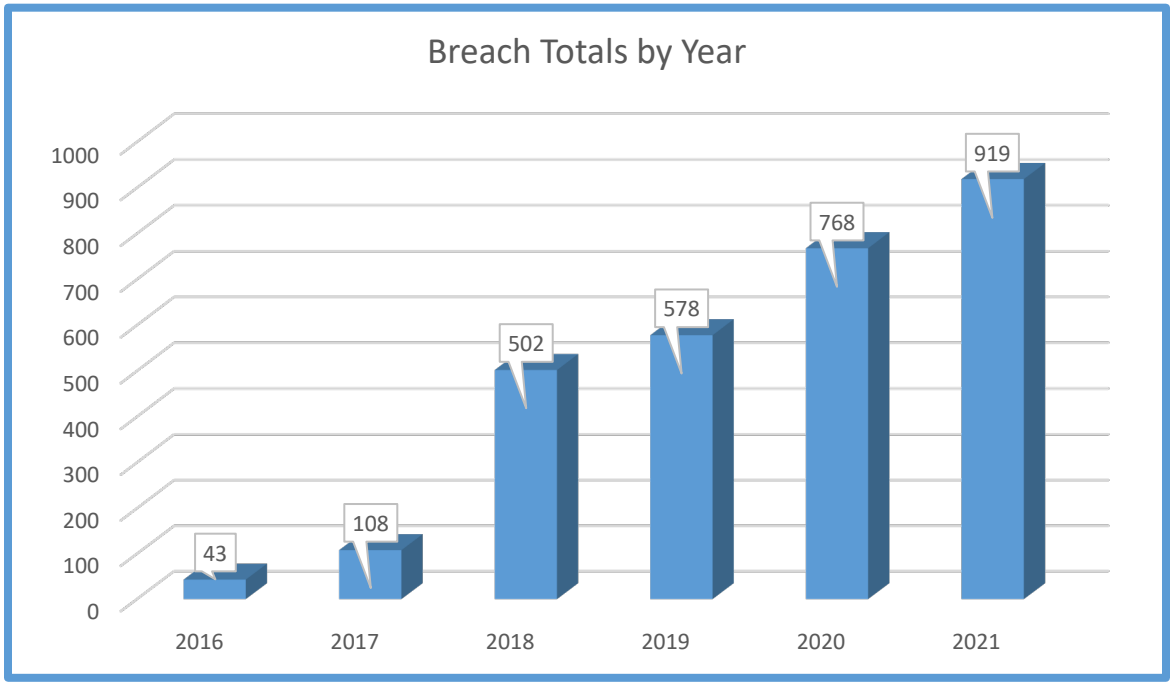
Fourth Annual Report on Cybersecurity in Nebraska

For the last four years, Baird Holm has studied, analyzed, and created a summary of the data breach notifications reported to the Nebraska Attorney General's office. The summary analysis includes information, numbers, and statistics derived from the information in the notifications reported from 2016 to the present, with an emphasis on 2021. Additionally, the report takes a deeper look at the types of attacks, businesses victimized, types of information stolen, estimated costs to respond to a breach, and an analysis of the correlation between the time to discover and the number of breached records.

This report aims to help all businesses plan for the consequences and expenses of a cyber-attack, present examples from past events and case studies, and provide warnings about the types and methods of future attacks.

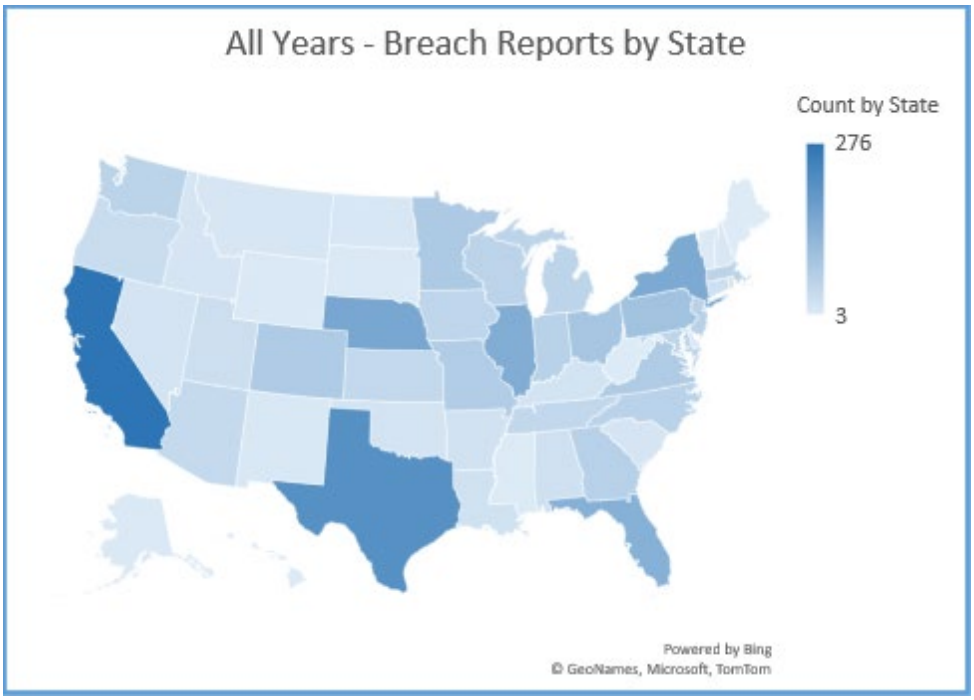
Number of Breaches Reported Affecting Nebraskans

The number of cyber breaches across the United States ("U.S.") continues to rise each year, and this rise is reflected in the Nebraska data as well. Cyber-breaches are also expected to continue to increase in the foreseeable future. The percentage increase had slowed from prior years. In 2021 we saw the year-over-year percentage decline from 27% in 2020 to 16% in 2021.



Company Location

The data collected by the Attorney General's office allows analysis of which states are home to the most companies who report cyber-breaches.



By 2021, companies located in all fifty (50) states and the District of Columbia reported at least one (1) breach to the Nebraska Attorney General. Of those states, all but nine (9) reported at least double-digit breaches and six (6) reported triple-digit breaches. California led the count with 276, followed by Texas with 212 total breaches reported. Nebraska-based companies reported 160 breaches. Just behind Nebraska were the states of New York, Illinois, and Florida.

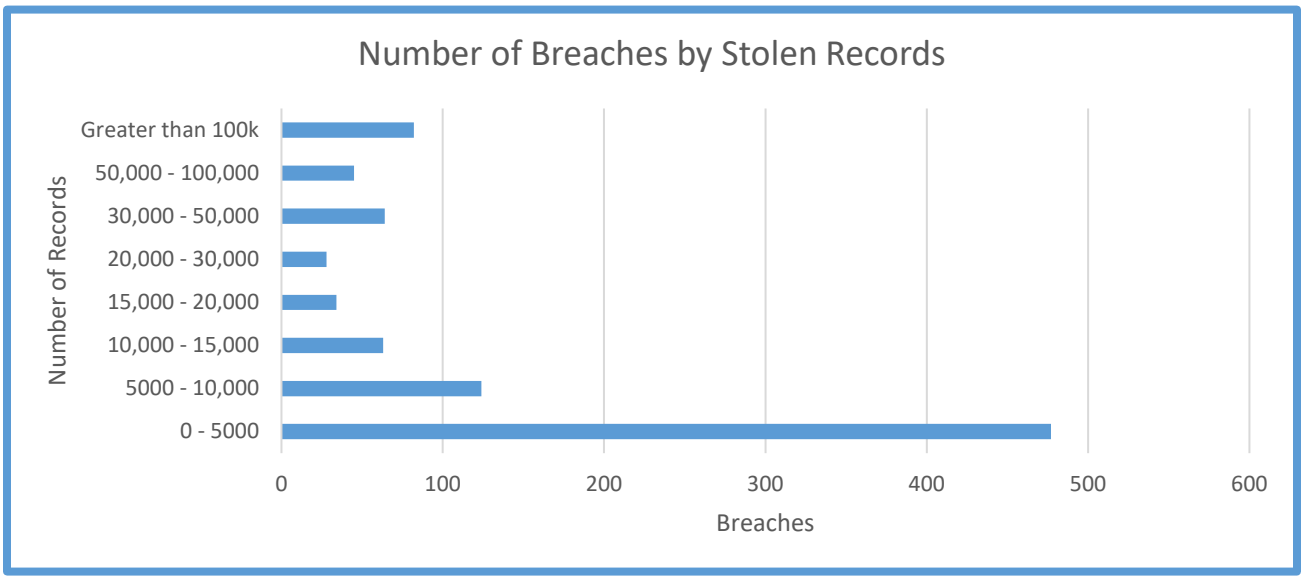
Company Size Analysis

When contrasted with the rise in the total number of breaches, a drop in total U.S. records suggests that cyber-attacks victimize small and medium-sized companies with smaller data sets. In comparison, larger companies with larger data sets protect their data better.

This past year's breaches did not include any breaches involving over 100M records but included twenty (20) breaches reporting more than 1M records affected. These twenty (20) breaches alone accounted for fifty-six million (68%) of the eighty-two million records stolen in 2021. While larger companies are becoming much more vigilant in protecting data, they are still susceptible to breaches of large data sets. Organizations responsible for these twenty (20) breaches were: General Business – 9; Financial and Insurance Services – 4; Healthcare – 4; and Other – 3.

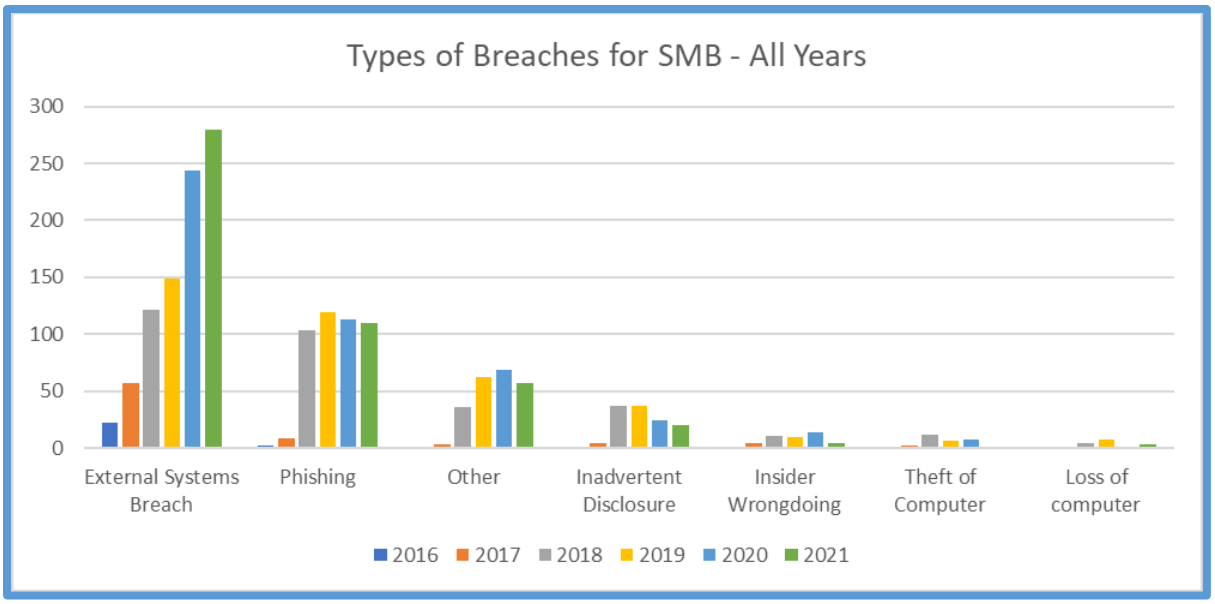
An important point to make while reviewing the size of breaches, attackers often do not know the amount or type of information maintained by a company or the size of a company or its network until they gain access. Many small or medium-sized businesses ("SMB") are reluctant to spend money on cyber-security because they believe their network does not have any data worth stealing.

The risk to SMBs is evident when reviewing the data breaches by size. The majority of data breaches were of companies that only maintained fewer than 5,000 records:



Cyber-attackers are targeting companies based on system vulnerabilities. An Exchange server vulnerability is a vulnerability whether it exists as part of a Fortune 500 company's network or a single-member LLC's network. SMBs tend to have smaller Information Security (InfoSec) and IT staff. The fewer the staff, the harder it becomes to keep up with zero-day and other vulnerabilities and patches. And this past year has seen a number of vulnerabilities that have affected SMBs, such as the MS Exchange zero-days announced in March 2021.[1] These vulnerabilities affected on-prem Exchange servers, something most likely used by SMBs and less likely used by Fortune 500 firms.

[1] These zero-days include CVE-2021-26855, 26857, 27065, and 26858.

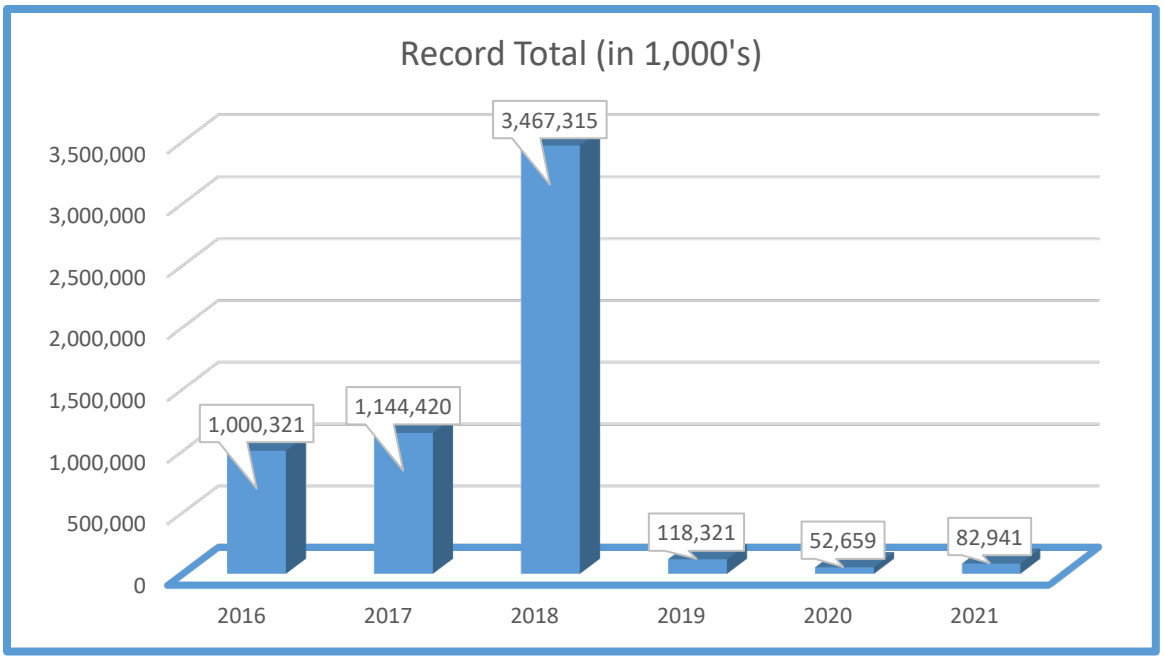


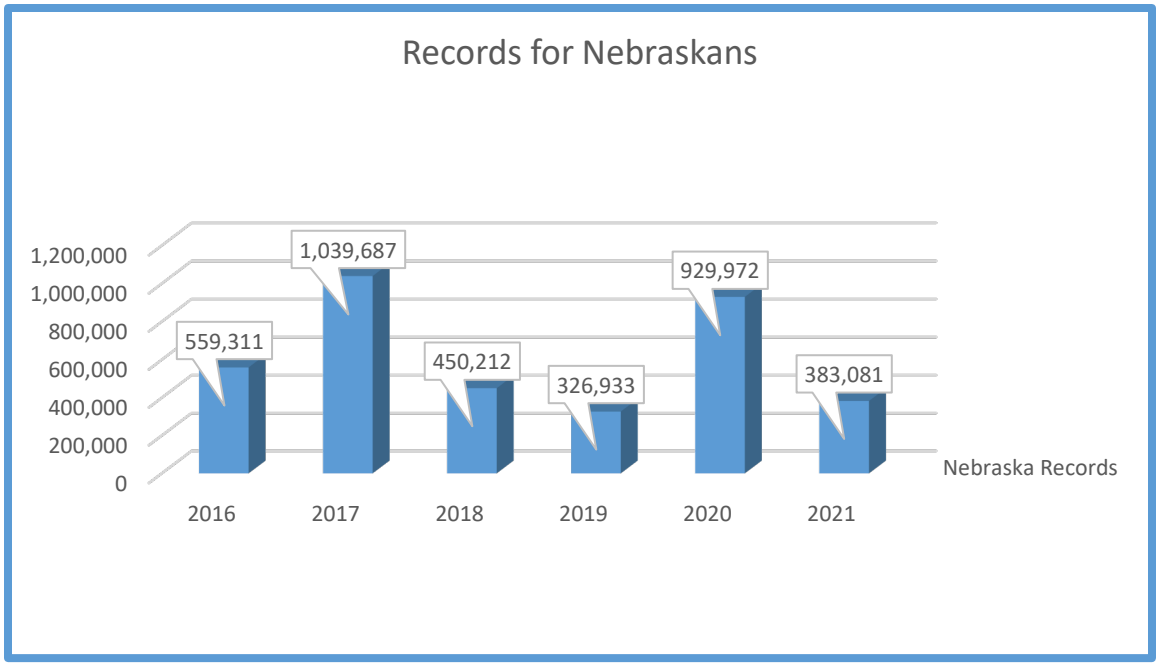
All businesses, and especially SMBs with limited staff, time, and budgets, need to take precautions to protect their network and company.

Resident / Victim Analysis

The Nebraska breach notification form requires submitters to report not only the number of Nebraska residents affected by the breach, but also, the total number of U.S. residents affected by the breach. This information presents a national view of the types of information being taken, types of breaches, types of companies victimized by cyber-attackers, and the number of records per incident.

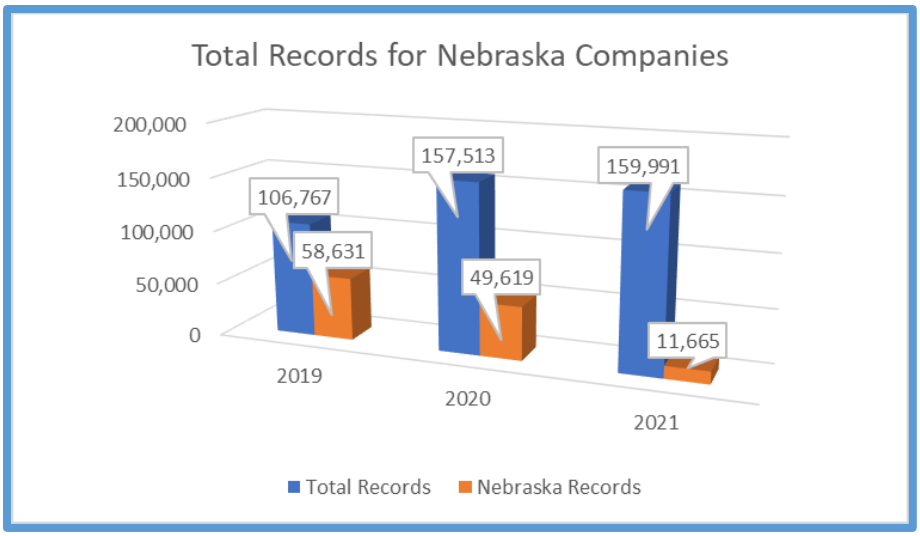
Below are charts which represent the total number of U.S. residents affected by the reported breaches, and the number of affected Nebraska residents.



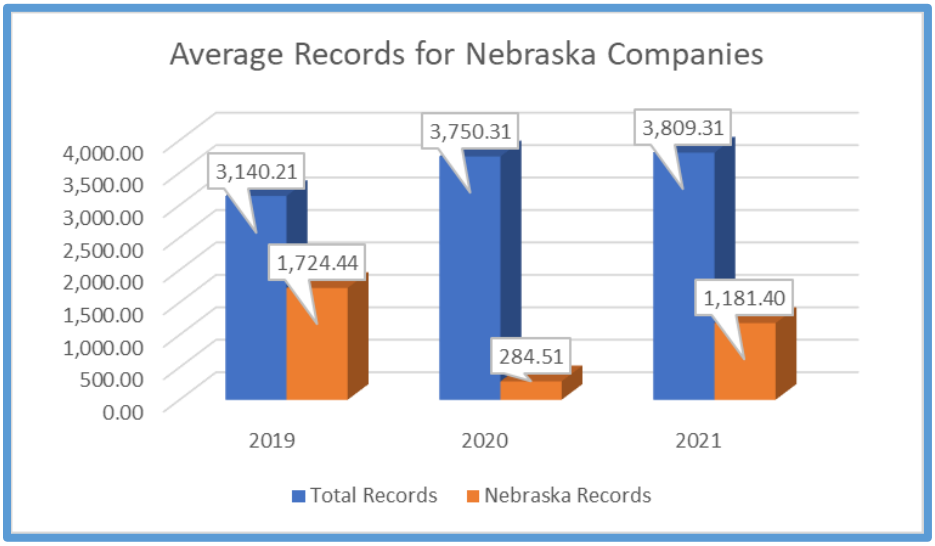


In 2021, the total number of affected Nebraska residents declined from the previous year, while the number of total U.S. residents jumped to 82 million records.

Nebraska-based companies reported a total number of U.S. residents affected equal to 157,513 in 2020 and 159,991 in 2021, while the number associated with Nebraska residents decreased from 49,619 to 11,665, respectively.



The average number of records per breach are as follows:



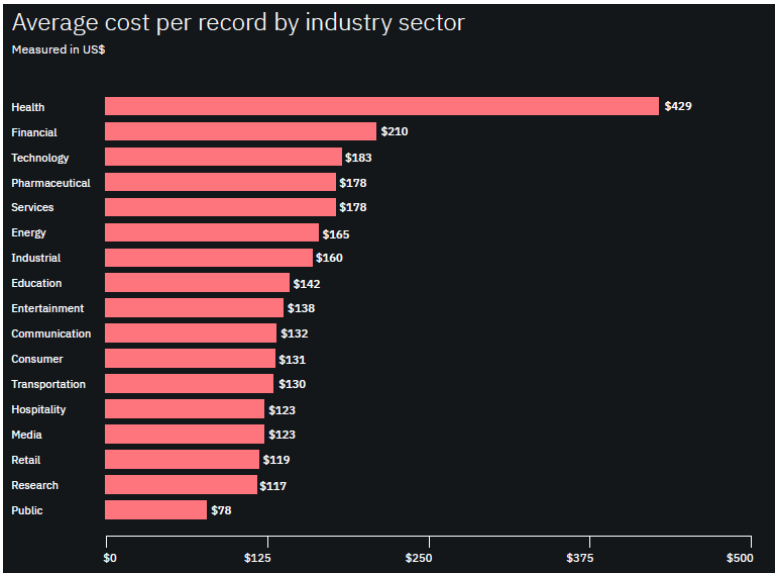
The average number of total records reported for Nebraska based companies is 3,140 in 2019, which rose to 3,750 in 2020 and 3,809 in 2021. These averages can be used for determining average costs for breach recovery restoration services and total company risk.

Per-Record Costs and Estimating Response and Recovery Costs

Several studies have attempted to define a methodology to determine per-record cost ("PRC") for response and recovery from a data breach. Such a methodology, if based on sound research and reasoning, can provide companies with a means to estimate costs and create financial plans to respond to cyber-security breaches. Two of the more comprehensive and widely cited studies are discussed below.

IBM and the Ponemon Institute Study

IBM and the Ponemon Institute ("IBM Study") publish an annual report reviewing yearly breach response costs and contributing factors in recovery expenses. In the IBM Study, the average costs to respond and recover from a data breach were approximately $150 PRC globally and approximately $205 PRC in the United States.[2] The study also determined the costs for response and recovery by industry as follows:



It should be noted, however, that these figures are *very rough* estimates, and caution should be taken when using these figures for an "across-the-board" analysis. The PRC can vary greatly depending on the size of an organization; the location of the company and the network; whether or not the recovery is outsourced; if outside counsel is retained; the complexity of the system; the number of users, computers, and networks; and many other factors.

The best method to determine the cost and time for restoration and recovery expenses is to conduct a tabletop exercise. Such an exercise will estimate the upper limits of data breach expenses a company may face. The exercise will aid in determining the time and expense involved in a complete system restoration and the costs to notify all individuals whose records would be involved in a complete system breach.

Nebraska based companies suffer breaches in the range from 1 to approximately 100,000[3] records. Using the IBM study, Nebraska based companies can calculate a

---

[2] See Cost of a Data Breach, IBM and the Ponemon Institute, pg. 27 (https://www.ibm.com/security/services?p1=Search&p4=43700056097600187&p5=b&gclid=EAIaIQobChMIpsTP4Or07wIVdP_jBx1L3A7YEAAYASAAEgKOdvD_BwE&gclsrc=aw.ds last visited on April 10, 2021).

[3] 40 out of 43 reported breaches had between 1 and 4,000 records. The remaining three breaches were over 10,000 records. The average of 3,750 per breach exclude one anomalous entry of 2.6M records for one breach. Including this one breach skews the range and the average, while every other breach is under 1M records and the amount appears to be an estimate and/or rounded for reporting purposes.

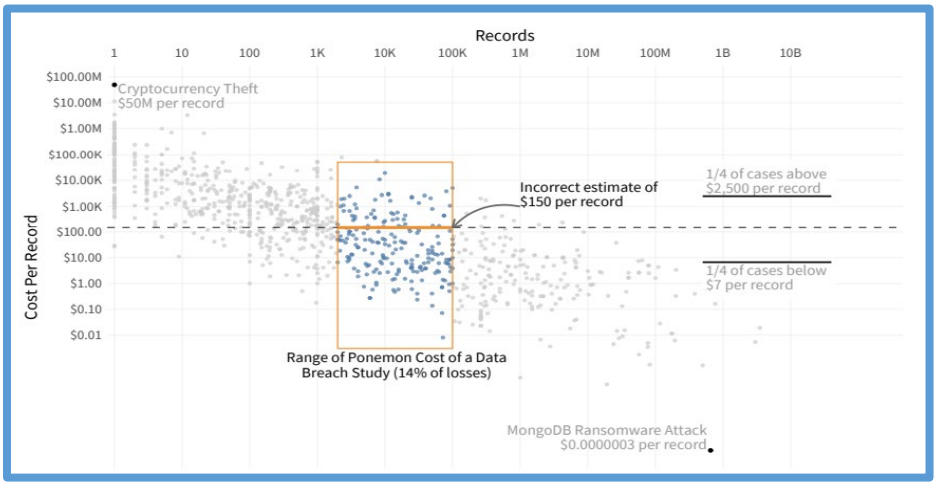
very general breach-cost analysis. Using the figures from the IBM Study, and with all other factors being equal, a Nebraska based company can estimate that they will spend approximately $768,750 (3,750 x $205) for the response and recovery costs due to a data breach.

Cyentia Institute Study

The Cyentia Institute ("Cyentia") noted that individual PRC may vary during the course of incident response depending on the size and scope of the breach. Thus, an across-the-board approach used by IBM may not be accurate.

Cyentia noted that the PRC would be higher than average in the initial investigative stages. In contrast, the PRC costs towards the later stages of an investigation will be much lower than average. For example, the initial response costs would be similar whether a company has 100 records or 1000 records. The initial response steps would be similar, such as wiping and restoring workstations and servers, initiating the response team, retaining outside counsel, hiring a computer forensics firm, etc. But, after the initial expenditures become sunk costs, the PRC costs of additional records identified and recovered will decline over time.

This disparity in the PRC motivated Cyentia to analyze the PRC based on breach size and company size to provide an alternative to the across-the-board approach used in the IBM Study. The below graph from this report depicts how the PRC of additional records decreases as a data breach increases in size. The graph also illustrates the small range of cases to which the IBM Study is restricted and the inherent inaccuracies of such a small sample size. [4]



With a larger sample size than the IBM Study, Cyentia also created a probability analysis of the total costs based on the size of the breach suffered. That probability analysis is depicted as follows:

[4] Information Risk Insights Study Cyentia Institute, pg. 18 (https://www.cyentia.com/wp-content/uploads/IRIS2020_cyentia.pdf last visited March 16, 2021).

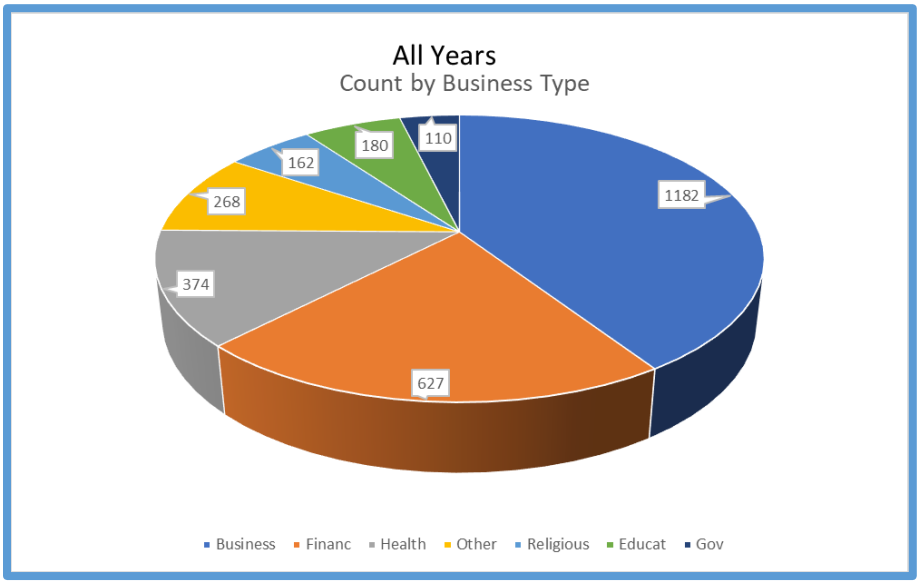
Records	Probability of At Least This Much Loss					
	$10K	$100K	$1M	$10M	$100M	$1B
100	82.0%	49.9%	17.8%	3.3%	0.3%	0.0%
1K	88.4%	60.9%	26.0%	5.9%	0.7%	0.0%
10K	93.0%	71.1%	35.8%	10.0%	1.4%	0.1%
100K	96.0%	79.8%	46.7%	15.8%	2.7%	0.2%
1M	97.9%	86.7%	57.7%	23.5%	5.0%	0.5%
10M	99.0%	91.8%	68.2%	32.8%	8.6%	1.1%
100M	99.5%	95.3%	77.4%	43.4%	13.9%	2.3%
1B	99.8%	97.4%	84.9%	54.5%	21.0%	4.2%
10B	99.9%	98.7%	90.5%	65.3%	30.0%	7.4%

Using this information to extrapolate probabilities and costs to Nebraska-based companies' average of 3,809 records breached did not materially change the conclusions from last year. An average company has an 89.8% chance of incurring at least 10K in fees, 64.1% chance of incurring at least $100K in fees, and 29.1% chance of incurring at least $1M in expenses, etc.[5] Thus, the combined total loss expected across all probabilities is $461,891[6].

[5] This extrapolated figures were calculated using a weighted average based on the percentages provided by Cyentia for probabilities at 1K and 10K records in a breach.
[6] This figure is within two standard deviations of the mean and thus accurate to 95% of the expected loss.

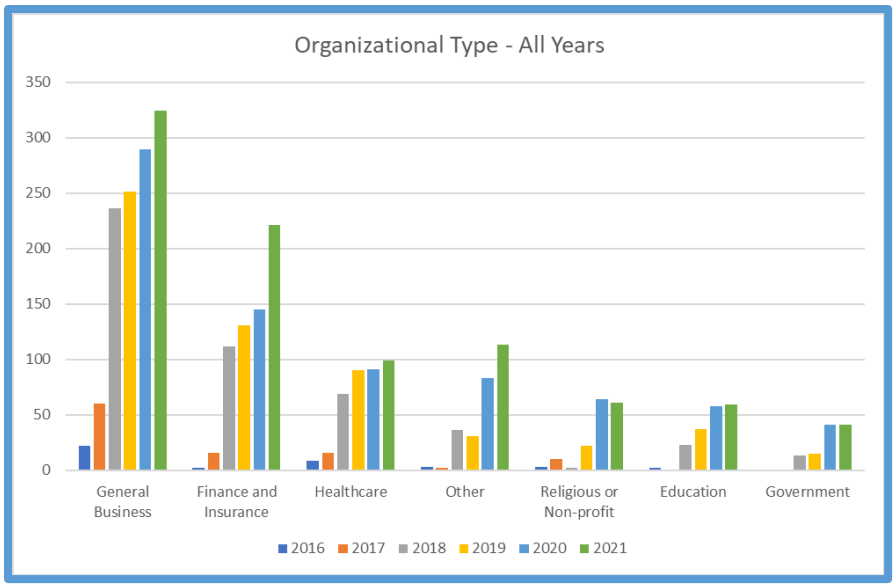
Business Types Victimized

The types of businesses victimized by a cyber-attack range from small local businesses to international companies. The types of businesses reporting cyber-attacks are as follows:



The largest organizational type is “General Business,” which includes retail, online retail, Internet services, construction firms, accounting firms, trucking companies, hotels, and more. The type “Financial” includes banks, insurance companies, wealth advisors, mortgage companies, and other financial institutions. As a group, general business, financial, and healthcare organizations account for over 75% of all attacks. The obvious reasons for the attacks are the value and number of data points that can be gathered from attacks on such an organization. Such organizations have large caches of names, Social Security numbers, credit card or other financial account numbers, and healthcare information.

In relation to each other, the proportion of businesses have remained relatively similar throughout the years. The following graph depicts the year-over-year changes for each of the business types:

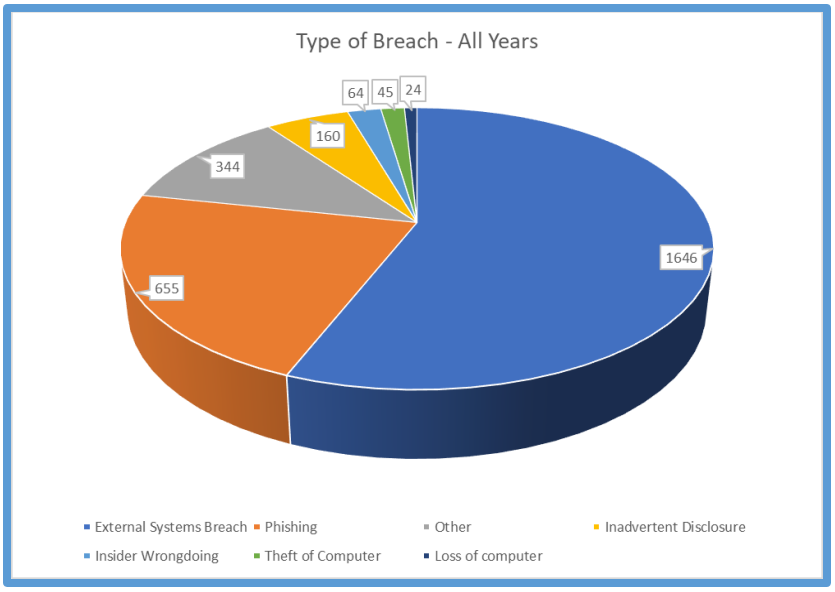


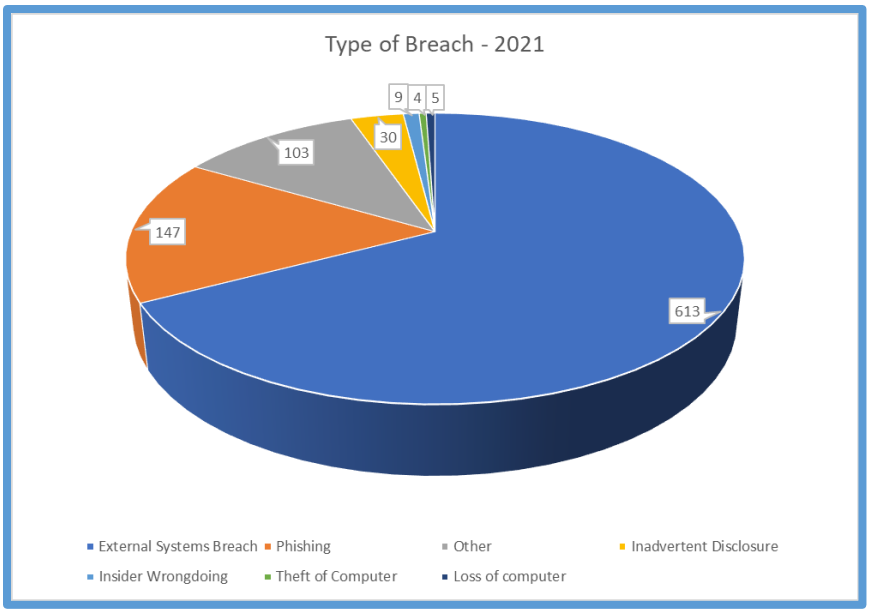
While the General Business category continues to dominate as the most targeted business, there have been substantial relative increases in the “Finance and Insurance” category over the past two (2) years.

Types of Breaches

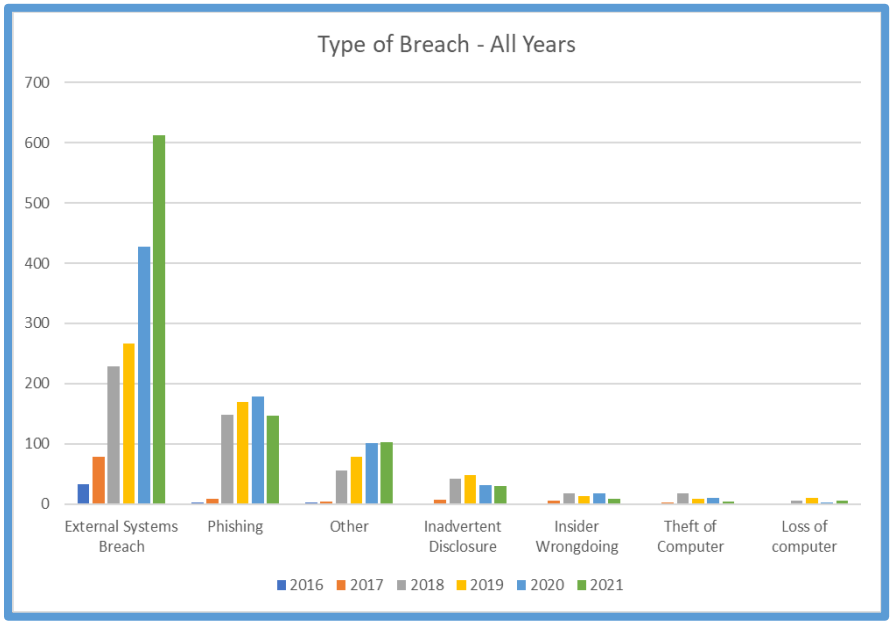
In reviewing the data one the most interesting areas of study is the type of breach used by hackers. Knowing the most common types of attacks can help companies conduct risk assessments of their organization, network, or Internet-facing services to determine which attack vectors are being used.

The following graph presents the types of breaches reported during 2021 and that the most common attacks are still external attacks and phishing attacks.





Below is a year-over-year comparison by breach type:



External attacks include direct attacks on company web servers (Log4J) and email servers (MS Exchange exploit) and against third-party vendors such as credit card skimming software and cross-site scripting attacks.

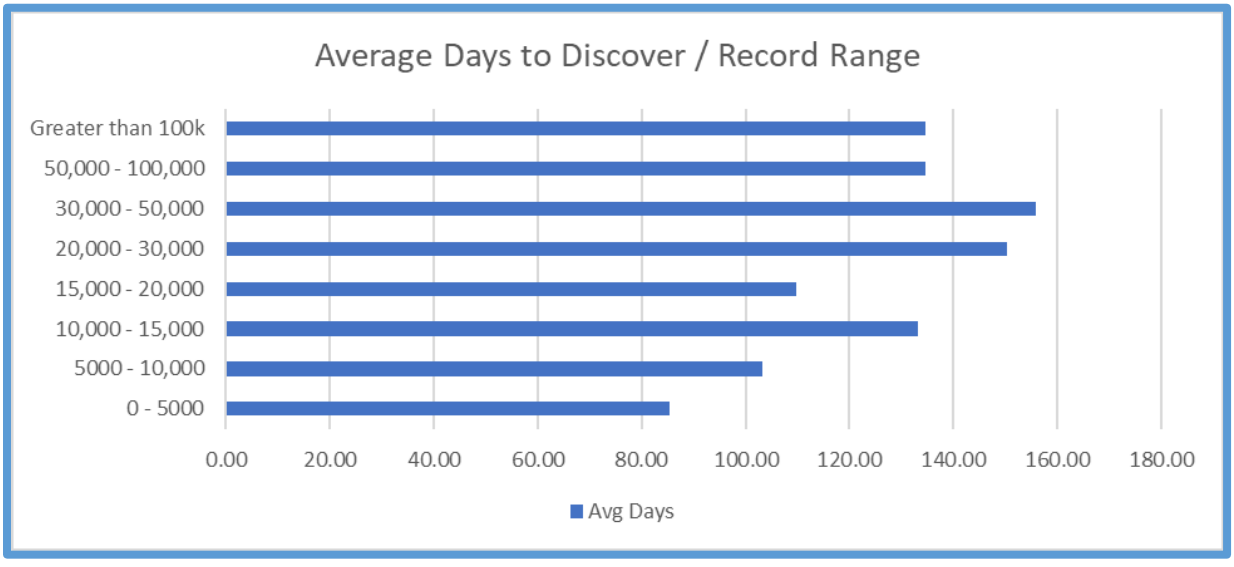
There are several reports in which phishing attacks were categorized as external attacks and several more reports whose description indicates that phishing attacks may have been used as an attack vector. Because of this, the number of phishing attacks may be under-reported as it is an attack vector used to launch additional direct attacks and an attack mechanism against email and RDP services.

It is worth noting that many of these attacks targeted third-party vendors who have been engaged to conduct or process payment transactions on behalf of the reporting company. Attacks on third-party vendors should serve as a warning to all companies, particularly SMBs, that an attack on a third-party vendor may require reporting and notifications by SMB itself. Third-party vendors often limit their duties and responsibilities in the case of a cyber-attack to the notification of the contracting company. Contracts and Managed Service Agreements require careful legal review to determine notification responsibilities.

Number of Days to Discover

Finally, an additional analysis was undertaken this past year to determine the relationship between the days to identify a breach as compared to the number of records affected in the breach. There are several studies that purport to show that there is a direct relationship between the time an attacker is in a system and the recovery costs. This relationship between attacker time on the network and recovery costs can be studied by reviewing the relationship between time to detection and records compromised.

After slicing the size of the total records into ranges, there is a direct correlation between the time it takes to discover a breach and the number of records breached. This relationship between time and the number of records is logical and intuitive. The longer an attacker can access a system, the more data the attacker can identify, access, view, and acquire/steal.



This data should be a warning that attackers are often in a network for several weeks and months prior to discovery.

Conclusions

Nebraska residents and Nebraska-based companies continue to face threats from cyber-attacks. Although the number of breaches continues to rise, the number of records affected by such breaches has decreased. The indirect correlation between the two trends suggests that threat actors target small and medium-sized businesses.

The average number of records involved in a data breach for a Nebraska-based company is 3,750. It translates to an average of $768,750 using the IBM Study or $461,891 using the Cyentia study. These response and recovery costs include restoration expenses, cyber-breach coaching, investigation and report fees, and notification and monitoring expenses.

Phishing and external attacks continue to lead the types of attack vectors used to perpetrate data attacks. These attacks target companies of all sizes and types. Attackers often attempt to breach a company without knowing the amount or types of information gathered from such an attack, and thus all companies are targets.

The longer an attacker is in your system, the more data and information is subject to being accessed and exfiltrated, making recovery costs even more expensive. Companies should monitor their networks early and often to find indicators of compromise before attackers export data.

Robert L. Kardell (Bob) is an attorney whose practice focuses on cyber-breach incident response, legal and technology-based risk management solutions, technology and cyber-defense policy and protections, intrusion remediation, and fraud prevention and investigation. Bob has more than twenty-two (22) years of experience working for the Federal Bureau of Investigation as a Special Agent and Supervisory Special Agent.

Published by

Cyber Law & Security Group

Baird Holm, LLP
1700 Farnam Street
Suite 1500
Omaha, NE 68102-2068
www.bairdholm.com

402.636.8313 Direct Dial Phone
402.344.0588 Fax
bkardell@bairdholm.com

BAIRD HOLM LLP
ATTORNEYS AT LAW

DOCS/2769339.7