2021 CONSUMER CYBERSECURITY POLL

Executive Report

CONSUMER PERCEPTIONS SHED LIGHT ON THE NEED FOR CONTINUED CYBERSECURITY EDUCATION

After a tumultuous year of a global pandemic, rapid transitions to remote work and headline-making cyberattacks, consumers have experienced vast changes and spent more time online using digital channels to conduct business than in previous years. So, it's no surprise that 85% of American consumers reported cybersecurity concerns pertaining to their personal confidential data in a recent survey of more than 2,000 U.S. adults age 18 and above, conducted online by global market research firm The Harris Poll on behalf of CSI.

What is surprising, however, is that 92% of Americans expressed cybersecurity concerns in 2019, as reported through a similar survey conducted by The Harris Poll on behalf of CSI.[1] As the risk of ransomware and other cyberattacks seemingly increase, are consumers less concerned about cybersecurity?

This executive report provides key insight into this year's survey results and a comparison to data from 2019, exploring how consumers' cybersecurity perceptions and concerns have shifted.

KEY FINDINGS FROM 2021

- **The top cybersecurity issues** that worry consumers as related to their personal confidential information are identity theft (60%) and stolen credit or debit card information (60%).
- **More than 3 in 4 Americans (76%)** believe their financial institution can protect their personal and payment information from hackers.
- **Nearly half of consumers (48%)** would leave their institution if it suffered a data breach, a decrease of 10 percentage points from 2019 (58%).
- **30% of consumers** believe it is okay to use the same password for an online bank account that they use for other online accounts, which is up from 24% in 2019.
- **A majority of Americans (69%)** believe they know what to do if their personal confidential data is compromised.
- **Half of Americans (50%)** believe a person's payment information is more likely to be compromised when using a physical card versus a digital payment, such as contactless cards or P2P.

FATALISTIC ACCEPTANCE: IS CONSUMER PERCEPTION OF CYBER RISK CHANGING?

Although a substantial number of Americans (85%) reported cybersecurity concerns pertaining to their personal confidential data, that leaves 15% who are not worried about cybersecurity, a number that raises some eyebrows considering the surge in pandemic-related cyberattacks and the impending threat of breaches for both consumers and institutions.

It also marks an increase of seven percentage points in those not concerned about cybersecurity compared to 2019 (8%), which could signal that consumers are becoming desensitized to cybersecurity risks. It's possible that the size, scope and frequency of cybersecurity events are making these breaches appear abstract and distant to the average consumer. And the constant barrage of media coverage on this topic also could be contributing to greater risk tolerance among Americans.

When considering these factors, it is not far-fetched to deduce that many consumers have a collective attitude of fatalistic acceptance. Since many Americans perceive cyberattacks to be beyond their control, it seems they have accepted this risk as part of everyday life. This acceptance may have resulted in lower security standards and lax practices in their personal lives, further exacerbating the likelihood of falling victim to an attack. And consumers with more tolerance for risk and lower security expectations could have adverse effects for financial institutions, making effective cybersecurity education even more important.

Since many Americans perceive cyberattacks to be beyond their control, it seems they have accepted this risk as part of everyday life.

TOP CONCERNS:

Identity Theft and Stolen Card Information

Identity theft and stolen credit or debit card information tie as the top cybersecurity concerns among consumers in 2021, at 60% each. This is down significantly from 2019, when identity theft topped the list of concerns at 73%, followed closely by stolen card information (72%). Despite this change in consumer perceptions, vigilance against both threats is warranted.

As Americans traded in their rush-hour commutes for remote work amid the pandemic, incidents of identity theft skyrocketed. In 2020, the Federal Trade Commission received 1.4 million reports of identity theft—double the number from the previous year.[2] Due to the devastating effects of identity theft and the vast amount of time and resources needed to remedy this issue when it occurs, institutions should continue educating consumers about this risk, along with strategies to avoid it.

And, consumers are right to be wary of stolen card information. Payment-related data, such as card numbers, is valuable if criminals can reuse that information for fraudulent purposes. The pandemic drove Americans to online shopping, and incidents of e-skimming—which occurs when a hacker obtains credentials during an online transaction by installing malicious code in a retailer's website—rose substantially.[3] As the number of consumers who regularly shop online continues to increase, both consumers and institutions must enhance their efforts to combat payment fraud.

Other Cybersecurity Concerns

Nearly half of Americans are also worried about the following as it relates to their personal confidential information:

- **Malicious software being installed on their devices:** 52%
- **Computer viruses and/or worms:** 50%
- **A company they do business with experiencing a data breach:** 45%

The most recent results indicate that a unique opportunity exists for financial institutions to continue building trust with their customers and members by strategically delivering cybersecurity education.

> **"When bank branches closed due to the pandemic in 2020, millions of consumers were forced to use digital channels for the first time. New to online or mobile banking and shopping online, these consumers were focused on learning how to conduct their lives in a digital world. More education on how to protect themselves digitally would be very beneficial as many consumers fell for a wide variety of scams during the past year and a half."**
>
> – Shirley Inscoe
> Senior Analyst at Aite-Novarica Group

Consumers can take precautions to protect themselves from their top concerns and emerging scams, but financial institutions must also find ways to reach them with useful information. In today's rapidly changing world, they must meet customers and members where they are and deliver information using the channels most convenient to them, such as email or virtual trainings.

KEY TAKEAWAY: Americans are becoming increasingly desensitized to the risk of security breaches, making it more critical than ever for financial institutions to break through the noise and educate them on cybersecurity best practices.

CONFRONTING THE COSTS OF A DATA BREACH

According to the 2021 results, nearly half of survey respondents (48%) strongly or somewhat agree they would leave their financial institution if it suffered a data breach. It's interesting to note that more consumers agreed with this statement in 2019 (58%). While this is likely a consequence of how commonplace breaches have become in the minds of consumers, this does not mean institutions should reduce preparedness.

Further, this year's results reveal 59% of respondents in the 35-44 age range would leave their institution after a breach. Considering that 54% of consumers with an annual household income of $100,000 or above also agreed with this statement, institutions have cause for concern, as these important demographics could represent a significant market opportunity.

Breaking the findings down further, 60% of survey respondents who identified a big bank (e.g., Chase, Wells Fargo, etc.) as their primary financial institution agreed that a breach would cause them to leave, compared to 51% of community bank customers and only 45% of credit union members—indicating slightly higher levels of consumer loyalty among community financial institutions.

Considering this data, how would losing nearly half of your client base affect your institution, including high income earners? It's critical that your institution have a plan in place that outlines how you would respond in the event of a breach.

IS YOUR INSTITUTION PREPARED FOR A BREACH?

In July 2021, U.S. banks and credit unions were among the nearly 1,500 businesses affected by the supply chain ransomware attack levied on Kaseya, an IT solutions developer.[4] Many of these institutions and other businesses were forced to contend with the aftermath of the attack, weighing the costs of impact on operations or paying for the decryption tool from the cybercriminals. Businesses were threatened with ransom amounts varying from $45,000 to $5 million depending on their size.[5] Though Kaseya obtained a universal key to unlock customer files a few weeks after the attack without paying a ransom, the outcome in all ransomware attacks is not always so positive.

According to the 2021 results, nearly half of survey respondents (48%) strongly or somewhat agree they would leave their financial institution if it suffered a data breach. It's interesting to note that more consumers agreed with this statement in 2019 (58%).

More Food for Thought

The IBM 2020 Cost of a Data Breach Report[6] found the following:

- The average cost of a data breach in 2020 was $3.86 million, with the U.S. as the country with the highest associated costs.
- 52% of breaches were caused by malicious attacks vs. human error or system glitches.
- The financial services industry experienced an average total cost of a breach of $5.85 million, higher than the average total costs of less regulated industries.

Financial institutions are attractive targets for ransomware due to the types of personal information they store about customers and members. Segmented approaches to security are not enough to defend against ransomware and other attacks; a holistic, layered approach to cybersecurity will strengthen an institution's protections.

In addition to the latest security defenses, institutions should have a strong incident response team that is backed up by an effective—and regularly tested—incident response plan. It's critical that institutions know the procedures for notifying customers or members and communicating what steps are being taken to protect them. Institutions should also avoid going silent in response to a security breach; any silence is likely to be filled in with misinformation. If consumers believe their institution is handling a security incident well, they are likely less inclined to leave.

Americans who said they would leave their institution after a breach:

KEY TAKEAWAY: To mitigate the risk of customer attrition, institutions should have an incident response plan in place to direct their actions in the event of a breach.

INCIDENT RESPONSE PLAN BEST PRACTICES

Pre-Incident

1. Identify and allocate appropriate internal and external resources
2. Understand objectives and identify assets
3. Develop a clear picture of connectivity
4. Define "incident"
5. Identify the most likely incidents
6. Create specific procedures
7. Train responsible staff
8. Develop a communication plan focused on a rapid, transparent and accurate message
9. Test and update the plan

Post-Incident

1. Activate the plan immediately
2. Assess and contain the incident as quickly as possible
3. Identify and eradicate the source/cause
4. Collect and preserve forensic data
5. Begin recovery procedures
6. Initiate communication plan
7. Analyze the effectiveness of the plan and adjust

STRONG AUTHENTICATION:

The Key to Enhancing Account Security

One of the most troubling results of this year's survey is that 30% of Americans agree that it is okay to use the same password for an online bank account that they use for other online accounts, representing an increase of six percentage points from 2019 (24%).

Alarmingly, 43% of Americans ages 18-44 believe it is okay to use the same password. Looking across different primary financial institutions, 33% of big bank customers, 25% of credit union members and just 22% of community bank customers believe this to be true.

Clearly, there is a need for financial institutions to reinforce the importance of secure passwords. For this, think outside the box; consider witty or humorous approaches to drive home your message.

> **Passwords are like toothbrushes. You should never share them, and you should change them periodically.**

Ensure customers or members understand that a password is a key. Would you use the same key to unlock your car as you would a vault filled with priceless valuables? Likely not. Accounts with more critical data—such as bank accounts—require a stronger key.

In addition, to make it more difficult for cybercriminals to obtain unauthorized account access, financial institutions should provide multi-factor authentication (MFA) and encourage customers and members to adopt this technology. Since MFA requires multiple credentials, a cybercriminal cannot gain account access just by cracking or obtaining the password. MFA can also help prevent the spread of malware—including ransomware—by enforcing a secondary authentication process that malware cannot use. A recent Javelin report found that consumers who are more aware of cyber threats are less likely to mind some friction when logging into an account, such as the additional step of MFA.[7]

Consumers who use the same password for multiple accounts are at risk for various cyber threats, including credential stuffing attacks. If a cybercriminal obtains lists of usernames, email addresses and passwords on the dark web, they can use this information to launch credential stuffing attacks—automated attacks in which the usernames and passwords are used on other sites in attempt to gain access to customer accounts. The SEC's Office of Compliance Inspections and Examinations issued an alert in 2020 about increased incidents of this type of attack.[8] A consumer using the same password for their online bank account as they do for their favorite ecommerce site leaves an opportunity ripe for hacking.

KEY TAKEAWAY: Financial institutions should provide MFA and reinforce the importance of strong passwords to mitigate the risk of unauthorized account takeover.

PASSWORD SAFETY TIPS FOR CONSUMERS

1. Create passwords with at least 15 characters
2. Prioritize length but don't rule out complexity as it amplifies the strength
3. Use unique passwords for all important accounts
4. Always use multi-factor authentication when available to supplement passwords
5. Change password if evidence of compromise exists
6. Avoid using identifying information (e.g., spouse's name, important dates, hobbies, etc.)
7. Consider using phrases or full punctuated sentences as passwords and avoid using words from the dictionary
8. Use a secure password manager or password generator
9. Never share passwords

ARE CONSUMERS TOO CONFIDENT?

An overwhelming majority of Americans (69%) claim they know what to do if their personal confidential data is compromised. Credit union members are more likely than big bank customers to be confident that they know what to do if their data is compromised (75% vs. 68%), possibly a result of the strong relationships credit unions cultivate with their members. But this still indicates that one in four credit union members could require additional guidance.

Though similar to the results from 2019—in which 70% of survey respondents agreed they knew what to do in the event of a breach—evidence exists that consumers may be overconfident in this assessment.

Consider these findings from the sixth annual Norton Cyber Safety Insights Report[9]:

- **2 in 5 Americans (40%)** admit they don't know how to protect themselves from cybercrime
- **Almost half of Americans (46%)** would not know what to do if their identity was stolen
- **77%** wish they had more information on what to do in the event of identity theft

An opportunity exists for institutions to educate customers or members on the necessary steps to take after their information is potentially compromised. Institutions should reinforce their commitment to their client base by making it easy for them to reach out for assistance in the event they suspect a breach. A community financial institution that prioritizes consumer education could become the go-to institution for advice and assurance, which could help expand market reach.

WHAT SHOULD CONSUMERS DO POST-BREACH?

1. **Notify:** Notify their financial institutions, insurance company and credit reporting agencies.
2. **Change:** Close all financial accounts and reopen them. Change passwords and/or PIN for each account.
3. **Action:** Take action! Work with credit reporting agencies to remove incorrect data from their credit report, work with financial services providers to reverse fraudulent charges and file a police report.
4. **Monitor:** Monitor their credit report for the next year, evaluating diligently after the first 30 days post-breach and then quarterly.

KEY TAKEAWAY: As cybersecurity threats continue to evolve, educate customers and members on steps to take if a potential breach has occurred.

WHAT DO CONSUMERS THINK ABOUT PAYMENTS SECURITY?

The pandemic accelerated adoption of digital payments for many consumers, so it is noteworthy that half of Americans (50%) agree that a person's personal payment information (i.e., account number) is more likely to be compromised when using a physical card vs. a digital payment such as a P2P payment or digital wallet. This belief is more prevalent among respondents in the 18-34 (52%), 35-44 (56%) and 45-54 (58%) age ranges compared to those ages 55+ (41%).

Because of the increased reliance on digital channels, including digital payments, financial institutions should embrace cryptography and tokenization instead of static magstripe processes, as the former offer enhanced security protections. Tokenization creates dynamic tokens that are device or merchant specific, protecting a consumer's transaction. If a breach were to occur at one merchant, this technology limits the potential of compromised data and prevents subsequent fraud if the same credentials were used elsewhere.

Since certain risks exist with physical cards (e.g., losing the card, skimming, etc.) ensure customers or members have enhanced security controls on cards, and provide them access to secure digital payments. Even though the pandemic accelerated adoption of digital, institutions should continue education around using digital payments as well as how to be more responsible with physical cards, including encouraging customers or members to be mindful about where they use their cards and only making purchases from trusted sites and entities.

KEY TAKEAWAY: Embrace the latest payments technology and provide consumers with resources on best practices for using secure digital payments.

CONSUMER CONFIDENCE IN FINANCIAL INSTITUTIONS

A top priority of financial institutions is protecting consumer data. The good news? This year's poll revealed about 3 in 4 Americans (76%) agree that their financial institution can protect their personal and payment data from hackers. Nearly 4 in 5 credit union members (79%) and community bank customers (78%) believe their financial institution can protect their data from hackers.

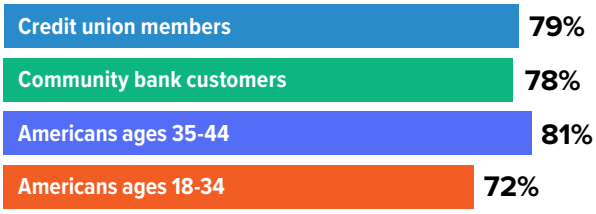
Another interesting result: 81% of survey respondents ages 35-44 believe their institution can protect their data, but this dropped to 72% for ages 18-34. This indicates a prime opportunity for institutions to focus on building confidence with the latter group, which represents potential long-term customers or members.

As a community financial institution, take advantage of this consumer trust and build upon it by reinforcing how you are safeguarding customer or member data through institution-sponsored cybersecurity awareness training.

Another effective way to build trust among consumers is by avoiding your institution making headlines for a cyberattack. Implementing strong security controls and multiple layers of protection will better position your institution to fend off threats.

Additionally, consider partnering with a trusted managed services provider (MSP) to empower your cybersecurity initiatives and ensure your data, systems and users remain protected. Teaming up with an MSP allows you to leverage their security and compliance expertise, further strengthening the cybersecurity posture of your institution and offering enhanced protections for customers and members.

Consumers who believe their financial institution can protect their personal and payment data from hackers:



KEY TAKEAWAY: Community financial institutions should continue building trust among consumers by promoting how they safeguard data and hosting cybersecurity awareness training.

EMPOWERING CONSUMERS WITH INFORMATION

Criminals are continually adopting new tactics and methods to target more victims. Empowering consumers with information through cybersecurity awareness campaigns is an important step in the fight against cybercrime. As evident in these survey results, consumers might be desensitized to the growing risk of cybersecurity incidents, posing risks to your institution.

Security-conscious consumers lower the level of risk for institutions. If a consumer is following cybersecurity best practices, then they are less likely to be the victim of a breach, and in turn, the institution is less likely to spend time and resources reimbursing the consumer and responding to the effects of the breach.

Providing valuable education and promoting good cyber hygiene will mitigate cybersecurity risk for consumers and your institution while increasing the potential for new business through knowledge sharing.

TIPS FOR DEVELOPING CYBERSECURITY AWARENESS CAMPAIGNS

1. **Avoid a one-size-fits-all approach;** different consumers have varying needs and concerns
2. **Create campaigns** to reach different groups, tailoring based on age, work schedules, etc.
3. **Think creatively** about how best to communicate with consumers
4. **Meet customers and members** where they are by leveraging digital channels to deliver your message
5. **Go virtual** to reach a broader audience – don't limit the size and scope of your event to physical locations
6. **Motivate consumers** through actionable tips and inspire confidence in your institution

THE OVERALL SURVEY TAKEAWAY

The Best Defense? Embracing a Layered Approach to Cybersecurity

As cybercriminals adopt the latest tactics to carry out malicious attacks against organizations and consumers, financial institutions should embrace a layered approach to cybersecurity to strengthen their defenses. A key component of a layered, holistic approach to cybersecurity includes continued education among consumers, reinforcing the importance of security awareness and best practices. Cyberattacks will likely continue to make headlines but deploying multiple layers of protection mitigates risk and safeguards data and systems while providing peace of mind for consumers.

Survey Methodology

This survey was conducted online within the United States by The Harris Poll on behalf of CSI June 10-14, 2021, among 2,066 adults, age 18 and older. This online survey is not based on a probability sample and therefore no estimate of theoretical sampling error can be calculated. For complete survey methodology, including weighting variables and subgroups sample sizes, please contact Laura Sewell at laura.sewell@csiweb.com.

ABOUT COMPUTER SERVICES, INC.

Computer Services, Inc. (CSI) delivers core processing, digital banking, managed cybersecurity, cybersecurity compliance, payments processing, print and electronic document distribution, and regulatory compliance solutions to financial institutions and corporate customers, both foreign and domestic. Management believes exceptional service, dynamic solutions and superior results are the foundation of CSI's reputation and have resulted in the Company's inclusion in such top industry-wide rankings as IDC Financial Insights FinTech 100, Talkin' Cloud 100 and MSPmentor Top 501 Global Managed Service Providers lists. CSI has also been recognized by Aite Group, a leading industry research firm, as providing the "best user experience" in its 2019 AIM Evaluation: The Leading Providers of U.S. Core Banking Systems. In addition, CSI's record of increasing its dividend each year for 49 years has earned it a designation of one of the financial media's "Dividend Aristocrats." CSI's stock is traded on OTCQX under the symbol CSVI. For more information, visit csiweb.com.

RESOURCES

[1] CSI, Executive Report: CSI Consumer Cybersecurity Poll 2019.
[2] Federal Trade Commission, Identity Theft Awareness Week Starts Today.
[3] PYMNTS.com, Deep Dive: Responding to The Rising Threat of eSkimming.
[4] CISA, Kaseya Ransomware Attack: Guidance for Affected MSPs and Their Customers.
[5] Washington Post, Company Hit by Massive Ransomware Attack Obtains Key to Unlock Customer Files.
[6] IBM.com, 2020 Cost of a Data Breach Report.
[7] Javelin, The Weakest Link: Changing Consumers' Cybersecurity Behaviors.
[8] Office of Compliance Inspections and Examinations, Cybersecurity: Safeguarding Client Accounts against Credential Compromise.
[9] Norton LifeLock, COVID-19 Pandemic Leaves Consumers Vulnerable to Cybercrime.