Welcome

So much has changed in such a short amount of time.

January 2020 started off like any other year, with breaches ranging from the relatively mundane to the incredibly painful. At Advocate Lawrenceville Internal Medicine, a failure to use the BCC field accidentally revealed contact information for 8,031 patients. Meanwhile the REvil/Sodinokibi ransomware event at Travelex triggered widespread disruption of their operations for weeks, and ultimately, as reported by The Wall Street Journal, forced the company to pay a $2,300,000 extortion demand.

By March, it was clear that information security teams were in for a wild ride. Attackers shifted focus to take advantage of the COVID-19 pandemic crisis, as millions of employees around the world switched to remote working. The scramble to accommodate the new normal has forced many organizations to make quick decisions around which additional technologies to deploy in order to support remote operations and re-evaluate long-held security practices that may no longer be viable. Perhaps one of the most public examples of this made headlines on March 17th, when the U.S. Health and Human Services’ Office for Civil Rights announced they were suspending the enforcement of penalties against health care providers for the good faith use of noncompliant remote communications technologies.

We will soon see how these changes will impact breach activity over the coming months. For now though, this report covers publicly disclosed data breaches first reported between January 1, 2020 and March 31, 2020. Our analysis is presented in a series of charts, graphs, and commentary, each highlighting a unique view into the trends taking shape in 2020. We hope you’ll find this report to be a valuable resource and an interesting read.

Key Highlights

- The number of publicly reported breaches in Q1 2020 decreased by 58% compared to Q1 2019.
- The decline in the number of disclosed breaches is attributed to two factors: reporting disruption brought on by COVID-19 and the unusually high number of breaches reported in Q1 2019.
- The number of records exposed in Q1 2020 skyrocketed to 8.4 billion - a 273% increase compared to Q1 2019 and the most records exposed in any Q1 period since we began tracking data breaches in earnest in 2005.
- The increase in records compromised was driven largely by one breach: a misconfigured ElasticSearch cluster that exposed 5.1 billion records. Adjusting for this incident, the number of records still increased 48% compared to Q1 2019.
- Approximately 70% of reported breaches were due to unauthorized access to systems or services, while approximately 90% of the records exposed were attributable to exposing/publishing data online.
- 11 breaches exposed more than 100 million records each, and five breaches exposed between 10 and 99 million records.
- On a positive note, despite the number of large breaches driving the number of records exposed, approximately 68% of the breaches with confirmed record counts exposed fewer than 1,000 records.
In This Issue

FEATURED VIEWPOINTS FROM

Inga Goddijn  
Executive Vice President,  
Risk Based Security

Jake Kouns  
Chief Executive Officer  
and CISO,  
Risk Based Security

WELCOME
Key Highlights .......................................................................................................................... 2
In This Issue .................................................................................................................................. 3
Viewpoints ...................................................................................................................................... 4
   The Coronavirus Ripple Effect ................................................................................................. 4
   When the Going Gets Tough, Cybercrime Gets Going .............................................................. 6
Data Breach Trends in 2020 ........................................................................................................ 10
   2020 At A Glance .................................................................................................................... 10
   Who Has Been Breached? ...................................................................................................... 13
   Where Did Breaches Occur in 2020? .................................................................................... 15
In Closing .................................................................................................................................... 17
   Methodology and Terms ......................................................................................................... 17
   Data Standards and the Use of “Unknown” ............................................................................ 17
About Risk Based Security ......................................................................................................... 18
   About Cyber Risk Analytics .................................................................................................... 18
   No Warranty ............................................................................................................................ 18

© Copyright 2020 Risk Based Security, Inc. All Rights Reserved
The Coronavirus Ripple Effect

Inga Goddijn, Executive Vice President, Risk Based Security

Inga found her way to information security after working for twenty years in the insurance industry. During her time managing a multi-million dollar portfolio of technology and cyber insurance coverages, Inga witnessed first-hand the impact of ineffective security program management and the financial fallout from data breach events. At Risk Based Security, she is responsible for Cyber Risk Analytics and YourCISO. Inga has presented at a variety of industry forums and has led many education sessions throughout the U.S. She currently holds a CIPP/US designation.

How do we talk about breaches while the slow-motion disaster of the coronavirus wreaks havoc around us? I will be the first to admit, staying focused this quarter has been a challenge. However, as we adapt to the new normal and take stock of events, it’s clear that COVID-19 is having an impact on practically every aspect of life. Breach activity is no exception.

Having conducted breach research for 20+ years now, we knew from the outset that a major event like COVID-19 would have two effects on our research. First, as the news cycle becomes dominated by crisis coverage, other newsworthy events go under-reported or uncovered. News articles are an important source of information and one of many sources our breach research team uses for gathering intelligence. From prior experience we would normally expect to see a few slow news days during a major event, however the effect is typically short lived and plays itself out relatively quickly. Not so with the pandemic. We observed a decline in breach news coverage beginning in early March with the trend continuing throughout April.

Second, malicious actors thrive in chaos. Fear, uncertainty, and doubt are more than a sales strategy; they are an exploitable opportunity for hackers and fraudsters. From the earliest days of the crisis, we’ve witnessed a variety of strategies being deployed to take advantage of COVID-19. We see phishing attacks disguised as urgent pandemic updates used to steal data and spread malware, bogus applications mimicking popular remote working tools, and spurious “official” websites proliferating at every turn. The collision of a global health crisis with a distracted workforce, coupled with IT teams managing a radical shift to remote working, has created the perfect environment for successful attacks. It’s only a matter of time before we see the current situation manifest itself as an increased number of breaches.

RIPPLES IN Q1

There were 1,196 breaches reported in the first three months of 2020, the lowest number of breaches disclosed during the first quarter since 2016. This number will increase as additional information comes to light and more breaches are confirmed, but it is telling that the rise of COVID-19 coincides with a relatively quiet start to the year. We will dig into this effect throughout this report, highlighting where we think COVID-19 is at play and where other trends hold sway.

THE SPREADING WAVE – WHAT’S COMING NEXT

In our next section, we present an in depth analysis of how economic crises like those triggered by the coronavirus containment efforts impacts cyber security. Read on for our take on how recessions fuel crimewaves and lay the groundwork for successful cyber attacks.
The standard for actionable data breach intelligence, risk ratings and supply chain monitoring.

- Cyber Insurance
- Security & Vulnerability Management
- Vendor Risk Management
- Procurement
- Governance & Management

REQUEST A DEMO
sales@riskbasedsecurity.com

LEARN MORE
www.cyberriskanalytics.com
When the Going Gets Tough, Cybercrime Gets Going

Jake Kouns, Chief Executive Officer and Chief Information Security Officer, Risk Based Security

Jake is an expert in the security industry who has briefed the DHS and Pentagon and is frequently interviewed by Forbes, Information Week, PC World, CSO, and CIO Magazine. He has appeared on CNN and presented at many well-known security conferences, including RSA, Black Hat, DEF CON, CISO Executive Summit, FIRST, and HiTB Cyberweek. Jake is also co-author of Information Technology Risk Management in Enterprise Environments, Wiley, 2010, and The Chief Information Security Officer, IT Governance, 2011.

The ongoing “Coronavirus” (COVID-19) pandemic has had a profound impact on the world economy in a short time, especially within the United States where unemployment has risen sharply. While much is still unknown, many analysts are predicting that the market decline will continue before we see any kind of meaningful or sustained recovery.

In the United States, a major part of the economic damage already done has been from COVID-19's impact due to “social distancing” and “shelter in place” mandates. The unemployment rate has risen significantly, from 211,000 to 22 million, shattering initial projections of 2 million. Back when the pandemic started, analysts believed that 5 million unemployed or an unemployment rate of 10% would be the worst case scenario. However, as of now, the employment rate is believed to be somewhere between 12-15%.

Even though Congress and The White House pushed out a stimulus package, many economists seem to agree that we are currently on track, or already experiencing, the next recession, with some even believing that it could become a depression.

"We are going into a global recession. We are going to see a spread of economic sudden stops."

Mohamed El-Erian, Allianz Chief Economic Advisor

While not everyone agrees on the exact impact, or how long it will last, there are clearly substantial concerns about just how quickly the economy will be able to recover once COVID-19 is under control.
CYBERCRIME INCREASES DURING A RECESSION

The past has shown us there is a correlation between recession and cybercrime as evidenced during and before the 2008 – 2009 Great Recession. News publications reported that fraud on the internet increased by 33% during the last recession, with the broken economy and increased digitization making data more vulnerable than ever.

This is more than just our opinion. In conducting our research on this topic we uncovered a substantial amount of information that provides some very compelling insights. Here are just some of the key points and references:

**U.S. recession fuels crime rise, police chiefs say, Reuters, January 2009,**

“Crime has increased during every recession since the late 1950s, sociologists said.”

“There has long been debate over the connection between crime and the economy, but criminologists, sociologists and police chiefs interviewed by Reuters in October predicted a rise in crimes as the United States sinks deeper into recession.”

Ross Colvin

**Economic recession to spur ‘dramatic increase’ in cybercrime, TechTarget, February 2009,**

“Bad times always bring a rise in crime. But this economic recession is setting us up for a wave of cybercrime. The broken economy, combined with increased digitization as retail and operations move online and ever-more sophisticated hackers, means more data is more vulnerable than ever. That was the warning from former federal prosecutor and securities fraud attorney Orin Snyder, speaking at a data security panel at yesterday’s LegalTech conference in New York.”

Linda Tucci

**Report says online crime surging in recession, Reuters, March 2009,**

“Fraud on the internet reported to U.S. authorities increased by 33 percent last year, rising for the first time in three years, and is surging this year as the recession deepens, federal authorities said on Monday.”

Jason Szep

**Recession ‘adds to boom in cybercrime’, Telegraph, August 2009**

“The recession is adding to a boom in cybercrime as computer-literate criminals in poorer countries turn their hand to electronic scams, British researchers said.”

“Criminals there can take advantage of cybercrime opportunities, and the current global recession will likely increase this trend still further, “said Prof Rush.”

The Telegraph


“We asked the question: Will cyber crime increase in a time of global economic recession? One study by KMPG found that many enterprises believed that the recession put their business at greater risk from out-of-work IOT workers tempted to join the criminal underground to make ends meet (Kirk 2009).”
“Economic theory predicts that the global recession will probably increase the amount of cyber crime as the recession deepens. This could result from a variety of causes an increase in attacks on more vulnerable and desperate people from those with cyber skills joining the cyber criminal ranks for needed income; and a decreased focus on and investment in computer security as a result of fewer resources.”

Peter Guerra

The same factors and trends from the 2009 timeframe are even more present now in 2020: global economic distress, increased widespread digitization, and an increase of potentially exposed confidential data. Sadly, even though a vast majority of industries are struggling in today's economy, it isn't a new concept that cybercrime itself is recession-proof.

THE PERFECT CONDITIONS FOR CYBERATTACKS

Whether we are in, or heading for, a recession doesn't matter. Economic hardship historically guarantees that organizations will face increased cyberattacks.

A few months ago, we wrote that PSIRT and other security teams are often caught in a Catch-22 situation, wherein a successful job creates the perception that there is less need for a security team.

As such, IT jobs not considered critical (perhaps even some security programs) are often the first to be under review to be cut during times of economic hardship in a short-sighted attempt to save money.

The cycle is as follows:

1. Economic hardship prompts organizations to reduce or even cut “non-essential” programs and personnel to save money;
2. Organizations haven't experienced a data breach or unauthorized compromise (the result of an effective security team), so IT and security teams are deemed non-essential and are downsized;
3. Malicious attackers who were previously foiled now have increased opportunities to infiltrate systems due to a lack of staffing and focus;
4. Organizations suffer an expensive or embarrassing data breach and reflexively hire additional security personnel.

As financial pressures continue to mount, and unemployment numbers increase, organizations will need to work hard to ensure that necessary IT and cybersecurity personnel are not among them, and that the proper resources are allocated to their security intelligence programs. This is especially true during our current time, when cyber attacks will become more frequent and sophisticated.

As more organizations are forced to temporarily shutter their brick-and-mortar operations, more people are shifting their work and purchasing online, putting substantial strain on the Internet. Security is not, and should not be viewed as, an unnecessary expense.

In today's business world, security is a required cost of doing business at a minimum to meet customer's privacy expectations and meet regulatory requirements. Cutting security budgets increases organizational risk in ways that might not seem readily apparent, and doing so may have a long-lasting impact.
THE UNSEEN DANGERS

Many organizations have been forced to rapidly turn to Virtual Private Networks (VPNs) as they implement work from home policies to help slow the spread of COVID-19. However, doing so gives malicious attackers more opportunities to compromise systems.

While remote working isn't new, endpoints for many organizations have shifted dramatically, with much of the workforce moving to unmonitored personal systems, giving attackers a new vector to gain a foothold. Security Monitoring in this kind of decentralized environment was already considered daunting and had caused issues for those that had been working for years to solve the problems. So organizations recently having to deal with these challenges, while also potentially implementing widespread cyber security budget cuts, will not be able to effectively understand or remediate their vulnerabilities and may not have full visibility into devices being used for corporate functions.

Attackers thrive on heightened emotions and targets of opportunity, so employees now coping with school closings and other unplanned events are more likely to be distracted. Even with the best intentions, less attention will be given to secure phone calls, instant messages, and emails. That suspicious link may be even more likely to get clicked on, and that abnormal system behavior may be missed while dealing with family issues, or pets and kids running around the house. As such, the number of COVID-19 related phishing attacks has been growing; and this is just the start.

BETTER DATA IS MORE IMPORTANT THAN EVER

Security should never be considered an optional expense, but should be recognized as a minimum cost of doing business. While the exact cost of security incidents is the cause of some debate, there's no doubt that cutting security budgets could inflict a terrible impact on the entire organization's bottom line, especially if a data breach occurs. Informed, risk-based decisions are more vital than ever, and you can only make proper decisions if you have the proper intelligence.

Organizations need to do their best in these trying times to ensure that security budgets remain funded and that IT personnel have the resources they need to properly mitigate risks. The number of threats is constantly increasing, and vulnerabilities are constantly being disclosed, so when there are reduced IT resources, it requires a laser focus to ensure the limited time and money available is spent addressing, analyzing and fixing the most important issues representing risk for the most important assets. The corporate landscape is currently primed for cyberattack and organizations need to prepare accordingly.
Data Breach Trends in 2020

2020 is off to an unusual start, but in several ways the trends that have defined the past few years continue to hold sway. We continue to observe unauthorized access to systems and services, labeled “hacking” in our schema, as the primary contributor to the overall number of events. However it is the human element, simple oversights or mistakes, that ultimately exposes the most records. In this report, we highlight the who / what / when / where and how of breach activity that shaped the start of this year.

2020 At A Glance

![Figure 1: Number of breaches reported in Q1 each year](image1)

![Figure 2: Number of records lost (in millions) reported in Q1 each year](image2)

The total number of publicly disclosed breaches in Q1 2020 dropped dramatically compared to 2019. The obvious question is why? We observed two factors driving this change. First, in early 2019, research identified a large number of illicit data leaks and dumps, resulting in a temporary spike in activity. This is not the first time we've seen this effect. Similar spikes have been captured in the fall of 2019, and again in 2018 and 2017. This trend was absent from the start of 2020.

The second factor, we believe, is the disruption triggered by COVID-19. As the virus spread, so did a decline in breach disclosures. Based on our experience, this should not be interpreted as a decline in breach activity. Quite the contrary. The turmoil brought on by the pandemic has created a unique opportunity for malicious actors and a stressful environment primed for mistakes. Once the dust settles, we anticipate the number of reported breaches will be on par with, if not exceed, 2019.

Despite the decline in the number of breaches reported, the number of records exposed hit a new Q1 high. Eleven breaches in Q1 exposed over 100,000,000 records each, with ten of those due to misconfigured databases or services.
A common theme continuing into 2020, the majority of breach events are attributed to unauthorized access to systems, but the vast majority of data exposed is attributed to disclosure on the internet. On average, hacking exposed an average of approximately 850,000 records per breach. Web disclosure exposed an average of approximately 106,000,000 records per breach.

With hacking as the top breach type, it follows that most breaches originate from outside the organization. Insiders can also do their fair share of damage, however. In Q1 of 2020, malicious insiders took coating technology from Eastman Chemical; marketing research, strategic planning, and customer lists from Hershey; and 1,182 patient records from Beaumont Health (which were then shared with a personal injury lawyer).
It is useful to note that despite some very large breaches, approximately 68% of the incidents with confirmed record counts exposed less than 1,000 records. This indicates that most breaches are far less extreme than casual observations of other reports might suggest.

Do you think most attackers are out to steal credit card data or other juicy financial information? Think again. In Figure 6, we can see that the most frequently exposed data types are access credentials. These typically take the form of passwords in combination with email addresses or usernames.

The increase in the percentage of events with “Unknown” data types exposed is due in large part to the increase in ransomware events that also involve access to, and in some cases exfiltration of, data. In these events, detailed descriptions of what type of data was put at risk are rarely provided. However, now that groups behind ransomware attacks such as REvil/Sodinokibi, Maze, DopplePaymer and Nefilim have elevated their extortion racket to include publication of data taken in the course of launching their malware, this may in due course provide additional insights into the types of data compromised.

<table>
<thead>
<tr>
<th>Records Lost</th>
<th>Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown</td>
<td>391</td>
</tr>
<tr>
<td>1 to 9</td>
<td>17</td>
</tr>
<tr>
<td>10 to 99</td>
<td>200</td>
</tr>
<tr>
<td>100 to 999</td>
<td>334</td>
</tr>
<tr>
<td>1,000 to 9,999</td>
<td>114</td>
</tr>
<tr>
<td>10,000 to 99,999</td>
<td>56</td>
</tr>
<tr>
<td>100,000 to 999,999</td>
<td>47</td>
</tr>
<tr>
<td>1,000,000 to 9,999,999</td>
<td>21</td>
</tr>
<tr>
<td>10,000,000 or above</td>
<td>16</td>
</tr>
</tbody>
</table>

Table 1: Number of incidents with records lost in these ranges in Q1 2020

<table>
<thead>
<tr>
<th>Data</th>
<th>2020</th>
<th>2019</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>54.0</td>
<td>76.0</td>
<td>44.0</td>
</tr>
<tr>
<td>Password</td>
<td>49.0</td>
<td>70.0</td>
<td>40.0</td>
</tr>
<tr>
<td>Names</td>
<td>32.0</td>
<td>21.0</td>
<td>40.0</td>
</tr>
<tr>
<td>Unknown</td>
<td>24.0</td>
<td>6.0</td>
<td>12.0</td>
</tr>
<tr>
<td>Misc.</td>
<td>21.0</td>
<td>17.0</td>
<td>17.0</td>
</tr>
<tr>
<td>Address</td>
<td>16.0</td>
<td>10.0</td>
<td>20.0</td>
</tr>
<tr>
<td>SSN</td>
<td>16.0</td>
<td>11.0</td>
<td>22.0</td>
</tr>
<tr>
<td>DoB</td>
<td>13.0</td>
<td>7.0</td>
<td>12.0</td>
</tr>
<tr>
<td>Credit Card</td>
<td>10.0</td>
<td>8.0</td>
<td>16.0</td>
</tr>
<tr>
<td>Medical</td>
<td>9.0</td>
<td>4.0</td>
<td>7.0</td>
</tr>
<tr>
<td>Account</td>
<td>7.0</td>
<td>11.0</td>
<td>7.0</td>
</tr>
<tr>
<td>Financial</td>
<td>7.0</td>
<td>5.0</td>
<td>14.0</td>
</tr>
</tbody>
</table>

Table 2: Top data types lost in breaches reported in Q1 for the past three years
Who Has Been Breached?

What makes one organization more likely to experience a breach than another? Ask that question at any security conference and you will find no shortage of opinions on the topic. Some reasons are self evident: investing in security resources and baking strong controls into everyday processes go a long way toward reducing the likelihood of a breach. Other factors that might appear to be important at first glance, like meeting regulatory standards or contractual obligations, actually have little correlation with the likelihood of a breach occurring. Case in point is the healthcare industry. Healthcare providers have been subject to HIPAA's privacy and security rules since the summer of 1996, yet the sector is repeatedly at, or near, the top of economic sectors experiencing the most breaches.

Figure 7: Number of reported Q1 2020 breaches experienced according to economic sectors
Four economic sectors, Health Care, Information, Public Administration, and Financial Services accounted for 53.2% of the breach activity reported in Q1. Continuing a trend seen in prior quarters, software creators, websites, and hosting services make up the vast majority of breaches in the Information sector. The Information sector consists of eleven industry groups, three of which make up the software, website and hosting grouping. That means only 27.2% of the Information industry groups account for 88% of the breaches in the information sector.
Where Did Breaches Occur in 2020?

No industry is immune to the risk of a breach and no location is a breach-free zone. With 40% of the quarter’s breaches reported in the United States, it can be tempting to assume that the U.S. is the epicenter of data losses. Our research tells us that is not entirely the case. Rather, it is the strong disclosure requirements, coupled with the availability of such information, that explains the high number of reports in the U.S.

![Figure 9: Number of breaches by global location, reported in Q1 2020](image-url)
Does this mean that states with the strongest breach notification regulations will experience the most breaches? In short - no. Breach notification obligations are triggered when a person residing in the state is impacted by the event. As such, we can expect to see a correlation between the population in general and the number of breaches by state. Figure 10 shows breaches by state with California experiencing the most events at 60. New York, Texas, and Florida then follow behind with about 30 breach events.

*Figure 10: Map of the US, colored according to number of breaches experienced by state, reported in Q1 2020*
In Closing

Q1 breach reports are always interesting to assemble. Larger trends that will shape the year are generally present despite the narrow three month time period reviewed, yet it still allows a few quirks to bubble to the surface. We saw this effect in this quarter's report with the number of breaches reported. The large drop in disclosed breaches compared to Q1 2019 is due to the combination of a short term spike in breach reports in 2019 coupled with a short term decline in breach reporting in 2020. As the year goes on and more data is added to the analysis, we anticipate the effects of these brief fluctuations will moderate. Tune in to the mid-year report this July to see whether this prediction holds true, or if these quirks develop into larger trends that will further impact the year to come.

Methodology and Terms

Risk Based Security's research methods include automated processes coupled with traditional human research and analysis. Our proprietary applications crawl the Internet 24x7 to capture and aggregate potential data breaches for our researchers to analyze. In addition, the research team manually verifies news feeds, blogs, and other sources looking for new data breaches as well as new information on previously disclosed incidents.

The database also includes information obtained through Freedom of Information Act (FOIA) requests, seeking breach notification documentation from various state and federal agencies in the United States. The research team extends our heartfelt thanks to the individuals and agencies that assist with fulfilling our requests for information.

Data Standards and the Use of “Unknown”

In order for any data point to be associated with a breach entry, Risk Based Security requires a high degree of confidence in the accuracy of the information reported as well as the ability to reference a public source for the information. In short, the research team does not guess at the facts. For this reason, the term “Unknown” is used when the item cannot be verified in accordance with our data validation requirements. This can occur when the breached organization cannot be identified but leaked data is confirmed to be valid or when the breached organization is unwilling or unable to provide sufficient clarity to the data point.
About Risk Based Security

Risk Based Security (RBS) provides detailed information and analysis on Vulnerability Intelligence, Vendor Risk Ratings, and Data Breaches. Our products, Cyber Risk Analytics (CRA), VulnDB and YourCISO, provide organizations access to the most comprehensive threat intelligence knowledge bases available, including advanced search capabilities, access to raw data via API, and email alerting to assist organizations in taking the right actions in a timely manner.

For more information, visit www.riskbasedsecurity.com or call +1 855-RBS-RISK.

About Cyber Risk Analytics

Cyber Risk Analytics (CRA) provides actionable threat intelligence about organizations that have experienced a data breach or leaked credentials.

Along with our PreBreach Risk Ratings, this provides a deep dive into the metrics driving cyber exposures, as well as understanding the digital hygiene of an organization and predicting the likelihood of a future data breach.

The integration of PreBreach ratings into security and underwriting processes, vendor management programs, and risk management tools allows organizations to avoid costly risk assessments, while enabling businesses to act quickly and appropriately to proactively protect its most critical information assets.

REQUEST A DEMO
sales@riskbasedsecurity.com

LEARN MORE
www.cyberriskanalytics.com

NO WARRANTY

Risk Based Security, Inc. makes this report available on an “As-is” basis and offers no warranty as to its accuracy, completeness or that it includes all the latest data breaches. The information contained in this report is general in nature and should not be used to address specific security issues. Opinions and conclusions presented reflect judgment at the time of publication and are subject to change without notice. Any use of the information contained in this report is solely at the risk of the user. Risk Based Security, Inc. assumes no responsibility for errors, omissions, or damages resulting from the use of or reliance on the information herein. If you have specific security concerns please contact Risk Based Security, Inc. for more detailed data loss analysis and security consulting services.

*Figure 10 of this report was generated using mapchart.net®