239 NW 13th Ave., #205
Portland, OR 97209
503.220.0575

www.dhmresearch.com

Oregonians' Attitudes about Cyberattacks and Corporate Reputation

INTRODUCTION & METHODOLOGY

From September 10 to 18, 2019, DHM Research and ReputationUs conducted a survey of Oregonians to assess their experiences and opinions about cybersecurity and corporate reputation.

Research Methodology: The online survey consisted of 562 adults in Oregon and took approximately 12 minutes to complete. This is a sufficient sample size to assess opinions generally and to review findings by multiple subgroups.

Respondents were members of a professionally maintained online panel. Panelists are recruited randomly by telephone. Once becoming members of the panel, they are surveyed on a monthly basis about civic, social and cultural affairs.

A variety of quality control measures were employed, including questionnaire pre-testing and validation. A combination of quotas and weighting by age, gender, area of state, and education were used to match the demographic makeup of Oregon's adult population.

Statement of Limitations: Any sampling of opinions or attitudes is subject to a margin of error. The margin of error is a standard statistical calculation that represents differences between the sample and total population at a confidence interval, or probability, calculated to be 95%. This means that there is a 95% probability that the sample taken for this study would fall within the stated margin of error if compared with the results achieved from surveying the entire population. The margin of error for this survey is ±4.1%.

DHM Research Background: DHM Research has been providing opinion research and consultation throughout the Pacific Northwest and other regions of the United States for over 40 years. The firm is nonpartisan and independent and specializes in research projects to support public policy making.

Oregonians are increasingly victims of cyberattacks and online fraud.

- To provide context to Oregonians' experiences, the survey started by asking a series of questions from a national study conducted by Pew Research in 2017. There are striking increases in negative experiences over the last two years.
    - 73% of Oregonians now report that they been notified that their personal information, such as an account number, has been compromised. In 2017, just 35% of Americans reported that this had happened to them.
    - 56% of Oregonians say that they have noticed fraudulent charges on their debit or credit cards, an increase from 41% in the 2017 study.
    - And 41% of Oregonians have received a notice that their Social Security number has been compromised. Just 15% of Americans had reported this happening in 2017.

Oregonians believe banks and healthcare providers protect their customers' personal information. They find internet and cell phone providers the least trusted.

- 84% of Oregonians are at least "somewhat confident" that their bank effectively protects their personal financial information, and 74% are similarly confident that their healthcare provider will protect their medical information. However, this confidence is not absolute. Much smaller percentages say that they are "very" confident in their banks and healthcare providers (33% and 22% respectfully).
- Oregonians have less confidence in the internet (50%) and cell phone (48%) providers.

When companies are hit by cyberattacks, Oregonians are likely to hold the companies partially responsible.

- Survey respondents were given the following scenario: a large corporation is a victim of a cyberattack that exposed their customers' financial and personal information. They were then asked to allocate responsibility to the corporation and the hacker. Oregonians said the corporation shared 46% of the responsibility and the hacker 54%.

Companies that are not able to keep personal information secure are at risk of losing their customers.

- More than four in ten Oregonians said that it is "very unlikely" that they would remain a customer of a company—even one that they had been loyal to—if their personal information was stolen to: set up a fake credit card account (48%); shared on the internet (43%); or caused their credit score to decline (41%).

Helping cyberattack victims understand their risk is important when communicating about cyberattacks.

- 70% of Oregonians said that they would be more concerned if their bank or credit union information were "one of hundred" stolen in a cyberattack, compared to 19% who said they would be more concerned if their account information was "one of thousands" stolen.
- Oregonians would also be more concerned by an attack from an American cybercriminal (49%) than by an attack carried out by a foreign government (33%).

Companies that communicate the steps they are taking to upgrade their security procedures are more trusted than those that stay silent about attacks and their security.

- Oregonians in this survey were asked which they would trust more to protect their personal information: a large business that was a cyberattack victim but responded by upgrading its security procedures, or a large business than never said whether or not they have been a victim of a cyberattack. By a margin of 60% to 8%, Oregonians said they would have more trust in a business that was attacked and upgraded their systems than a business that kept quiet about the attack.
- An overwhelming 96% of Oregonians would prefer a corporation acknowledge a cyberattack and offer free credit monitoring *even if there was no evidence that their personal information was stolen*, rather than the corporation not say anything about the attack so as to not unnecessarily worry their customers.
- Given the fact cyberattacks are on the rise, and most Oregonians have some experience of being a victim, they are likely to assume that large businesses are under threat. This result indicates that rather than trying to minimize or be silent about an attack, a more effective approach for businesses is to acknowledge the threat, be upfront about incidents, and aggressively communicate about what they are doing to continually enhance customer safety.

Oregonians do not want companies or their local governments to pay ransoms to cybercriminals.

- In the last few years, there have been high-profile cyberattacks on businesses and local governments. The criminals freeze access to files and records and demand a ransom to unlock them. The City of Baltimore was locked out of much of their computer systems for weeks, and paid $18 million to rebuild their system, rather than paying a $75,000 ransom demand.
- Oregonians were asked what they would like their local government and their bank to do if they experience this kind of attack. A strong majority do not want their local government (73%) or bank (66%) to pay the ransom.

DHM Panel
Cybersecurity

September 10–18, 2019
N=562; ±4.1% margin of error
12 minutes

WARM UP

1. All things considered, do you think Oregon is headed in the right direction, or off on the wrong track?

Response category	n=562
Right direction	40%
Wrong track	45%
Don't know	15%

[New page]

CYBERSECURITY

These first questions are about your personal information and cybersecurity.

[New page]

To the best of your knowledge, have you ever: **[Randomize]**

Response category	Yes	No	Not applicable	Don't know
2. Received a notice that your Social Security number had been compromised				
DHM Panel n=559	41%	57%	--	2%
Pew Research (2017)	15%	84%	--	1%
3. Received a notice that other sensitive personal information, such as your account number, had been compromised				
DHM Panel n=560	73%	26%	--	1%
Pew Research (2017)	35%	64%	--	1%
4. Noticed fraudulent charges on your debit or credit card				
DHM Panel n=560	56%	43%	--	1%
Pew Research (2017)	41%	58%	--	--
5. Had someone take over your email account without your permission				
DHM Panel n=560	11%	82%	<1%	7%
Pew Research (2017)	19%	80%	--	1%
6. Had someone take over your social media account without your permission				
DHM Panel n=560	16%	76%	5%	3%
Pew Research (2017)	21%	79%	--	--

[New page]

How confident are you that the following are effectively protecting your private financial, medical or other personal information? **[Randomize]**

Response category	Very confident	Somewhat confident	Not too confident	Not at all confident	Not applicable	Don't know
7. Your bank	33%	51%	9%	4%	--	2%
8. Your credit card company	21%	43%	21%	7%	7%	1%
9. Your healthcare provider	22%	52%	14%	7%	1%	4%
10. Your health insurance provider	20%	46%	19%	8%	1%	5%
11. Your employer	19%	32%	7%	5%	36%	1%
12. Your internet provider	9%	41%	28%	14%	3%	4%
13. Your cell phone provider	11%	37%	26%	16%	5%	6%

[New page]

14. Generally speaking, which would you trust most to protect your personal information from a cyberattack?

Response category	n=544
A small, local business	18%
A mid-sized, regional business	23%
A large, national business	18%
Don't know	40%

15. Generally speaking, which would you trust most to protect your personal information from a cyberattack?

Response category	n=544
A private company	44%
A publicly traded company	13%
The federal government	15%
Don't know	29%

16. Which of these hypothetical businesses would trust most to protect your personal information from a cyberattack?

Response category	n=544
A large business that you knew was recently a victim of a cyberattack and then upgraded all its security procedures	60%
A large business that has never said whether or not they have been a victim of a cyberattack	8%
Don't know	32%

17. Would you support or oppose a law that requires publicly traded or private companies to report to their customers and shareholders if they have been a victim of a cyberattack?

Response category	n=541
Strongly support	76%
Somewhat support	16%
Somewhat oppose	1%
Strongly oppose	3%
Don't know	5%

[New page]

18. Indicate which would concern you the most:

Response category	n=541
Your bank or credit union account information was one of thousands stolen in a cyberattack	19%
Your bank or credit union account information was one of one hundred stolen in a cyberattack	70%
Don't know	11%

19. Indicate which would concern you the most:

Response category	n=541
Your bank or credit union was hacked by a foreign government	33%
Your bank or credit union was hacked by an American cyber criminal	49%
Don't know	18%

[New page]

People may feel differently about their personal information being compromised based on the circumstances and impacts.

Imagine a company that you like and are a loyal customer to. If that company experienced a cyberattack and your personal and financial information was stolen, how likely would you be to remain a customer if the following happened: **[Randomize]**

Response category	Very likely	Somewhat likely	Somewhat unlikely	Very unlikely	Don't know
20. You were not aware of any negative outcomes that affect you personally	25%	40%	16%	12%	8%
21. The stolen data was used to illegally set up a credit card in your name	3%	20%	23%	48%	7%
22. Your credit score declined because of the stolen information	5%	22%	22%	41%	9%
23. Your personal and financial information was shared on the Internet for others to steal	3%	25%	23%	43%	6%

[New page]

Imagine the following scenario.

A large corporation with your credit card and other personal information, such as birthdate and home address, is breached. While there is no evidence that any information was stolen, the hackers had access to the information for one month.

24. In this scenario, which of these actions would you prefer the corporation take if you were a customer of the corporation:

Response category	n=524
Publicly acknowledge the hacking and offer free credit monitoring for one year, even though there is no evidence that your information was stolen.	96%
Do not say anything publicly. You would rather not worry about this unless there is actual evidence that your information is at risk.	2%
Don't know	2%

25. In this scenario, which of these actions would you prefer the corporation take if you owned stock in the corporation:

Response category	n=524
Publicly acknowledge the hacking and offer free credit monitoring for one year, even though there is no evidence that your information was stolen. This would cost the company millions and decrease future profits.	80%
Do not say anything publicly. Large corporations are under constant attack from hackers. There is little reason to worry customers or risk declining profits unless there is clear evidence that the personal information was stolen.	9%
Don't know	11%

[New page]

This year, the City of Baltimore was the victim of a cyberattack. The attackers were able to gain control of the City's computer systems and prevent the City from accessing them. The attackers demanded that the City pay a ransom of $75,000 to unlock their computer systems. The City of Baltimore refused to pay the ransom. So far, the City estimates that it has cost them more than $18 million to rebuild its systems. Because of the attack, residents were temporarily unable to buy or sell a home, pay their water bills or parking tickets, and nearly all employees were unable to access their email.

26. If the city or county that you lived in were a victim of a cyberattack, what would you like your government leaders to do?

Response category	n=521
Pay the ransom to unlock the computer system, even if there is no guarantee the attackers will follow through and it will encourage them to strike again.	9%
Do not pay the ransom, even if it will likely cost your local government more money to restore its systems and government services grid to a halt.	73%
Don't know	18%

[New page]

Many private companies have also been victims of cyberattacks like the one in Baltimore. Imagine that your bank or credit union is a victim of a cyberattack that locks them out of their computer systems and the hackers demand a ransom. Your financial information is on the bank's computer system.

27. If your bank or credit union were a victim of a cyberattack, what would you like the financial institution's leaders to do?

Response category	n=519
Pay the ransom to unlock the computer system, even if there is no guarantee the attackers will follow through and it will encourage them to strike again.	15%
Do not pay the ransom, even if it will likely make it difficult to access your bank accounts and expose your financial information to criminals.	66%
Don't know	18%

[New page]

28. Imagine that a large corporation's computer system is hacked, and its customers' financial records and personal information are stolen. In this scenario, what percent do you think each party is responsible? The total should equal 100%.

Response category	n=505
The corporation	46%
The hacker	54%
Total	**100%**

29. Imagine a local coffee shop that uses a third-party application to handle customer credit cards. The third-party application is hacked and the coffee shop customers' credit card information is stolen. In this scenario, what percent do you think each party is responsible? The total should equal 100%.

Response category	n=505
The coffee shop	9%
The third-party application that handles customer credit cards	42%
The hacker	49%
Total	**100%**

[New page]

DEMOGRAPHICS

These last questions are for demographic purposes only. Your responses are confidential

30. What is your zip code? **[Open]**

31. In what year were you born?

Response category	n=560
18-44	26%
45–64	55%
65+	19%

32. With which of the following gender identities do you identify? Check all that apply.

Response category	n=562
Male	49%
Female	50%
Non-binary or gender non-conforming	1%
Trans	1%
Other	n=3

33. What is your party registration?

Response category	n=503
Democrat	47%
Republican	28%
Non-affiliated/other	26%

34. When it comes to politics and elections are you?

Response category	n=502
Very liberal	17%
Somewhat liberal	29%
Middle of the road	20%
Somewhat conservative	24%
Very conservative	9%

35. What is the highest level of education you have received?

Response category	n=503
High school/GED or less	12%
2-year degree/some college	61%
4-year degree+	27%

36. What was your total household income for 2018? Remember to include everyone and your best guess is okay.

Response category	n=496
Less than $25,000	11%
$25,00–$49,999	18%
$50,000–$74,999	25%
$75,000–$99,999	15%
$100,000–$149,999	24%
$150,000 or more	7%