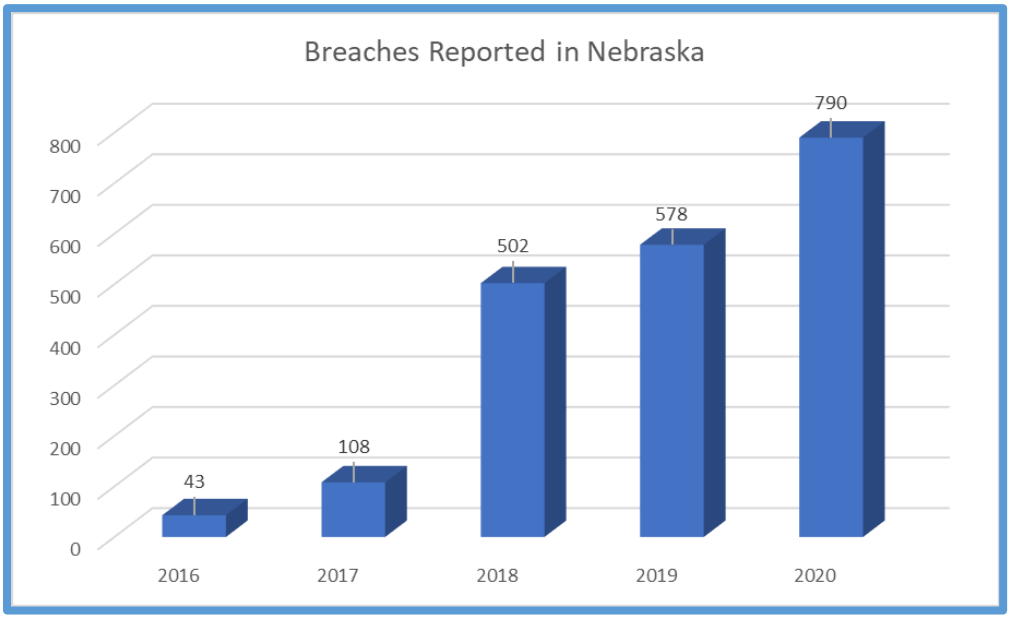
THIRD ANNUAL REPORT ON CYBERSECURITY IN NEBRASKA

For the last three years Baird Holm has studied, analyzed and created a summary of the Data Breach Notifications as reported to the Nebraska Attorney General's office. The summary includes analyses of the information, numbers and statistics derived from the information in the notifications reported during 2020 as well as all prior years. Additionally, the summary takes a deeper look at the types of attacks, businesses victimized, types of information stolen, estimated costs to responds to a breach and includes a new analysis of the correlation between the time to discovery and the number of breached records.

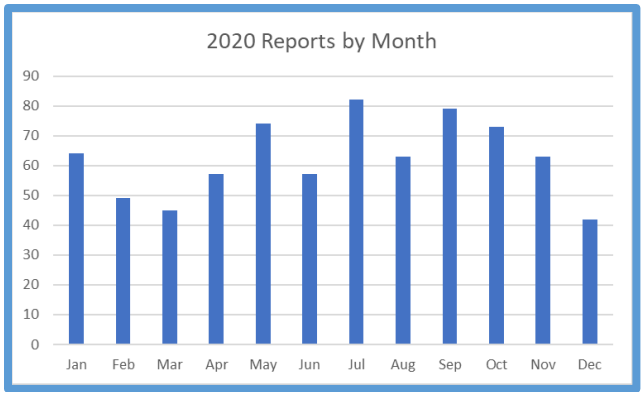
The goal of this report is to help all businesses plan for the consequences of a cyber-attack, to present examples from past events and case studies, and to provide warnings about types and methods of future attacks. All companies need to take steps to protect their data; cyber-attacks are more than just an IT risk, cyber-security is a business risk!

NUMBER OF BREACHES REPORTED

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 for the foreseeable future. Many reports attribute a portion of this year's increase in cyber-attacks as a result of an increase in remote workers due to COVID-19 and the global pandemic. Remote workers have always posed a higher risk because they are outside of the security of workplace firewalls and network monitoring, but the pandemic has exacerbated the issue. Therefore, it was not surprising to see a larger percentage increase in the number of breaches reported from the year before. The percentage increase had slowed in prior years, but in 2020 we saw the percentage increase to 27%.



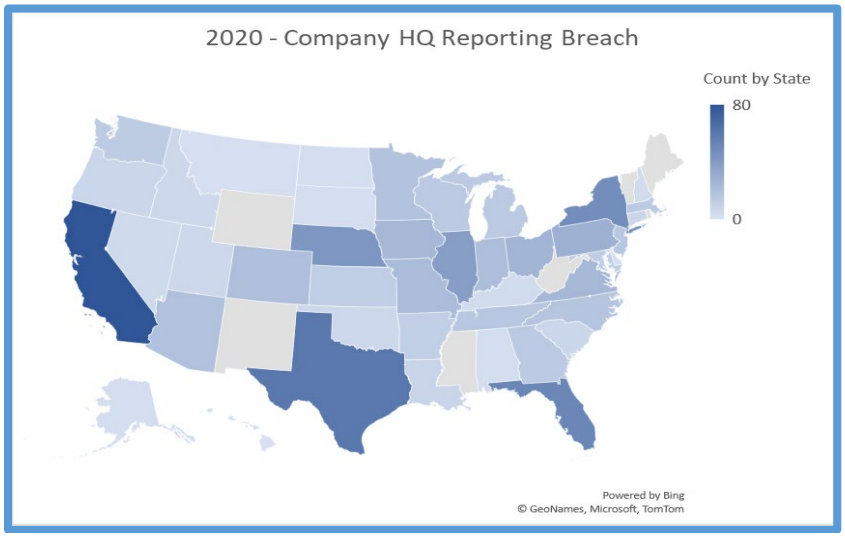
The COVID-19 pandemic forced employees to begin working remotely in March of 2020. To determine if the pandemic caused any increase in the number of cyber-breaches, an analysis was prepared to count and graph the number of reports per month during 2020.



The graph appears to show that after March there was an uptick in the number of breaches reported, but these numbers then decreased towards the end of the year. Thus, the pandemic appears to have had an immediate impact on cyber-breaches, but the threat appears to have waned towards the end of 2020. The downward trend could be a sign that companies employed additional precautions for home-based employees and/or that companies now have cyber-risks of remote employees under control.

COMPANY LOCATION

The data also elicits an analysis as to which companies in which states report the most breaches.

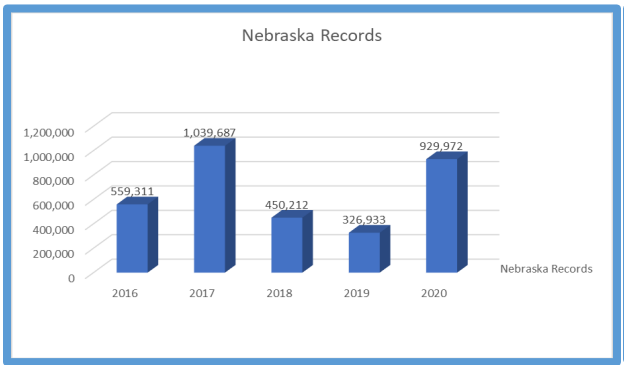


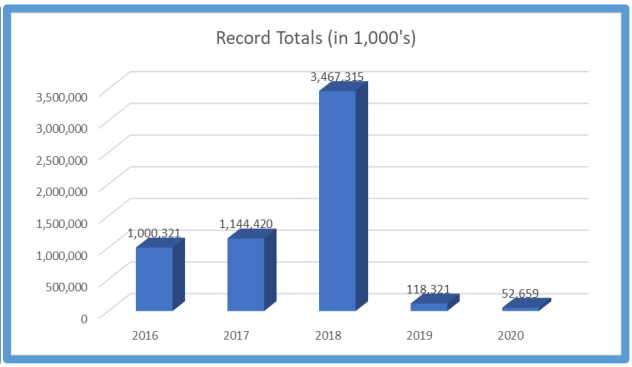
In 2020, companies located in 45 different states and the District of Columbia reported at least one breach to the Nebraska Attorney General. Of those states, 26 reported double-digit breaches. California led the count with 80 total breaches while Nebraska-based companies only reported 43 breaches. Nebraska-based companies had the fifth highest total for reporting to the Nebraska Attorney General, behind California, Texas, Florida and New York.

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. When reviewing this information a national view emerges of the types of information being taken, the types of breaches, the types of companies victimized by cyber-attackers, and the number of records per incident.

Below are graphs of the number of Nebraska residents affected each year and the total number of U.S. residents affected.



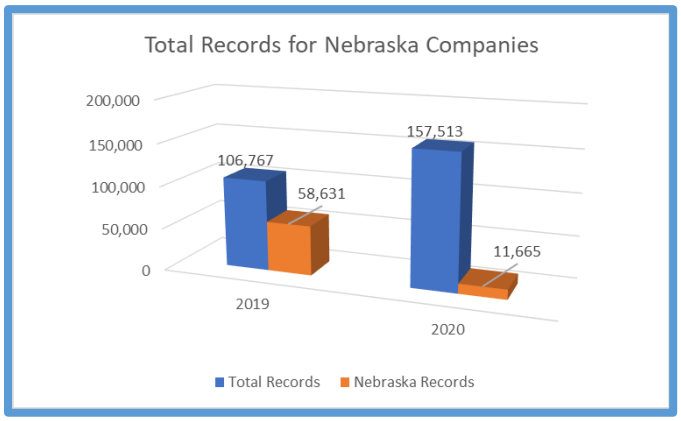


The total number of affected Nebraska residents had been declining in the previous two years, but in 2020 the number of Nebraska residents rose substantially while the number of total U.S. residents continues to drop. The drop in total U.S. records when contrasted with the rise in the total number of breaches suggests that small and medium sized companies with smaller data sets are being victimized by cyber-attacks while larger companies with larger data sets are protecting their data better. This year's breaches also did not include any breaches involving over 100M records and only 8 breaches reporting more than 1M records affected.

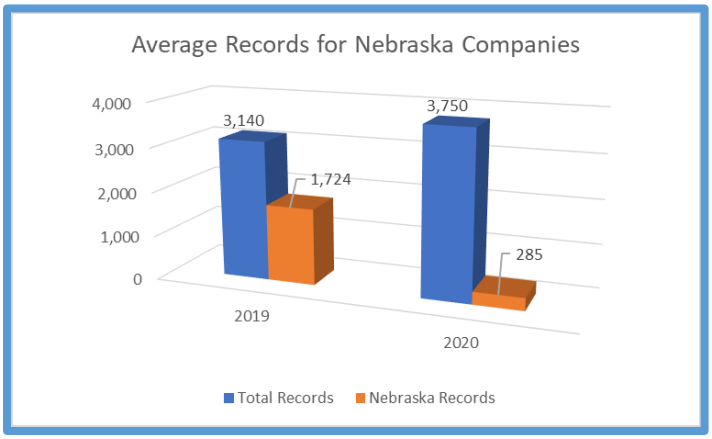
An important point to make while reviewing the size of a breaches, attackers often do not know the amount or type of information maintained on a network or the size of a company or its network until they gain access. Many small or medium-sized businesses ("SMB") are reluctant to spend money on cyber-security because they believe their network does not have any data worth stealing. But, cyber-attackers are not only targeting companies based on size or number of records, but rather the attackers are targeting 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. Thus, all businesses, and especially SMBs, need to take precautions to protect their network and company.

Another way of slicing the breach records data is to focus the review on Nebraska-based companies. In 2019 and 2020 Nebraska-based companies reported a total number of U.S. residents affected equal to 106,767 in 2019 and 157,513 in 2020 while the number associated with Nebraska residents decreased from 58,631 to 11,665, respectively.



When converted to averages the numbers 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. These averages can be used for determining average costs for breach recovery restoration services and also to determine total company risk.

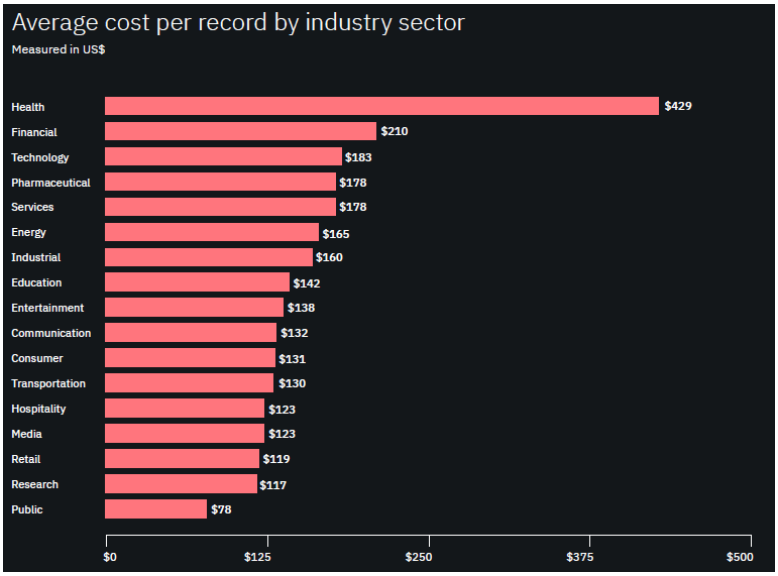
PER-RECORD COSTS AND ESTIMATING RESPONSE AND RECOVERY COSTS

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.[1] The study also determined the costs for response and recovery by industry as follows:



It should be noted, however, that these figures are only *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, among many other factors. A good method for an individual company to determine its own restoration and recovery expenses is to conduct a table-top exercise and determine the time and expense involved in a complete system restoration, as well as the costs to notify all individuals whose records would be involved in a complete system breach. Such an exercise will provide an estimate as to the upper-limits of data breach expenses a company may face.

Nebraska-based companies suffer breaches in the range from 1 to approximately 100,000[2] records lost which is very similar to the size range of the breaches used in the IBM Study. Thus,

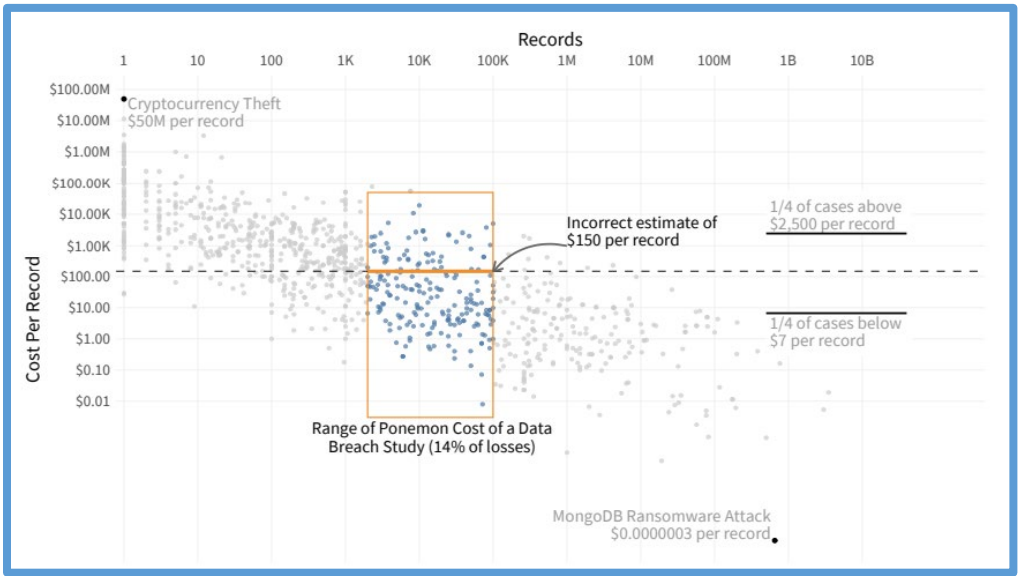
[1] See Cost of a Data Breach, IBM and the Ponemon Institute, pg. 27 (https://www.ibm.com/security/services?p1=Search&p4=43700056097600187&p5=b&gclid=EAIaIQobChMIpsTP4Or07wIVdP_jBx1L3A7YEAAYASAAEgKOdvD_BwE&gclsrc=aw.ds last visited on April 10, 2021).
[2] 40 out of 43 reported breaches had between 1 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

we can generally use the IBM Study figures due to the similarity in breach sizes. 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

During the course of restoration and recovery the PRC may vary as well. In the initial investigative stages the PRC will be higher than average while the PRC costs towards the later stages of an investigation will be much lower than average. For example, whether a company has 100 records or 100,000 records the initial response costs will be similar and include steps such as restoration from backup if possible, 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 will be relatively less expensive.

This disparity in the PRC motivated the Cyentia Institute ("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 as a data breach increases in size the PRC of additional records decreases. The graph also depicts the small range of cases to which the IBM Study is restricted and the inherent inaccuracies of such a small sample size.[3]



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.

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

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:

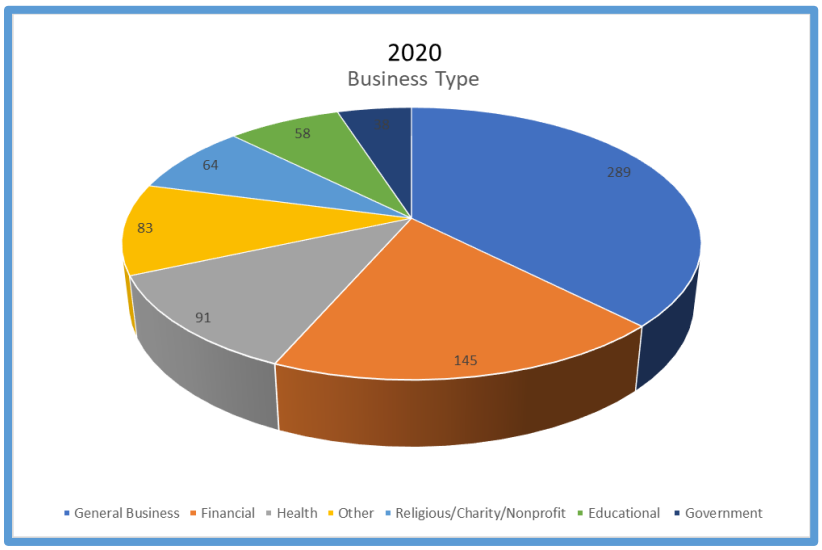
Records	Probability of At Least This Much Loss					
	$10K	$100K	$1M	$10M	$100M	$1B
100	82.0%	49.9%	17.8%	3.3%	0.3%	0.0%
1K	88.4%	60.9%	26.0%	5.9%	0.7%	0.0%
10K	93.0%	71.1%	35.8%	10.0%	1.4%	0.1%
100K	96.0%	79.8%	46.7%	15.8%	2.7%	0.2%
1M	97.9%	86.7%	57.7%	23.5%	5.0%	0.5%
10M	99.0%	91.8%	68.2%	32.8%	8.6%	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 3,750 records breached, it can be estimated that on average a company has an 89% chance of incurring at least 10k in fees, 64% chance of incurring at least $100k in fees, and has a 29% chance of incurring at least $1M in expenses.[4] The combined expected loss is then $362,970 per breach[5].

BUSINESS TYPES VICTIMIZED

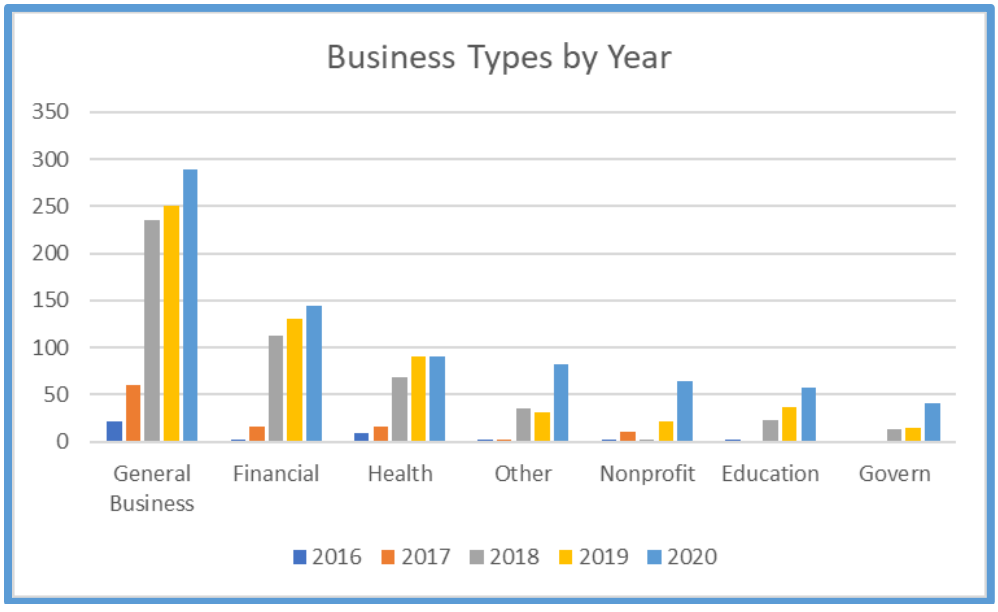
The types of businesses victimized by a cyber-attack range from small local businesses to international companies. The types of businesses reporting cyber-attacks are as follows:

[4] 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.
[5] This expectation is with 99% probability and excluding a .9% probability of incurring $100M in fees at the high end of the probability scale.



The largest organizational type is “General Business” which includes retail, online retail, Internet services, construction firms, law firms, accounting firms, and more. The type “Financial” includes banks, insurance companies, wealth advisors, and could include Certified Public Accountant (“CPA”) firms. The vast majority of the attacks have been on general business, financial, and healthcare organizations. The obvious reasons for the attacks are the value and number of data points that can be gathered from an attack on such an organization. Such organizations have large caches of names, Social Security numbers, credit card or other financial account numbers, and healthcare information.

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

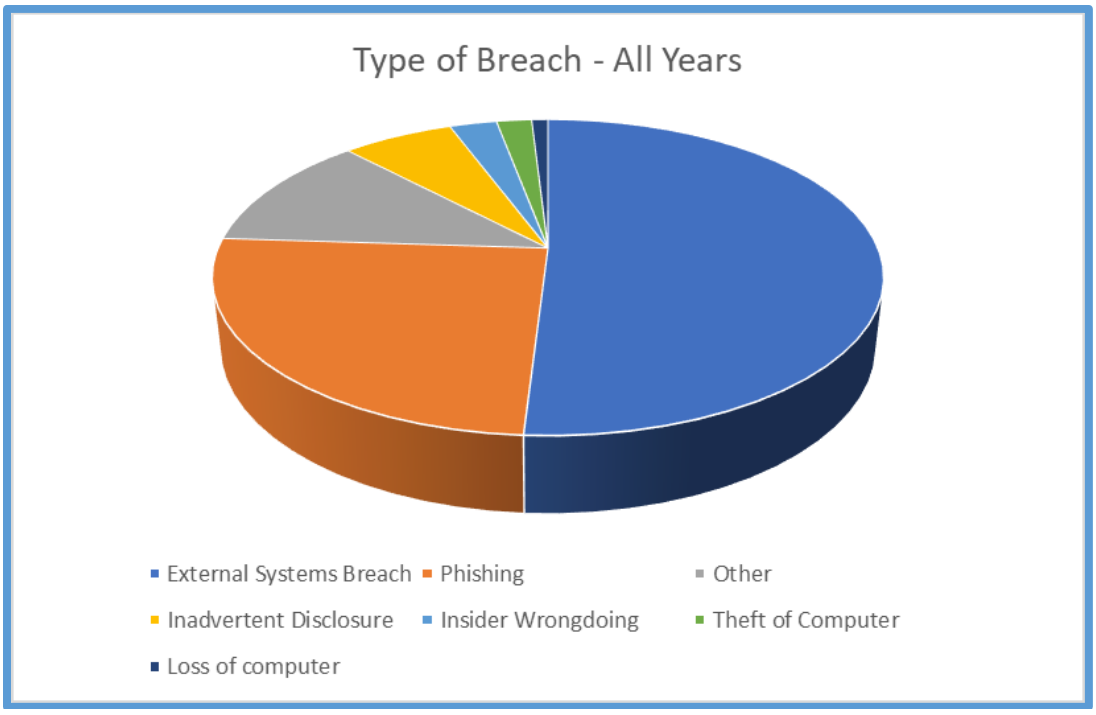


While the General Business category continues to dominate the other categories, there have been substantial relative increases in the other categories over the past year.

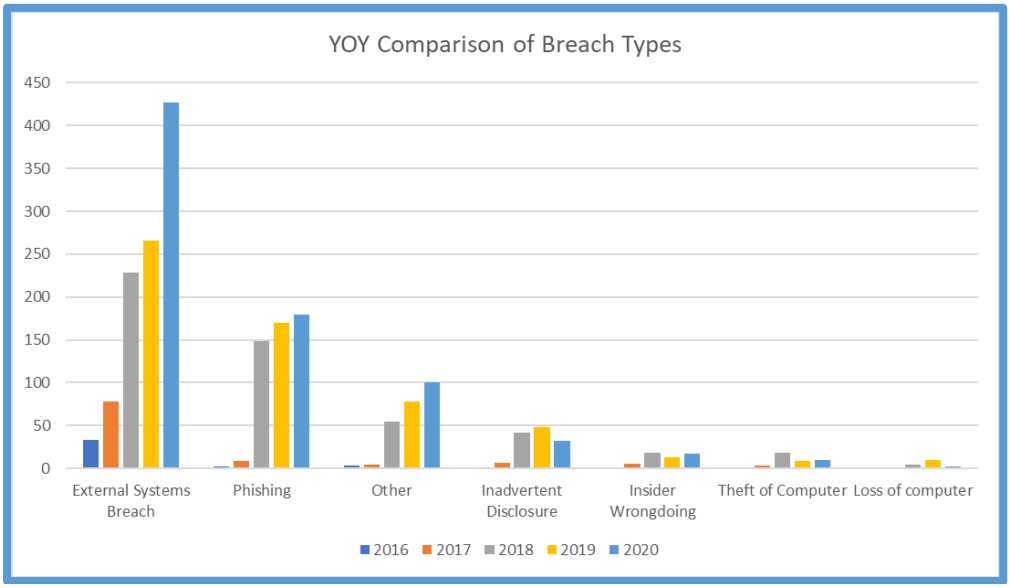
TYPES OF BREACHES

In reviewing the data, one the most interesting areas of study is the types of breaches being perpetrated. Knowing the most common types of attacks can help companies conduct risk assessments of their own organization, network, or internet footprint to determine which attack vectors are being used.

The following graph presents the types of breaches which were reported during 2020 and the following chart shows that the most common attacks are still external attacks and phishing attacks.



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



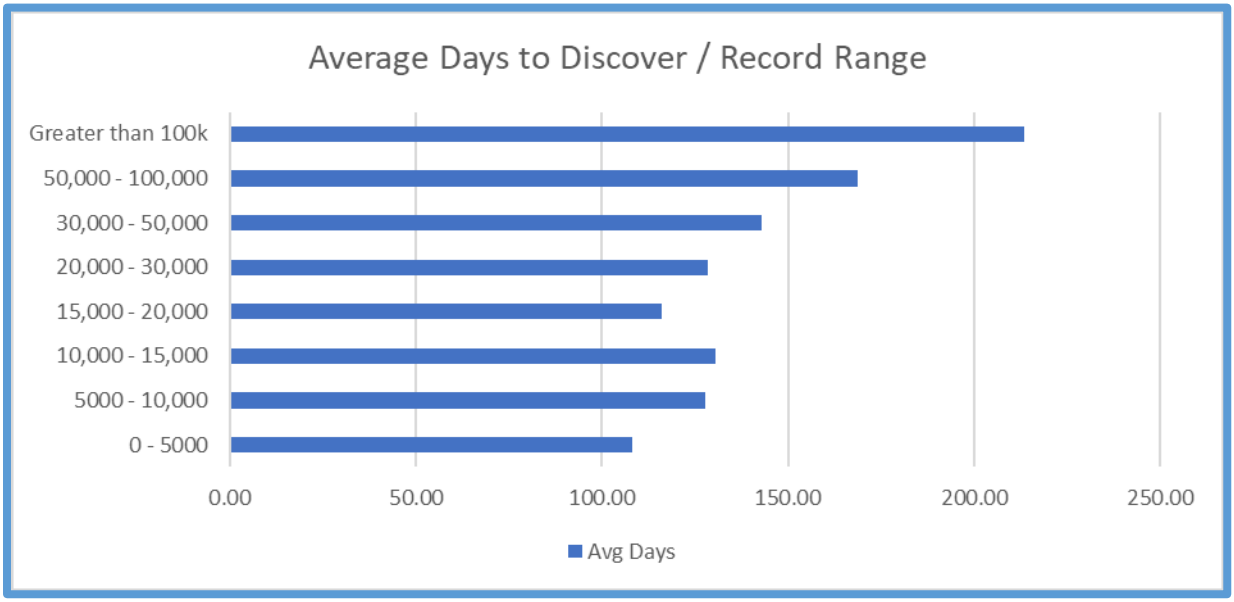
External attacks include credit card skimming software and cross-site scripting attacks as well as direct, brute-force attacks on the company network. There are several reports in which phishing attacks were categorized as external attacks and several more reports whose description indicates that phishing attacks may have been used as an attack vector. Because of this, the number of phishing attacks may be under-reported in the phishing category.

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, and in particular SMBs, that an attack on a third-party vendor may require reporting and notifications by the contracting company. 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 year to determine the relationship between the days to identify a breach as compared to number of records affected in the breach. There are a number of studies which purport to show that there is a direct relationship between the time an attacker is in a system and the recovery costs, but what relationship is there, if any, between the number of records in a breach and time to discovery?

After slicing the size of the total records into ranges, there does appear to be a direct correlation between the time it takes to discover a breach and number of records breached. Logically and intuitively this makes sense because the longer an attacker is able to access a system, the more data the attacker can identify and steal. This data should be a warning to companies to regularly search for indicators of compromise within their network.



CONCLUSIONS

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

The average number of records involved in a data breach for a Nebraska-based company is 3,750 and translates to an average of $768,750 using the IBM Study or $362,970 using the Cyentia study. These response and recovery costs include expenses such as 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 which may be 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.

Published by the Cyber Law & Security Group at Baird Holm LLP

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 22 years of experience working for the Federal Bureau of Investigation as a Special Agent and Supervisory Special Agent.

Bob can be reached at 402.636.8313 or bkardell@bairdholm.com.

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