Cyberint

Impactful Intelligence

SECURITY MATTERS

Consumer Views On Cybersecurity

Retail & Finance 2024

A comprehensive survey exploring consumer attitudes to cyber threats in the retail & finance sectors

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Cyberint's 'Security Matters: Consumer Views on Cybersecurity Retail & Finance 2024' report delves into the cybersecurity landscape of the finance and retail sectors, revealing business-essential statistics and consumer sentiments.

Data gathered from over

1000 respondents

60% consumers

likely cease shopping with a retailer post-breach

83% respondents

consider abandoning finance apps if their data is compromised

81% consumers

show a willingness to embrace additional security measures

Findings from the survey emphasize the strategic importance of cybersecurity in maintaining consumer loyalty and the need for businesses to adopt proactive and targeted cybersecurity approaches.

BACKGROUND

Cybersecurity plays an increasingly pivotal role in the digital landscape as both the frequency cost, and sophistication of attacks multiply. Finance and retail are among the most targeted sectors for their vast data, making them especially enticing for cybercriminals.

Cyberint's survey exploring consumer attitudes to cybersecurity threats in retail and finance takes what we know about the importance and impact of cyber one step further. Not only does it reinforce the fact that cyber defenses shield against direct financial losses, but it also shows just how impactful a breach is on a brand's reputation. Lastly, it provides insights into consumers' willingness to partner with companies in each industry to remediate those threats.

The finance industry faces unprecedented cybersecurity challenges, making client data protection and risk mitigation paramount. Cybercrime poses a persistent and costly threat, with an IBM survey revealing that a data breach in the industry typically costs around $5.85 million. It's no wonder that 10% of all attacks are financial breaches.

> "Comprehensive threat intelligence in today's cyber landscape isn't complete without fully understanding who you protect. We put together this tailored report for the retail and finance sectors to both show the incredible impact a strong cybersecurity posture can create, as well as some direction on how to achieve it.
>
> **Yochai Corem** | CEO of Cyberint

> Cyberint's report illuminates the urgent need for robust cybersecurity measures in finance and retail. With staggering statistics revealing the repercussions of breaches and consumer sentiments that drive brand loyalty, the report serves as a critical guide for businesses navigating the evolving landscape of digital vulnerabilities.
>
> **Danny Miller** | VP Marketing at Cyberint

Threat actors are increasingly targeting e-commerce businesses that are reliant on technology for critical functions, from order processing and inventory management to fulfillment. The frequency of attacks is already disturbing, with 19% of retailers already self-reporting as victims and a large majority remaining apprehensive, ranking it as the third-highest business concern behind supply chain risk and economic uncertainty.

This report aims to deliver a comprehensive overview of the state of cybersecurity in the retail and finance sectors and the existing gaps they have in securing customer data using external sources. The findings speak to the importance of businesses in the retail and finance industries adopting proactive and targeted cybersecurity approaches that are both practical and effective. While the potential loss of business due to cyber attacks is likely alarming for many organizations, cyber's impact on brand and the bottom line also presents an opportunity to adopters of effective cyber approaches in each sector.

METHODOLOGY

To capture consumers' insights in the retail and finance sectors, Cyberint surveyed 1,034 respondents across the US, using a representative sampling method of varying ages, genders, device types used, and household incomes. Cyberint asked ten questions regarding valuable data on consumer awareness, concerns, and expectations regarding the security of their personal information.

KEY INSIGHTS

Consumer behavior in the aftermath of data breaches reveals significant trends and underscores the real and tangible consequences that security breaches can have on a brand's reputation and customer base.

over **60%** consumers

likely cease shopping with a retailer post-breach

A solid majority of retail sector consumers (over 60%) we surveyed expressed some likelihood that they would cease shopping with a retailer post-breach, with higher-income individuals exhibiting an even more pronounced inclination at 74%. To put that in perspective, a "pretty catastrophic" drop for retailers at the beginning of the COVID-19 pandemic was around 8.7%, with the UK experiencing a drop in the low double digits.

Over 60% is a huge deal. While 22% of stolen credentials in the retail sector come from ransomware attacks, the costs of those attacks might be higher in terms of brand damage than the ransom itself.

83% respondents

would consider abandoning finance apps if their data was compromised

In the finance industry, the figures are even more extreme with 83% of respondents indicating they would consider abandoning finance apps if their data was compromised. This underscores the heightened sensitivity surrounding personal finances, revealing a discernibly lower threshold for consumer forgiveness. In 2023, financial organizations shelled out an average of $2.23 million to fully recover after a ransomware attack, with the loss of customers likely adding significantly to that amount.

DETAILED FINDINGS & IMPACT

Q //

HOW LIKELY ARE YOU TO STOP SHOPPING WITH A RETAILER IF YOU READ ABOUT A DATA BREACH THAT COMPROMISED CUSTOMER DATA?

ANSWERED: 1,034
SKIPPED: 0

VERY LIKELY	SOMEWHAT LIKELY	NEUTRAL	NOT VERY LIKELY	NOT LIKELY AT ALL
27%	33%	28%	9.5%	2.5%

According to our survey respondents, the preferred communication method, with 63% isdirect email. While the youngest age group selected push notifications as a close second choice (behind email by 13%), across every age group, finding out from the news or social media was overwhelmingly not preferred. According to IBM, data breaches take almost a year to uncover and mitigate. While reporting incidents is straightforward regarding regulatory requirements, how and when to communicate with customers is far less clear and has high stakes for the customers and the brand's reputation.

Brands must proactively inform consumers via email before they find out elsewhere, or they'll pay a high price.

Q //

HOW WOULD YOU PREFER TO BE INFORMED ABOUT A DATA BREACH INVOLVING ARE TAILER YOU HAVE SHOPPED WITH?

ANSWERED: 1,034
SKIPPED: 0

DIRECT EMAIL NOTIFICATION
63%

PUSH NOTIFICATION ON A RETAILER'S MOBILE APP
18.5%

NEWS ALERT FROM A TRUSTED SOURCE
15%

SOCIAL MEDIA ANNOUNCEMENT FROM THE RETAILER
3.5%

Of all respondents surveyed, 83% indicated they would consider abandoning finance apps if their data is compromised. A sky-high percentage that is even head and shoulders above what consumers indicated about retail suggests that the critical nature of personal finances makes consumers even less forgiving. With 64% of cyberattacks in the financial sector resulting in a data leak, the vulnerability of personal information is a critical concern. Those "very likely" to abandon the app decreased as the age group decreased - 71% of respondents over 60 vs. 41% for those in the 18-29 range.

The message: change may come with new generations, but all are still extremely harsh on finance apps. Even if users aren't likely to abandon a finance app because of a breach, don't count on them as loyal customers when a competitor comes along.

Q //

HOW LIKELY ARE YOU TO ABANDON A FINANCE APP IF YOUR PERSONAL INFORMATION, SUCH AS CREDIT CARD DETAILS OR SOCIAL SECURITY NUMBER, IS LEAKED?

ANSWERED: 1,034
SKIPPED: 0

VERY LIKELY
58%

SOMEWHAT LIKELY
25%

NEUTRAL
12%

NOT VERY LIKELY
4%

NOT LIKELY AT ALL
1%

Frictionless. It's what most great companies aspire to make their experience. With a few clicks, the customer should be able to select their order, pay for it, and have it at their door ASAP. The same goes for finance apps, where money transfers and investments are done simply with as few clicks as possible. By that logic, barriers are the enemy, but our data suggests that, surprisingly, that's not the case regarding security.

Companies have a clear opportunity to embrace their customers as part of their security posture by implementing advanced security features that can contribute to building and maintaining consumer trust. 81% of consumers are universally ready to embrace additional security measures retailers offer. Among the preferred security measures, strong data encryption is widely embraced, with 65% of respondents saying it's important, while two-factor authentication is considered crucial by 69% of respondents when selecting finance apps.

Q //

HOW LIKELY ARE YOU TO USE ADDITIONAL SECURITY MEASURES, SUCH AS TWO-FACTOR AUTHENTICATION, WHEN PROVIDED BY A RETAILER?

ANSWERED: 1,034
SKIPPED: 0

VERY LIKELY 48%

SOMEWHAT LIKELY 33%

NEUTRAL 15%

NOT VERY LIKELY 3%

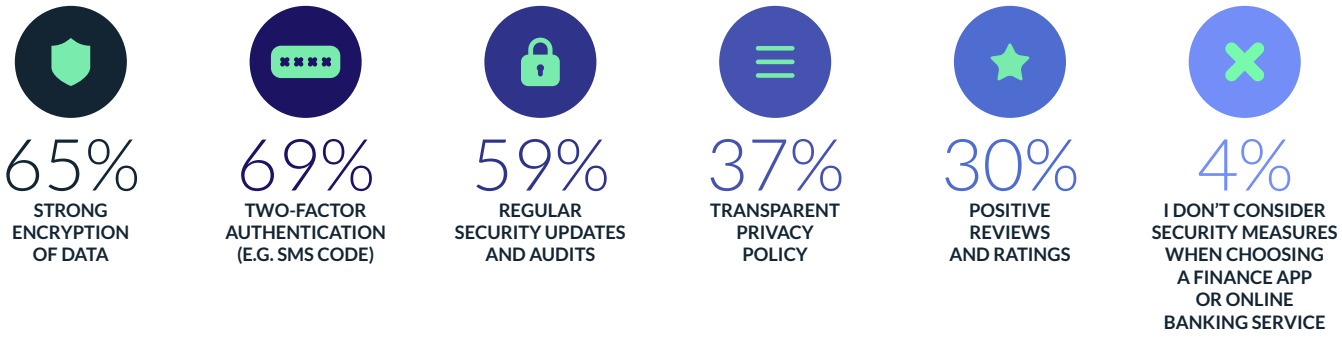
NOT LIKELY AT ALL 1%

Q //

WHICH SECURITY MEASURES DO YOU CONSIDER IMPORTANT WHEN CHOOSING A FINANCE APP OR ONLINE BANKING SERVICE?

Select all that apply

ANSWERED: 1,034
SKIPPED: 0



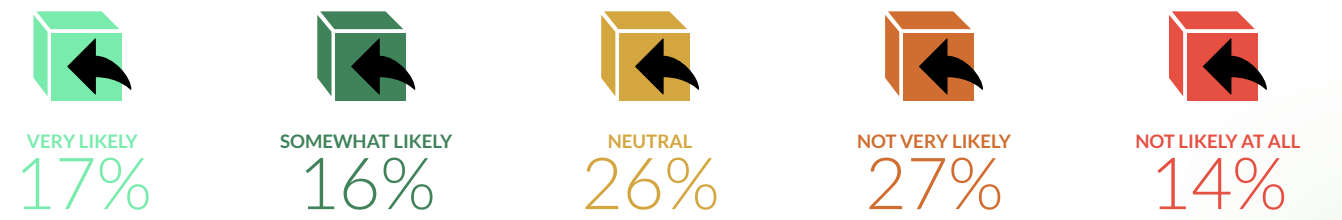
Only 16% of respondents were "very likely" to return to the retailer, with only 13% of female shoppers (compared to 21% of their male counterparts) responding with that same answer. Retail businesses have a consumer trust score 12% less than other B2C sectors, and only 29% of consumers consider themselves to 'highly trust' businesses in the financial services sector, highlighting the opportunity for security to bolster brand trust.

That low trust is connected with a strong consideration of leaving the retailer. Data leaks are the ultimate game of Russian roulette for retailers desperately trying to cultivate customer loyalty.

Q //

HOW LIKELY ARE YOU TO RETURN TO A RETAILER IF YOUR OWN DATA HAS BEEN LEAKED?

ANSWERED: 1,034
SKIPPED: 0



RETAIL

The retail sector's current efforts to contain cybersecurity vulnerabilities aren't working, as it saw a 42% rise in cyberattacks during the first half of 2023, with exploited vulnerabilities being a dominant root cause for ransomware attacks (41%).

The vulnerabilities and string of high-profile cyberattacks in the retail sector have translated to a significant portion of consumers (81%) expressing awareness of cybersecurity threats faced by retailers. This awareness is likely correlated to a willingness to implement protective measures such as two-factor authentication. However, it also shows that consumers' willingness to consider leaving a retailer in the event of a data leak is unlikely to be met with understanding no matter the circumstances.

Q //

ARE YOU AWARE OF THE POTENTIAL CYBERSECURITY THREATS FACED BY RETAILERS?

ANSWERED: 1,034
SKIPPED: 0

YES, I AM WELL-INFORMED
36%

SOMEWHAT AWARE
45%

I HAVE LIMITED KNOWLEDGE
14%

NO, I AM NOT AWARE
5%

FINANCE

Banks finance institutions! In the event of a data leak, financial sector vendors bear the responsibility of securing their customers' data, even if a third party is really to blame. Our survey found that 47% of consumers blame the financial institution or bank associated with the financial app affected by a data leak, with only 21% blaming the hackers, 27% blaming the third-party app developer, and only 4% blaming themselves. Those racing to digitize and expand access must be incredibly careful when it comes to their digital supply chain and other partners because they will bear the blame for a breach.

Q //

IF YOUR PERSONAL DETAILS WERE LEAKED FROM A FINANCE APP, WHO WOULD YOU PRIMARILY BLAME?

ANSWERED: 1,034
SKIPPED: 0

47%
THE FINANCIAL INSTITUTION/BANK ASSOCIATED WITH THE APP

28%
THE APP DEVELOPER/ COMPANY

21%
THE HACKERS RESPONSIBLE FOR THE DATA BREACH

4%
MYSELF FOR NOT TAKING ENOUGH PRECAUTIONS

Our findings express the magnified level of safety concerns in the financial sector when it comes to online banking apps, with an average score of 6.1 (out of 10) regarding consumers' level of concern for securing financial data when using online banking apps.

The sensitive nature of the data financial institutions hold is directly associated with consumers' money, hence the harsher reactions of consumers when facing a data leak. For example, the Angel One brokerage firm saw its shares fall by 2% immediately after a cyberattack.

Q //

HOW CONCERNED ARE YOU ABOUT THE SECURITY OF YOUR FINANCIAL INFORMATION WHEN USING ONLINE BANKING SERVICES OR FINANCIAL APPS?

ANSWERED: 1,034
SKIPPED: 0

The more modern approach to financial services catered to by online banking apps has already garnered a level of security concerns specific to mobile apps. Strengthened by the fact that there has been an 80% growth in malware threats on Android smartphones, as well as financial app consumers being generally more cautious, with 10% of Americans completely avoiding the use of digital wallets due to security concerns.

CONCLUSION - SECURITY AS AN OPPORTUNITY TO MAINTAIN CONSUMER TRUST & LOYALTY

Understanding and addressing cybersecurity threats is paramount in comprehending the expansion of a business and ensuring the presence of pertinent signals to proactively mitigate risks. A proactive approach not only fortifies a brand's resilience but also cultivates unwavering customer loyalty. Being proactive in cybersecurity safeguards not only the business itself but also nurtures a robust foundation for sustained trust and brand allegiance among consumers and customers.

As cyber threats become increasingly sophisticated and consumer awareness reaches an impressive 81%, the need for a proactive and targeted approach to safeguarding consumer data is more pressing than ever. Our report brings to light a disconcerting trust deficit between financial institutions, retailers, and consumers. The enduring consequences of security lapses underscore a critical nexus between cybersecurity measures and consumer loyalty, a universal concern cutting across age groups.

Consumers overwhelmingly demand accountability, with over three-quarters insisting that retailers compensate them in the event of a data breach and displaying a strong inclination to abandon finance apps after a personal information leak. Despite these concerns, there is a simultaneous willingness to adopt additional security measures in order to safeguard personal data.

Consumer interest in additional security precautions signals the potential for businesses to actively involve consumers in their security efforts and foster trust and loyalty in the process. Organizations can enhance their relationships with consumers and gain a competitive edge in an environment marked by constant technological evolution and heightened consumer distrust by effectively addressing the multifaceted concerns surrounding data security. The fortification of these relationships hinges on proactive measures that navigate the challenges posed by evolving technology and instill confidence in consumers.

Learn more about the cyberint platform

Cyberint

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

ISRAEL
Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM
Tel: +44-203-514-1515
6 The Broadway, Mill Hill NW7 3LL, London

USA – TX
Tel: +1-646-568-7813
7700 Windrose Plano, TX 75024

SINGAPORE
Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

USA - MA
Tel: +1-646-568-7813
22 Boston Wharf Road Boston, MA 2210

JAPAN
Tel: +81 080-6611-7759
27F, Tokyo Sankei Building, 1-7-2 Otemachi,
Chiyoda-ku, Tokyo 100-0004

ABOUT CYBERINT

Cyberint's impactful intelligence solution fuses real-time threat intelligence with bespoke attack surface management, providing organizations with extensive integrated visibility into their external risk exposure.

Leveraging autonomous discovery of all external-facing assets, coupled with open, deep & dark web intelligence, the solution allows cybersecurity teams to uncover their most relevant known and unknown digital risks - earlier.

Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to prevent, detect, investigate, and remediate phishing, fraud, ransomware, brand abuse, data leaks, external vulnerabilities, and more, ensuring continuous external protection from cyber threats.