HYPORI™
VIRTUAL MOBILITY

Data Breaches: Current Trends and Major Costs to Businesses and Individuals

WHITEPAPER

Summary

In the age of COVID-19, a remote-work explosion, a continued boom in mobile device use, and an increased reliance on cloud computing, cybersecurity issues have never been more prevalent. Data breach costs, anticipated to reach $5 trillion worldwide by 2024, have widespread implications for both businesses and individuals. For most organizations, the shift to more remote work and increased employee use of mobile devices compounds the data breach response challenge. Of all data breached, 80% includes customer personally identifiable information (PII) exposing individuals, like banking customers and healthcare patients, at an assuredly high rate. As our economic and social paradigms shift, bad actors capitalize while legitimate IT and security leaders seek answers.

The Situation

Today's high-tech mobile environment, at both work and play, presents a robust opportunity for cybercriminals with the cybercrime economy estimated to be worth $1.5 trillion.

For businesses, activities to discover and respond to data breaches are time-consuming, distracting, and costly. Compromised security impacts an organization at every level, with cost being the most significant, but also includes data integrity, competitive status, IT infrastructure, and customer and employee relationships. For individuals, malware, phishing schemes, and other breaches mean financial loss, identity theft, invasion of privacy, and more.

Current trends in cyberattacks follow the times. Even before COVID-19 remote work, telehealth, mobile banking, and personal device use at work were on the rise. Today, nearly 80% of organizations predict increased difficulty in data breach response. IT departments face new oversight and management challenges with multiple points of entry, mobile app downloads, and cloud storage. The problem intensifies with the mobile device use explosion in healthcare, financial services, education, and government.

An IBM 2020 Cost of a Data Breach Report found that the average cost of a malicious attack was $4.27 million. Alternatively, the average cost of *any* data breach, including malfeasance, was $3.86 million. Organizations with in-place security processes see average cost-per-breach declines, while those without are struggling.

Individuals pay dearly as well. Hackers target everything from passwords to banking information to social security numbers. In 2018, 3.3 million identity fraud victims were held financially liable for losses against them. For individuals, total out-of-pocket fraud costs more than doubled from 2016 to 2018 to $1.7 billion.

General data breach trends run the gamut from email attacks to fraudulent app downloads to the particularly challenging fileless attacks. In fileless attacks, hackers use already installed, trusted applications, existing software, and authorized protocols; they execute without malware.

One particularly disturbing trend is the use of COVID-19-related attacks and ransomware strains, such as a fake contact tracing app, that when downloaded, compromises sensitive personal data. Overall, cyberattacks are reportedly up 63% since the pandemic hit.

The Problem

Data breaches occur as a result of three possible factors. One is system glitches, which include both IT and business process failures. The second is human error in the form of employee negligence or unintentional misstep. Finally, there are malicious attacks caused either by hackers or criminal insiders.

The IBM Data Breach Report confirms that 52% of all breaches are due to malfeasance, a 14% increase from 2014. These malicious attacks are more prevalent in the healthcare, financial services, and technology industries. Given the dramatic rise in personal device use to conduct private transactions and work functions, personal and corporate data have never been more intertwined, leaving devices and organizations more vulnerable than ever.

Fifty-three percent of all attacks are financial, 21% are a result of unknown origin, and 13% are nation-state actors and hacktivists, respectively. Nation-state attacks are the costliest of all attacks on average at $4.43 million, hacktivist breaches cost an average of $4.28 million, and financially motivated attacks average $4.23 million. When it comes to financially motivated attacks, the costliest and most frequent are compromised credentials increasing the average cost per breach to $4.77 million. At the same time, misconfigured cloud servers resulted in the average cost per breach rising to $4.41 million.

Healthcare represents the highest industry cost per breached record, where each breach can cost $429. According to a ForgeRock 2020 Consumer Identity Breach Report, at 43%, the healthcare industry has the highest percentage of breaches per industry and lost $17.76 billion in 2019. That same year, hackers breached the American Medical Collection Agency (AMCA) and accessed 11.9 million Quest Diagnostics' patient records. The exposed information included credit card numbers and bank account information, medical information, and other personal data, like social security numbers. The AMCA breach impacted 24 other companies affecting over 26 million individuals. AMCA filed for Chapter 11 bankruptcy and took out a $2.7 million loan to cover breach-associated losses.

A financial services breach costs an average of $210 per record. However, a mega breach can cost up to $388 per record. We saw a mega breach in the 2019 Capital One breach, an event that went unchecked for five months. One hundred six million customers and applicants lost confidential credit card numbers, social security numbers, and personal contact information. As a result, Capital One may lose $300 million, not to mention potential public relations costs.

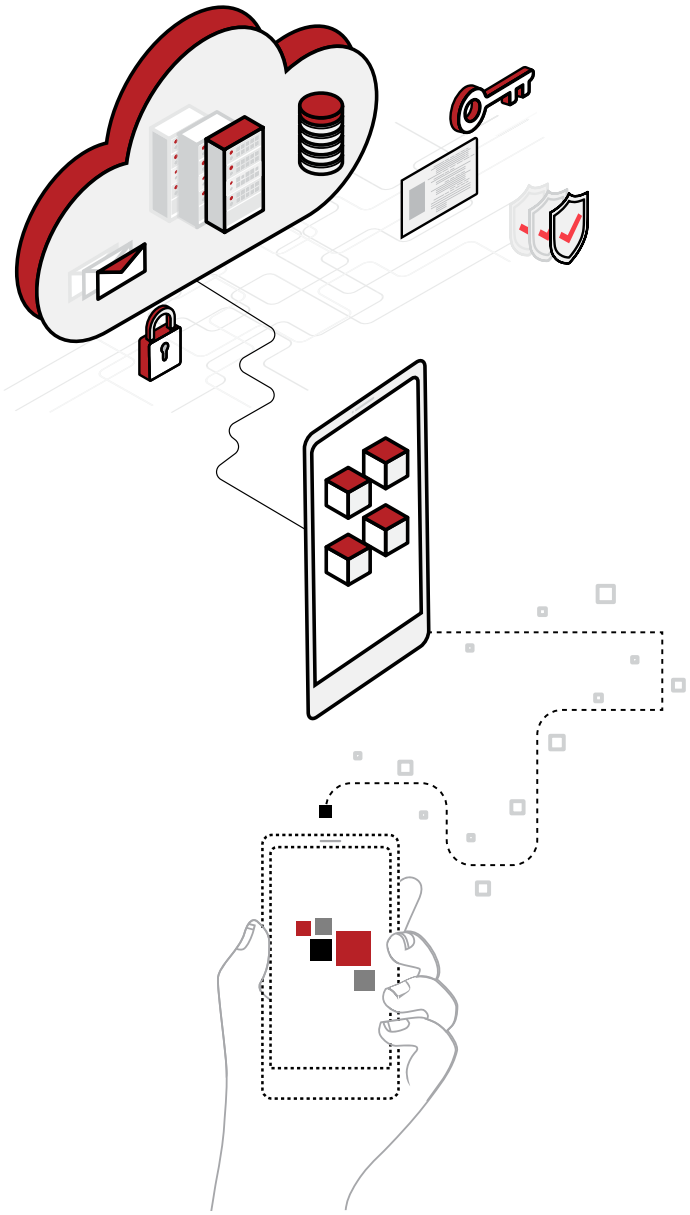
The Problem (continued)

Data breach costs are high for all organizations. In the first breach year, most companies experience significant financial losses. However, highly regulated industries experience higher costs after the first year. In less regulated industries like retail and entertainment, 77% of average costs incur in year one while in highly regulated organizations like banking and healthcare, that number is only 44%. Given the higher rate of breaches in more highly regulated industries, these numbers point to an even greater need for across-the-board solutions. Without a way to protect valuable corporate and personal data while enabling employees and customers to perform work and other functions, the cybercriminals will continue to strike and win.

Breach cost and attack frequency are rising. Recent economic and social shifts like remote work, telehealth, and cloud computing have made us even more vulnerable to data breaches. All organizations have more remote workers now than ever, with some shifted to 100% permanent remote work. Mobile device use is commonplace, meaning organizations have multiple points of daily entry to networks and systems and most employees and contractors use personal devices to perform work functions. As a result, corporate data is often accessed from and sits on personal devices. Cyberthreats are everywhere at every level, and without a way to address them, organizations and individuals face significant losses, financial and otherwise.

The Solution

Hypori Virtual Mobility eliminates the data breach risks associated with all mobile device use such as mobile banking, remote work, and cloud computing. Because Hypori secures all data in a corporate-owned data center, there is 100% separation of personal and enterprise data. Since no company data resides on the personal device, bad actors have no inroads via app downloads, email providers, or other typical end-user avenues. Employees use their own devices, increasing productivity and adoption, and minimizing IT costs. Compromises on the organization side are solvable without accessing individual devices, reducing costs, and simplifying IT management. Hypori provides military-grade security, FISMA, HIPPA, NIAP, CSfC*, NSA, and PCI DSS compliance, and is Common Criteria certified. Hypori Virtual Mobility delivers a highly secure, manageable, and user-friendly solution to address your cybersecurity concerns and improve your bottom line.



To learn more about Hypori Virtual Mobility, contact us for a demonstration today.

Contact us

info@hypori.com

*The National Security Agency Commercial Solutions for Classified (CSfC) provides DoD entities the ability to conduct secure classified communications using Commercial-off-the-Shelf (COTS) products. Under this program the Mobile Access Capability Package v2.0 provides a framework for how to secure these communications from mobile end user devices into government enterprise resources. Under the MACP v 2.0, communications must be established using an inner and outer tunnel to provide the secure communications path. Intelligent Waves, LLC's Hypori Client v4.1 for iOS and Android is eligible to be used as a TLS Software Application Product component in a CSfC solution. This means that in combination with a CSfC eligible TLS Protected Server, Hypori is eligible to provide the inner tunnel for secure communications.

11 March 2019

hypori.com