THE COST OF **CREDENTIAL STUFFING**

SPONSORED BY **AKAMAI TECHNOLOGIES**

Independently conducted by Ponemon Institute LLC

Publication Date: October 2017

Ponemon Institute© Research Report

The Cost of Credential Stuffing

Ponemon Institute, October 2017

Part 1. Introduction

We are pleased to present *The Cost of Credential Stuffing,* sponsored by Akamai Technologies. The purpose of this study is to quantify the potential cost to prevent, detect and remediate credential stuffing attacks. The research also includes the financial consequences to companies if attackers are able to use stolen credentials to make fraudulent purchases or transactions.

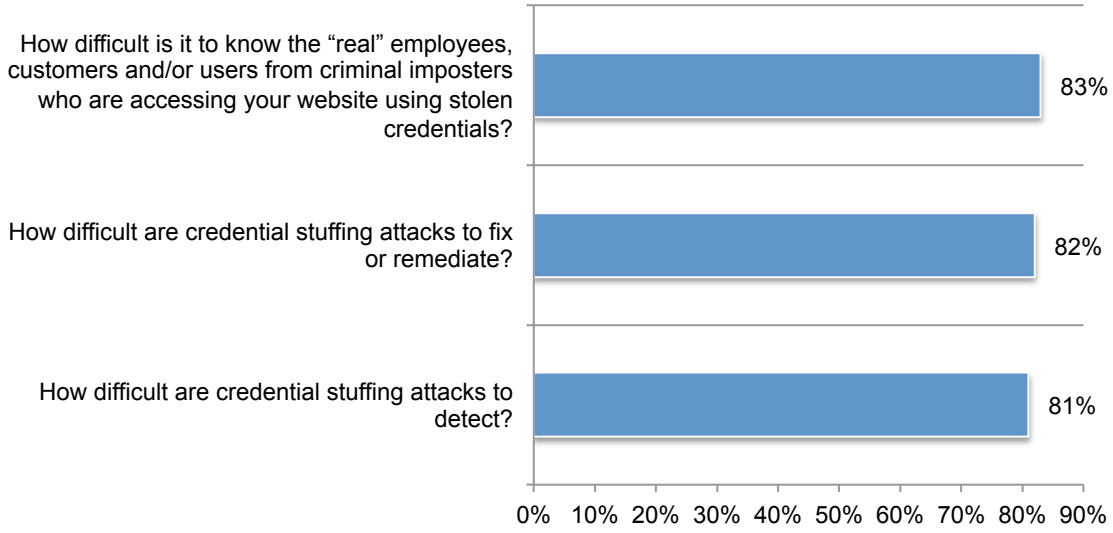
Ponemon Institute surveyed 569 IT security practitioners who are familiar with credential stuffing attacks and are responsible for the security of their companies' websites. According to respondents, these attacks cause costly application downtime, loss of customers and involvement of IT security that can result in an average cost of $1.7 million, $2.7 million and $1.6 million annually, respectively.

In addition, the companies represented in this research estimate that the monetary cost of fraud due to credential stuffing attacks can range from an average of more than $500,000 if 1 percent of all compromised accounts result in monetary loss to more than $54 million if 100 percent of all compromised accounts result in monetary loss.

Almost all respondents, as shown in Figure 1, believe it is difficult to identify the criminal and imposters who are accessing their website using stolen credentials (83 percent), remediate credential stuffing attacks (82 percent) and detect these attacks (81 percent).

Figure 1. How difficult is the detection and remediation of credential stuffing attacks and identification of criminal imposters?

Very difficult, difficult and somewhat difficult responses combined



In the context of this study credential stuffing results from fraudsters purchasing lists of stolen credentials, such as user ID and passwords, on the dark web and using a botnet to validate those lists against an organization's login page. The end result is typically an account takeover, in which fraudsters then use the stolen validated credential to take over accounts and commit fraud. The focus of this crime can be to make fraudulent purchases, engage in fraudulent financial transactions and steal additional confidential information.

The 2016 Yahoo breaches are examples of how serious this threat is. The Yahoo breaches involved a total of 1.5 billion credentials spilled to the Internet, protected by the weak MD5 hashing algorithm. The thefts took place in 2012 and 2013 giving the criminals up to four years to crack weak protection.[1]

The following findings from this research reveal why companies are vulnerable to credential stuffing attacks.

- On average, companies experience an average of 12.7 credential stuffing attacks each month, wherein the attacker is able to identify valid credentials.
- The volume and severity of credential stuffing attacks are increasing.
- It is difficult to differentiate the criminal from the real customers, employees and users who have access to the companies' websites.
- Migration to the cloud is an important IT strategy, but participants in this study believe it increases the risk of credential stuffing attacks.
- Companies do not have sufficient solutions or technologies today for preventing and/or containing credential stuffing attacks.

[1] "Credential Stuffing: A Successful and Growing Attack Methodology," by Kevin Townsend, Security Week, January 17, 2017

Part 2. Key Findings

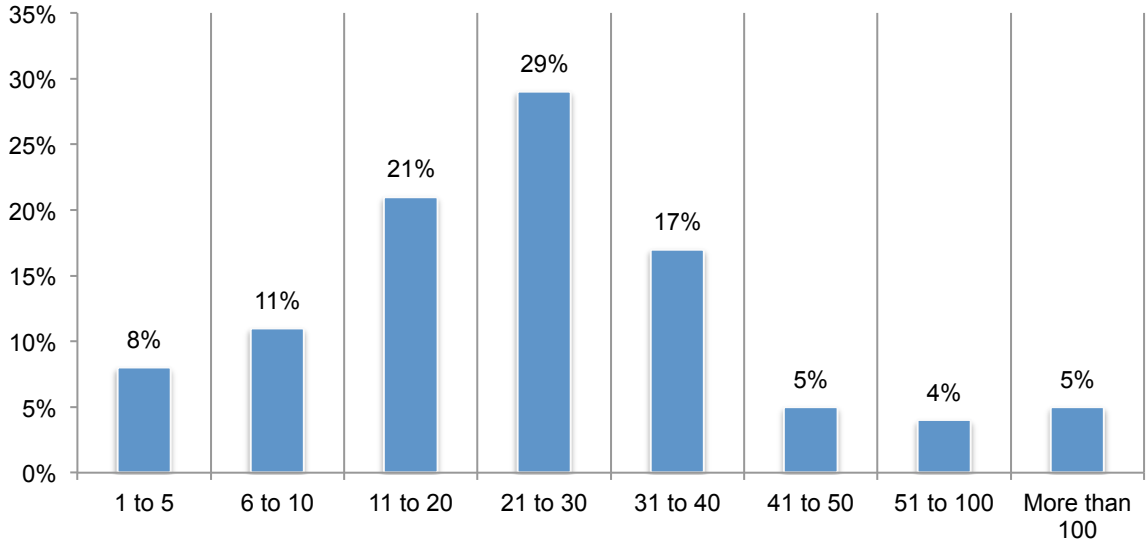
In this section, we present an analysis of the key findings. The complete audited findings are presented in the Appendix of this report. The topics are organized according to the following topics:

- Application and organizational challenges
- Ability to prevent, detect and remediate credential stuffing
- Quantifying credential stuffing attacks
- Consequences and cost of credential stuffing

Application and organizational challenges

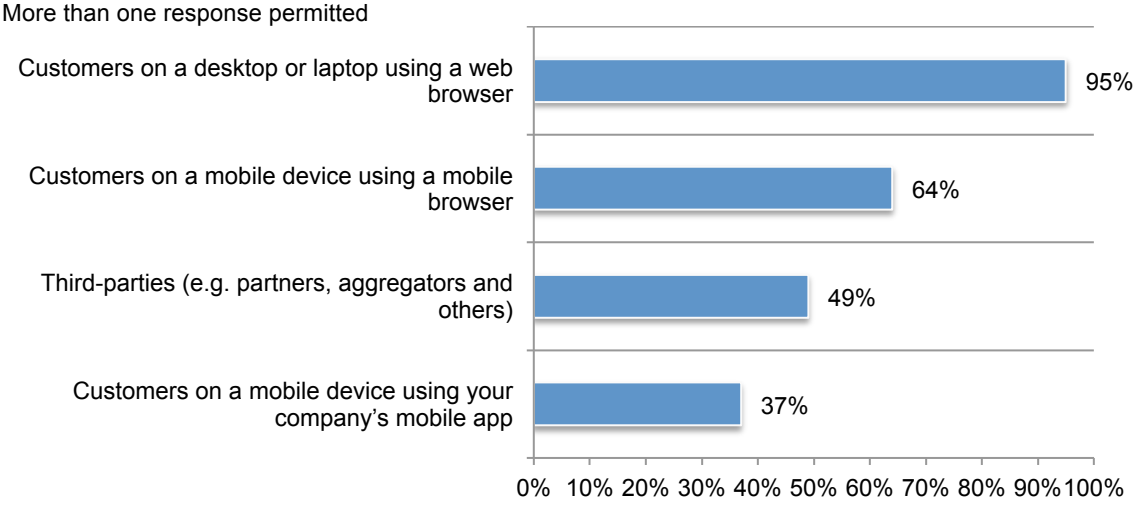
Organizations have a complex credential abuse attack surface. This complexity exacerbates the challenge of protecting against credential stuffing attacks. As shown in Figure 2, customers have an average of 30 customer and/or customer-facing websites in production today.

Figure 2. Number of customer and/or customer-facing websites



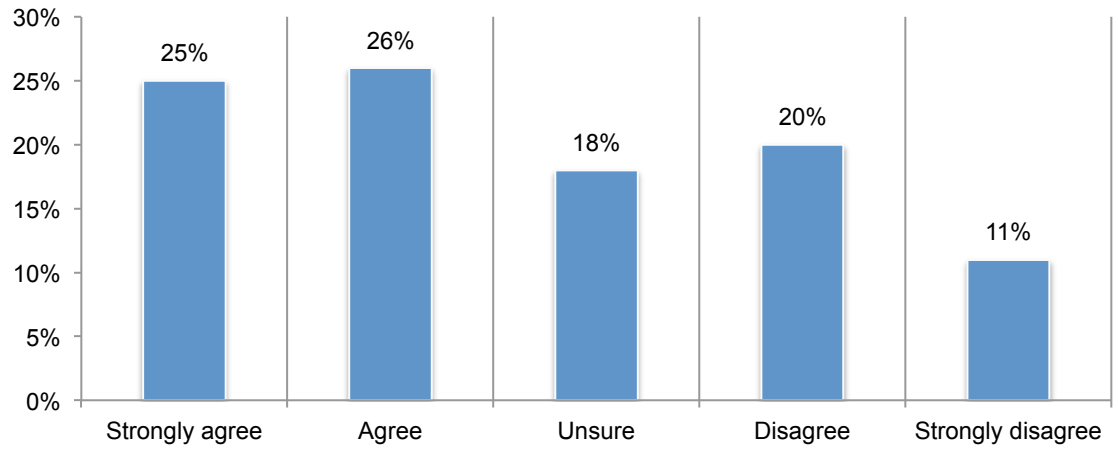
Organizations typically have to provide login access for different types of clients. Typical clients who login are shown in Figure 3. While the top two are customers on a desktop or laptop using web browsers (95 percent of respondents) and customers on a mobile device using a mobile browser (64 percent of respondents), APIs supporting mobile apps (37 percent of respondents) and third-parties (49 percent of respondents) are a significant source of login traffic. In addition, mobile traffic is only expected to increase over time; for example, eMarketer projects that mobile retail commerce sales will grow from 34.5 percent in 2017 to 53.9 percent in 2021.

Figure 3. Types of website clients
More than one response permitted



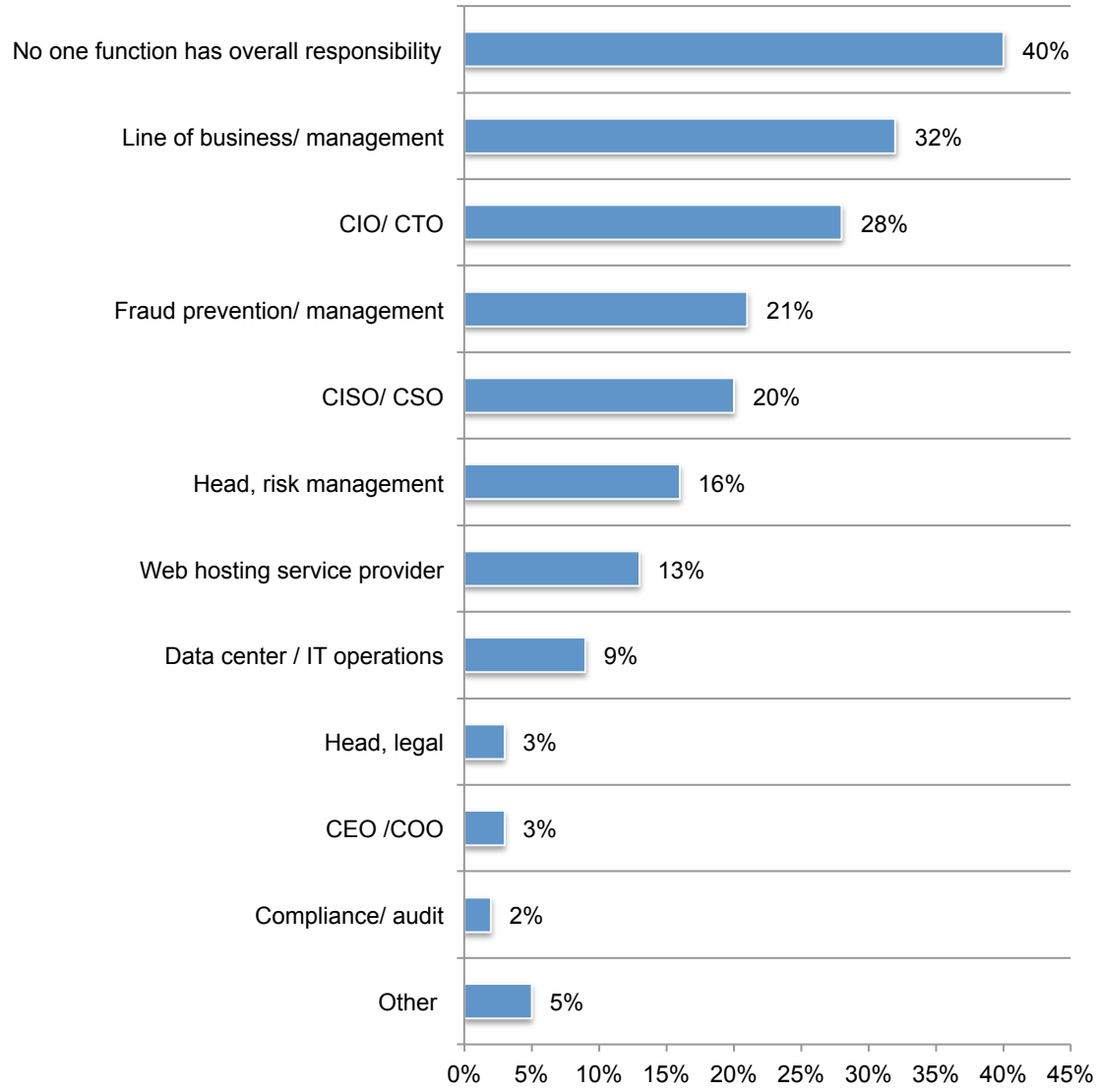
The cloud increases the risk of credential stuffing. As shown in Figure 4, over 50 percent of respondents agreed that the migration of applications to the cloud increased the risk posed by credential stuffing. As with many aspects of security, an organization's broader cloud strategy can impact the ability of a security team to secure the growing number of applications (and endpoints supporting different types of clients) across different computing platforms.

Figure 4. Migration to the cloud has increased the risk of credential stuffing



Accountability for preventing credential stuffing attacks is dispersed throughout the organization. As shown in Figure 5, the responsibility for addressing credential stuffing attacks is assigned to many functions within an organization. Organizations' application and management teams clearly have ultimate responsibility for the impact, with 32 percent, 28 percent, and 20 percent of respondents stating line business/management, CIO/CTO, and CISO/CSO, respectively. However, fraud prevention/management had responsibility 21 percent of the time, and risk management heads had responsibility 16 percent of the time. Because of this split, 40 percent of respondents stated that no one function has overall responsibility for addressing every aspect of the problem.

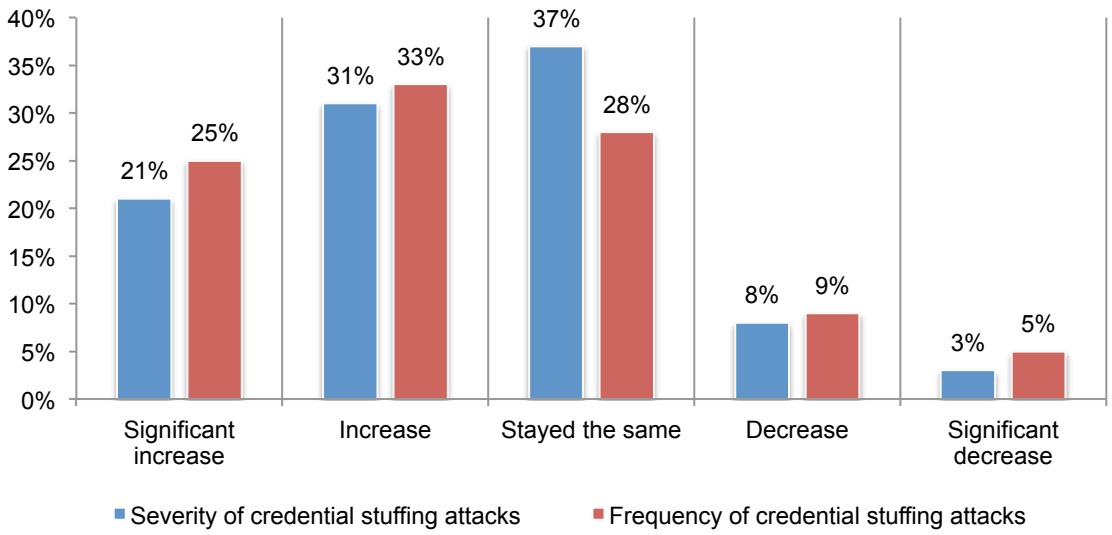
Figure 5. Who is most responsible for curtailing credential stuffing attacks on your company's websites?
Two responses permitted



Ability to prevent, detect and remediate credential stuffing

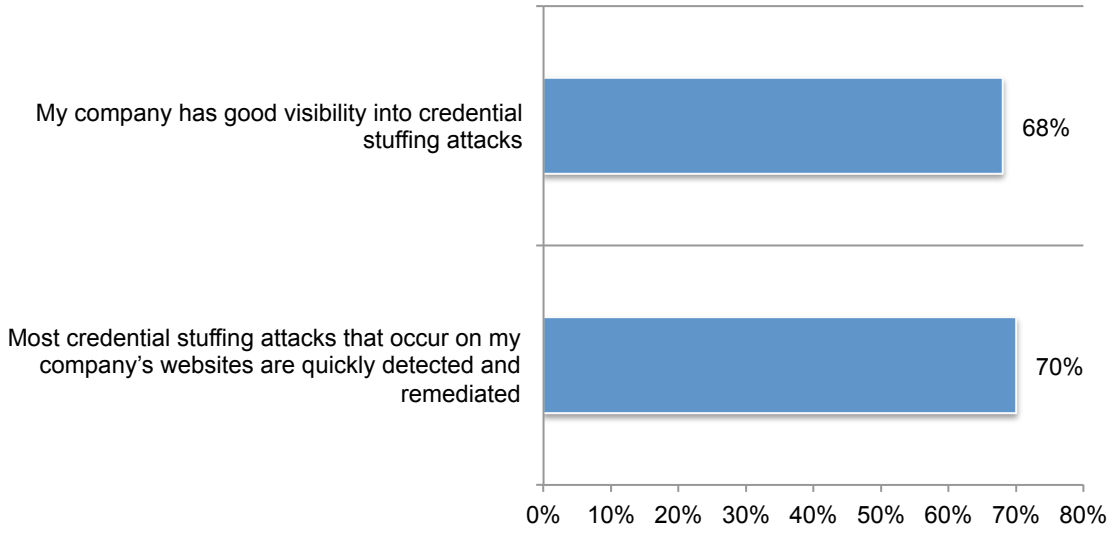
Credential stuffing attacks are increasing in frequency and severity. The data in Figure 6 demonstrate that, according to 86 percent of respondents, these attacks are increasing or staying the same in terms of volume or frequency. Moreover, 89 percent of respondents say these attacks are becoming more severe or staying the same.

Figure 6. The increase in the volume or frequency and severity of credential stuffing attacks



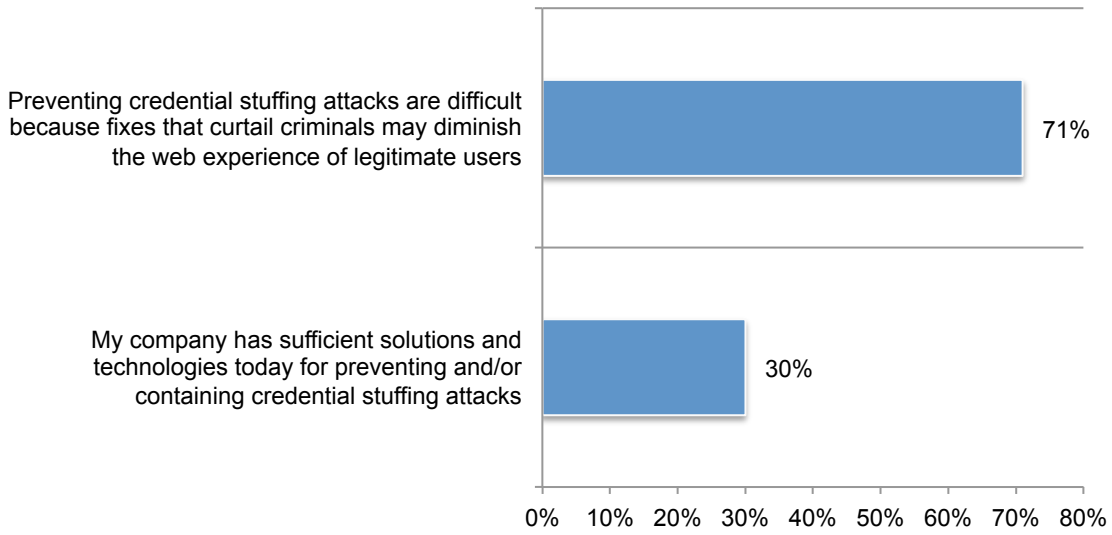
Organizations are struggling to respond to credential stuffing attacks. According to Figure 7, only 68 percent of respondents say they **do not** have good visibility into credential stuffing attacks. Seventy percent **do not** believe that credential stuffing attacks against their websites are quickly detected and remediated.

Figure 7. How effective are companies at dealing with credential stuffing attacks?
Strongly disagree and disagree responses



Organizations face multiple challenges to preventing and/or containing credential stuffing attacks. As shown in Figure 8, the majority (71 percent) of respondents agree with the statement that preventing credential stuffing attacks are difficult because fixes that curtail such criminal actions may diminish the web experience of legitimate users. Only 30 percent say that their companies have sufficient solutions and technologies for preventing and/or containing credential stuffing attacks.

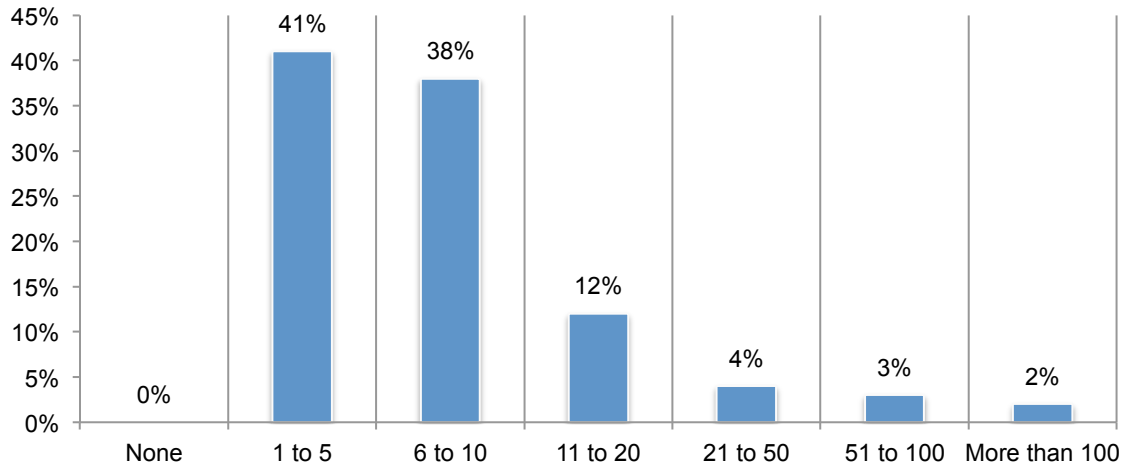
Figure 8. Challenges to dealing with credential stuffing attacks
Strongly agree and agree responses



Quantifying credential stuffing attacks

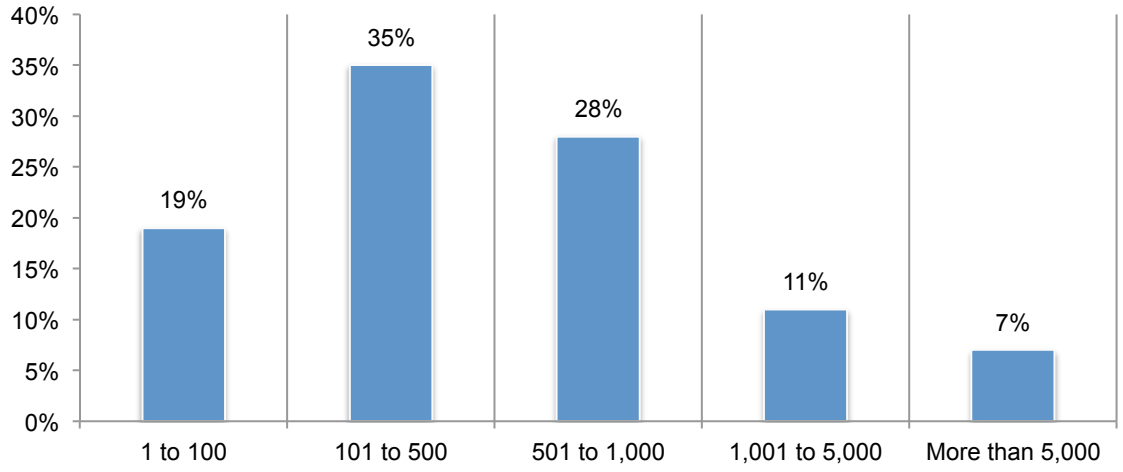
Credential stuffing is a persistent and ongoing challenge. Companies in this research experience an average of 12.7 credential stuffing attacks each month. In addition, a significant percentage of attacks go undetected, with the number estimated to be 33.5 percent on average.

Figure 9. Number of credential stuffing attacks per month



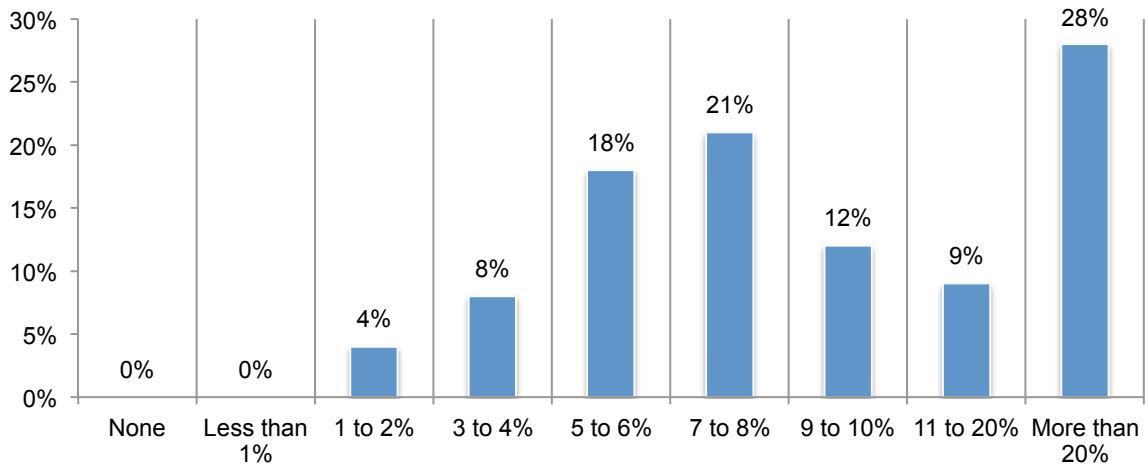
Attacks impact large numbers of user accounts. As shown in Figure 10, respondents reported that an average of 1,252 user accounts are typically targeted in each credential stuffing attack.

Figure 10. Number of user accounts targeted per attack



Attackers are successful often enough. According to respondents, approximately 12.4 percent of credential stuffing attempts on average are successful in identifying valid user credentials, as can be seen in Figure 11.

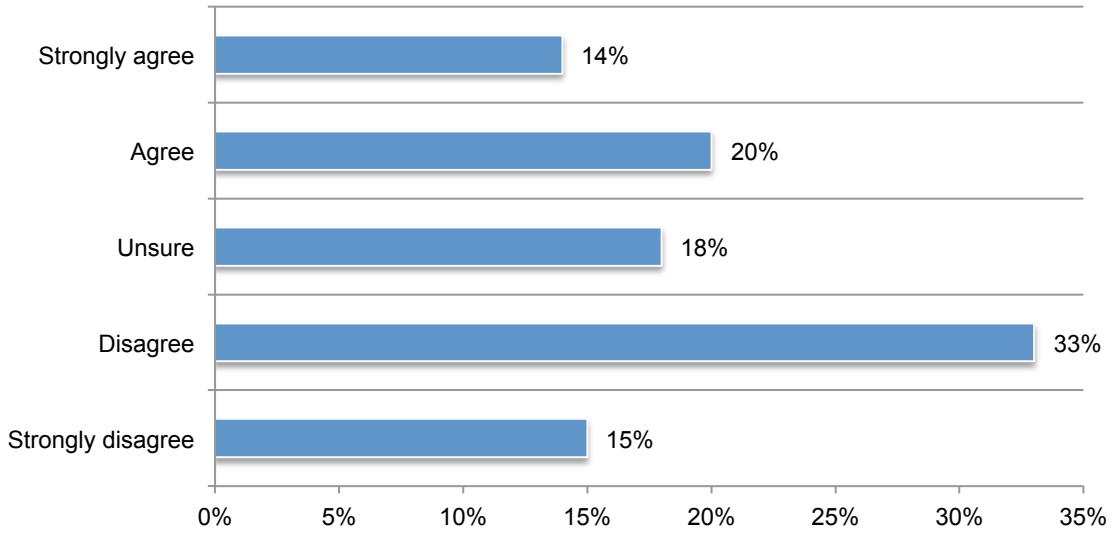
Figure 11. Percentage of credential stuffing attempts that are successful



Consequences and costs of credential stuffing

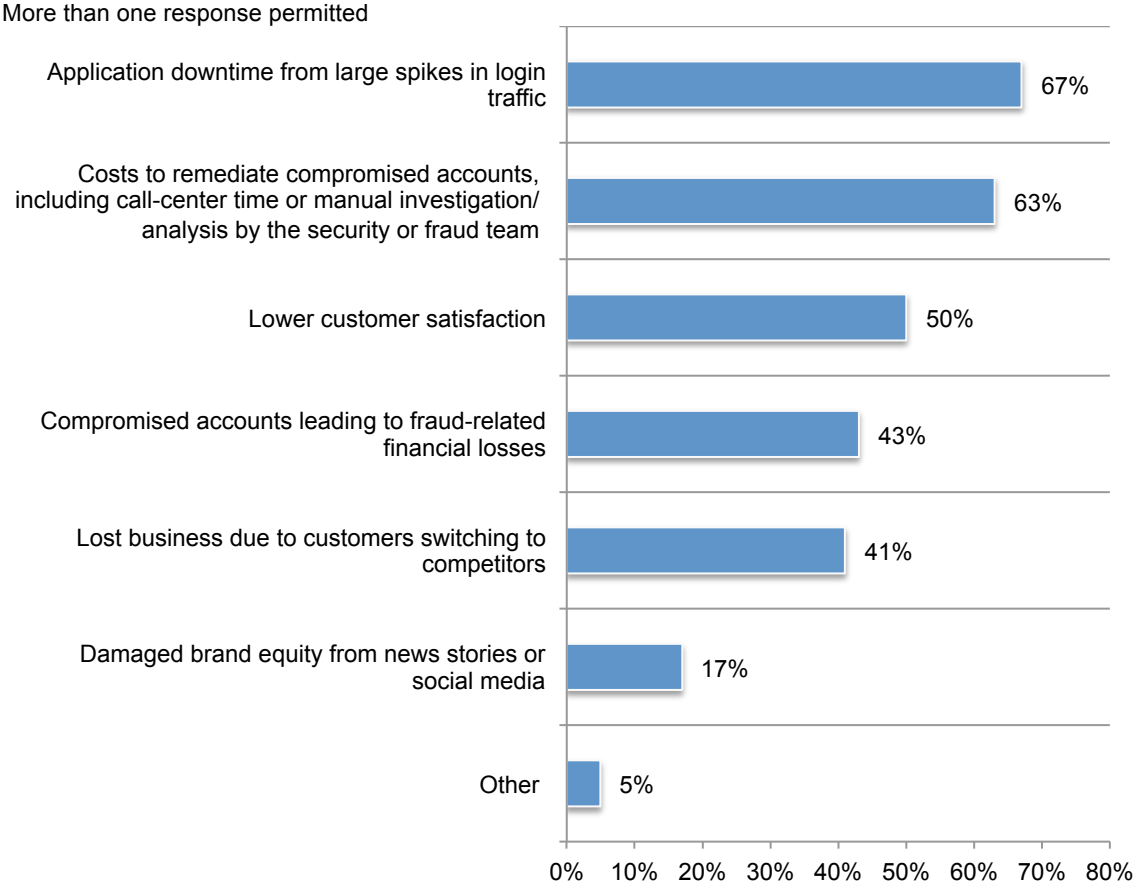
Organizations do not budget enough today to address the problem. As shown in Figure 12, only 34 percent of respondents agree with the statement that their companies' security budget is sufficient for preventing and/or containing credential stuffing attacks. Eighteen percent are unsure, while 48 percent either disagree or strongly disagree.

Figure 12. Existing security budget is sufficient for preventing and/or containing credential abuse attacks



While organizations may not be budgeting enough to properly address credential abuse attacks, survey respondents report the financial impact in a broad number of areas. In terms of frequency, Figure 13 shows the most reported negative consequences are application downtime (67 percent of respondents) and costs to remediate compromised accounts, including call-center time or manual investigation/analysis by the security or fraud team (63 percent of respondents).

Figure 13. Negative consequences resulting from a credential stuffing attack
More than one response permitted



The total annualized cost of credential stuffing, excluding fraud, can average more than $6 million. Table 1 presents the cost for a security team to deal with this type of attack.

Table 1. Time spent preventing, detecting and remediating credential stuffing	Average hours spent each week	Cost per hour*
Organizing & planning approaches to the detection & containment of credential abuse	73	$4,564
Analyzing & investigating possible credential stuffing attacks	146	$9,101
Conducting forensic analysis for accounts believed to have been compromised via credential stuffing	63	$3,935
Documenting and/or reporting on credential stuffing incidents	63	$3,942
Containing & remediating credential-based attacks	156	$9,769
Total per week	501	$31,311
Total per year	26,051	$1,628,185

*IT and IT security fully loaded pay rate per hour is $62.50 (source: Ponemon Institute)

Table 2 presents the cost of application downtime.

Table 2. Cost of downtime	Per month	Per annum
Average time (hours) each month incurred by all organizations	7.42	89.04
Average cost per hour of application downtime	$19,389	$232,667
Total cost per year	$143,866	$1,726,388

Table 3 presents the cost of customer churn.

Table 3. Cost of customer churn	Survey question	Calculus
A=Average value of customer	Q24	$1,494
B=Percentage of customers who churn as a result of a credential stuffing attack	Q23	7.56%
C=Average number of user accounts that are typically targeted	Q6	1,252
D=Percentage of successful credential stuffing attacks	Q7	12.40%
E=Average number of credential stuffing attacks per month	Q4	12.72
F=(A x B x C x D x E)	Per month	$222,804
G=F x 12	Per annum	$2,673,648

All three components = Total annualized cost of credential stuffing, excluding fraud	Grand total	$6,028,221

The monetary cost of fraud due to credential stuffing attacks ranges from $546,000 to over $54 million a year. The cost of fraud can often be difficult to predict because the attackers performing credential stuffing attacks are often middlemen, reselling validated user account credentials to others who take over the account and perform fraudulent transactions. Therefore, a compromised account does not necessarily lead to a fraud-related loss.

The expected cost will depend on the percentage of all compromised accounts that experienced monetary losses over a one-year period. Hence, if the monetary fraud rate is one percent, our extrapolated total monetary cost of fraud for one year would be $546,153. If this rate is 100 percent – in other words, all compromised accounts experienced monetary losses – the total monetary cost of fraud would be $54,615,300. Please note that these figures are based on the average-sized company in our sample.

Table 4. Monetary cost of fraud	Survey question	Calculus
Frequency of credential stuffing attacks detected each month	Q4	12.7
Percentage of credential stuffing attacks that are not detected	Q5	33.50%
Adjusted frequency of credential stuffing attacks each month	12.7/(1-Q5)	19.1
Number of accounts per each credential stuffing attack	Q6	1,252
Percentage of credential stuffing attacks that result in valid credentials being identified	Q7	12.40%
Frequency of accounts that are compromised each month	19.1 X 1,252 X 12.4%	2,965
Amount of money lost to fraud per compromised account each month	Q9	$1,535
Amount of money lost to fraud per compromised account each year	Q9 X 12	$18,420
Percentage of compromised accounts that resulted in monetary loss=100%	$18,420 X 2,965 X 100%	$54,615,300
Percentage of compromised accounts that resulted in monetary loss=75%	$18,420 X 2,965 X 75%	$40,961,475
Percentage of compromised accounts that resulted in monetary loss=50%	$18,420 X 2,965 X 50%	$27,307,650
Percentage of compromised accounts that resulted in monetary loss=25%	$18,420 X 2,965 X 25%	$13,653,825
Percentage of compromised accounts that resulted in monetary loss=10%	$18,420 X 2,965 X 10%	$5,461,530
Percentage of compromised accounts that resulted in monetary loss=5%	$18,420 X 2,965 X 5%	$2,730,765
Percentage of compromised accounts that resulted in monetary loss=1%	$18,420 X 2,965 X 1%	$546,153

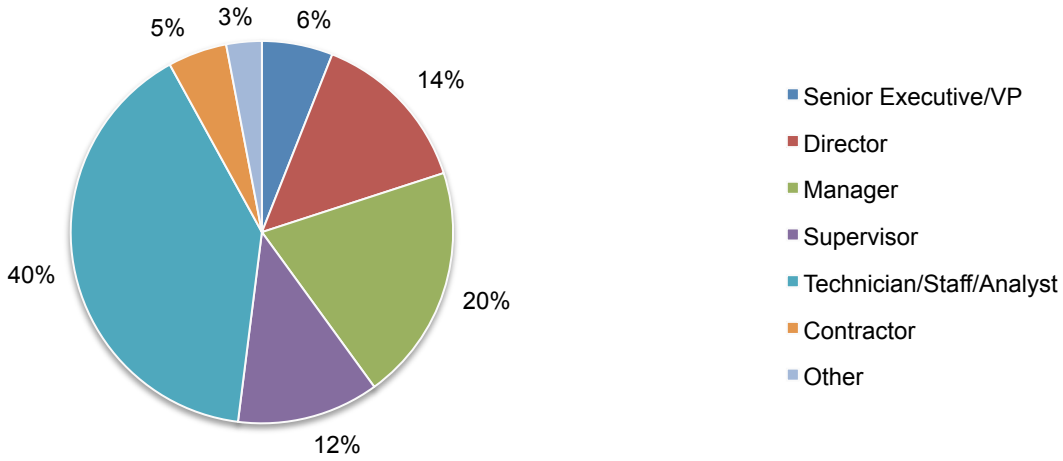
Part 3. Methods

A sampling frame of 14,561 IT security practitioners who are familiar with credential stuffing attacks and are responsible for the security of their companies' websites were selected as participants in the research. Table 5 shows that there were 614 total returned surveys. Screening and reliability checks led to the removal of 45 surveys. Our final sample consisted of 569 surveys, a 3.9 percent response rate.

Table 5. Sample response	Freq	Pct%
Sampling frame	14,561	100.0%
Total returns	614	4.2%
Rejected or screened surveys	45	0.3%
Final sample	569	3.9%

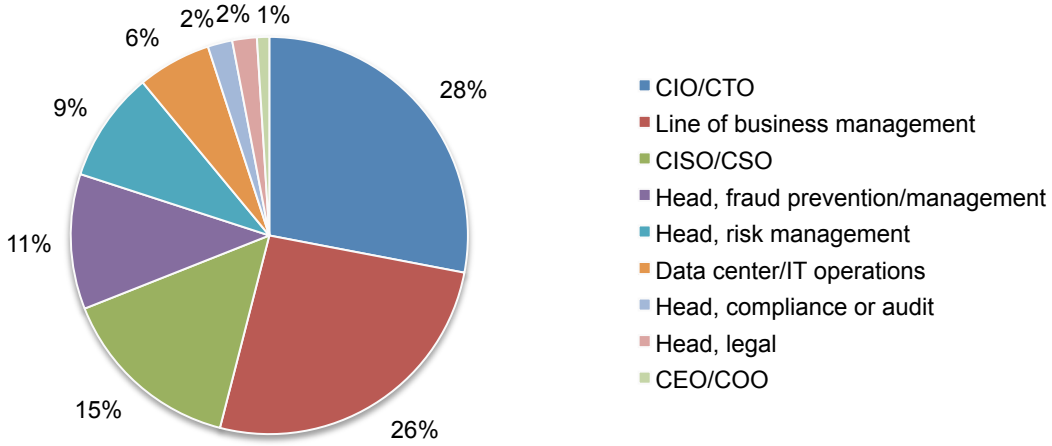
Pie Chart 1 reports respondents' organizational level within participating organizations. By design, slightly more than half of respondents (52 percent) are at or above the supervisory levels.

Pie Chart 1. Position level within the organization



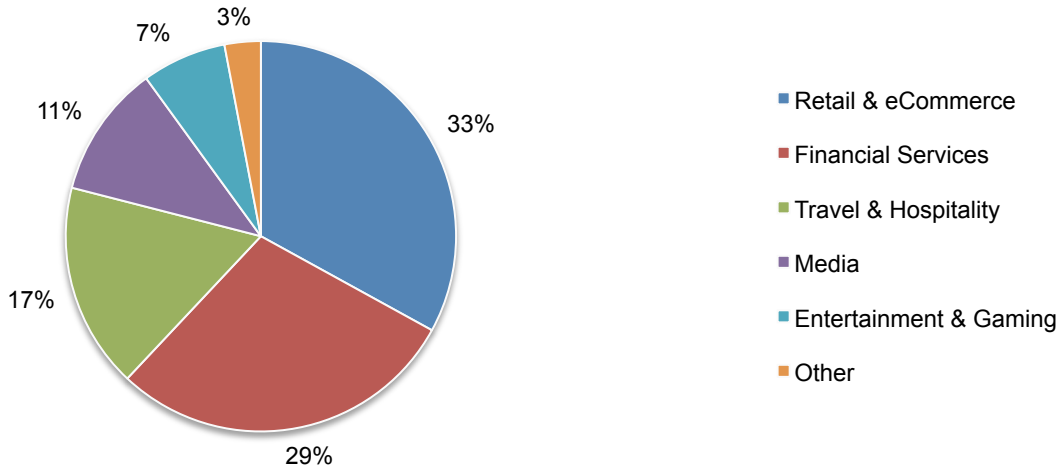
Pie Chart 2 reveals that 28 percent of respondents report to the CIO/CTO, 26 percent report to the line of business management and 15 percent indicated they report to the CISO/CSO.

Pie Chart 2. Primary person reported to within the organization



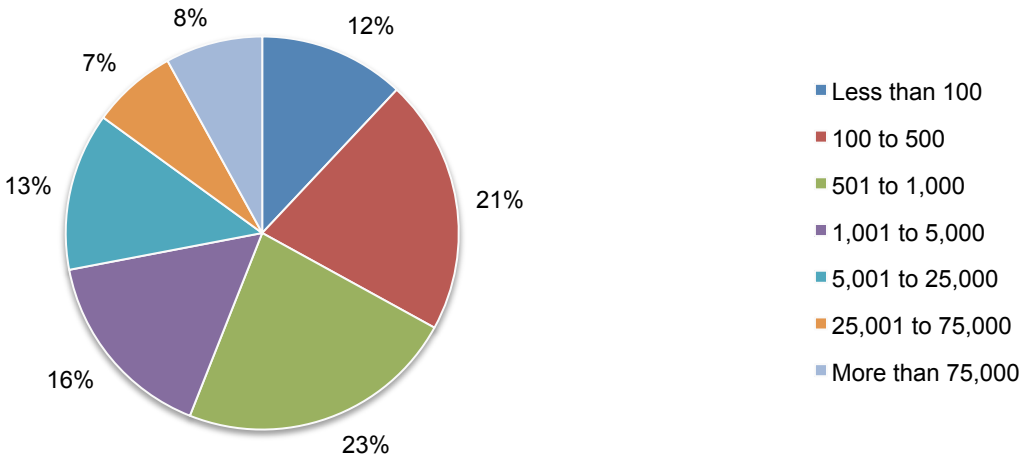
Pie Chart 3 reports the industry focus of respondents' organizations. This chart identifies retail and eCommerce (33 percent) as the largest segment, followed by financial services (29 percent), travel and hospitality (17 percent), and media (11 percent).

Pie Chart 3. Industry focus of respondents' organizations



As Pie Chart 4 illustrates, 44 percent of respondents are from organizations with a global headcount exceeding 1,000 employees.

Pie Chart 4. Global employee headcount of respondents' organizations



Part 4. 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 security practitioners that are familiar with credential stuffing attacks and are responsible for the security of their companies' website. 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 specified time 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 accurate responses.

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 May 2017.

Survey response	Freq	Pct%
Total sampling frame	14,561	100.0%
Total returns	614	4.2%
Rejected surveys	45	0.3%
Total	569	3.9%

Part 1. Screening questions

S1. How familiar are you with credential-abuse and credential stuffing attacks (as defined)?	Pct%
Very familiar	35%
Familiar	43%
Somewhat familiar	22%
No knowledge (stop)	0%
Total	100%

S2. Approximately, what percentage of your organization's revenues (gross sales) are from website-related activities?	Pct%
None (stop)	0%
1 to 10%	12%
11 to 20%	6%
21 to 30%	15%
31 to 40%	13%
41 to 50%	10%
51 to 60%	9%
61 to 70%	4%
71 to 80%	3%
81 to 90%	9%
91 to 100% (virtually all)	19%
Total	100%
Extrapolated value	50%

S3. Do you have any responsibility for the security of your organization's website traffic?	Pct%
Yes, full responsibility	26%
Yes, some responsibility	55%
Yes, minimum responsibility	19%
No responsibility (stop)	0%
Total	100%

Part 2. Attributions

Q1. Please rate each one of the following ten (10) statements using the opinion scale from “strongly agree” to “strongly disagree” provided below each item.	
Q1a. Credential stuffing represents a significant security challenge for my company.	Pct%
Strongly agree	27%
Agree	30%
Unsure	18%
Disagree	17%
Strongly disagree	8%
Total	100%

Q1b. Most credential stuffing attacks that occur on my company’s websites are quickly detected and remediated.	Pct%
Strongly agree	13%
Agree	17%
Unsure	28%
Disagree	24%
Strongly disagree	18%
Total	100%

Q1c. My company has good visibility into credential stuffing attacks.	Pct%
Strongly agree	16%
Agree	16%
Unsure	26%
Disagree	28%
Strongly disagree	14%
Total	100%

Q1d. Bad bot traffic is on the rise because of credential stuffing attacks.	Pct%
Strongly agree	40%
Agree	31%
Unsure	13%
Disagree	12%
Strongly disagree	4%
Total	100%

Q1e. My company’s security budget is sufficient for preventing and/or containing credential stuffing attacks.	Pct%
Strongly agree	14%
Agree	20%
Unsure	18%
Disagree	33%
Strongly disagree	15%
Total	100%

Q1f. My company has sufficient solutions and technologies today for preventing and/or containing credential stuffing attacks.	Pct%
Strongly agree	14%
Agree	16%
Unsure	24%
Disagree	32%
Strongly disagree	14%
Total	100%

Q1g. My company's migration to the cloud has increased the risk of credential stuffing attacks.	Pct%
Strongly agree	25%
Agree	26%
Unsure	18%
Disagree	20%
Strongly disagree	11%
Total	100%

Q1h. The **frequency** of credential stuffing attacks experienced by my company is on the rise.	Pct%
Strongly agree	25%
Agree	29%
Unsure	22%
Disagree	18%
Strongly disagree	6%
Total	100%

Q1i. The **severity** of credential stuffing attacks experienced by my company is on the rise.	Pct%
Strongly agree	27%
Agree	27%
Unsure	21%
Disagree	18%
Strongly disagree	7%
Total	100%

Q1j. Preventing credential stuffing attacks are difficult because fixes that curtail criminals may diminish the web experience of legitimate users.	Pct%
Strongly agree	30%
Agree	41%
Unsure	16%
Disagree	10%
Strongly disagree	3%
Total	100%

Part 3. Background

Q2. Approximately, how many customer and/or consumer-facing websites does your company have in production today? Your best guess is welcome.	Pct%
1 to 5	8%
6 to 10	11%
11 to 20	21%
21 to 30	29%
31 to 40	17%
41 to 50	5%
51 to 100	4%
More than 100	5%
Total	100%
Extrapolated value	30.2

Q3. What types of clients login to your website? Please check all that apply.	Pct%
Customers on a desktop or laptop using a web browser	95%
Customers on a mobile device using a mobile browser	64%
Customers on a mobile device using your company's mobile app	37%
Third-parties (e.g. partners, aggregators and others)	49%
Total	245%

Q4. In an average month, how many credential stuffing attacks does your company detect? Your best guess is welcome.	Pct%
None	0%
1 to 5	41%
6 to 10	38%
11 to 20	12%
21 to 50	4%
51 to 100	3%
More than 100	2%
Total	100%
Extrapolated value	12.7

Q5. What percentage of credential stuffing attacks do you think go undetected by your company? Your best guess is welcome.	Pct%
None	2%
1 or 10%	13%
11 or 25%	31%
26 or 50%	34%
51 or 75%	12%
76 or 100%	8%
Total	100%
Extrapolated value	33.5%

Q6. How many user accounts are typically targeted per credential stuffing attack? Your best guess is welcome.	Pct%
1 to100	19%
101 to 500	35%
501 to 1,000	28%
1,001 to 5,000	11%
5,001 to 10,000	5%
More than 10,000	2%
Total	100%
Extrapolated value	1,252

Q7. What percentage of credential stuffing attempts is successful (i.e. valid credentials are identified)? Your best guess is welcome.	Pct%
None	0%
Less than 1%	0%
1 to 2%	4%
3 to 4%	8%
5 to 6%	18%
7 to 8%	21%
9 to 10%	12%
11 to 20%	9%
More than 20%	28%
Total	100%
Extrapolated value	12.4%

Q8. What negative consequences resulting from a credential stuffing attack have you experienced? Please check all that apply	Pct%
Application downtime from large spikes in login traffic	67%
Compromised accounts leading to fraud-related financial losses	43%
Costs to remediate compromised accounts, including call-center time or manual investigation/analysis by the security or fraud team	63%
Lower customer satisfaction	50%
Lost business due to customers switching to competitors	41%
Damaged brand equity from news stories or social media	17%
Other (please specify)	5%
Total	286%

Part 4. Estimating money lost to fraud

Q9. Please estimate the amount of money lost to fraud per compromised account. You can use any metric appropriate to your company, such as average order value, average account balance or monthly fees avoided.	Pct%
Less than $100	25%
$100 to $500	29%
$501 to $1,000	22%
$1,001 to $5,000	14%
$5,001 to $10,000	8%
More than $10,000	2%
Total	100%
Extrapolated value	$1,535

Q10. In the past 12-month period, what percentage of your company's total revenues (gross sales) were lost due to Internet fraud? Your best guess is welcome.	Pct%
None	2%
Less than 1%	6%
1 to 2%	22%
3 to 4%	20%
5 to 6%	17%
7 to 8%	15%
9 to 10%	8%
More than 10%	10%
Total	100%
Extrapolated value	5.1%

Q11. In the past 12-month period, what percentage of Internet fraud was enabled by credential stuffing attacks? Your best guess is welcome.	Pct%
None	3%
Less than 5%	11%
5 to 10%	16%
11 to 25%	29%
26 to 50%	21%
51 to 75%	10%
76 to 100%	10%
Total	100%
Extrapolated value	30%

Part 5. Estimating the cost of preventing fraud

Q12. Within your organization, how many security or anti-fraud personnel are involved in the **detection and containment** of credential stuffing attacks?	Pct%
None	2%
Less than 5	31%
5 to 10	26%
11 to 15	23%
16 to 20	8%
21 to 25	6%
More than 25	4%
Total	100%
Extrapolated value	10.2

Q13. In your opinion, how has the volume or frequency of credential stuffing attacks changed over the past 12 months?	Pct%
Significant increase	25%
Increase	33%
Stayed the same	28%
Decrease	9%
Significant decrease	5%
Total	100%

Q14. In your opinion, how has the severity of credential stuffing attacks changed over the past 12 months?	Pct%
Significant increase	21%
Increase	31%
Stayed the same	37%
Decrease	8%
Significant decrease	3%
Total	100%

Q15. Please rate each of the following six solutions and capabilities for effectiveness against credential stuffing attacks using the 10-point scale provided below each item. Please skip each question if it is not applicable.	
Q15a. Manually identifying attacks based on spikes in login attempts	Pct%
1 or 2	9%
3 or 4	13%
5 or 6	33%
7 or 8	34%
9 or 10	11%
Total	100%
Extrapolated value	6.00

Q15b. Blocking individual attackers by IP address	Pct%
1 or 2	8%
3 or 4	12%
5 or 6	26%
7 or 8	25%
9 or 10	29%
Total	100%
Extrapolated value	6.60

Q15c. Rate limiting individual IP addresses based on the number login attempts	Pct%
1 or 2	8%
3 or 4	14%
5 or 6	21%
7 or 8	31%
9 or 10	26%
Total	100%
Extrapolated value	6.56

Q15d. Using a web application firewall (WAF) solution	Pct%
1 or 2	4%
3 or 4	12%
5 or 6	29%
7 or 8	36%
9 or 10	19%
Total	100%
Extrapolated value	6.58

Q15e. Using a dedicated bot detection or mitigation solution	Pct%
1 or 2	5%
3 or 4	6%
5 or 6	15%
7 or 8	36%
9 or 10	38%
Total	100%
Extrapolated value	7.42

Q15f. Using an identity management solution to identify compromised accounts	Pct%
1 or 2	4%
3 or 4	9%
5 or 6	17%
7 or 8	37%
9 or 10	33%
Total	100%
Extrapolated value	7.22

Q16. Approximately, how many hours each week are spent **organizing and planning** the organization's approaches to the detection and containment of credential stuffing? Please estimate the aggregate hours of the IT and IT security (SecOps) and fraud teams.	Pct%
Less than 5	6%
5 to 10	13%
11 to 25	18%
26 to 50	24%
51 to 100	19%
101 to 250	15%
251 to 500	5%
More than 500	0%
Total	100%
Extrapolated value	73.03

Q17. Approximately, how many hours each week are spent **analyzing and investigating possible** credential stuffing attacks? Please estimate the aggregate hours of the IT security (SecOps) and fraud team.	Pct%
Less than 5	0%
5 to 10	2%
11 to 25	14%
26 to 50	12%
51 to 100	29%
101 to 250	26%
251 to 500	13%
More than 500	4%
Total	100%
Extrapolated value	145.62

Q18. Approximately, how many hours each week are spent conducting **forensic analysis** for those accounts, believed to have been compromised via credential stuffing? Please estimate the aggregate hours of the IT security (SecOps) and fraud team.	Pct%
Less than 5	10%
5 to 10	7%
11 to 25	11%
26 to 50	30%
51 to 100	27%
101 to 250	14%
251 to 500	1%
More than 500	0%
Total	100%
Extrapolated value	62.96

Q19. Approximately, how many hours each week are spent **documenting and/or reporting** upon credential stuffing incidents in conformance with policies or compliance mandates)? Please estimate the aggregate hours of the IT, security (SecOps) and fraud team.	Pct%
Less than 5	2%
5 to 10	10%
11 to 25	17%
26 to 50	33%
51 to 100	24%
101 to 250	12%
251 to 500	2%
More than 500	0%
Total	100%
Extrapolated value	63.07

Part 6. Estimating the cost of remediating compromised accounts

Q20. What remediation efforts are conducted when you identify a compromised account? Please select all that apply	Pct%
Send the account owner a password reset email	88%
Call the account owner to explain the situation	18%
Lock down the account	69%
Investigate the history of the account to identify previously undetected fraud	54%
Other (please specify)	4%
Total	233%

Q21. Approximately, how many hours each week are spent **containing and remediating** credential-based attacks? Please estimate the aggregate hours of the IT and IT security (SecOps) team.	Pct%
Less than 5	0%
5 to 10	2%
11 to 25	10%
26 to 50	15%
51 to 100	26%
101 to 250	29%
251 to 500	12%
More than 500	6%
Total	100%
Extrapolated value	156.31

Part 7. Estimating other costs resulting from credential stuffing

Q22a. In an average month, how much application downtime resulting from credential stuffing attacks do you experience? Please frame your response for all customer-facing websites (taken together).	Pct%
None	4%
Less than 1 hour	10%
1 to 2 hours	16%
3 to 5 hours	21%
6 to 10	30%
11 to 24 hours	12%
More than 24 hours	7%
Total	100%
Extrapolated value (hours)	7.42

Q22b. On average, what is the total cost your organization incurs for one (1) hour of application downtime resulting from credential stuffing attacks. Your best guess is welcome.	Pct%
Less than $100	1%
$100 to $500	6%
$501 to $1,000	12%
$1,001 to $5,000	21%
$5,001 to $10,000	30%
$10,001 to $50,000	19%
$50,001 to $100,000	4%
More than $100,000	7%
Total	100%
Extrapolated value	$19,389

Q23. What is the percentage of customers that leave or switch to a competitor after learning their credentials were violated (stolen)? Your best guess is welcome.	Pct%
None	20%
Less than 5%	35%
5 to 10%	36%
11 to 20%	4%
21 to 50%	2%
51 to 75%	2%
76 to 100%	1%
Total	100%
Extrapolated value	7.6%

Q24. What is the average value per customer? Please use any metric appropriate to your company such as the average order value, average account balance or monthly fees avoided. Your best guess is welcome.	Pct%
Less than $100	25%
$101 to $500	23%
$501 to $1,000	31%
$1,001 to $5,000	11%
$5,001 to $10,000	7%
More than $10,000	3%
Total	100%
Extrapolated value	$1,494

Part 8. Other questions

Q25a. In your opinion, how difficult are credential stuffing attacks to **detect**?	Pct%
Very difficult	25%
Difficult	28%
Somewhat difficult	28%
Not difficult	10%
Easy	9%
Total	100%

Q25b. In your opinion, how difficult are credential stuffing attacks to **fix or remediate**?	Pct%
Very difficult	31%
Difficult	26%
Somewhat difficult	25%
Not difficult	13%
Easy	5%
Total	100%

Q25c. In your opinion, how difficult is it to know the "real" employees, customers and/or users from criminal imposters who are accessing your website using stolen credentials?	Pct%
Very difficult	26%
Difficult	28%
Somewhat difficult	29%
Not difficult	9%
Easy	8%
Total	100%

Q26. Who are **most responsible** for curtailing credential stuffing attacks on your company's websites? Please check no more than two choices.	Pct%
CEO /COO	3%
CIO/ CTO	28%
CISO/ CSO	20%
Head, legal	3%
Compliance/ audit	2%
Data center / IT operations	9%
Fraud prevention/ management	21%
Head, risk management	16%
Line of business/ management	32%
No one function has overall responsibility	40%
Web hosting service provider	13%
Other (please specify)	5%
Total	187%

Part 9. Your role and organization

D1. What organizational level best describes your current position?	Pct%
Senior Executive/ VP	6%
Director	14%
Manager	20%
Supervisor	12%
Technician/ Staff/ Analyst	40%
Contractor	5%
Other	3%
Total	100%

D2. Check the primary person you or your management reports to within the organization.	Pct%
CEO/ COO	1%
CIO/ CTO	28%
CISO/ CSO	15%
Data center/ IT operations	6%
Head, compliance or audit	2%
Head, fraud prevention/ management	11%
Head, legal	2%
Head, risk management	9%
Line of business management	26%
Total	100%

D3. What industry best describes your organization's industry focus?	Pct%
Entertainment & Gaming	7%
Financial Services	29%
Media	11%
Retail & eCommerce	33%
Travel & Hospitality	17%
Other	3%
Total	100%

D4. What is the worldwide headcount of your organization?	Pct%
Less than 100	12%
100 to 500	21%
501 to 1,000	23%
1,001 to 5,000	16%
5,001 to 25,000	13%
25,001 to 75,000	7%
More than 75,000	8%
Total	100%

Please contact research@ponemon.org or call us at 800.887.3118 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.