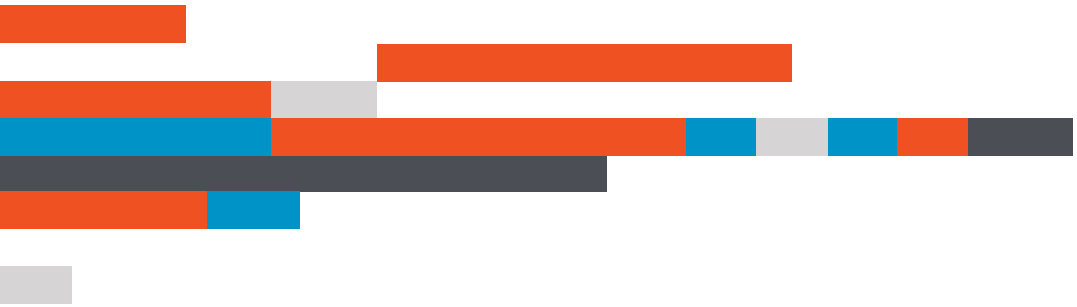
TERBIUM LABS

RESEARCH REPORT



THE UNDERRATED RISKS OF DATA EXPOSURE

October 2019

terbiumlabs.com | contact@terbiumlabs.com

TABLE OF CONTENTS

INTRODUCTION

The world we live in today is one where data breaches have become the new reality. From the latest Capital One data breach that affected millions of customers to the infamous Sony Pictures hack of 2014, organizations have become more vulnerable to a multitude of security risks that could leave sensitive corporate data exposed. This new reality is crystal clear when you look at the numbers. According to a newly published report by Risk Based Security, the first six months of 2019 have seen more than 3,800 publicly disclosed breaches exposing a whopping 4.1 billion compromised records.

Despite this new reality and these startling figures, organizations aren't taking the risks of exposed data seriously enough. To add fuel to the flames, many organizations still don't feel a sense of urgency or need to modify their perspective on data compromise. As a result, they are much less inclined to improve the methods by which they monitor and detect potential incidents of data exposure. While organizations are beginning to recognize the main ways information can be exposed, through credential leaks and dumps of personal identifiable information (PII), they have stopped short of identifying the broader risks to corporate data and financial details as a result of an initial exposure. The lack of follow-through in measuring and visualizing potential risk of data exposure can create catastrophic fallout for an organization that may have a major breach go undetected for months on end, all while security teams believe they have full visibility into existing threats. In this report, we will unveil the truth about how organizations measure, monitor, and map their risk levels of data compromise – with some startling revelations.

SURVEY METHODOLOGY & OBJECTIVES

We surveyed over 300 information technology (IT) professionals in the United States and Canada to better understand how businesses currently monitor and detect incidents of exposed data on the Internet, their current and future risks, and the potential negative outcomes. The survey was fielded in September 2019 and the respondents are comprised of full-time IT professionals who work in various industries, including but not limited to, retail, finance, healthcare, and ecommerce.

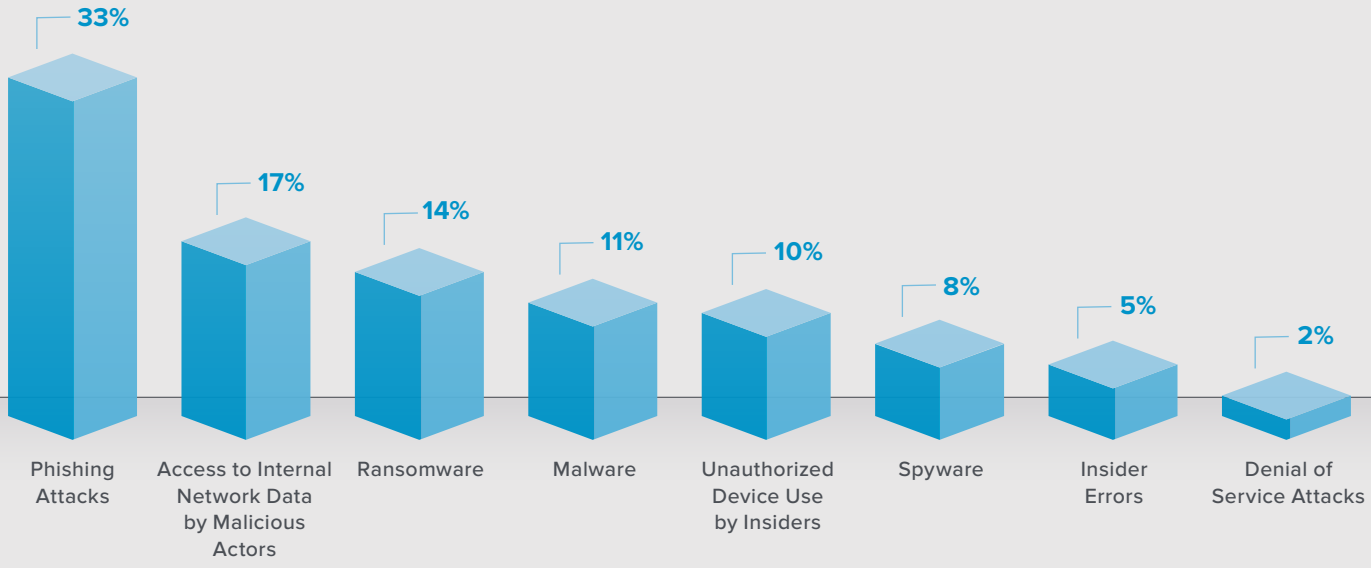
KEY FINDINGS & TRENDS

PHISHING IS THE CHIEF INSTIGATOR OF DATA EXPOSURE, MADE WORSE BY UNINFORMED EMPLOYEES

Phishing is a vicious cycle in security – it can be both the source and the result of data exposure. It allows attackers to access internal systems and compromise data to exploit for later exposure. Phishing is also one of the easiest ways for fraudsters to abuse data that has already been leaked into the criminal ecosystem. As we have seen first-hand in working with organizations to monitor and detect exposed data, email addresses are openly leaked by the tens of thousands each day on the Internet – across the open, deep, and dark web - and in criminal forums. Even without any additional information, an enterprising criminal can stuff batches of these email addresses into an existing phishing scheme and blast unsuspecting recipients with malicious messages. If the attackers are successful, they can gain access to additional information and may choose to share it with the rest of the criminal community – and the cycle begins again.

As our study's findings indicate, IT professionals have serious concerns about the risks associated with phishing. In fact, 33 percent of the respondents cited phishing as the most likely security incident to result in exposed data. This finding makes sense when you consider that Verizon's 2019 Data Breach Investigations Report (DBIR) found that 32 percent of data breaches involved phishing.

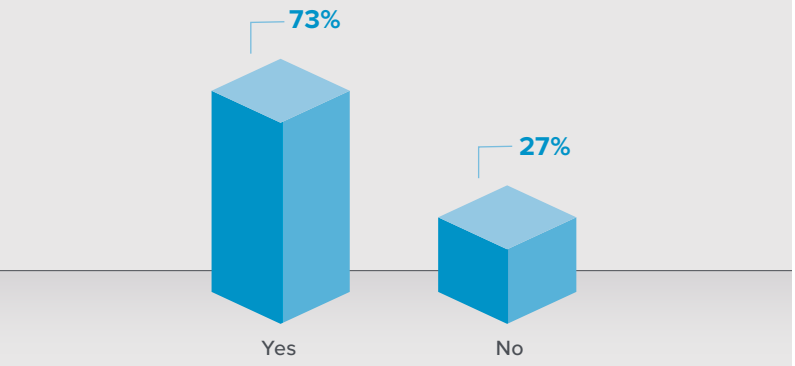
In your opinion, which of the following threats could result in sensitive corporate data being exposed, shared and sold on the Internet - across the open, deep and dark web?



To make matters worse, 27 percent of the respondents admitted they are not confident in their employees' ability to recognize phishing scams and avoid suspicious or fraudulent emails. That's troubling and problematic given the fact that phishing attacks have grown 65 percent in the last year and 76 percent of businesses reported being a victim of a phishing attack in 2018. This is further supported by the findings of the Spam and Phishing in 2018 report by Kaspersky Lab, which revealed that the company's anti-phishing system prevented over 482 million attempts to visit fraudulent pages last year, highlighting a significant surge in their use and popularity by cybercriminals.

Now consider this: In 2018, the Identity Theft Resource Center (ITRC) reported that hacking was the most used method of breaching data, with 482 data breaches resulting in almost 17 million records exposed. Unauthorized access, meanwhile, ranked second with 377 data breaches affecting the highest number of records exposed by data breach type—404 million. Accidental exposure had the third highest number of breaches, 114, with 22 million records exposed. It's then interesting to note that 17 percent of the respondents in our study, believe access to internal networks by malicious actors could be a culprit, while five percent cited insider error as being the possible cause of data exposure.

Are you confident in your employees' ability to recognize a phishing scam and avoid opening suspicious/fraudulent emails, which could result in corporate data being stolen, exposed, shared and sold on the Internet?



More than 52 percent of users re-use passwords across multiple platforms, meaning a single successful phishing campaign could unlock dozens of accounts for each user. As a result, hackers that attempt to perpetrate phishing scams could very well gain access to the online login credentials for financial accounts, social media accounts, healthcare, and insurance accounts, and a host of other unsuspecting third parties (including employers).

Phishing attacks are convenient and low-cost schemes for the fraud community to execute. In the same way that the open web provides businesses with avenues to market and communities to connect with consumers, the dark web provides hackers with similar tools and recommendations in crafting a phishing campaign. Fraudsters can now purchase complete, fully designed phishing pages designed to mimic the user experience on popular banking and technology websites. Vendors even sell these pre-fabricated phishing pages as a bundle, with recommendations on how to lure recipients in to entering personal details and billing information.

If phishing attacks are occurring so frequently and growing year on year, then it's highly likely that sensitive data will be exposed on the Internet and could be used for nefarious purposes. As such, it's critical that organizations are proactive, not reactive,

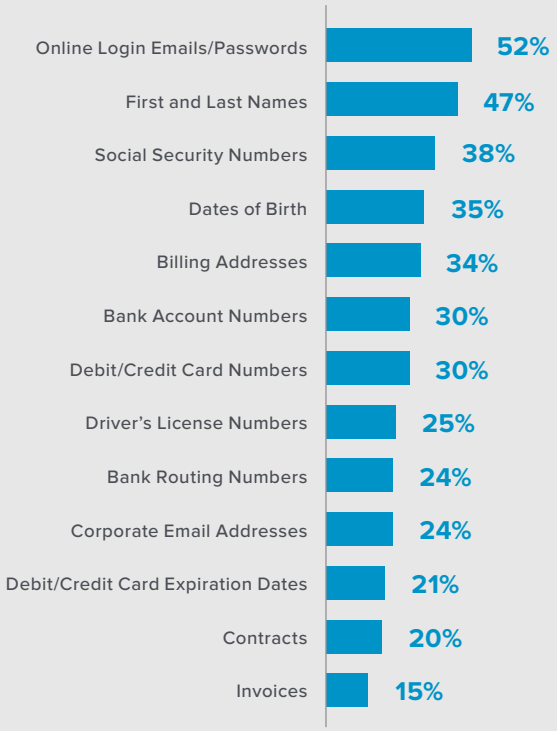
in the methods and tools used to monitor and detect if and when sensitive data has been exposed, which could result in lost customers, lost sales, lawsuits, regulatory violations, fines, reputational damage, and more.

WALKING THE DATA BREACH TIGHTROPE: ONLINE LOGIN CREDENTIALS, SOCIAL SECURITY NUMBERS, AND CREDIT CARD NUMBERS ARE DEEMED HIGH-RISK CUSTOMER DATA

Although security practitioners are beginning to recognize the risks associated with data exposure, they still drastically underestimate the likelihood that sensitive data could be shared and even sold online. When we asked the survey respondents to specify which types of customer data they believe could be at high risk of being exposed online, email address and password combinations (login credentials) came in as the number one type of customer data, at 52 percent.

Credentials often serve as an early warning signal for increased exposure and risk in the future. The presence of exposed credentials online indicates an existing security risk for organizations, but the risk does not stop there. There are ongoing downstream implications to data exposure that businesses need to understand and plan for. If credentials are appearing online, malicious actors may have already accessed the account or accounts associated with those credentials and accessed sensitive data sets to exploit additional information. Essentially, the appearance of the data online means that many other criminals are likely to try again.

Which of the following types of customer data do you believe could be at a high risk of exposure on the Internet?

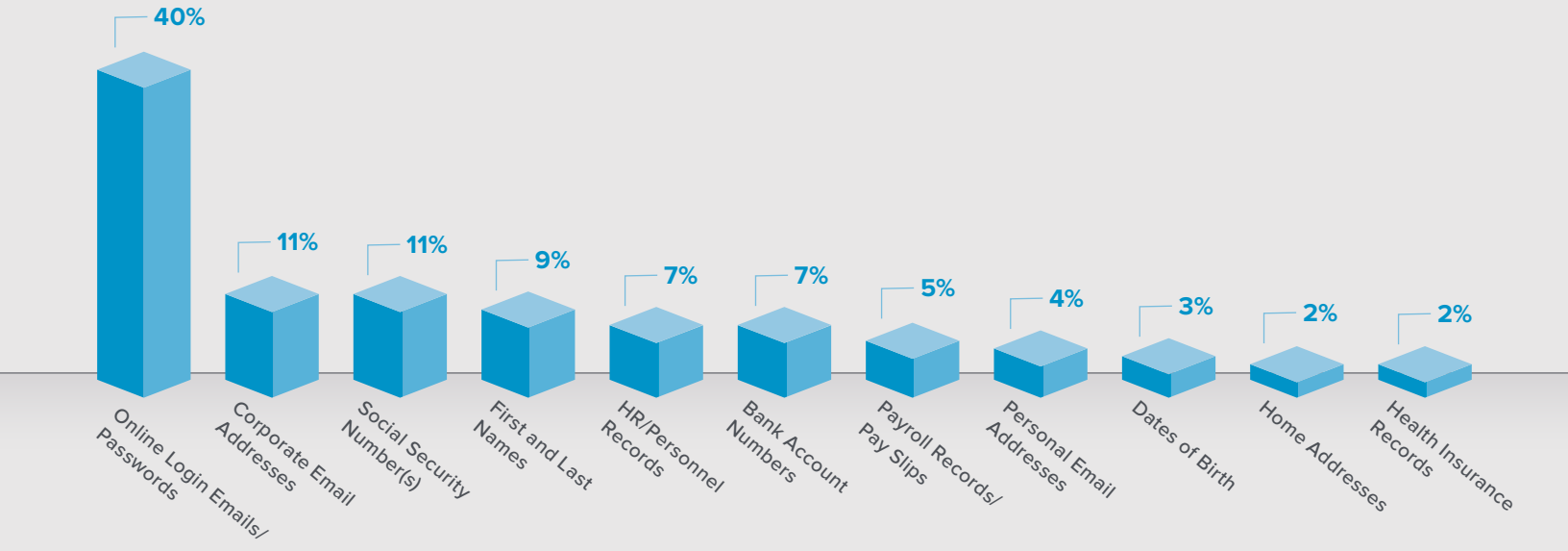


Meanwhile, customer Social Security number(s) came in slightly lower at 38 percent, followed by debit/credit card numbers (30 percent). These percentages are concerningly low. Based on what we have seen first-hand when monitoring exposed data on the dark web, compromised Social Security number(s) and payment card information are widely available online. Social Security number(s) are, more often than not, sold off for pennies, while hundreds of millions of stolen payment cards circulate in criminal markets and forums. This reflects similar types of data that were exposed in the 2019 Capital One data breach, which affected approximately 100 million individuals in the United States and approximately 6 million in Canada. According to court papers and Capital One, the hacker stole 140,000 Social Security numbers and 80,000 bank account numbers in the breach.

DESPITE INCREASE IN ACCOUNT TAKEOVER ATTACKS AND FRAUD, EMPLOYEE PERSONAL INFORMATION AND FINANCIAL DETAILS ARE DEEMED LOW-RISK

If IT professionals are underestimating the risks of exposure for customer information, then awareness about the exposure risks facing employee data is in even more dire straits. This is evidenced by our study's findings, whereby the surveyed IT professionals ranked employee credentials at a high risk of exposure (40 percent), but drastically underrated the risk of exposure for effectively all other employee data types. For instance, a mere nine percent of the respondents reported a high risk of exposure for employee names, while less than two percent were concerned about the risks of having employee home addresses exposed. Even employee Social Security number(s) failed to raise significant concern, with just 11 percent of the respondents indicating a high risk of exposure. Compare these responses to the same levels of concern about customer data appearing online, with 46 percent concerned about customer names, 34 percent concerned about customer addresses and 38 percent indicating a high risk of exposure for Social Security number(s).

Which of the following types of employee data do you believe could be at a high risk of exposure on the Internet?



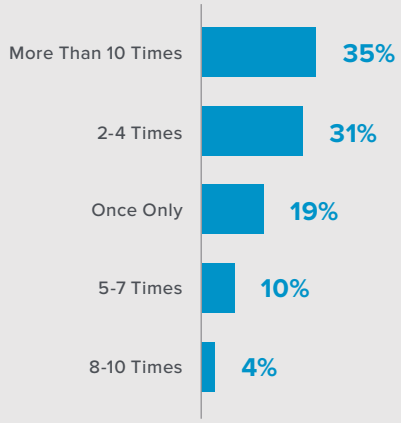
Why do organizations underrate the risk of exposure for employee information, while reporting such high rates of concern over the likelihood of customer information being exposed? Let's explore this further. Account takeover and identity theft impact employees and customers alike. According to 2018 Identity Fraud: Fraud Enters a New Era of Complexity from Javelin Strategy & Research, there were 16.7 million victims of identity fraud in 2017 – that's a record high that followed a previous

record the year before. Given these figures, it's both surprising and worrying that organizations would be so deeply unconcerned about the risk of exposure of employee data.

This begs the question: Are organizations overconfident in their ability to lock down employee information compared to the way they store and process customer information? Are they more concerned about the implications of customer information surfacing compared to employee data? The overarching California Consumer Protection Act specifically excluded employee data from its language, largely absolving employers of responsibility for monitoring and protecting employee information. This exclusion is a symptom of a larger issue: a disconnect between the risks associated with employee data and the risks associated with customer data. This disconnect creates a dangerous sense of overconfidence – especially given employee data provides a valuable gateway to not only other employee records, but also to sensitive customer data. The disparity in perceived risk of exposure has an unavoidable effect in the way organizations evaluate their data security and data monitoring practices, likely leaving a huge portion of valuable corporate data unmonitored and vulnerable.

REPEAT OFFENSES OF DATA EXPOSURE ARE A MATTER OF FACT, NOT FICTION

How frequently do you believe sensitive corporate data could be exposed, shared and sold on the Internet - across the open, deep and dark web?



We often talk about the risks and concerns surrounding data exposure, but the industry stops short of informed conversations about the risks associated with data re-exposure. In tracking stolen data across the dark web for several years, we have seen first-hand evidence that the same data sets are repackaged, leaked, and sold more than a dozen times over. This falls in line with our study's findings, with 41 percent of the surveyed IT professionals saying they believe sensitive corporate data could be exposed, shared, and sold on the Internet between two and seven times. An additional 35 percent said they believe it could be shared and exposed more than 10 times.

The reality is that high-profile breaches may result in compromised data being leaked hundreds of times. How could this be possible, you may be asking? Sometimes data gets re-leaked in a blast effect, with the same leak being spread dozens of times in a row, hour after hour. In other cases, high-profile leaks, particularly those attributed to government or military sources, can be re-leaked multiple times

in a given month or year, with new actors claiming to take credit for the leak of information in an effort to gain some traction or credibility with their peers (especially amongst younger actors).

This same tactic made headlines early in 2019 with the Collections data set. Highly publicized as a leak of billions of records, streaking through criminal forums with hundreds of requests for download links and access points, the collection data set turned out to be largely older, repurposed data from leaks several years past, as reported by Vice. Despite the older data sets, criminals were still eager to get their hands on the information to try to exploit the data once it became available. This example highlights two key points. First, not all leaked data is freshly exposed. Second, all leaked data, no matter how old, can still garner attention and increase security risks.

The moral of the story here is clear: Information, once exposed, continues to add risk to a business. The initial exposure creates a spike in risk, but the long-tail effects can multiply a company's baseline level of risk going forward. Given 50 percent of the respondents in our study believe information can only be shared fewer than four times – and 18 percent believe information can only be shared once – this information gap puts businesses at a disadvantage in accurately assessing their exposure risks and may generate additional overconfidence in creating comprehensive monitoring strategies going forward.

APATHY IS CLOUDING ITS JUDGMENT ABOUT NECESSITY AND VALUE OF DARK WEB MONITORING

One of the more startling findings of our study points to a sense of apathy among IT professionals about the need and value of staying abreast of potential exposed data. Despite the fact that 23 percent of the surveyed IT professionals admitted that their organization has had sensitive corporate data exposed, shared, and sold on the Internet in the last 12 months, 16 percent indicated that they 'don't know' whether or not their organization has had information exposed.

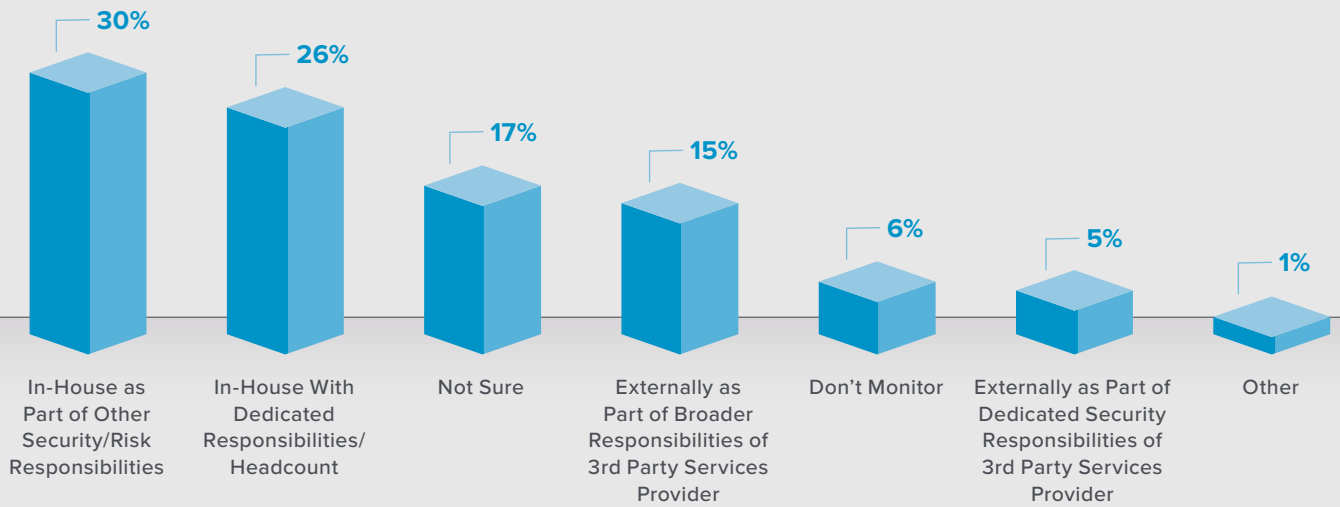
Has your organization had sensitive corporate data exposed, shared and sold on the Internet in the last 12 months?

The ‘don’t know’ answer just isn’t good enough in today’s environment where data breaches have become the rule, not the exception. Those ‘don’t know’ responses signal apathy and a general lack of knowledge about the current state of data security within the organization and across any third party contractors or partners.

This lack of awareness can come back to harm companies in more than one way. According to the 2019 Cost of a Data Breach study by Ponemon and IBM Security, the average global cost of a data breach is $3.92 million. Ponemon found that it took organizations an average of 279 days to detect a data breach – meaning a breach that occurred in January would go undetected for most organizations until September of that year. Worse yet, six percent of the respondents in our study said they don’t currently take any steps to monitor and detect data exposure, with an additional 17 percent admitting they aren’t sure if their organization currently takes any steps to monitor the internet for sensitive information.

Lack of awareness, meanwhile, increases the period of time where information is exposed without detection, which results in greater costs to an organization – loss of customers, brand and reputation issues, to say nothing of the security incidents that may develop as a result of exposed information increasing access for threat actors. Since most organizations are informed about a security incident by a third party, this increased time between exposure and detection puts organizations at a greater risk, as third parties will likely discover the breach first, reducing the opportunity for the exposed organization to take stock of the damage and control the story. Being proactive in monitoring reduces detection time and reduces overall cost for each exposure event by putting organizations in control.

How do you currently monitor and detect if sensitive corporate data has been exposed, shared and sold by a third party on the Internet – across the open, deep and dark web?

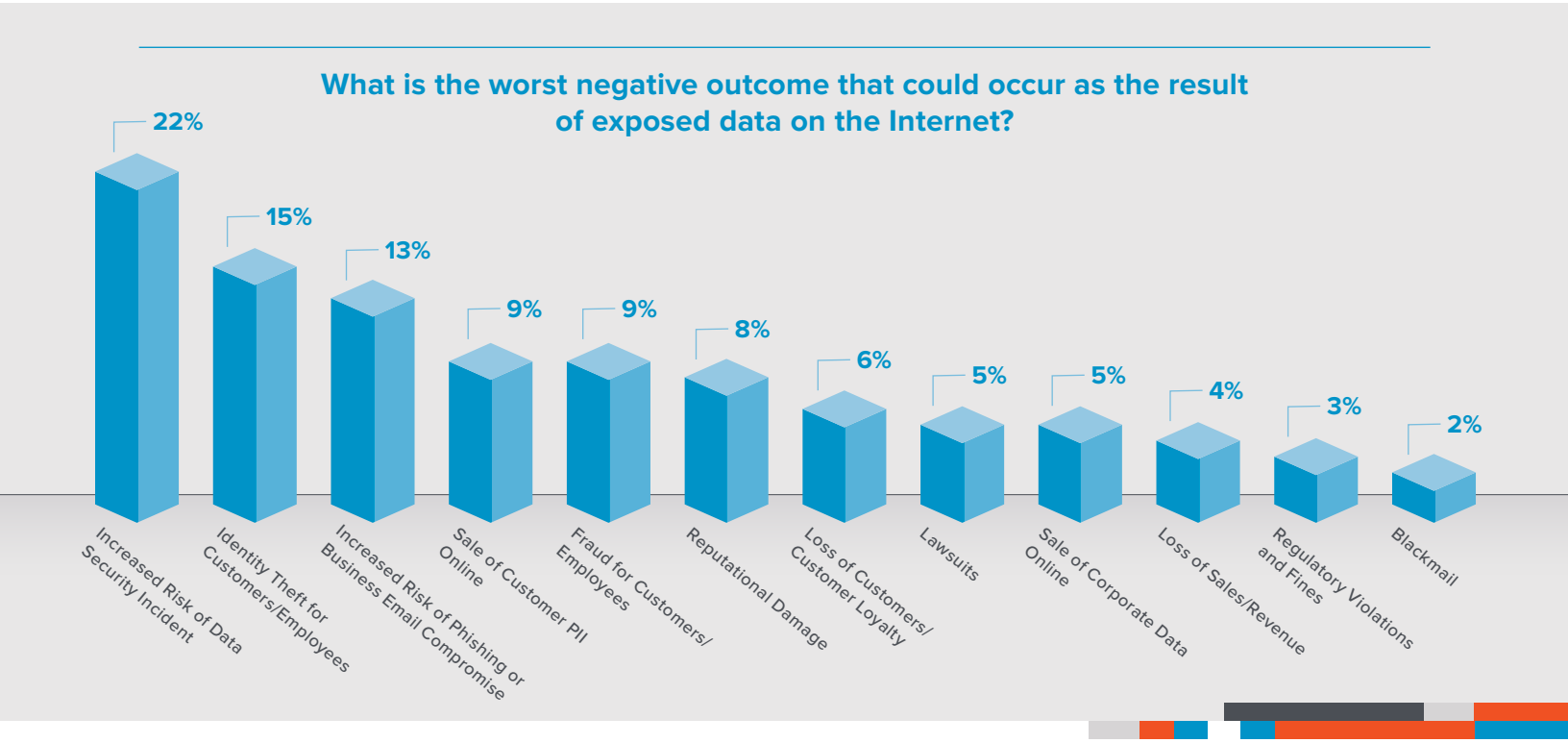


CONSEQUENCES BE DAMNED: A RECIPE FOR LOST CUSTOMERS, DECLINE IN SALES, AND REPUTATIONAL DAMAGE

While a significant portion of the surveyed IT professionals believe exposed data could result in an increased risk of a security incident (22 percent) and phishing scams (13 percent), far fewer are worried that exposed data could result in loss of sales/revenue (four percent), loss of customers/customer loyalty (six percent), and reputational damage (eight percent). A mere two percent of respondents expressed concerns about regulatory violations as a result of data exposure.

These responses are overconfident, at best, and largely divorced from reality, at worst. Take the Uber data breach of 2016, for example, which exposed the personal information of 57 million Uber users and 600,000 drivers. The breach is believed to have cost Uber dearly in both reputation and money. At the time that the breach was announced, the company was in negotiations to sell a stake to Softbank. Initially, Uber's valuation was $68 billion. By the time the deal closed, its valuation dropped to $48 billion, and while a number of factors contributed to that drop, the catastrophic breach undoubtedly played a role. Likewise, during Verizon's 2016-2017 acquisition of Yahoo!, news broke about a series of legacy data breaches impacting billions of Yahoo's customers. As a result, Verizon considered walking away from the deal entirely, but ultimately negotiated a $350 million price reduction of the acquisition specifically linked to the expansive security failures.

Meanwhile, eBay faced significant reputational damage from its May 2014 data breach, which left 145 million users compromised. The company was criticized at the time for a lack of communication informing its users about the breach and for poor



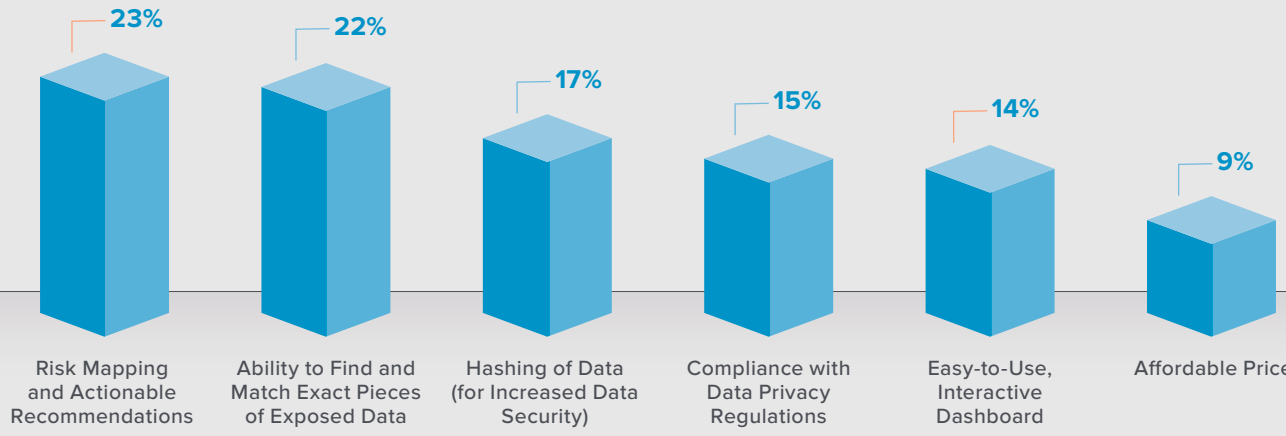
implementation of the password-renewal process. CEO John Donahue was quoted as saying the breach resulted in a decline in user activity (even though it didn't impact the bottom line).

What's even more troubling is that IT professionals seem largely unconcerned about data ending up for sale online. In fact, only five percent of the respondents said they're worried that corporate data could be sold after being exposed, while just nine percent believe customers' personally identifiable information could end up with the same ill fate. With billions of records circulating on the dark web, and tens of thousands of listings for sensitive information for sale on dark web marketplaces, these responses are naive at best, and negligent at worst. These attitudes and the broad lack of concern about potential fallout from breaches influence the way organizations monitor and track their sensitive information. If IT professionals believe there are no meaningful threats or losses associated with data exposure, they run the risk of putting their organizations and their customers at a significantly increased risk, purely through professional indifference.

MONEY'S GOT NOTHING TO DO WITH IT – THE TRUE VALUE OF DARK WEB MONITORING LIES IN PRECISE DETECTION, RISK MAPPING, AND DATA PRIVACY

When we asked the surveyed IT professionals to cite the most important factor when choosing a dark web monitoring tool, money didn't seem to come into the equation at all. In fact, only nine percent cited affordable price as an influential factor. On the other hand, risk mapping and actionable recommendations came in much higher at 23 percent, followed by the ability to find and match exact pieces of data (22 percent) and hashing of data (for increased data security) at 17 percent.

What is the most important factor when choosing a dark web monitoring tool to monitor and detect incidents of exposed data on the Internet?



These results reinforce the development of a market searching for actionable intelligence based on specific pieces of exposed data, with security built in to the foundation of the product. IT professionals face increased alert fatigue, with 82 percent of respondents in a recent Threat Stack survey reporting that alert fatigue negatively impacts their organization's well-being and productivity. These teams look for solutions that can cut through the noise and provide clear, cohesive analysis – without putting the organization at increased risk.

A world of constant data exposure requires organizations to react quickly, generating demand for contextualized intelligence around specific data sets. Security teams need clarity and direction, while executives need historical insight into developing trends and risk areas that impact business operations and continuity. In the event of a major breach or third party security incident, businesses need to be alerted quickly and should be provided with detailed risk mapping so they can take the necessary actions to protect their customers' data and ensure compliance with data privacy regulations.

Organizations should expect more from their security providers. Monitoring for sensitive data should not require putting that data at additional risk; teams should be able to remain compliant, secure, and protected while still having full visibility into the exposure of sensitive information online. Terbium Labs developed its patented fuzzy hashing protocol ("data fingerprinting") specifically in response to this prompt, in efforts to find a way to provide comprehensive visibility into the information exposed online, without ever needing to access or hold the original client data under monitoring. As the demand for data monitoring increases, expectations for fully secure security providers should likewise increase. Otherwise, organizations are simply increasing the chance of data exposure in an effort to detect data exposure, which not only complicates compliance issues, but also has a net increase on potential risk of a third party security incident over time.

CONCLUSION

While some IT professionals show increased awareness about the risks to customer information, this research study highlights a major disparity between the potential for customer data exposure and employee data exposure. If organizations are beginning to recognize the risk of customer data appearing online but stop short of seeing the risk to their own employees, they have a great deal of work left to do in shoring up their IT security systems and methods. The fact of the matter is that employee data can be a skeleton key to the rest of the data stored in an organization. It goes without saying, therefore, that an organization's perceived risk of exposure – and the data monitoring methods and tools used by organizations – should match that level of risk.

Likewise, respondents in our study acknowledged that information can be leaked multiple times over, but seem largely unconcerned about the potential fallout from those leaks – even when the average breach costs an average of $3.92 million dollars. What was both surprising and disheartening is that regulatory consequences, brand and reputation issues, and even financial losses fail to raise an eyebrow, despite the fact that IT professionals fully acknowledge and expect sensitive information to be shared online upwards of ten times once exposed. Until recently, regulations and legislation have not hammered home the importance of data security, but the winds are changing. Organizations need to get ahead of those changes and make adjustments to their strategies now, or risk being left behind.

Nevertheless, organizations recognize the need for monitoring and have voiced strong opinions about the need for clear and actionable intelligence. As organizations become more aware of how data exposure impacts their risk levels and state of IT security, they should take a more proactive approach and implement the necessary methods and tools for a nuanced and cohesive digital risk protection program. A mature security strategy relies on fully private monitoring to discover exposed data quickly, provide clear and specific alert notifications, and help IT teams respond and remediate with regulatory compliance in mind.

ABOUT TERBIUM LABS

Terbium Labs empowers organizations to reduce the risk of inevitable data exposure. Matchlight, the company's comprehensive digital risk protection platform, features continual digital asset monitoring, robust analytics, and actional intelligence, to quickly identify and minimize the impact of exposed data across the Internet – whether it's the open, deep, or dark web. Featuring its patented data-fingerprinting technology that ensures private data stays private, and unique fusion of data science, machine learning, and dedicated analysts, Terbium Labs provides pinpoint accuracy for early detection and remediation to understand risk exposure and keep organizations safe. Learn more about Terbium Labs' unique approach to digital risk protection by visiting www.terbiumlabs.com or on twitter @terbiumlabs.