RISKY BUSINESS V2.0:
THE IMPACT OF TODAY’S DATA BREACHES ON A BUSINESS & ITS EMPLOYEES

INSIGHTS AND KNOW-HOW FOR MITIGATING CYBER & IDENTITY THREATS IN A CONNECTED WORLD
INTRODUCTION

Though the number of data breaches declined slightly in 2018, those that did occur were far more damaging, with a 126% increase in number of records exposed per incident. Consumers’ unprotected Personally Identifiable Information (PII) being leaked at such excessive rates is putting hundreds of millions of people at risk of identity theft and fraud. This alarming statistic indicates that the tactics of hackers and cybercriminals are becoming more effective, and the quantities of records in 2019 data breaches are not getting any smaller. Businesses everywhere need to be prepared for the fallout.

Fraudsters have gotten bolder going after organizations and employees while leveraging new angles to steal data, including:

- **Mobile Mania** | Verizon reports that one in three organizations have revealed they suffered a data breach because of a mobile device. And, senior IT professionals are on high alert, with 82% predicting unsecured Internet of Things (IoT) devices will likely cause a data breach in their organization (2018 Raytheon study).

- **Phone Scammers** | There were nearly 48 billion robocalls in the U.S. in 2018, a 57% increase over 2017. The Federal Trade Commission (FTC) reported that “vishing”, or voice-phishing, scams have seen a 20x increase since January 2018, and are targeting businesses and consumers.

- **Digital Skimming** | Cybercriminals are targeting ecommerce transactions at an estimated 17,000 websites and growing, collecting payment card information with malicious JavaScript injected into payment form code without consumers, or businesses, being any wiser. Large and small organizations are being targeted, including well-known names like British Airways, Forbes Magazine, and Topps Sports.

Then, there are the factors compromising business health, such as:

- **Impact to the Wallet** | The average data breach costs U.S. organizations $7.91 million in reparatory expenses.

- **Customer Exodus** | Loss of business after a breach now costs businesses an average of $1.42 million — that’s 36% of their total breach costs.

- **The Buck Stops Here** | The Supreme Court ruling against Zappos and the 2019 Equifax breach settlement with the Federal Trade Commission (FTC) are two examples of courts looking at the long-term impact of breaches on consumers, and indicate businesses may be held accountable for collateral damages.

1. 2018 End of Year Data Breach Report, Identity Theft Resource Center
THE EQUIFAX EFFECT

Approximately 148 million Americans, or nearly half of the U.S. population, had their personal data exposed in the Equifax mega breach between mid-May through July 2017, according to the company.2 What made this data breach so much more devastating than garden-variety hacks was that the crown jewels of personal identity — Social Security numbers (SSNs), names, and dates of birth — were stolen.

MAJOR DATA BREACHES BY THE NUMBERS

Although the Equifax data breach was not the largest theft of personal information in history, it may be the most potentially damaging because of the type of highly-sensitive personal and confidential data involved. Here are some quick facts about more recent, major data breaches that included similar sensitive details:

- **June 2019 |** A well-connected medical vendor, American Medical Collection Agency (AMCA), was breached, exposing the PII of more than 20 million patients from numerous medical labs, including Quest Diagnostics, LabCorp, and Opko Health. Data including credit card and bank account details, Social Security numbers, dates of birth, and medical information.

- **May 2019 |** First American Financial Corp., the leading title insurance provider in the U.S., exposed the PII from 885 million consumer records, documents that included Social Security numbers, bank account numbers, driver’s license images, and mortgage and tax records. This exposure likely impacted anyone who has bought or sold a home in the past 16 years.

- **March 2019 |** Facebook admitted to not properly securing user passwords dating back to 2012. As many as 600 million users’ passwords were available in plain text and accessible to more than 20,000 of the company’s employees. On July 24 2019, Facebook was penalized a record-breaking $5 billion dollars by the Federal Trade Commission (FTC) for deceptive data privacy practices.

- **November 2018 |** Marriott International disclosed a data breach affecting 328 million guests. A hacker infiltrated the reservation database of the 30-brand hotelier and had access until the breach was discovered. Names, physical and email addresses, dates of birth, phone numbers, gender, passport numbers, rewards information, travel details, and communication preferences were among the compromised details.

---

SPOTLIGHT: YOUR DATA IS EVERYWHERE

Data breaches are a constant part of our personal and professional lives. So, whether we are shopping at Target, Home Depot or Home Goods, banking with JPMorgan Chase, selling or buying on eBay, or have our medical insurance through Anthem/Blue Cross Blue Shield, if your data is included as part of the transaction it has the potential to be exposed.

The Dark Web — the area of the Internet that is unsearchable — is proof of that. There’s a buyer within those unindexed pages of the Internet that’s ready to reap the rewards using any stolen piece of your identity. However, not every breach that hits the news is cause for alarm, and it’s important to avoid breach fatigue by knowing what information to pay attention to when breaches hit.

SONTIQ’S SECURITY WATCH LIST: NOT ALL BREACHES ARE EQUAL!

<table>
<thead>
<tr>
<th>SIZE</th>
<th>TYPE</th>
<th>TIMELINE</th>
<th>NOTIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>How large is the impacted population, or number of records involved?</td>
<td>How sensitive is the information; is it easily replaceable?</td>
<td>How long was the date exposed; how soon was vulnerability fixed?</td>
<td>Were you personally notified your data was included in the breach?</td>
</tr>
</tbody>
</table>

So, what can be done? According to Gartner, global IT Security spending is expected to exceed $124 billion in 2019. As money and resources continue to increase, it’s time to take a good look at our businesses and even our own practices on how we allow our personal information to be handled. New breach reporting standards in the U.S. are also a significant step toward taking control of the fallout related to your information being exposed, requiring businesses to follow specific notification guidelines.

Shopping on the Dark Web: What's the Price of Your Identity?

- Passport — $18
- PayPal Login — $42
- Driver's License — $28
- Online Banking Details — $260
- Credit Card Details — $34
- Social Media Login — $9
- Amazon Login — $30
- Full Online Identity — $1,200

SOURCE | Dark Web Market Price Index 2019, Top10VPN
DATA BREACH CRISIS COMMUNICATION

The gap between detecting data theft and announcing it to the public can be varied, depending on several factors. Companies need to patch infrastructure security vulnerabilities, determine the scope of how much data was stolen, and inform law enforcement officials who likely want time to try to identify the hackers before a breach is made public. In the interim, the criminals may cover, or at least obscure, their digital tracks — making detection and capture that much more difficult.

For example, Facebook’s multitude of data breaches have often left users in the dark completely, such as when the company experienced one of several significant breaches late in 2018 impacting over 90 million accounts, and failed to warn their users of the risk to their identities. This failure to act led to a lawsuit claiming Facebook had known about the vulnerability for many years and never fixed it, ultimately exposing millions of users to compromised accounts and stolen data. This lawsuit was given the green-light by a federal appeals court, just before the record-breaking $5 billion dollar penalty was issued against Facebook in July, 2019, by the Federal Trade Commission (FTC) for deceptive data privacy practices.

What should not be lost in discussions about the scope of any data breach, or a company’s lackluster response, is the immutable fact that the PII of the impacted population is now jeopardized. Consumers real risk is much longer term than the typical two-year credit monitoring offered, if any, and that risk could have a detrimental impact on the economy and on businesses that rely on employees and customers trusting that their PII will be safeguarded. Further, legal decisions are demonstrating with consistency that companies will be held responsible for consumer data leaks well beyond previous perceived limitations.

“Fraudsters may already have enough of your personal information to access your existing bank or credit card accounts. So, the pieces of the puzzle to commit fraud could already exist even if you engage in a free credit freeze.”

— Rich Scott, Chief Revenue Officer, Sontiq
DISRUPTION TO YOUR EMPLOYEES: A SERIOUS PRESSURE COOKER

Not only can identity thieves potentially gain access to checking, savings, and 401(k) accounts, they can use this information to piece together new fake identities, known as synthetic identity theft.

The impact to business productivity and profits related to data breaches can be significant. The downtime for employees who need to confirm the integrity of their identity — or must go through the complex process of repairing a stolen identity — is estimated to take six months and 100 to 200 hours-worth of work. This takes a real toll on employees’ emotional states, and can lead to health issues including significant personal stress, chronic anxiety, and frustration. Your business may also suffer from an erosion of trust, as employees may be on edge and suspicious of how well you protect their personal data.

This message is clearly resonating with human resources professionals, as revealed in Sontiq’s 2019 survey of more than 125 Benefit Brokers. Identity theft protection is becoming increasingly in-demand, with more than 50% of benefit advisors reporting regular requests from their clients, an increase of 20% in one year. According to Willis Towers Watson, it is expected that 63% of employers will offer identity theft protection as an employee benefit by 2021. Further, data breaches and cyber threats are keeping organizations up at night, with 43% of benefit advisors reporting they’ve talked with their clients about these issues in the past 12 months.

THE PROGRESSIVE BENEFITS REQUESTED BY ORGANIZATIONS

<table>
<thead>
<tr>
<th>How often do clients request the following progressive benefits?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wellness Programs / Wellness Stipends: 32% Regularly Requested</td>
</tr>
<tr>
<td>Identity Theft Protection: 33% High-Demand</td>
</tr>
<tr>
<td>Telemedicine / Counseling: 32% Extremely High-Demand</td>
</tr>
<tr>
<td>Financial Counseling / Financial Advice: 30% Regularly Requested</td>
</tr>
</tbody>
</table>

SOURCE | 2019 Benefit Broker Survey, Sontiq

1 Javelin Strategy & Research
2 United States Department of Justice
A DATA BREACH IMPACTS YOUR WORKFORCE FOR YEARS TO COME

To a cyber thief, having access to PII — which could include addresses, phone numbers, credit information, SSNs, and more — is really the Holy Grail of digital crime. Not only can fraudulently obtained PII be quickly monetized on the Dark Web, it can be used to set up fake identities, in effect combining different names, home addresses and SSNs to defraud your employees. In fact, using the often less detectable SSNs of children and the elderly is a preferred scheme of cybercriminals, who can exploit this information for years while destroying the children’s future creditworthiness in the process. Here are some of the ways PII can be used by these thieves:

- Setting up fraudulent bank accounts to withdraw and drain funds
- Setting up fraudulent pension or 401(k) withdrawals
- Abusing health insurance benefits
- Applying for new credit cards using fake IDs
- Filing fraudulent tax returns to claim refunds

Impact on Children

Sometimes parents provide their children’s PII when setting up credit files, medical records, school enrollment or activity forms, or any number of vulnerable recordkeeping methods. Successful thieves can combine real and fake data to compile new identities. They then use these synthetic identities to obtain credit, open bank accounts, and apply for driver’s licenses and passports.

Age is Not a Theft Deterrent

- More than 1 million children have their identity stolen each year
- Two-thirds of victims are under 8-years-old
- Of data breach victims, 39% of minors become victims of fraud, versus 19% of adults
- Fraudsters steal an average of $2,303 per child victim

A Social Life

Identity thieves know the more information they have, the easier it is to pilfer an identity. Luckily for them, humans are social creatures — especially when it comes to social media oversharing by children and adults alike. Businesses social media accounts are just as susceptible to hacking, which can be damaging to a company’s reputation and even lead to business identity theft.

Social Media Weakness

- 61% of consumers view social media platforms as their greatest digital risk
- Social media accounted for 56% of global data breach exposure in 2018
- 22% of social media users say their accounts have been hacked, and 14% have been hacked more than once

Sources: Javelin Strategy & Research, 2018; Federal Trade Commission, 2019

Sources: Gemalto, 2018; Pew Research, 2019; Statista, 2019
STEPS FOR PROTECTING YOUR EMPLOYEES AND THEIR FAMILIES

There are six steps you and your employees can do together to help protect against identity theft:

1. **Stay vigilant** | Employees can request a free annual credit report and you should encourage them to monitor their credit card activity and bank statements. They can contact the non-profit Identity Theft Resource Center at (888) 400-5530 to get assistance with identify theft mitigation, and/or subscribe to an identity theft and credit monitoring service that will alert them when their personal information is being used.

2. **Get support** | If they are confirmed identity theft victims, they can create an Identity Theft Report with the Federal Trade Commission (FTC). Visit [www.identitytheft.gov](http://www.identitytheft.gov), the federal government’s resource for identity theft victims, for details. Note that law enforcement likely will request a copy of any Identity Theft Report filed.

3. **Stop cybercriminals in their tracks** | Put an extended fraud alert or security freeze on your credit. An extended fraud alert, which is available up to seven years in most states, allows creditors to see someone’s credit file, but they must contact him or her to identify before extending credit. A credit freeze generally prevents creditors from accessing someone’s credit file.

4. **File taxes early** | Filing early protects them from identity thieves who might try to file and collect tax refunds before the employees complete those steps.

5. **Contact the Social Security Administration** | By requesting a copy of their wage-earning report, your employees can verify that their Social Security numbers are not being used fraudulently, resulting in their being liable for taxes on wages reported by someone who’s stolen their information.

6. **Work with your employee benefits administrator** | Reassure your employees that you are monitoring accounts for any suspicious retirement plan withdrawals/activity and/or medical claims. Encourage them to request a copy of their statements to further stay on top of their benefits.

### THE TOLL OF IDENTITY THEFT

<table>
<thead>
<tr>
<th>Category</th>
<th>Impact Description</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severe Emotional Distress</td>
<td>77% Reported Increased Stress Levels</td>
<td><a href="http://www.identitytheft.gov">ITRC Identity Theft: The Aftermath 2018</a></td>
</tr>
<tr>
<td>LOST PRODUCTIVITY</td>
<td>6 months and 100 to 200 hours worth of work</td>
<td>Various Industry Stats</td>
</tr>
<tr>
<td>Consumer Cost</td>
<td>Average LOSS of $1,343 per ID Theft Incident</td>
<td><a href="http://www.javelinstrategy.com">Javelin Strategy &amp; Research</a></td>
</tr>
</tbody>
</table>
1. **Beware Of Stolen Funds**
   It's critical when personal information is publicly exposed to continuously review your bank and financial accounts so that you can rapidly report to your financial institutions any stolen funds.

2. **Monitor Your Social Media Accounts**
   Imposter accounts and account takeovers through any social media account can lead to fraudsters scraping personal information to even hack into email accounts, or to battle it out further on the Dark Web to buy and sell your personal information.

3. **Request A Free Copy Of Your Annual Credit Report**
   Take great care to review your credit reports. If you find inaccurate information, contact the companies listed on the credit report(s) directly. You can also contact the Identity Theft Resource Center, a non-profit, at (888) 400-5530 to assist you, and/or subscribe to an identity and credit monitoring service to alert you when your personal information is used.

4. **If You Confirm That You're A Victim Of Identity Theft, Create An Identity Theft Report With The Federal Trade Commission (FTC)**
   Expect law enforcement to request a copy of this report when you contact them. Learn more here: www.identitytheft.gov.

5. **Consider Placing An Extended Fraud Alert Or Security Freeze On Your Credit**
   Creditors will still have access to your credit file, even though you've placed a 7 year extended fraud alert, but must first contact you to verify your identity before extending credit. A credit freeze generally prevents creditors from accessing your credit file. To request one, you must call each credit bureau directly; laws vary by state.

6. **Enable Two-Factor Authentication**
   Two-Factor Authentication (2FA) helps protect your online accounts from unauthorized access. With 2FA, you use something you know (your username and password) and something you have (a one-time code sent to your phone) to verify your identity and log in to your account.

7. **Contact The Social Security Administration**
   Request a copy of your wage earning report to verify that your social security number is not being used fraudulently, which could result in your owing taxes for wages earned by someone who's stolen your information.

8. **Contact Your Health Insurance Carrier**
   Request a copy of your health insurance statement in order to identify any fraudulent medical claims.

9. **Audit Your Login Credentials**
   Change your passwords for all online accounts and sign up for a password manager tool to store all your online login credentials in one secure location.
SELECT THE RIGHT IDENTITY THEFT AND MOBILE CYBERSECURITY PROTECTION PARTNER

Sontiq, along with its trusted brands EZShield and IdentityForce, is the industry's best-in-class provider of digital identity theft protection and cybersecurity solutions for both the individual and the enterprise. Through our comprehensive identity protection solution, we monitor each employee's digital footprint and detect suspicious changes in the user's personal, financial, credit, and social media information.

Through a subscription service, our members are protected 24/7 with comprehensive monitoring. We continuously scan the Internet, including the hidden areas not publicly visible known as the Dark Web, and alert members of any suspiciously activity tied to their identity. We provide an early warning system with rapid notification to our members' mobile devices (via email and text messaging) when the security of PII is deemed to be at risk. Should one of our members become victim of identity theft, they can rest easier knowing that they have access to EZShield Restoration, our fully-managed recovery services, and up to $1 million of identity theft coverage.

We provide mobile cyber security through our Mobile Defense Suite, which helps people keep their devices safe, and organizations recognize cyber threats before they turn into data breaches.

Prepare your organization to deal with potential breaches, efficiently and effectively, with our Data Breach Response services. Sontiq's Breach Readiness Program empowers business stakeholders to get ahead of a data breach through educational resources, planning, threat response, and victim assistance. If your company were to experience its own data breach, we are ready to act: RapidResponse with EZShield Restoration can be implemented in a matter of days or even hours to mitigate damages for businesses of any size.

We built the Small Business Suite to address the needs of Small and Medium-Sized Businesses, providing business identity protection and mobile cybersecurity solutions in tandem with employee identity theft protection.

EXCLUSIVE BREACH GUARANTEE

If your company were to experience its own data breach, we also offer an exclusive Breach Guarantee, providing white-glove restoration services to any of your employees affected by the breach for 12 months. All at zero cost to your company!

Learn More Today!

Contact Sontiq to learn how we are committed to helping employers, individuals and their families, and our partners protect personal information and remove the emotional stress and hardship that identity theft can have on people everywhere.
TWO POWERHOUSES IN ONE

EZShield®  
IdentityForce®