phishing.** Malware **not contained** is malware at the device level that has evaded traditional defenses such as firewalls, anti-malware software and intrusion prevention systems. Following are two attacks caused by an active malware attack that are difficult to contain: (1) data exfiltration (a.k.a. material data breach) and (2) business disruptions. The total cost of malware not contained has increased from $3.1 million to $5.3 million.

**A malware attack resulting in a data breach due to data exfiltration could cost an organization an average of $137.2 million.** The following formula is used to determine the probable maximum loss (PML) and the likelihood of such an attack:

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 an active malware attack.[1] Figure 5 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 $137.2 million, an increase from $105.9 million in 2015.

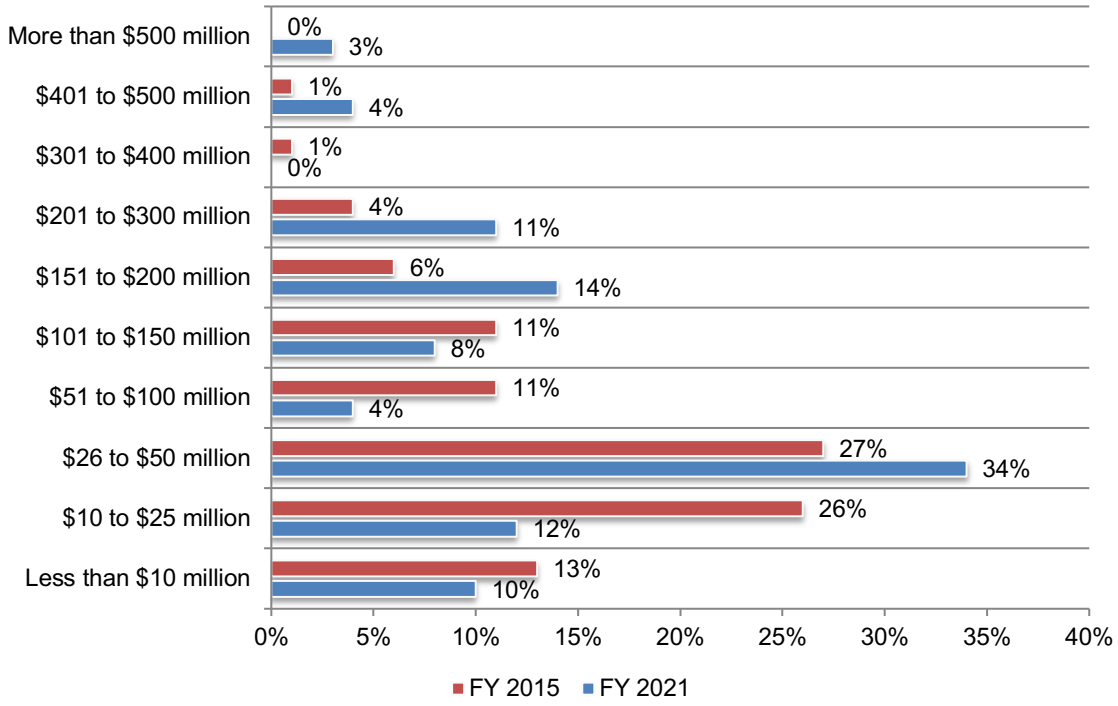
**Figure 5. Maximum loss resulting from data exfiltration caused by a malware attack**
Extrapolated PML FY 2021 = $137.2 million
Extrapolated PML FY 2015 = $105.9 million




[1]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.

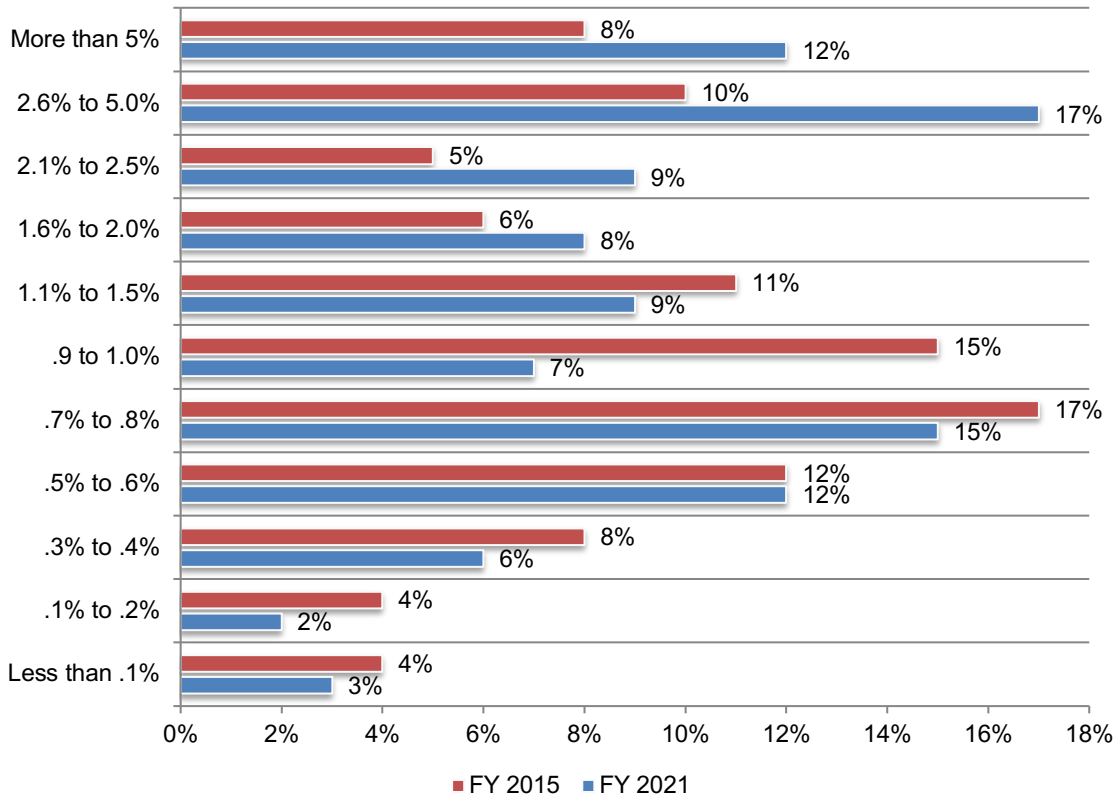
**What is the cost of business disruption due to a malware attack?** Respondents were asked to estimate the PML resulting from business disruptions caused by a malware attack. Business disruptions include denial of services, damage to IT infrastructure and revenue losses. Figure 6 shows the distribution of maximum losses ranging from less than $10 million to $500 million. The extrapolated average PML resulting from data exfiltration is $117.3 million, an increase from $66.3 million.

**Figure 6. Maximum loss resulting from business disruptions caused by a malware attack**
Extrapolated PML in FY 2021 = $117.3 million
Extrapolated PML in FY 2015 = $ 66.3 million



**How likely are business disruptions caused by a malware attack will affect your organization?** Respondents were asked to estimate the likelihood of material business disruptions caused by 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 2.1 percent over a 12-month period, an increase from 1.6 percent in 2015.

**Figure 7. Likelihood of business disruption caused by a malware attack (over 12 months)**
Extrapolated likelihood of occurrence in FY 2021 = 2.1%
Extrapolated likelihood of occurrence in FY 2015 = 1.6%

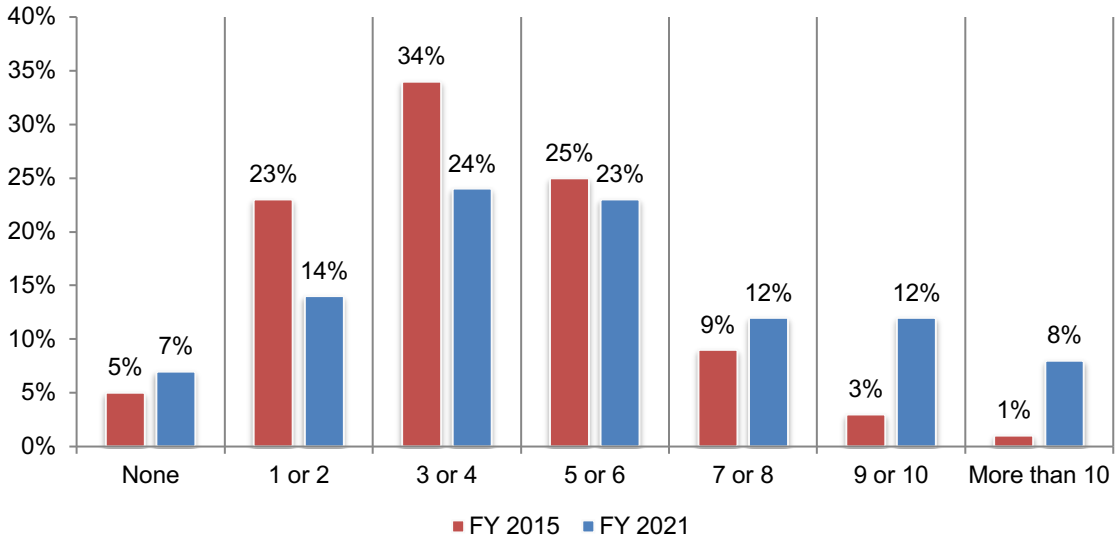


**Cost to contain credential compromises**

**Credential compromises increase (see Table 1) and represent 10 percent of the total cost of phishing. As a result, organizations are spending more to respond to these attacks.** The cost to contain credential compromises increased from $381,920 in 2015 to $692,531 in 2021. The costs are based on what organizations incurred to contain credential compromises that originated from a successful phishing attack, including the theft of cryptographic keys and certificates. The first step in this analysis is to estimate the total number of compromises expected to occur over the next 12 months.

Figure 8 shows the distribution of credential compromises caused by phishing scams estimated over the past 12-month period. The range of responses includes zero to more than 10 incidents. The extrapolated average is 5.3 compromises that originated from phishing.

**Figure 8. Distribution of credential compromises caused by phishing scams**
Extrapolated compromises per year in FY 2021 = 5.32
Extrapolated compromises per year in FY 2015 = 4.00

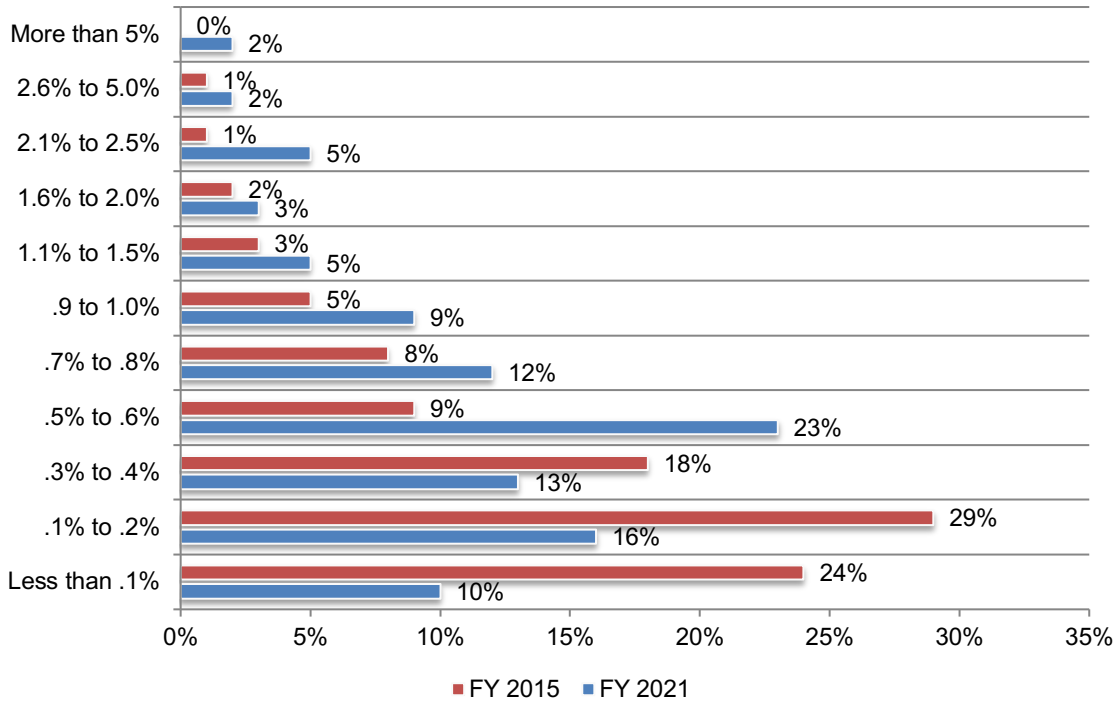


Based on an earlier study on the cost of key or credential compromise, we estimate a total of 2,050 hours of tech time investigating and responding to one compromise or 10,906 hours estimated over the next 12 months.[2] Assuming an average annual rate of $63.50 for tech support, we estimate a total annual cost of $692,531, an increase from $381,920 in 2015 ($62).

| **Table 5. Cost of credential compromises caused by phishing** | Calculus FY 2015 | Calculus FY 2021 |
|---|---|---|
| Estimated number of credential compromises over the next 12 months | 4.0 | 5.32 |
| Tech time investigating and responding to one compromise | 1,540 | 2,050 |
| Tech time investigating and responding to all compromise per year | 6,160 | 10,906 |
| Fully loaded average hourly rate ($) for IT security ops* | $62 | $63.50 |
| Total cost of tech time | $381,920 | $692,531 |

**Organizations are more likely in 2021 than in 2015 to have a data breach due to credential compromises.** 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 .81 percent over a 12-month period, an increase from .40 percent in 2015.

**Figure 10. Likelihood of data exfiltration caused by credential compromises (over 12 months)**
Extrapolated likelihood of occurrence in FY 2021 = .81%
Extrapolated likelihood of occurrence in FY 2015 = .40%




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

Respondents were asked to estimate the likelihood of material business disruption caused by credential compromises not contained. Figure 11 shows the probability distribution ranging from less than .1 percent to 5 percent. The extrapolated average likelihood of occurrence is 1.42 percent over a 12-month period, an increase from .9 percent.

**Figure 11. Likelihood of business disruptions caused by credential compromises not contained (12 months)**
Extrapolated likelihood of occurrence in FY 2021 = 1.42%
Extrapolated likelihood of occurrence in FY 2015 = 0.9%

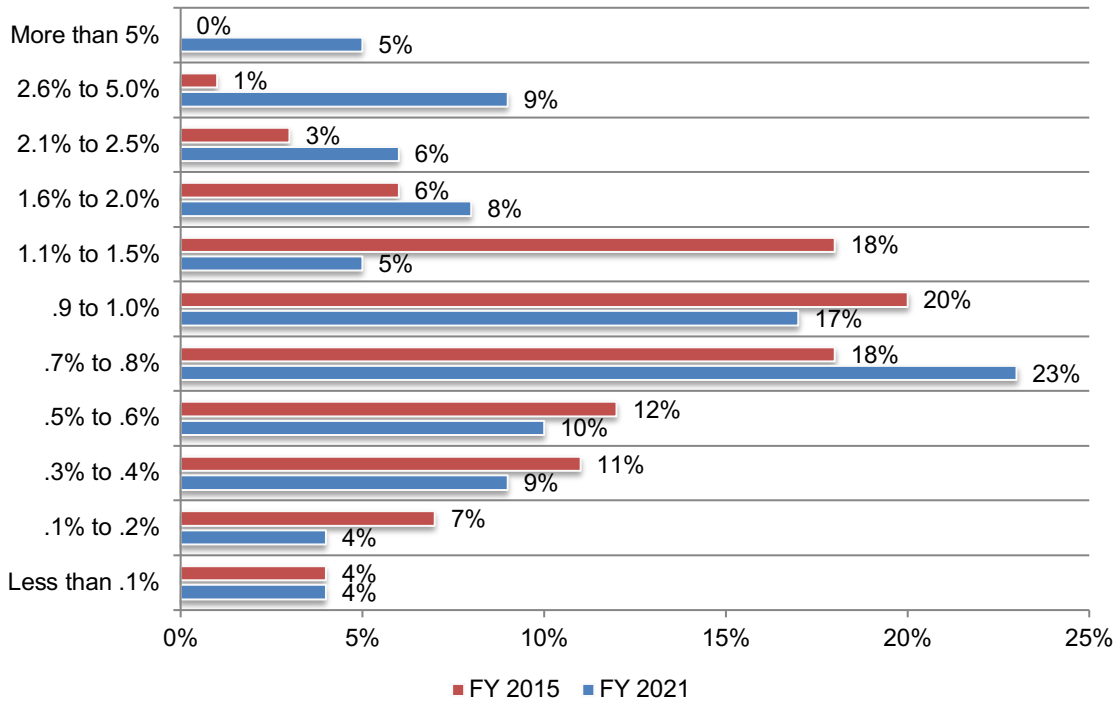



Table 6 reports the expected cost relating to data exfiltration is $1,111,077 and disruptions to IT and business processes is $1,665,660, which originated from credential compromises not contained. The total cost of credential compromised not contained is $2,076,737 and has increased significantly since 2015.

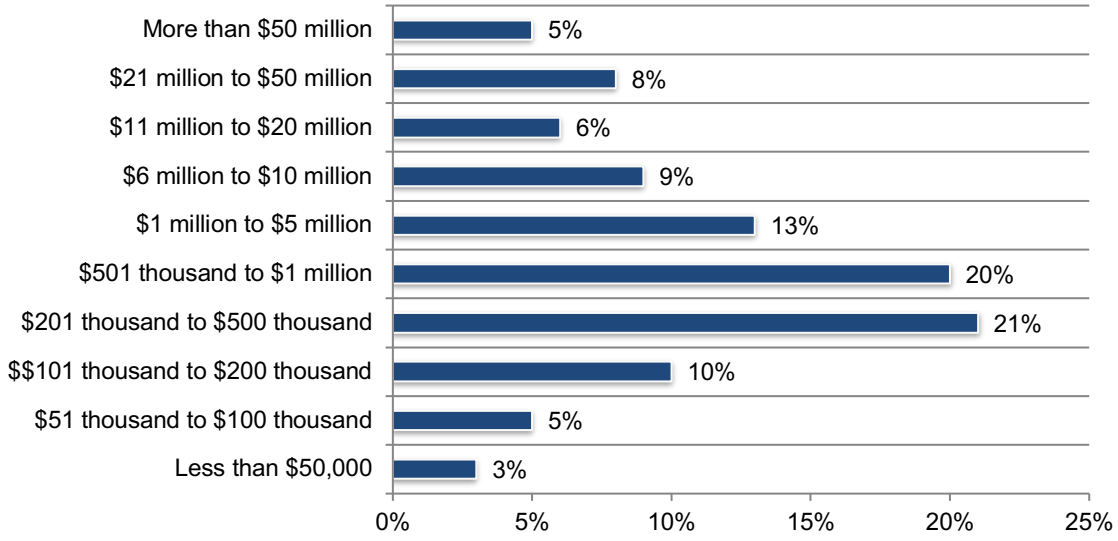
| **Table 6. The cost of credential compromises not contained** | Calculus FY 2015 | Calculus FY 2021 |
|---|---|---|
| Probable maximum loss resulting from data exfiltration | $105,900,000 | $137,170,000 |
| Likelihood of occurrence over the next 12 months | .4% | 0.81% |
| Expected value | $423,600 | $1,111,077 |
| | | |
| Probable maximum loss resulting from business disruptions (including denial of services, damage to IT infrastructure and revenue losses) | $66,345,000 | $117,300,000 |
| Likelihood of occurrence over the next 12 months | .9% | 1.42% |
| Expected value | $597,105 | $1,665,660 |
| | | |
| Total cost of credential compromises not contained | $1,020,705 | $2,776,737 |

**Business email compromises (BEC) and ransomware**

BEC is a security exploit in which the attacker targets an employee who has access to company funds or data. The attacker convinces the victim to transfer data or money to the attacker. For the first time in this research, we study the cost consequences of such attacks.

Respondents in our survey were asked to estimate the maximum loss resulting from a successful BEC attack. Figure 12 shows the distribution of maximum losses ranging from less than $50,000 to more than $50 million. The extrapolated average maximum loss resulting from a BEC attack is $8.12 million.

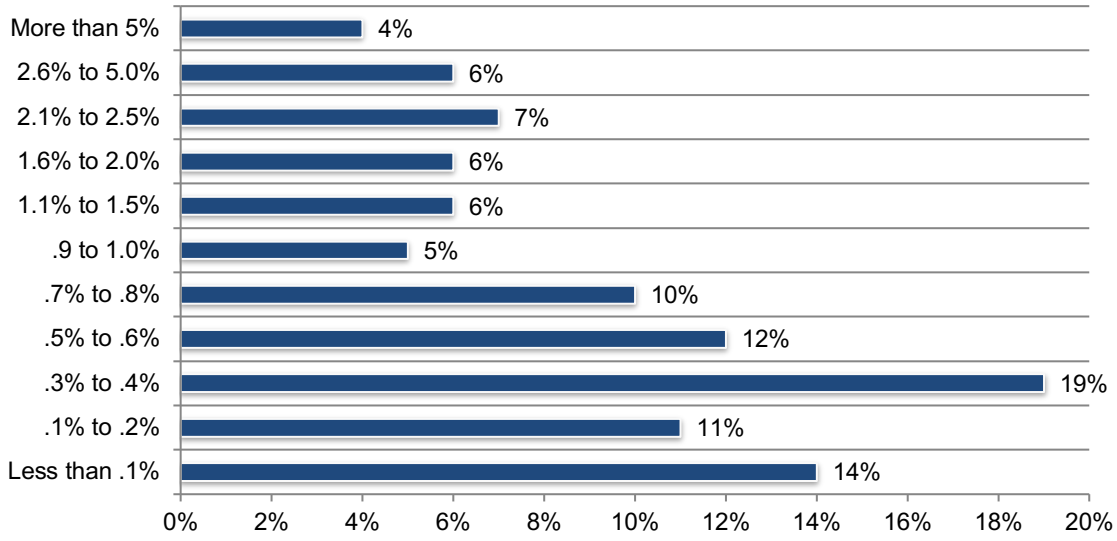
**Figure 12. Maximum loss resulting from a successful BEC attack**
Extrapolated PML in FY 2021 = $8.12 million



**What is the likelihood of a catastrophic BEC attack within the next 12 months?** In the context of this research a catastrophic BEC attack is so severe that it impacts the ability to operate as a growing concern even though, as shown in Figure 14, the likelihood of such an attack is low.

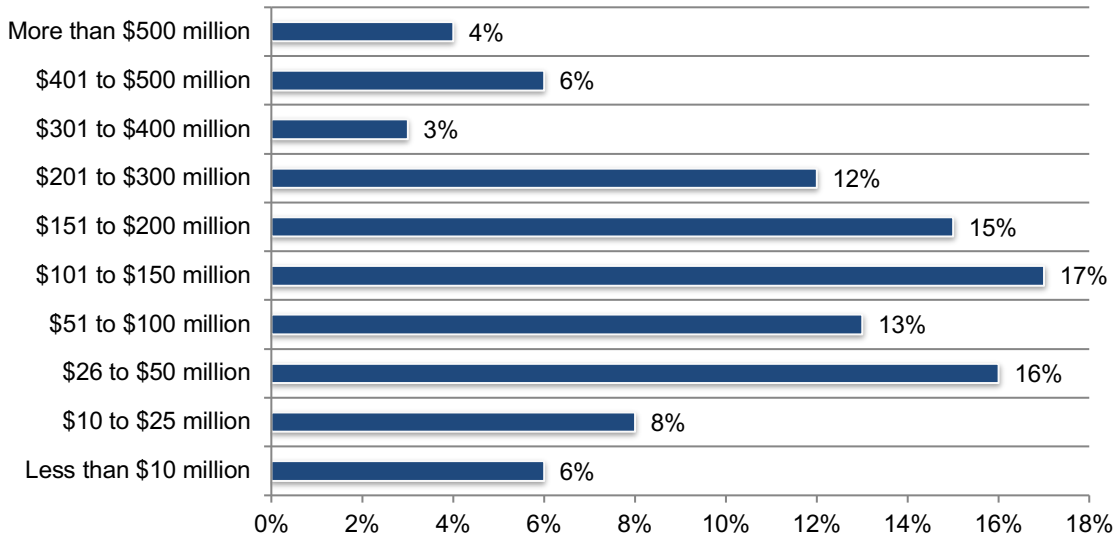
Respondents were asked to estimate the likelihood of such an attack occurring. According to Figure 13, the probability distribution ranging from less than .1 percent to more than 5 percent. The extrapolated average likelihood of occurrence is 1.09 percent over a 12-month period.

**Figure 13. Likelihood of a catastrophic BEC attack within the next 12 months**
Extrapolated likelihood of occurrence in FY 2021 = 1.09%



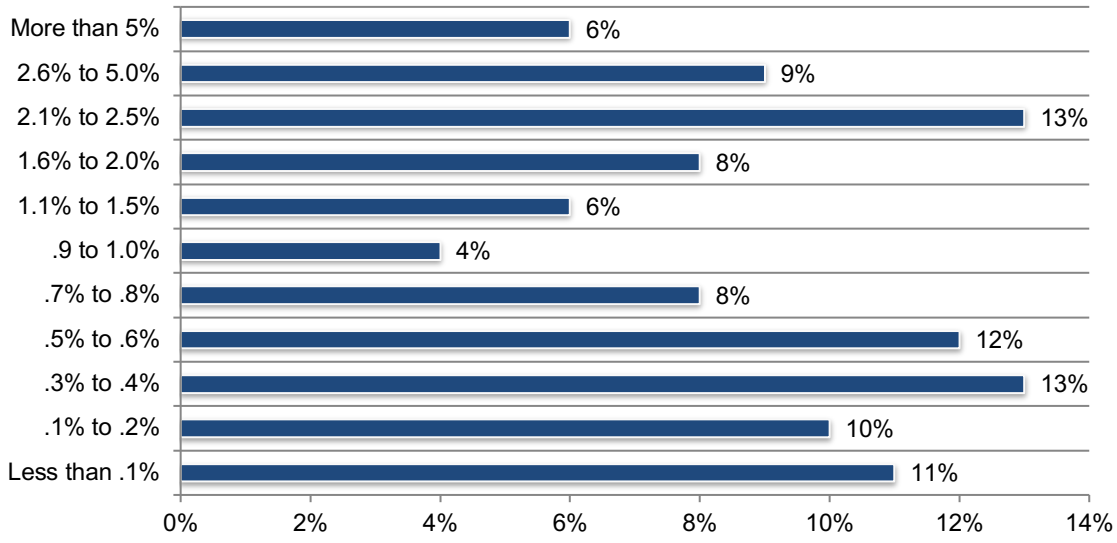
**What is the cost of business disruption caused by a BEC attack?** Respondents were asked to estimate the PML resulting from business disruptions caused by a BEC attack. Business disruptions include denial of services, damage to IT infrastructure and revenue losses. Figure 14 shows the distribution of maximum losses ranging from less than $10 million to more than $500 million. The extrapolated average PML resulting from business disruptions is $157 million.

**Figure 14. Maximum loss resulting from material disruptions caused by BEC**
Extrapolated PML in FY 2021 = $157 million




**How likely are business disruptions caused by BEC?** Respondents were asked to estimate the likelihood of material business disruptions caused by BEC. As shown in Figure 15, shows the probability distribution ranging from less than .1 percent to more than 5 percent. The extrapolated average likelihood of occurrence in 2021 is 1.45 percent.

**Figure 15. Likelihood of a business disruption caused by BEC**
Extrapolated likelihood of occurrence in FY 2021 = 1.45%



**Organizations transferred an average of $1.17 million to BEC attackers in the past 12 months.** Figure 16 shows the distribution of funds transferred to attackers from less than $50,000 to more than $5 million. An average of $1.17 million was transferred in the past year.

**Figure 16. Funds transferred to attackers due to BEC in the past year**
Extrapolated funds transferred = $1.17 million

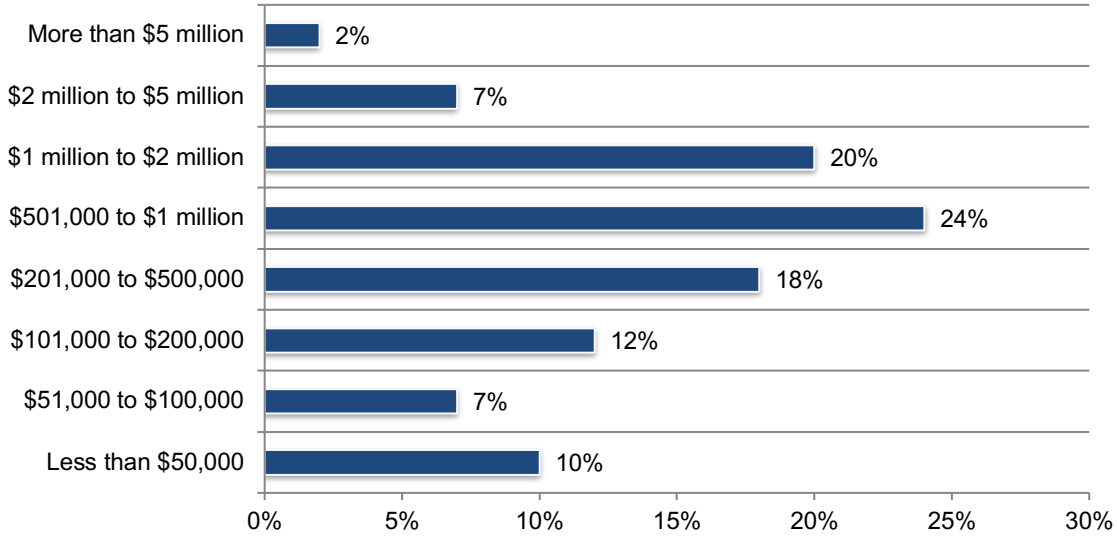


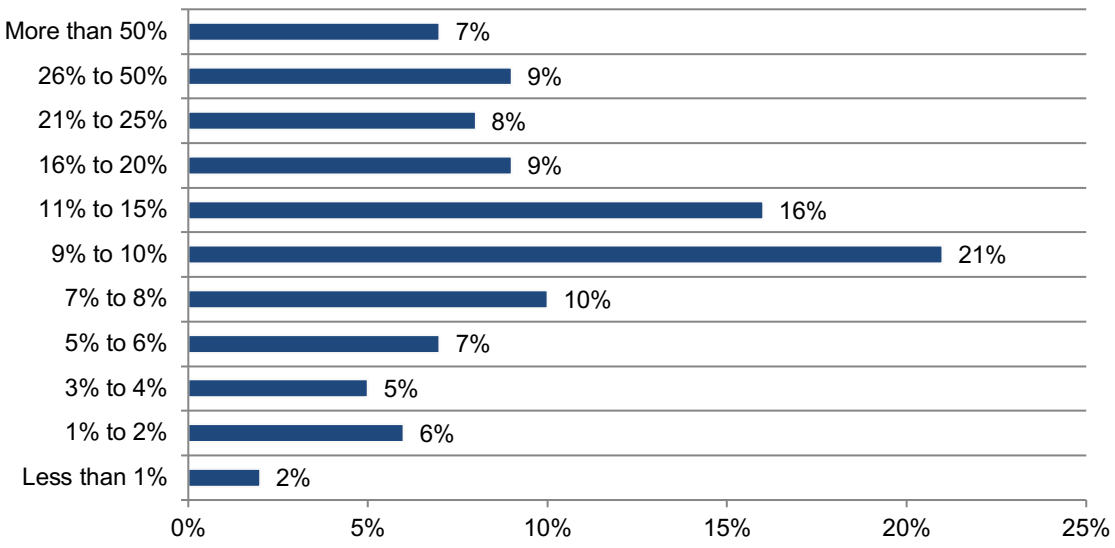
Table 7 presents the factors that determine the total cost of business email compromise.

| **Table 7. The total cost of BEC** | Calculus FY2021 |
|---|---|
| Probable maximum loss resulting from data exfiltration | $8,120,000 |
| Likelihood of occurrence over the next 12 months | 1.09% |
| Expected value | $88,508 |
| | |
| Probable maximum loss resulting from business disruptions caused by business email compromise | $157,000,000 |
| Likelihood of occurrence over the next 12 months | 1.45% |
| Expected value | $2,276,500 |
| | |
| Costs to contain BEC (38,276 hours x $63.5 IT hourly wage) | $2,430,526 |
| | |
| Cost of funds transferred in BEC attacks (Figure 17) | $1,170,000 |
| | |
| Total cost of business email compromise from phishing | $5,965,534 |

**Ransomware**

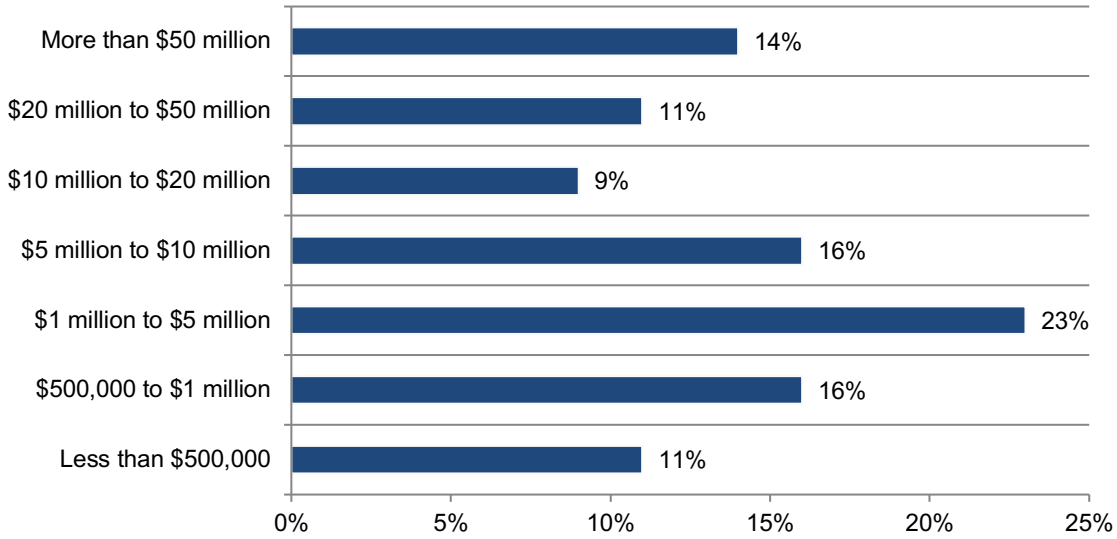
Ransomware is a sophisticated piece of malware that blocks the victim's access to his/her files. As shown in Figure 17, the average percentage rate of ransomware experienced from phishing by organizations is 17.6 percent.

**Figure 17. Percentage rate of ransomware from phishing**
Extrapolated value = 17.6%



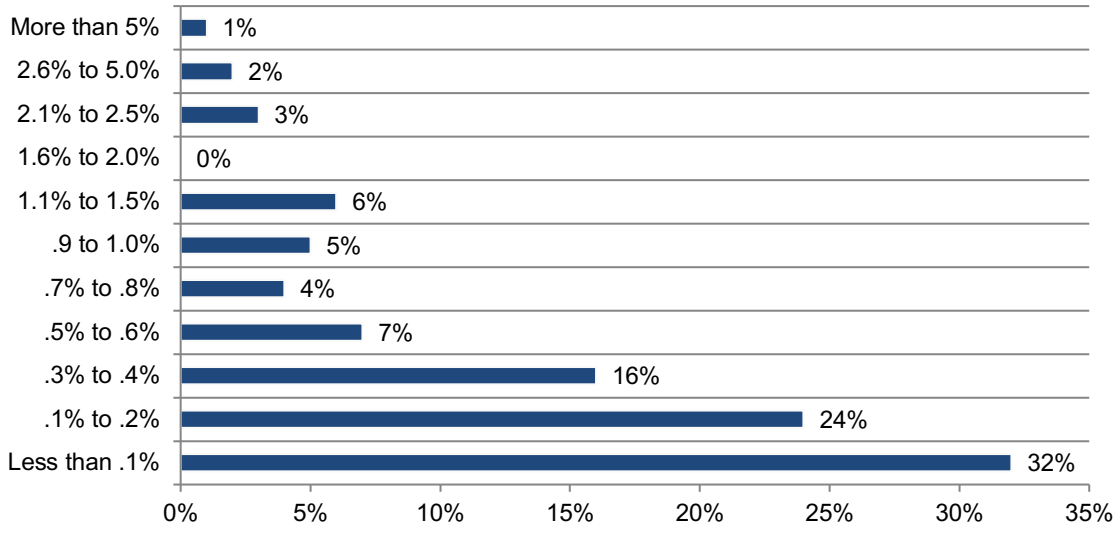
Respondents in our survey were asked to estimate the PML resulting from a successful ransomware attack. Figure 18 shows the distribution of maximum losses ranging from less than $500,000 to more than $50 million. The extrapolated average PML resulting from ransomware is $15.64 million.

**Figure 18. Maximum loss resulting from a material and successful ransomware attack**
Extrapolated PML in FY 2021 = $15.64 million



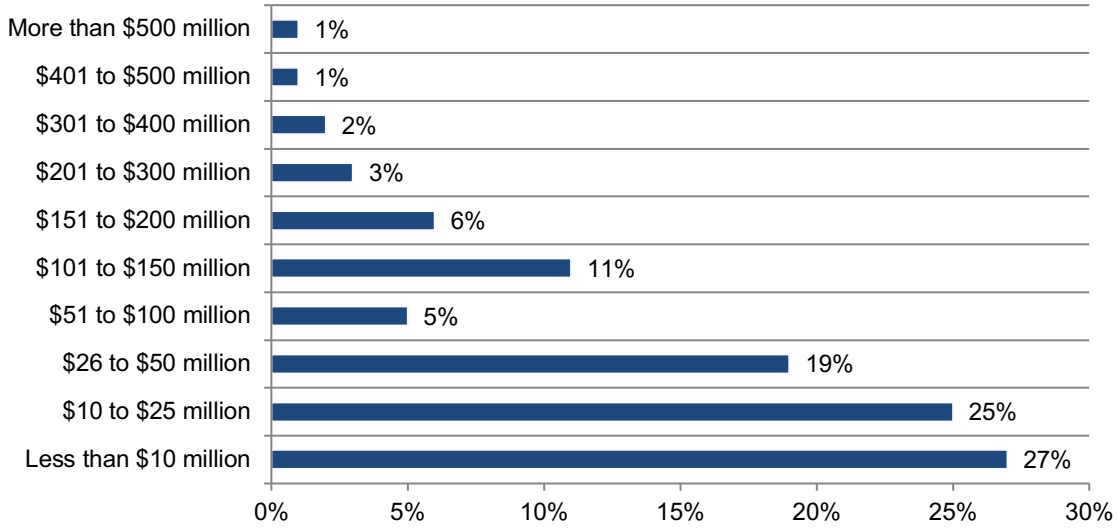

**What is the likelihood of a ransomware attack in the next 12 months?** Respondents were asked to estimate the likelihood of this occurring. According to Figure 19, the probability distribution ranges from less than 1 percent to more than 5 percent. The average likelihood of such an attack is 3 percent.

**Figure 19. Likelihood of a catastrophic ransomware attack in the next 12 months**
Extrapolated likelihood of occurrence in FY 2021 = 3.0%



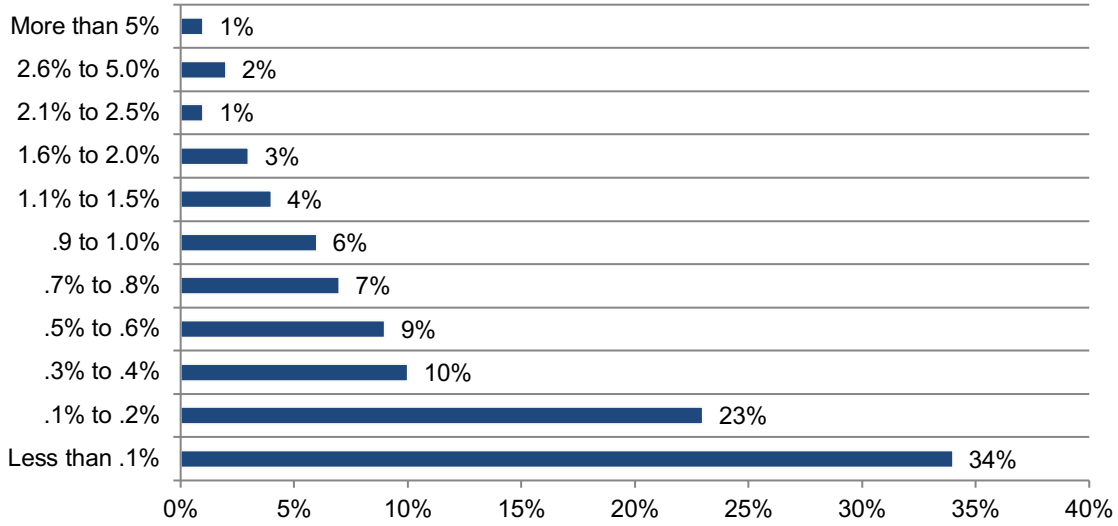
**What is the cost of business disruption due to ransomware?** Respondents were asked to estimate the PML resulting from business disruptions caused by ransomware. Business disruptions include denial of services, damage to IT infrastructure and revenue losses. Figure 20 shows the distribution of maximum losses ranging from less than $10 million to more than $500 million. The average PML resulting from ransomware is $67.5 million.

**Figure 20. Maximum loss resulting from business disruptions caused by ransomware**
Extrapolated PML in FY 2021 = $67.5 million



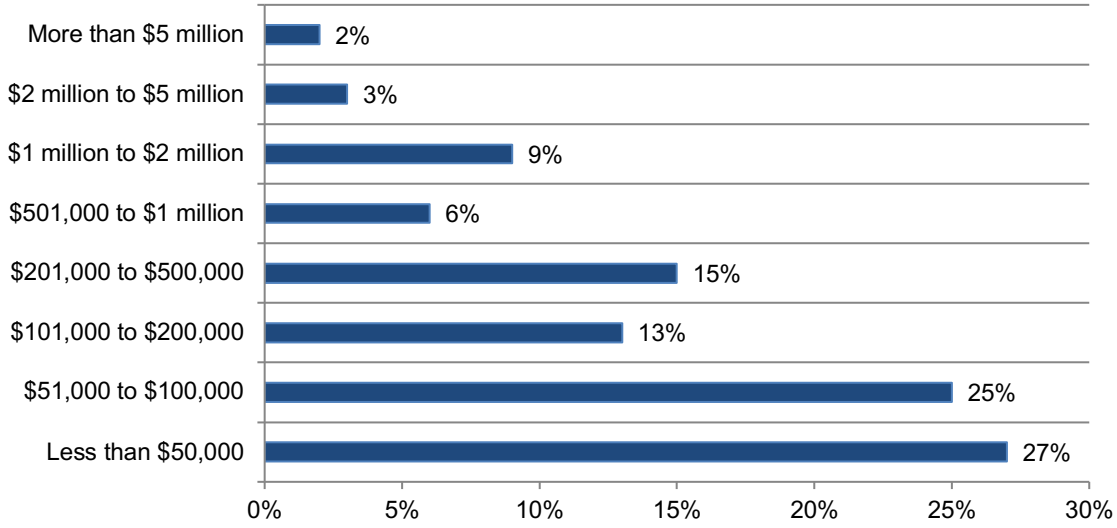

**How likely are business disruptions due to ransomware?** Respondents were asked to estimate the likelihood of material disruptions caused by ransomware. Figure 21 shows the probability distribution ranging from less than 1 percent to more than 5 percent. The average likelihood of occurrence in the next 12 months is 3.2 percent.

**Figure 21. Likelihood of material business disruptions caused by ransomware in the next 12 months**
Extrapolated likelihood of occurrence in FY 2021 = 3.2%



**Ransomware cost organizations $790,000 in the past year.** As shown in Figure 23, organizations paid an average of $790,000 in funds transferred directly to attackers in ransomware attacks.

**Figure 22. Cost of funds transferred in ransomware attacks**
Extrapolated funds transferred in FY 2021 = $790,000



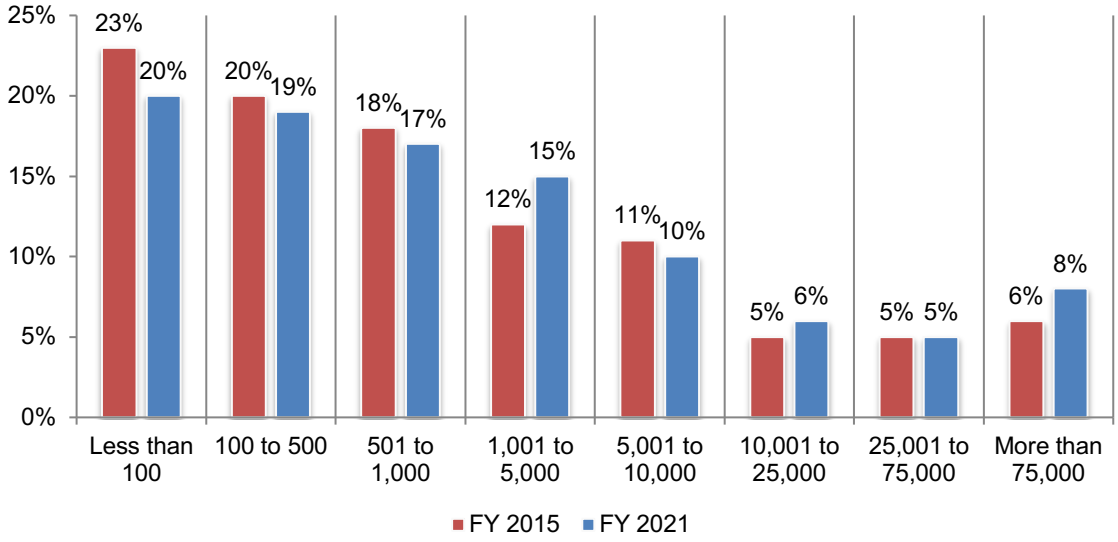

**The total cost of ransomware can be as high as $5.66 million.** As shown in Table 8, the expected value of the PML resulting from business disruptions caused by ransomware is $67.5 million. The average total cost of ransomware caused by phishing is $996 thousand for the current year.

| **Table 8. The cost of ransomware** | Calculus FY2021 |
|---|---|
| Probable maximum loss resulting from ransomware (US $millions) | $15.64 |
| Likelihood of occurrence over the next 12 months | 3.00% |
| Expected value (US$ millions) | $470,000 |
| | |
| Probable maximum loss resulting from business disruptions caused by ransomware (US$ millions) | $67.50 |
| Likelihood of occurrence over the next 12 months | 3.20% |
| Expected value (US$ millions) | $2.16 |
| | |
| Costs to contain Ransomware (35,285 hours x $63.5 IT hourly wage) | $2,240,598 |
| | |
| Cost of funds transferred in ransomware attacks ($US) | $790,000 |
| | |
| Total cost of ransomware (US$ millions) | $5.66 |
| Percentage rate of ransomware caused by phishing scams (Figure 18) | 17.6% |
| | |
| Total cost of ransomware (US$ millions) | $996,265 |

## Part 4. Demographics and methods

**Headcount in organizations represented in this study ranges from less than 100 to more** employees with access to corporate email systems. In this study, headcount is used as a surrogate for organizational size. The extrapolated average headcount in 2021 is 9,567 users with email access, as shown in Figure 23.

**Figure 23. Average headcount of employees with access to corporate email**
Extrapolated headcount in FY 2021 = 9,567
Extrapolated headcount in FY 2015 = 9,552

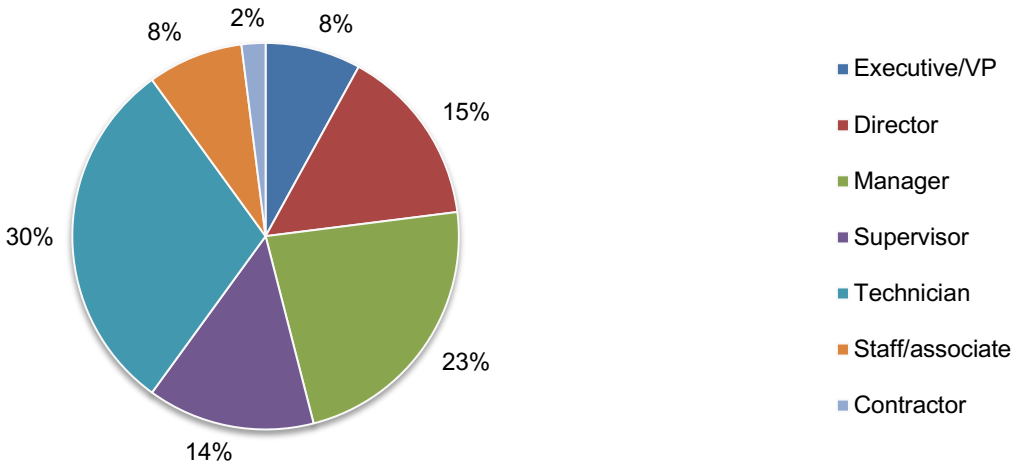



Our sampling frame is composed of 14,550 IT and IT security practitioners located in the United States, whose job involves the protection of sensitive or confidential information. As shown in Table 9, 641 respondents completed the survey. Screening removed 50 surveys. The final sample was 591 surveys (or a 4.1 percent response rate).

| **Table 9. Sample response** | FY 2015 | FY 2021 |
|---|---|---|
| Total sampling frame | 12,442 | 14,550 |
| Total survey returns | 415 | 641 |
| Rejected surveys | 38 | 50 |
| Final sample | 377 | 591 |
| Response rate | 3.0% | 4.1% |

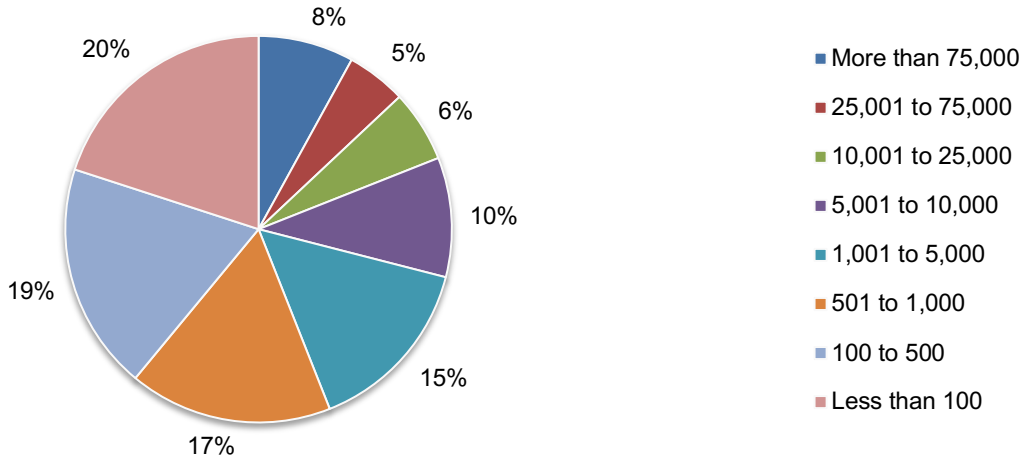
Pie Chart 2 reports the current position or organizational level of the respondents. Half of the respondents reported their current position as supervisory or above. The largest segment at 30 percent of respondents is the technician position.

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



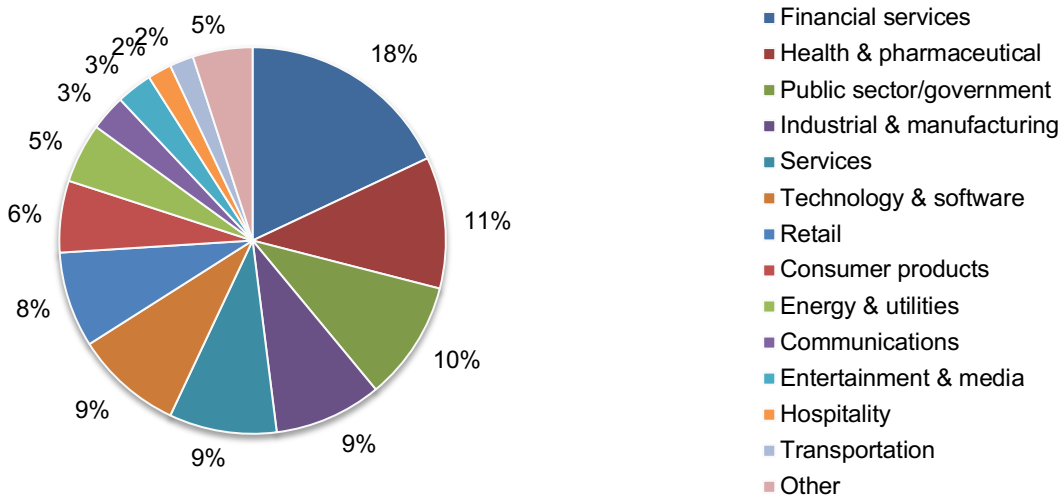

According to Pie Chart 3, 1,000 or more employees have access to corporate email systems according to 44 percent of the respondents. Fifty-six percent of respondents indicated up to 1,000 employees have access to corporate email systems.

**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 of respondents) as the largest segment, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by followed by health and pharmaceutical (11 percent of respondents), and public sector/government (10 percent of respondents). Industrial/manufacturer, services, and technology and software are each at 9 percent of respondents.

**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.

## Appendix: Detailed Survey Results

| Survey response | Freq |
|---|---|
| Total sampling frame | 14,550 |
| Total survey returns | 641 |
| Rejected surveys | 50 |
| Final sample | 591 |

**Part 1. Background**

| Q1. What best describes your current position level within the organization? | Pct% |
|---|---|
| Executive/VP | 8% |
| Director | 15% |
| Manager | 23% |
| Supervisor | 14% |
| Technician | 30% |
| Staff/associate | 8% |
| Contractor | 2% |
| Other (please specify) | 0% |
| Total | 100% |

| Q2. How many full-time employees have access to corporate email systems within your organization? Your best estimate is welcome. | Pct% |
|---|---|
| Less than 100 | 20% |
| 100 to 500 | 19% |
| 501 to 1,000 | 17% |
| 1,001 to 5,000 | 15% |
| 5,001 to 10,000 | 10% |
| 10,001 to 25,000 | 6% |
| 25,001 to 75,000 | 5% |
| More than 75,000 | 8% |
| Total | 100% |

| Q3. What best describes your organization's primary industry sector? Please select only one best choice. | Pct% |
|---|---|
| Agriculture & food services | 1% |
| Communications | 3% |
| Consumer products | 6% |
| Defense & aerospace | 1% |
| Energy & utilities | 5% |
| Entertainment & media | 3% |
| Financial services | 18% |
| Health & pharmaceutical | 11% |
| Hospitality | 2% |
| Industrial & manufacturing | 9% |
| Public sector/government | 10% |
| Retail | 8% |
| Services | 9% |
| Technology & software | 9% |
| Transportation | 2% |
| Other (please specify) | 3% |
| Total | 100% |

**Part 2. Cost of phishing and email-based threats**

Q4. The following table provides seven (7) cost categories of phishing and other email-based threats such as malware and ransomware. Please allocate all 100 points to provide the relative distribution of each cost category. Please keep in mind that the total points must equal 100.

| **Distribution of phishing-related cost categories** | Points |
|---|---|
| Productivity losses from phishing | 24 |
| Cost of credential compromises not contained | 20 |
| Cost of ransomware | 15 |
| Cost to contain credential compromise from phishing | 13 |
| Cost of business email compromise (a.k.a. email fraud) | 11 |
| Cost of malware not contained | 9 |
| Cost of malware containment | 8 |
| Total points (100 points) | 100 |

Q5. Following are six tasks to contain malware infections caused by email-based threats over a 12-month period. Please select the total hours the cybersecurity team spent dealing with each activity.

| **Q5a. Planning** | Pct% |
|---|---|
| Less than 10 hours | 4% |
| 10 to 50 hours | 8% |
| 51 to 100 hours | 15% |
| 101 to 250 hours | 27% |
| 251 to 500 hours | 17% |
| 501 to 1,000 hours | 13% |
| 1,001 to 2,500 hours | 5% |
| 2,501 to 5,000 hours | 3% |
| 5,001 to 10,000 hours | 5% |
| More than 10,000 hours | 3% |
| Total | 100% |

| **Q5b.Capturing intelligence** | Pct% |
|---|---|
| Less than 10 hours | 0% |
| 10 to 50 hours | 6% |
| 51 to 100 hours | 5% |
| 101 to 250 hours | 4% |
| 251 to 500 hours | 9% |
| 501 to 1,000 hours | 6% |
| 1,001 to 2,500 hours | 15% |
| 2,501 to 5,000 hours | 19% |
| 5,001 to 10,000 hours | 21% |
| More than 10,000 hours | 15% |
| Total | 100% |

| **Q5c. Evaluating intelligence** | Pct% |
|---|---|
| Less than 10 hours | 0% |
| 10 to 50 hours | 0% |
| 51 to 100 hours | 3% |
| 101 to 250 hours | 7% |
| 251 to 500 hours | 8% |
| 501 to 1,000 hours | 15% |
| 1,001 to 2,500 hours | 15% |
| 2,501 to 5,000 hours | 21% |
| 5,001 to 10,000 hours | 21% |
| More than 10,000 hours | 10% |
| Total | 100% |

| Q5d. Investigating | Pct% |
|---|---|
| Less than 10 hours | 0% |
| 10 to 50 hours | 0% |
| 51 to 100 hours | 0% |
| 101 to 250 hours | 0% |
| 251 to 500 hours | 6% |
| 501 to 1,000 hours | 6% |
| 1,001 to 2,500 hours | 3% |
| 2,501 to 5,000 hours | 0% |
| 5,001 to 10,000 hours | 11% |
| More than 10,000 hours | 74% |
| Total | 100% |

| Q5e. Cleaning & fixing | Pct% |
|---|---|
| Less than 10 hours | 0% |
| 10 to 50 hours | 1% |
| 51 to 100 hours | 0% |
| 101 to 250 hours | 0% |
| 251 to 500 hours | 0% |
| 501 to 1,000 hours | 0% |
| 1,001 to 2,500 hours | 3% |
| 2,501 to 5,000 hours | 3% |
| 5,001 to 10,000 hours | 12% |
| More than 10,000 hours | 81% |
| Total | 100% |

| Q5f. Documenting | Pct% |
|---|---|
| Less than 10 hours | 9% |
| 10 to 50 hours | 6% |
| 51 to 100 hours | 9% |
| 101 to 250 hours | 10% |
| 251 to 500 hours | 13% |
| 501 to 1,000 hours | 18% |
| 1,001 to 2,500 hours | 23% |
| 2,501 to 5,000 hours | 9% |
| 5,001 to 10,000 hours | 0% |
| More than 10,000 hours | 0% |
| Total | 97% |

| Q6. What is the percentage rate of malware infections caused by phishing or email-based threats? Your best estimate is welcome. | Pct% |
|---|---|
| More than 50% | 4% |
| 26% to 50% | 7% |
| 21% to 25% | 9% |
| 16% to 20% | 15% |
| 11% to 15% | 11% |
| 9% to 10% | 13% |
| 7% to 8% | 16% |
| 5% to 6% | 11% |
| 3% to 4% | 7% |
| 1% to 2% | 5% |
| Less than 1% | 2% |
| Total | 100% |

| Q7. What best describes the **maximum loss** that could be realized by your organization as a result of a catastrophic data exfiltration event caused by malware? Your best estimate is welcome. | Pct% |
|---|---|
| More than $500 million | 2% |
| $401 to $500 million | 4% |
| $301 to $400 million | 6% |
| $201 to $300 million | 11% |
| $151 to $200 million | 12% |
| $101 to $150 million | 16% |
| $51 to $100 million | 14% |
| $26 to $50 million | 8% |
| $10 to $25 million | 15% |
| Less than $10 million | 12% |
| Total | 100% |

| Q8. What best describes the **Likelihood** of a catastrophic data exfiltration event caused by malware within the next 12 months? Your best estimate is welcome. | Pct% |
|---|---|
| More than 5% | 14% |
| 2.6% to 5.0% | 21% |
| 2.1% to 2.5% | 6% |
| 1.6% to 2.0% | 9% |
| 1.1% to 1.5% | 7% |
| .9 to 1.0% | 10% |
| .7% to .8% | 12% |
| .5% to .6% | 13% |
| .3% to .4% | 4% |
| .1% to .2% | 3% |
| Less than .1% | 1% |
| Total | 100% |
| | |
| Q9. What best describes the **maximum loss** that could be realized by your organization resulting from **material business disruptions** caused by malware? Your best estimate is welcome. | Pct% |
| More than $500 million | 3% |
| $401 to $500 million | 4% |
| $301 to $400 million | 0% |
| $201 to $300 million | 11% |
| $151 to $200 million | 14% |
| $101 to $150 million | 8% |
| $51 to $100 million | 4% |
| $26 to $50 million | 34% |
| $10 to $25 million | 12% |
| Less than $10 million | 10% |
| Total | 100% |
| | |
| Q10. What best describes the **Likelihood** of material business disruptions caused by malware within the next 12 months? Your best estimate is welcome. | Pct% |
| More than 5% | 12% |
| 2.6% to 5.0% | 17% |
| 2.1% to 2.5% | 9% |
| 1.6% to 2.0% | 8% |
| 1.1% to 1.5% | 9% |
| .9 to 1.0% | 7% |
| .7% to .8% | 15% |
| .5% to .6% | 12% |
| .3% to .4% | 6% |
| .1% to .2% | 2% |
| Less than .1% | 3% |
| Total | 100% |

| Q11. How many hours per employee each year are spent dealing with phishing or any email-based threat/fraud? Your best estimate is welcome. | Pct% |
|---|---|
| More than 25 hours | 2% |
| 21 to 25 hours | 3% |
| 16 to 20 hours | 1% |
| 11 to 15 hours | 7% |
| 9 to 10 hours | 21% |
| 7 to 8 hours | 16% |
| 5 to 6 hours | 10% |
| 3 to 4 hours | 15% |
| 1 to 2 hours | 5% |
| Less than 1 hour | 20% |
| Total | 100% |
| Extrapolated value | - |

| Q12. What best describes the number of credential compromises caused by phishing or other email-based threats over the past 12 months? Your best estimate is welcome. | Pct% |
|---|---|
| More than 10 | 8% |
| 9 or 10 | 12% |
| 7 or 8 | 12% |
| 5 or 6 | 23% |
| 3 or 4 | 24% |
| 1 or 2 | 14% |
| None | 7% |
| Total | 100% |

| Q13. What best describes the **Likelihood of data exfiltration** caused by credential compromises over the next 12 months? Your best estimate is welcome. | Pct% |
|---|---|
| More than 5% | 2% |
| 2.6% to 5.0% | 2% |
| 2.1% to 2.5% | 5% |
| 1.6% to 2.0% | 3% |
| 1.1% to 1.5% | 5% |
| .9 to 1.0% | 9% |
| .7% to .8% | 12% |
| .5% to .6% | 23% |
| .3% to .4% | 13% |
| .1% to .2% | 16% |
| Less than .1% | 10% |
| Total | 100% |

| Q14. What best describes the **Likelihood of material business disruptions** caused by credential compromises over the next 12 months? Your best estimate is welcome. | Pct% |
|---|---|
| More than 5% | 5% |
| 2.6% to 5.0% | 9% |
| 2.1% to 2.5% | 6% |
| 1.6% to 2.0% | 8% |
| 1.1% to 1.5% | 5% |
| .9 to 1.0% | 17% |
| .7% to .8% | 23% |
| .5% to .6% | 10% |
| .3% to .4% | 9% |
| .1% to .2% | 4% |
| Less than .1% | 4% |
| Total | 100% |

**Part 3. Business email compromise:** Business email compromise (BEC) is a security exploit in which the attacker targets an employee who has access to company funds or data. They convince the victim to transfer data or money to the attacker.

| **Recap: Six tasks to contain business email compromise (hours)** | Hours |
|---|---|
| Planning | 1,019 |
| Capturing intelligence | 4,450 |
| Evaluating intelligence | 5,001 |
| Investigating | 12,336 |
| Cleaning & fixing | 14,395 |
| Documenting | 1,075 |
| Total | 38,276 |

| **Recap: Six tasks to contain business email compromise (cost)*** | Amount |
|---|---|
| Planning | $ 64,707 |
| Capturing intelligence | $ 282,575 |
| Evaluating intelligence | $ 317,564 |
| Investigating | $ 783,336 |
| Cleaning & fixing | $ 914,083 |
| Documenting | $ 68,263 |
| Total | $ 2,430,526 |

**Fully loaded average hourly rate for IT security practitioners = $63.5.*

| Q15. Likelihood of a business disruption caused by BEC | Pct% |
|---|---|
| Less than .1% | 11% |
| .1 to .2% | 10% |
| .3 to .4% | 13% |
| .5% to .6% | 12% |
| .7% to .8% | 8% |
| .9 to 1.0% | 4% |
| 1.1% to 1.5% | 6% |
| 1.6% to 2.0% | 8% |
| 2.1% to 2.5% | 13% |
| 2.6% to 5.0% | 9% |
| More than 5% | 6% |
| Total | 100% |
| Extrapolated value | 1.45% |
| | |
| Q16. What best describes the actual funds transferred to an attacker by your organization due to business email compromise in the past year? Your best estimate is welcome. | Pct% |
| Less than $50,000 | 10% |
| $51,000 to $100,000 | 7% |
| $101,000 to $200,000 | 12% |
| $201,000 to $500,000 | 18% |
| $501,000 to $1 million | 24% |
| $1 million to $2 million | 20% |
| $2 million to $5 million | 7% |
| More than $5 million | 2% |
| Total | 100% |
| Extrapolated value (US$ millions) | $ 1.17 |
| | |

| Q17. Percentage decrease in the cost of phishing as a result of employee training interventions | Pct% |
|---|---|
| < 10% | 5% |
| 10 to 20% | 9% |
| 21 to 30% | 4% |
| 31 to 40% | 8% |
| 41 to 50% | 13% |
| 51 to 60% | 21% |
| 61 to 70% | 19% |
| 71 to 80% | 7% |
| 81 to 90% | 8% |
| 91 to 100% | 6% |
| Expected value | 53% |

**Part 4. Ransomware**

| Q18. What is the percentage rate of ransomware caused by email-based attacks? Your best estimate is welcome. | Pct% |
|---|---|
| Less than 1% | 2% |
| 1% to 2% | 6% |
| 3% to 4% | 5% |
| 5% to 6% | 7% |
| 7% to 8% | 10% |
| 9% to 10% | 21% |
| 11% to 15% | 16% |
| 16% to 20% | 9% |
| 21% to 25% | 8% |
| 26% to 50% | 9% |
| More than 50% | 7% |
| Total | 100% |
| Extrapolated value | 17.6% |

| Q19. What best describes the maximum loss that could be realized by your organization as a result of a successful ransomware attack. Your best estimate is welcome. | Pct% |
|---|---|
| Less than $500,000 | 11% |
| $500,000 to $1 million | 16% |
| $1 million to $5 million | 23% |
| $5 million to $10 million | 16% |
| $10 million to $20 million | 9% |
| $20 million to $50 million | 11% |
| More than $50 million | 14% |
| Total | 100% |

| Q20. What best describes the Likelihood of a catastrophic ransomware attack within the next 12 months? Your best estimate is welcome | Pct% |
|---|---|
| Less than .1% | 32% |
| .1% to .2% | 24% |
| .3% to .4% | 16% |
| .5% to .6% | 7% |
| .7% to .8% | 4% |
| .9 to 1.0% | 5% |
| 1.1% to 1.5% | 6% |
| 1.6% to 2.0% | 0% |
| 2.1% to 2.5% | 3% |
| 2.6% to 5.0% | 2% |
| More than 5% | 1% |
| Total | 100% |
| Extrapolated value | 3.2% |

| Q21. What best describes the maximum loss that could be realized by your organization resulting from material business disruptions caused by ransomware? Your best estimate is welcome. | Pct% |
|---|---|
| Less than $10 million | 27% |
| $10 to $25 million | 25% |
| $26 to $50 million | 19% |
| $51 to $100 million | 5% |
| $101 to $150 million | 11% |
| $151 to $200 million | 6% |
| $201 to $300 million | 3% |
| $301 to $400 million | 2% |
| $401 to $500 million | 1% |
| More than $500 million | 1% |
| Total | 100% |
| Extrapolated value (US$ millions) | $ 67.50 |

| Q22. What best describes the Likelihood of material business disruptions caused by ransomware within the next 12 months? Your best estimate is welcome | Pct% |
|---|---|
| Less than .1% | 34% |
| .1% to .2% | 23% |
| .3% to .4% | 10% |
| .5% to .6% | 9% |
| .7% to .8% | 7% |
| .9 to 1.0% | 6% |
| 1.1% to 1.5% | 4% |
| 1.6% to 2.0% | 3% |
| 2.1% to 2.5% | 1% |
| 2.6% to 5.0% | 2% |
| More than 5% | 1% |
| Total | 100% |
| Extrapolated value | 3.2% |

| Q23. What best describes the actual cost of ransom by your organization due to ransomware in the past year. Your best estimate is welcome. | Pct% |
|---|---|
| Less than $50,000 | 27% |
| $51,000 to $100,000 | 25% |
| $101,000 to $200,000 | 13% |
| $201,000 to $500,000 | 15% |
| $501,000 to $1 million | 6% |
| $1 million to $2 million | 9% |
| $2 million to $5 million | 3% |
| More than $5 million | 2% |
| Total | 100% |
| Extrapolated value (US$ millions) | $ 0.79 |

| **Table 8. The cost of ransomware** | Calculus FY2021 |
|---|---|
| Probable maximum loss resulting from ransomware (US $millions) | $15.64 |
| Likelihood of occurrence over the next 12 months | 3.00% |
| Expected value (US$ millions) | $470,000 |
| | |
| Probable maximum loss resulting from business disruptions caused by ransomware (US$ millions) | $67.50 |
| Likelihood of occurrence over the next 12 months | 3.20% |
| Expected value (US$ millions) | $2.16 |
| | |
| Costs to contain Ransomware (35,285 hours x $63.5 IT hourly wage) | $2,240,598 |
| | |
| Cost of funds transferred in ransomware attacks ($US) | $790,000 |
| | |
| Total cost of ransomware (US$ millions) | $5.66 |
| Percentage rate of ransomware caused by phishing scams (Figure 18) | 17.6% |
| | |
| Total cost of ransomware from phishing (US$ millions) | $996,265 |

## Ponemon Institute

***Advancing Responsible Information Management***

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.