CONSUMER SENTIMENTS: CYBERSECURITY, PERSONAL DATA AND THE IMPACT ON CUSTOMER LOYALTY

The fastest way for businesses to erode customer loyalty is with a data breach. As cyberattacks and data breaches become common occurrences, the issue of data security has transitioned from the hallways of IT departments to mainstream conversation.

As a result, consumers are now concerned that the organizations with which they conduct business are proactive about safeguarding their information and how those organizations will fix a breach if one does occur. More than ever, consumer sentiments about the safety of their personal information and the relationship they have with business organizations are affected by security breaches.

To understand how consumers view cybersecurity, how they would react if their data was compromised and what it means for businesses today, Radware sought the opinions of more than 3,000 consumers in the United States. This piece summarizes the results from Radware's 2018 consumer sentiments on cybersecurity survey.

PERSONAL DATA ABOVE ALL ELSE

Perhaps nothing underscores the transition to the digital age more than the value of digital data over physical goods. Consumers are now more concerned about having their personal data stolen than their wallets, automobiles or house keys, according to the survey.

Consumers Value Personal Data Above All Else

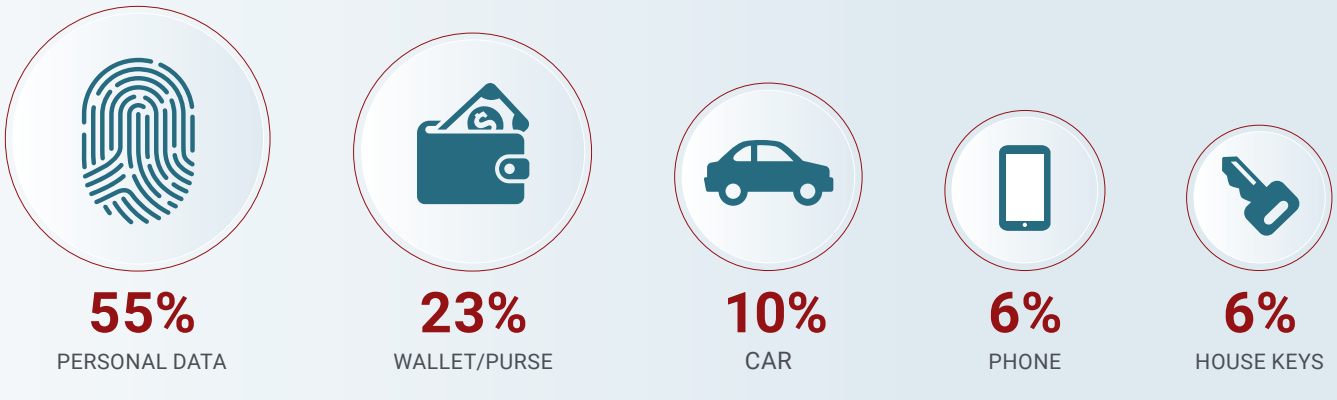

Figure 1: Which of the following items would concern you the most if stolen?

For organizations that keep consumers' personal information, the foundation of the customer experience is a mix of trust and availability. Customer loyalty takes a hit if either falters, resulting in customer, brand reputation and productivity/operational losses.[1]

When a company suffers a data breach, the vast majority (68%) of consumers must be convinced that the security issue has been addressed, and any damage has been rectified before continuing to do business with the brand. Even worse for the organization's bottom line, one of 10 consumers will walk away entirely from the brand.

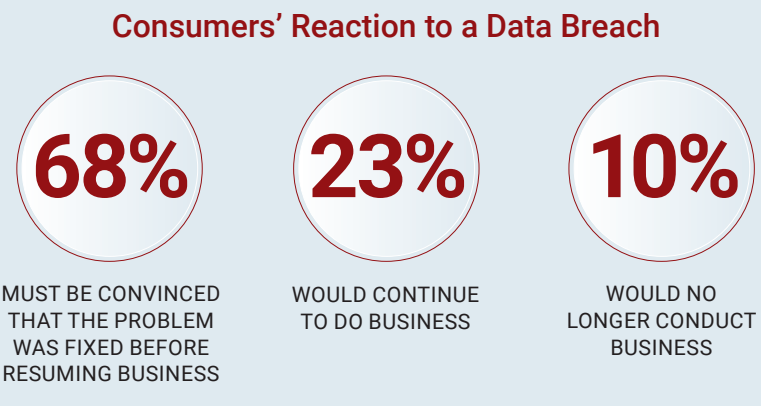

Figure 2: If one of your frequented and trusted businesses experienced a data breach, which of the following statements would most accurately reflect your relationship with that brand/business?

Consumers are willing to retaliate as well. According to Radware's *2018 C-Suite Perspectives: Trends in the Cyberattack Landscape, Security Threats and Business Impacts*, 41% of executives indicated that customers have taken legal action against their company following a data breach.

Lawsuits and brand damage aside, ultimately the impact of a data breach exceeds far beyond the reaction of a consumer and adversely affects customer lifetime value as well. If nearly three out of every four consumers must be convinced that the security issue has been addressed before continuing to do business with that brand, then executives must consider how much a data breach increases retention costs and decreases customer lifetime value to win back the trust of that consumer. Key factors that comprise customer lifetime value, including average spend, repeat sales, retention time, cost and risk expectancy, etc., can all be adversely affected by a data breach.

1 C-Suite Perspectives: Trends in the Cyberattack Landscape, Security Threats and Business Impacts Report

A DISPARITY BETWEEN THE HUNTER AND THE HUNTED

Personal data is valuable, both to consumers and the hackers who seek to steal it. But the data that is most valuable to each constituency is another matter entirely. Survey results show that the majority of American consumers value their social security number and information related to finances (banking and credit card data) as information that would concern them the most if stolen.

Those concerns don't align with their value to cybercriminals though. Based on the value of personal information at the time this survey was published, banking and credit card information has lost value in recent years. Credit card information has the potential to be highly valuable, but only if it includes all pertinent information, such as date of birth, billing address, three-digit security code, etc. On the other hand, personal information pertaining to health/medical records has recently risen dramatically in value.

Social Security Number Is Consumers' Biggest Concern

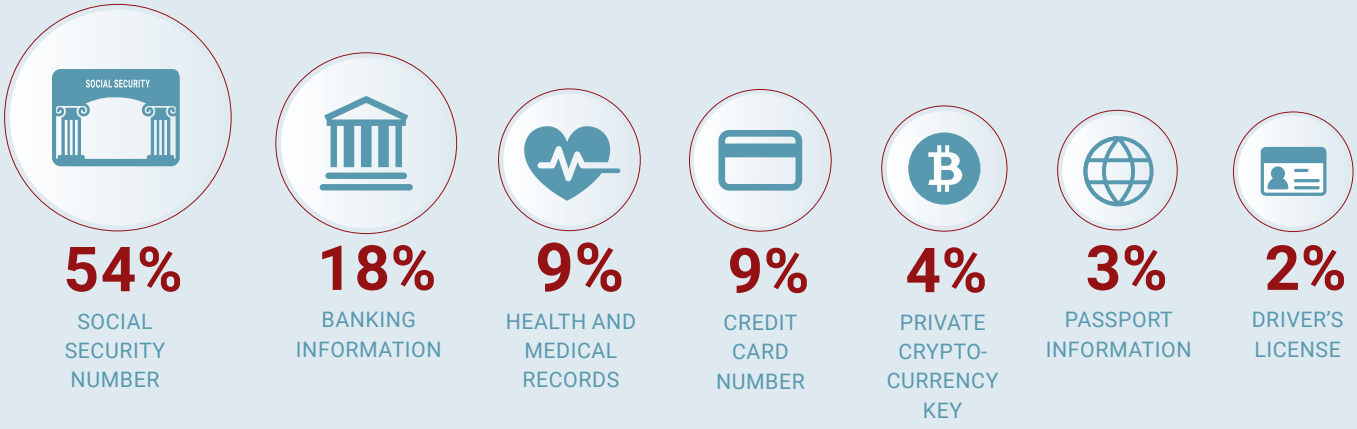

Figure 3: Rank which of the following would concern you the most if stolen or compromised.

Personal Data: What It's Worth and What Cybercriminals Can Do With It

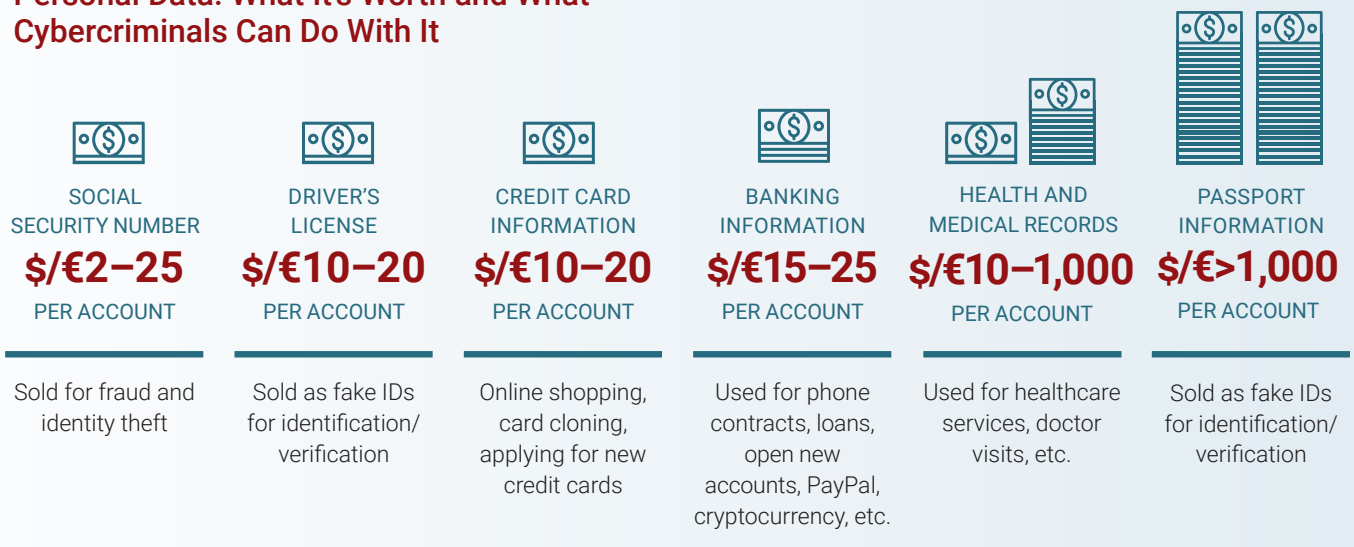

Figure 4: Value of personal information to cybercriminals at time of publishing.

2 Information based on research by Radware's Cybersecurity Threat Intelligence Team at time of publishing

The disparity between the data that consumers are the most worried about being compromised and their actual value to cybercriminals underscores the fluidity of the value of personal information. Just like financial markets, the value of personal information rises and falls based on political, economic and social factors. The economic principles of supply and demand also affect how cybercriminals sell and purchase stolen information. Lastly, the balance of accounts that have been compromised influences the value of the stolen information.

CONCLUSION

What does all of this mean for brands? Consumers have high expectations when it comes to safeguarding their most prized personal possessions, but they have even higher expectations of companies that they conduct business with safeguarding their personal information. Just because cyberattacks and resulting data breaches are becoming commonplace doesn't mean that consumers are willing to accept that as a cost of doing business.

For organizations, it is no longer about just delivering a world-class experience. It is about delivering a *SECURE*, world-class experience. In today's digitally driven, social media world where consumers own the relationship, security has to become the very fabric of the business. With the types of valued personal information constantly in flux, no industry is safe.

Although suffering a data breach can be damaging, the survey also underscores that honesty, transparency and a timely emergency response plan are critical. Companies must clearly communicate that a breach occurred, those likely impacted and remediation actions that will take place to address the issue. Organizations that don't admit to compromised consumer records until long after the breach took place suffer the greatest wrath from consumers.

Successful organizations must create a secure climate for customers by embracing technology and cultural change. Security threats and data breaches can seriously impact a customer's loyalty, thereby damaging the corporate brand, increasing customer churn and incurring lawsuits. Corporate leaders must recognize the multiple pressures on their organizations to integrate new network technologies, transform their businesses and defend against cyberattacks. Executives willing to embrace technology, cultural change and prioritize cybersecurity will be the ones to win the trust and loyalty of the 21st century consumer.

METHODOLOGY

This SurveyMonkey online poll was conducted in May 2018 among a sample of 3,024 U.S. adults ages 18 and older. Respondents for this study were selected from the nearly 3 million people who take surveys on the SurveyMonkey platform each day. This online survey is not based on a probability sample; therefore, no estimate of theoretical sampling error can be calculated.

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.