# A Study of Retail Banks & DDoS Attacks

**Sponsored by Corero Network Security**

Independently conducted by Ponemon Institute LLC

Publication Date: December 2012

# A Study of Retail Banks & DDoS Attacks

Ponemon Institute, December 2012

## Part 1. Introduction

Sponsored by Corero Network Security, Ponemon Institute is pleased to present the results of *A Study of Retail Banks & DDos Attacks*. This study was conducted to determine how these attacks are affecting retail banks and what is being done to prevent and detect these threats. We surveyed 650 IT and IT security managers in banks ranging from local or community to large national banks. The majority of respondents (64 percent) are in organizations with more than 1,000 full-time employees.

In recent months, it has been widely reported that U.S. banks are falling victim to distributed denial of service (DDoS) attacks that flood websites with extraneous data that essentially overwhelms the ability to respond to legitimate inquiries.[1] These attacks have crippled the websites of money center banks including Bank of America and JP Morgan Chase and more are expected to occur. However, DDoS attacks are not limited to the large national banks. Smaller retail banking institutions that might not have the necessary defenses in place are expected to be targeted in the coming months. [2]

The most noteworthy findings include the following:

- **There is more confidence in the ability to detect than prevent DDoS attacks.** Although the majority of respondents do not believe they are effective in detecting and preventing DDoS attacks, there is more confidence in their ability to detect these attacks**.**

- **The majority of retail banks surveyed had a DDoS attack.** Sixty-four percent of respondents say their organization had a DDoS in the past 12 months. We estimate that on average the retail banks in this study had 2.8 such attacks in the past 12 months.

- **Diminished productivity of the bank’s IT staff is by far the worst consequence of a DDoS attack.** Respondents in this study are concerned about the time and effort required to respond to these attacks. This is followed by reputation damage, which is critical to maintaining the loyalty of customers and diminished productivity for end users.

- **Zero day attacks and denial of service attacks are considered the most severe security threats to retail banks.** The least severe is the loss or theft of employee computers and malicious insiders.

- **A lack of resources threatens retail banks’ ability to deal with DDoS attacks.** While there is no strong consensus about the most critical barrier to preventing DDoS attacks, insufficient personnel and in-house expertise and inadequate technologies seem to be the most serious concerns. These barriers are followed by insufficient budget.

- **Traditional firewalls and on-premises anti-DDoS technologies are the most popular to prevent and detect these attacks.** These are followed by intrusion detection and prevention and anti-virus technologies.

- **The threat of DDoS attacks is not improving.** Forty-three percent of respondents expect the attacks will either significantly increase or increase. Thirty-five percent expect the threat will stay the same. Only 22 percent expect any decrease in these attacks.

- **IT respondents acknowledge that the DDoS threat is not abating.** However, only 30 percent are planning to purchase an anti-DDoS technology in the next 6 to 12 months.

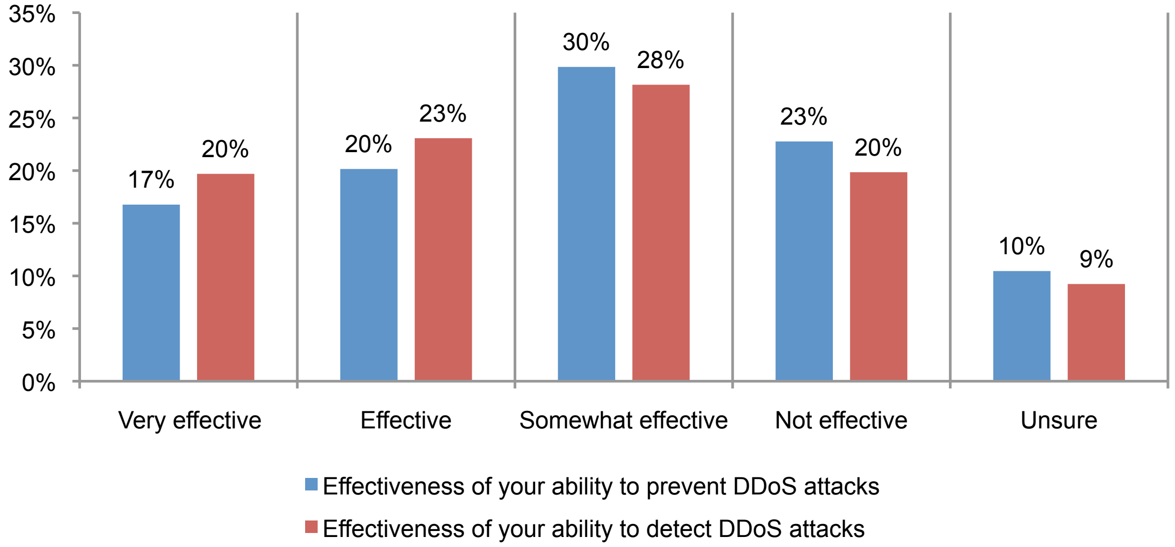
[1] *DDoS Hacker Attacks on Banks Escalate*, Robert McGarvey, Credit Union Times, September 28, 2012

[2] *Expert’s Warning: More Denial of Service Attacks Coming At You*, Robert McGarvey, Credit Union Times, October 1, 2012

## Part 2. Key Findings

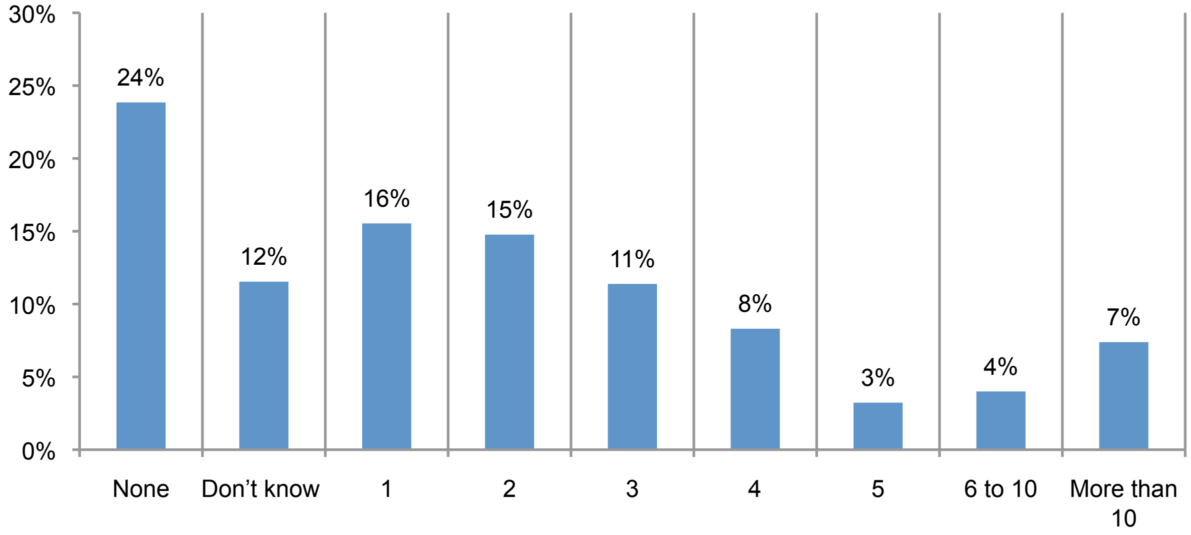
**There is more confidence in the ability to detect than prevent DDoS attacks.** Although the majority of respondents do not believe they are effective in detecting and preventing DDoS attacks, there is more confidence in their ability to detect these attacks**.** According to Figure 1, 43 percent of respondents say they rate their organization's ability to detect DDoS attacks as very effective or effective. However, 33 percent of respondents say their banks are either not effective or unsure about the ability to prevent these attacks.

**Figure 1. Effectiveness in the ability to prevent & detect DDoS attacks**



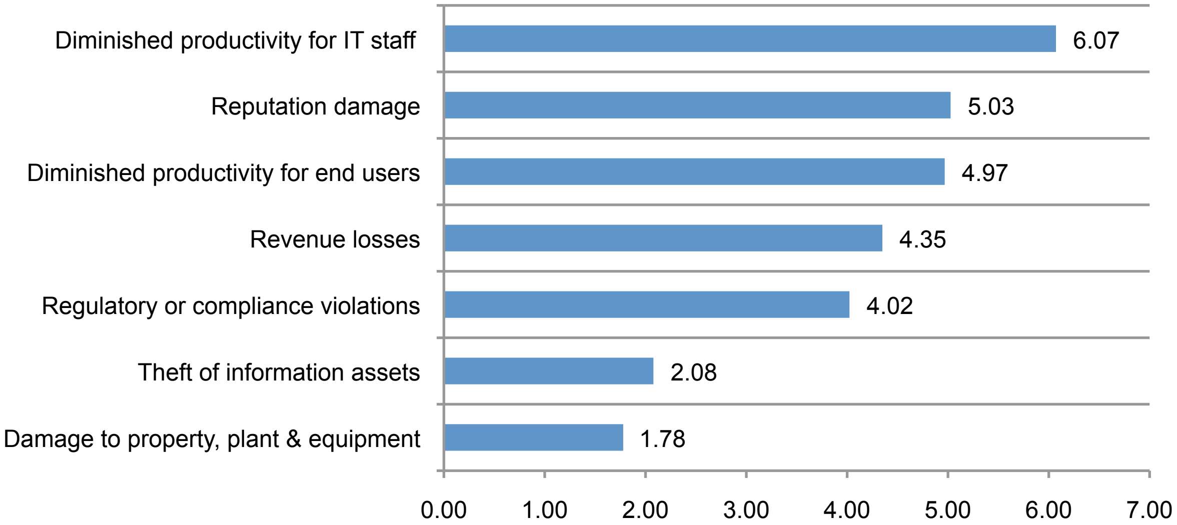
**The majority of retail banks surveyed had a DDoS attack.** According to Figure 2, 64 percent of respondents say their organization had a DDoS in the past 12 months. Only 24 percent say their bank has not had an attack and 12 percent do not know. We estimate that on average the retail banks in this study had 2.8 such attacks in the past 12 months.

**Figure 2. DDoS attacks experienced in the past 12 months**



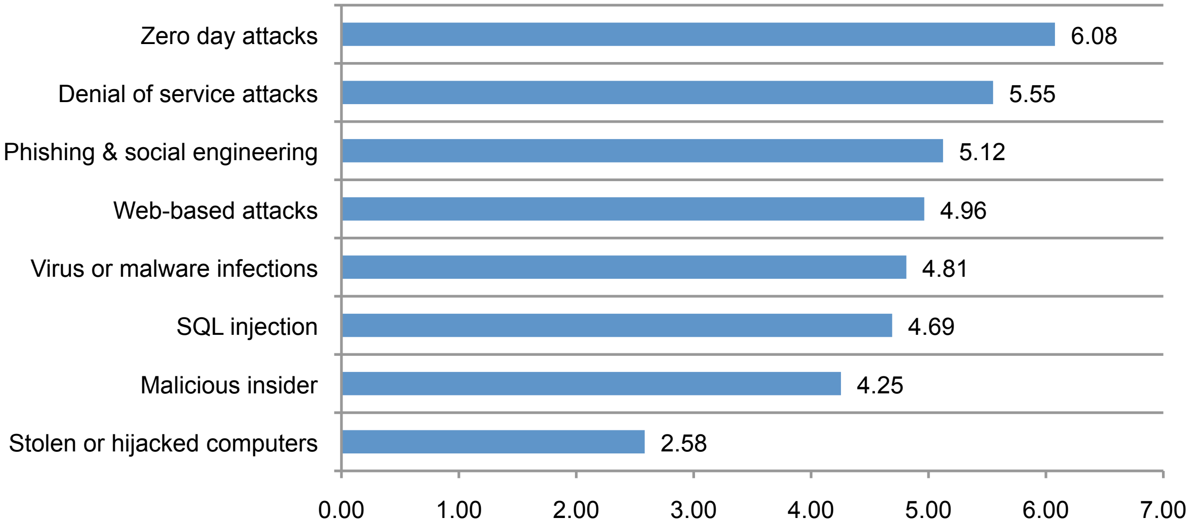
**Diminished productivity of the bank's IT staff is by far the worst consequence of a DDoS attack.** The most severe result of a DDoS attack is the time and efforts of the IT staff to deal with resolving the attack. Figure 3 shows that this is followed by reputation damage, which can have a negative impact on the loyalty of banking customers. Diminished productivity for end users is another negative result.

**Figure 3. Consequences of DDoS attacks**
7 = Most severe consequence to 1 = Least severe consequence



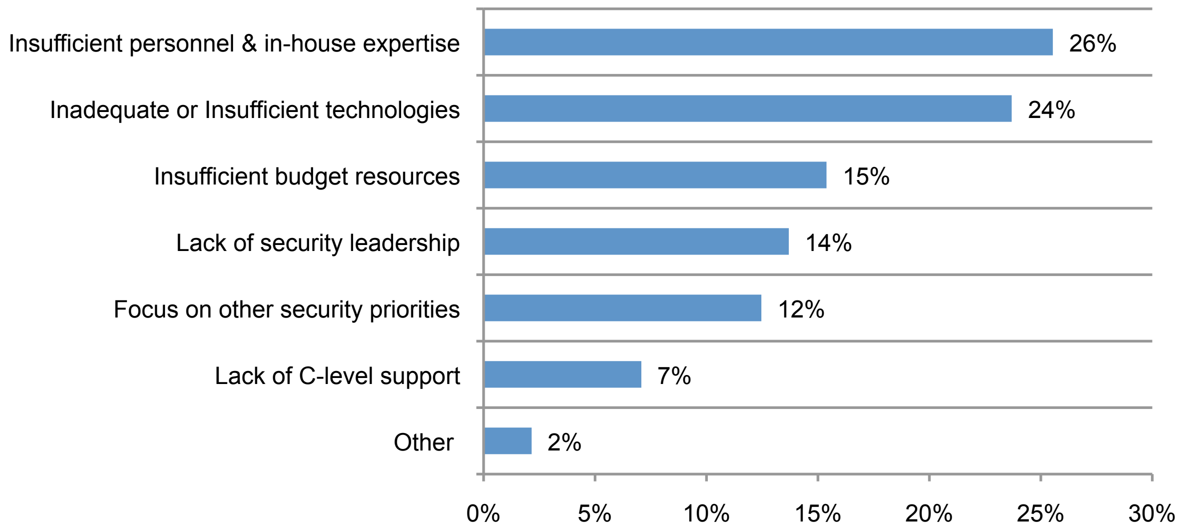
**Zero day attacks and denial of service attacks are considered the most severe security threats to retail banks.** Respondents were asked to rank the severity of eight security threats. By far the two most severe threats are zero day attacks and denial of service attacks followed by phishing & social engineering (Figure 4). The least severe is the loss or theft of employee computers and malicious insiders.

**Figure 4. Security threats considered most severe**
8 = the most severe to 1 = the least severe



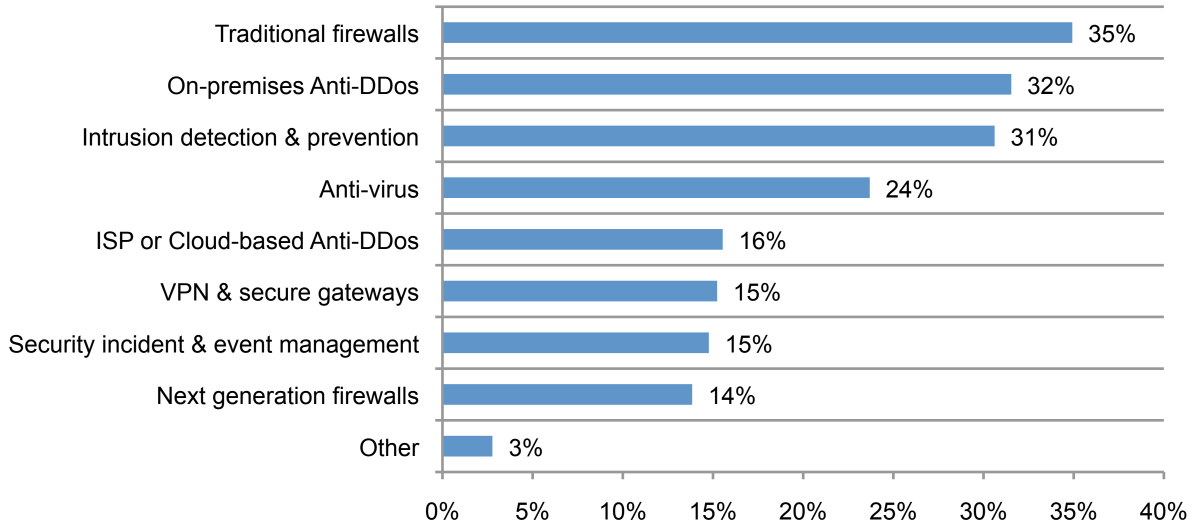
**A lack of resources threatens retail banks' ability to deal with DDoS attacks.** While there is no strong consensus about the most critical barrier to preventing DDoS attacks, insufficient personnel and in-house expertise and inadequate technologies seem to be the most serious concerns followed by insufficient budget, as shown in Figure 5.

**Figure 5. Critical barriers to preventing DDoS attacks**



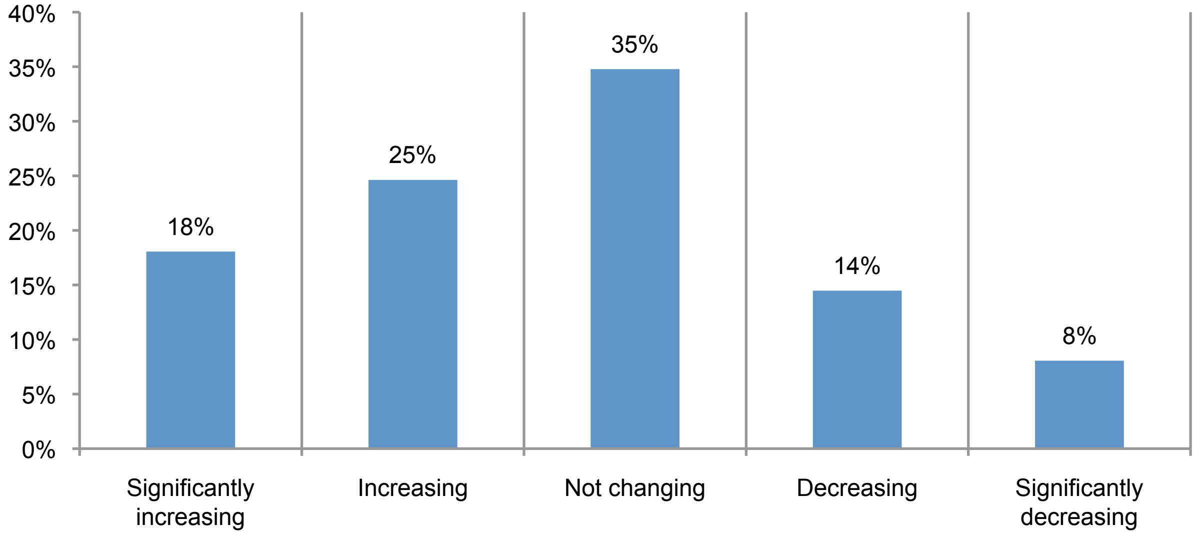
**Traditional firewalls and on-premises anti-DDoS technologies are the most popular to prevent and detect these attacks.** Respondents were asked to select the top two technologies most often used to address the threat of DDoS attacks. According to Figure 6, Traditional firewalls (35 percent of respondents) and on-premises anti-DDoS technologies are most often used. These are followed by intrusion detection and prevention and anti-virus technologies. Despite recognition that the threat is not abating, only 30 percent are planning to purchase an anti-DDoS technology in the next 6 to 12 months.

**Figure 6. Security technologies used to prevent and detect DDoS attacks**
Two responses permitted



**The threat of DDoS attacks is not improving.** According to Figure 7, 43 percent of respondents expect the attacks will either significantly increase or increase. Thirty-five percent expect the threat will stay the same. Only 22 percent expect any decrease in these attacks.

**Figure 7. The future state of DDoS attacks**



**Part 3. Conclusion**

We believe this study is important because it provides a perspective of what IT and IT security practitioners in retail banking think about the current state of DDoS attacks. According to the findings, these IT pros rank DDoS as one of the most severe security risks they face.

Further, when such an attack occurs their time and efforts are devoted to dealing with the problem instead of managing other IT operational and security priorities. What should banks be doing to reduce the threat? The respondents say they need technologies and in-house expertise to prevent and detect DDoS attacks.

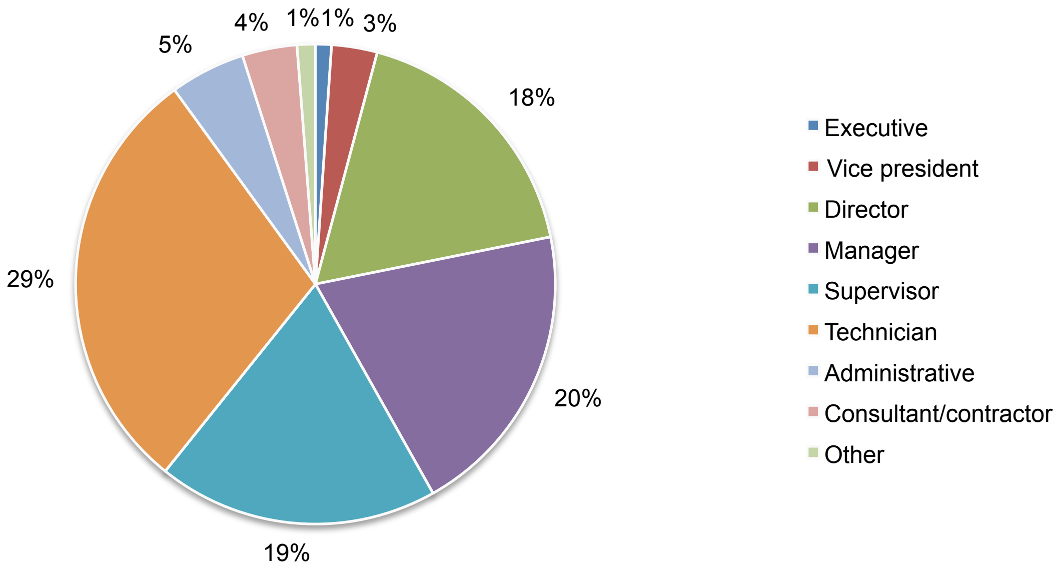
### Part 4. Methods

A random sampling frame of 16,318 IT and IT security managers located in all regions of the United States were selected as participants to this survey. Our omnibus sampling frames were built from several proprietary lists of experienced IT and IT security practitioners. As shown in Table 1, 698 respondents completed the survey. Screening removed 48 surveys resulting in a final sample of 650 surveys (or a 4.0 percent response rate).

| **Table 1. Sample response** | Freq | Pct% |
|---|---:|---:|
| Sampling frame (retail banking) | 16,318 | 100.0% |
| Total returns | 698 | 4.3% |
| Total rejections | 48 | 0.3% |
| Final sample | 650 | 4.0% |

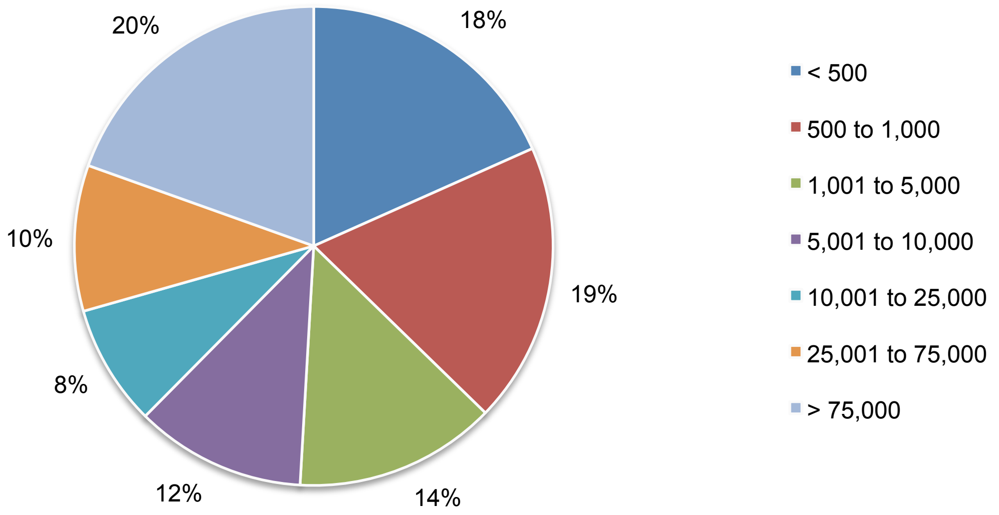
Pie Chart 1 reports the respondent's organizational level within participating organizations. The majority (61 percent) of respondents are at or above the supervisor level.

**Pie Chart 1. Position level**



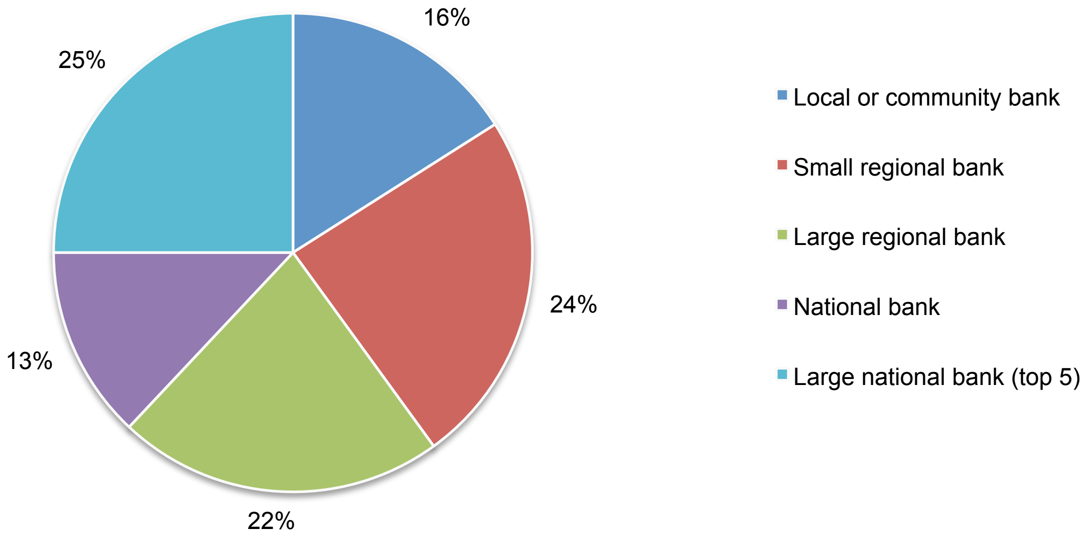
As shown in Pie Chart 2, 64 percent of the respondents are from banking institutions with more than 1,000 full-time employees.

**Pie Chart 2. Headcount**



According to Pie Chart 3, 60 percent of respondents are from a large regional bank, national bank or a large national bank (top 5).

**Figure 3. Banking institutions represented**



## Part 5. 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

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in November 2012.

| Sample response | Freq | Pct% |
|---|---|---|
| Sampling frame (retail banking) | 16318 | 100.0% |
| Total returns | 698 | 4.3% |
| Total rejections | 48 | 0.3% |
| Final sample | 650 | 4.0% |

| Q1a. How would you rate the effectiveness of your organization's ability **to prevent** DDoS attacks? | Freq | Pct% |
|---|---|---|
| Very effective | 109 | 17% |
| Effective | 131 | 20% |
| Somewhat effective | 194 | 30% |
| Not effective | 148 | 23% |
| Unsure | 68 | 10% |
| Total | 650 | 100% |

| Q1b. How would you rate the effectiveness of your organization's ability **to detect** DDoS attacks? | Freq | Pct% |
|---|---|---|
| Very effective | 128 | 20% |
| Effective | 150 | 23% |
| Somewhat effective | 183 | 28% |
| Not effective | 129 | 20% |
| Unsure | 60 | 9% |
| Total | 650 | 100% |

| Q2. How many DDoS attacks did your organization experience in the past 12 months? | Freq | Pct% |
|---|---|---|
| None (skip to Q4) | 155 | 24% |
| Don't know (skip to Q4) | 75 | 12% |
| 1 | 101 | 16% |
| 2 | 96 | 15% |
| 3 | 74 | 11% |
| 4 | 54 | 8% |
| 5 | 21 | 3% |
| 6 to 10 | 26 | 4% |
| More than 10 | 48 | 7% |
| Total | 650 | 100% |
| Extrapolated number of DDoS attacks in the past 12 months | 2.8 | |

| Q3. What were the consequences of the DDoS attacks experienced by your organization in the past 12 months? Please rank from 7 = Most severe consequence to 1 = Least severe consequence | Average rank | Rank order |
|---|---|---|
| Revenue losses | 4.35 | 4 |
| Diminished productivity for IT staff | 6.07 | 1 |
| Diminished productivity for end users | 4.97 | 3 |
| Theft of information assets | 2.08 | 6 |
| Damage to property, plant and equipment | 1.78 | 7 |
| Reputation damage | 5.03 | 2 |
| Regulatory or compliance violations | 4.02 | 5 |

| Q4. Please rank the following eight (8) security threats that your organization may face today (from 8 = the most severe to 1 = the least severe). | Average rank | Rank order |
|---|---|---|
| Denial of service attacks | 5.55 | 2 |
| Virus or malware infections | 4.81 | 5 |
| Web-based attacks | 4.96 | 4 |
| Stolen or hijacked computers | 2.58 | 8 |
| Malicious insider | 4.25 | 7 |
| SQL injection | 4.69 | 6 |
| Zero day attacks | 6.08 | 1 |
| Phishing & social engineering | 5.12 | 3 |

| Q5. In your opinion, what is the **most critical** barrier to preventing DDoS attacks? | Freq | Pct% |
|---|---|---|
| Insufficient budget resources | 100 | 15% |
| Lack of C-level support | 46 | 7% |
| Lack of security leadership | 89 | 14% |
| Focus on other security priorities | 81 | 12% |
| Insufficient personnel and in-house expertise | 166 | 26% |
| Inadequate or Insufficient technologies | 154 | 24% |
| Other (please specify) | 14 | 2% |
| Total | 650 | 100% |

| Q6. What security technologies do you use today to prevent and detect DDoS attacks? Please select only two top choices. | Freq | Pct% |
|---|---|---|
| On-premises Anti-DDos | 205 | 32% |
| ISP or Cloud-based Anti-DDos | 101 | 16% |
| Anti-virus | 154 | 24% |
| Intrusion detection and prevention | 199 | 31% |
| Traditional firewalls | 227 | 35% |
| Next generation firewalls | 90 | 14% |
| VPN and secure gateways | 99 | 15% |
| Security incident and event management | 96 | 15% |
| Other (please specify) | 18 | 3% |
| Total | 1189 | 183% |

| Q7. Is your organization planning to purchase an anti-DDoS technology in the next 6 to 12 months? | Freq | Pct% |
|---|---|---|
| Yes | 192 | 30% |
| No | 313 | 48% |
| Unsure | 145 | 22% |
| Total | 650 | 100% |

| Q8. In your opinion, are DDoS attacks going to increase decrease or stay at the same level or frequency over the next 12 to 24 months? DDoS frequency is . . . | Freq | Pct% |
|---|---|---|
| Significantly increasing | 121 | 18% |
| Increasing | 165 | 25% |
| Not changing | 233 | 35% |
| Decreasing | 97 | 14% |
| Significantly decreasing | 54 | 8% |
| Total | 670 | 100% |

**Organization and respondents' demographics**

| D1. What best describes your position level within the organization? | Freq | Pct% |
|---|---|---|
| Executive | 7 | 1% |
| Vice president | 20 | 3% |
| Director | 115 | 18% |
| Manager | 130 | 20% |
| Supervisor | 123 | 19% |
| Technician | 190 | 29% |
| Administrative | 33 | 5% |
| Consultant/contractor | 24 | 4% |
| Other | 8 | 1% |
| Total | 650 | 100% |

| D2. What range best describes the full-time headcount of your banking institution? | Freq | Pct% |
|---|---|---|
| < 500 | 121 | 18% |
| 500 to 1,000 | 125 | 19% |
| 1,001 to 5,000 | 90 | 14% |
| 5,001 to 10,000 | 76 | 12% |
| 10,001 to 25,000 | 54 | 8% |
| 25,001 to 75,000 | 65 | 10% |
| > 75,000 | 129 | 20% |
| Total | 660 | 100% |

| D3. What best describes your banking institution? | Freq | Pct% |
|---|---|---|
| Local or community bank | 102 | 16% |
| Small regional bank | 155 | 24% |
| Large regional bank | 141 | 22% |
| National bank | 87 | 13% |
| Large national bank (top 5) | 163 | 25% |
| Other (please specify) | 2 | 0% |
| Total | 650 | 100% |

**Please contact research@ponemon.org or call us at 800.877.3118 if you have any questions.**

## 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.

As a member of the **Council of American Survey Research Organizations (CASRO)**, 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.