NAS insurance

2019 Cyber Claims Digest

ANALYSIS OF 2018 CYBER CLAIMS DATA

Executive Summary

Cryptomining. Ransomware. Business email compromise. Spear phishing. This is the new language of business risk. Whether it's a massive data breach that exposes customer information like the Marriott incident reported in November 2018, or an automated ransomware attack that extorts bitcoin payments from a medi-spa owner, the cybercrime wave continues to swell as the cybercrime economy becomes more sophisticated.

The threat of cyber attacks continues to top the list of executive concerns around the globe. According to the latest survey by The Conference Board, US-based CEO's rank cybersecurity as their number one concern.[1]

And here's why...

As recently reported by Protenus, the patient data management company, 2018 saw a 3X increase in breaches of personal health records, exposing over 15 million records.[2] The ITRC (Identity Theft Resource Center) reports that in 2018, over 1,200 incidents have exposed 440 million records of personal information, an increase of 126% over 2017.[3]

CyberSecurity Ventures reports that ransomware cost businesses $5 billion worldwide in 2017 and upwards of $8 billion in 2018.[4] And a recent report from the Insurance Industry Cybercrime Task Force noted that ransomware payment demands have significantly increased. "Demands of $250,000 to $500,000 were non-existent six months ago and are now a weekly occurrence."[5]

According to the 2018 Verizon Data Breach Investigations Report, 58% of all cyberattacks targeted small businesses.[6] Costs to respond and recover from these attacks averaged almost $385,000. While the nature and extent of attacks on small business vary greatly, 67 percent of SMBs experienced a cyberattack and 58 percent experienced a data breach in the last 12 months.

To address the proliferation and growing complexity of the cyber attacks, the insurance industry is responding. According to Fitch, 2018 US cyber premiums were $2 billion and poised for continued 25% CAGR through 2023.

At NAS, we've seen continued growth in cyber claims across all segments of our business.
NAS cyber premium has increased 23%, topping $125MM. Not surprisingly, we've seen a significant uptick in cyber claims activity. In 2018, the number of closed claims reached almost 1,800, up 15% over 2017.

[1] The Conference Board, "C-Suite Challenge 2019," January, 2019.
Protenus, 2019 Breach Barometer Report, www.protenus.com/2019-breach-barometer
Identity Theft Resource Center, 2018 Data Breach Report
CyberSecurity Ventures, www.cybersecurityventures.com, June 2018
Insurance Industry Cybercrime Task Force, NetDiligence 2018 Report
Verizon, Data Breach Investigations Report, 2018
Ponemon Institute, 2018 State of Cybersecurity in Small and Medium Size Businesses, 2018
Ponemon Institute, 2018 State of Cybersecurity in Small and Medium Size Businesses, 2018

In the following report, we organize our cyber claims information into two distinct policyholder segments – healthcare and non-healthcare businesses. There are some significant differences in the data for each category, and we think it is valuable to look at breaches, cybercrime and breach response costs through these two separate lenses.

Cyber Risks Vary Between Healthcare and Non-Healthcare Businesses:

In analyzing our cyber claims data, we've identified the top 3 cyber causes of loss for healthcare and non-healthcare cyber business:

CAUSE OF CYBER LOSS
HEALTHCARE POLICYHOLDERS

	2017	2018
Most Common Cause	Employee Negligence	Employee Negligence
2nd Most Common Cause	Ransomware	Ransomware
3rd Most Common Cause	Physical Theft	Rogue Employee

CAUSE OF CYBER LOSS
NON-HEALTHCARE POLICYHOLDERS

	2017	2018
Most Common Cause	Hacking Attack	Hacking Attack
2nd Most Common Cause	Ransomware	Ransomware
3rd Most Common Cause	Physical Theft	Phishing Attack

Overall, healthcare-related businesses' cyber claims saw only a modest increase in claims (up 2%), while our non-healthcare policyholders' claims grew by 38%.

Cybercrime claims, across both segments, are up 68% over 2017 led by Financial Fraud, up 79%.

The shift in 2018 is most pronounced among our non-healthcare insureds. In this segment, the number of cybercrime claims almost doubled from 2017. And since 2016, we have seen a four-fold increase. The most significant increase of cybercrime activity is in Financial Fraud, again showing almost 4 times as many claims in 2018 as in 2016. These fraudulent transactions are often a result of email phishing schemes that lead to payments or wire transfers of funds to cybercriminals posing as our insured's clients or business partners.

RANSOMWARE CLAIM: Six-figure Ransom Demand

The Insured is a global visual, audio and collaboration solutions company. An employee of the company opened an email which introduced the "Ryuk" ransomware virus into Insured's computer system. Our insured confirmed that servers in the USA and Canada were affected but noted that servers in Australia, China and other countries may have also been affected. It is believed that up to 660 servers were affected internationally.

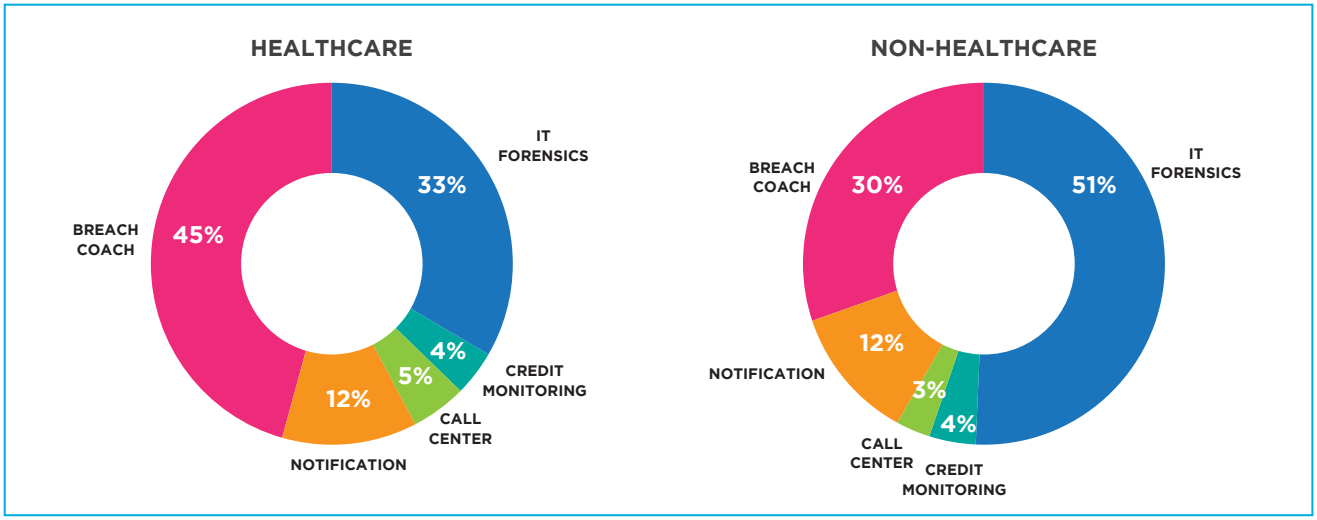
NAS retained a global IT forensics firm to obtain a ransom demand, negotiate with the hackers and complete a forensic investigation. The original ransom demand was 130 bitcoins, or approximately $540,000, however, the IT forensics team was able to engage the hacker and negotiate a lower ransom of $425,000 which was covered by the Cyber Extortion insuring agreement in their NAS NetGuard® Plus policy. Upon payment of the ransom, the forensics team was able to start decrypting the Insured's files.

Costs of Cyber Claims 2018:
Across healthcare and non-healthcare claims, consistent with 2017 data, the largest costs associated with cyber claims were IT Forensics and Breach Coach/Legal expenses. IT Forensics expenses are those related to the investigation of a breach, examination of what data may have been exposed or exfiltrated, crypto-currency procurement and payment, and data decryption and/or system restoration. Breach Coach/Legal expenses are related to the legal fees incurred in managing the breach response, coordination of vendors and defense costs (where applicable).

Among **healthcare** insureds, Breach Coach/legal expenses in 2018 led all categories and represented 45% of cyber claims costs vs only 9% in 2017. IT forensics expenses among healthcare policyholders were relatively flat vs 2017, however they comprise 33% of overall claims expenses for the category.

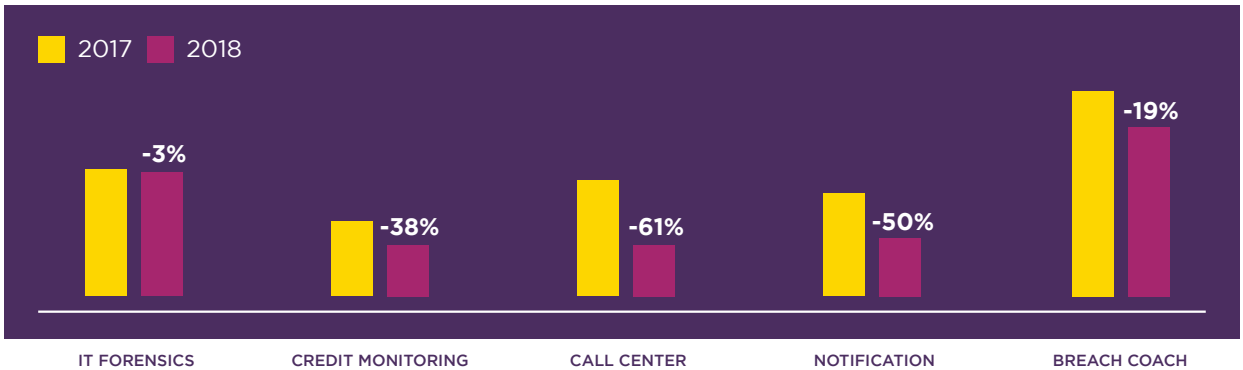
For **non-healthcare** claims, the IT Forensics costs were up 105% over 2017 and represent 51% of the overall costs of cyber claims. Breach Coach/ Legal Expenses were up 72% over 2017, and represent 30% of overall cyber claims expenses.

2018 ALLOCATION OF CYBER CLAIMS COSTS



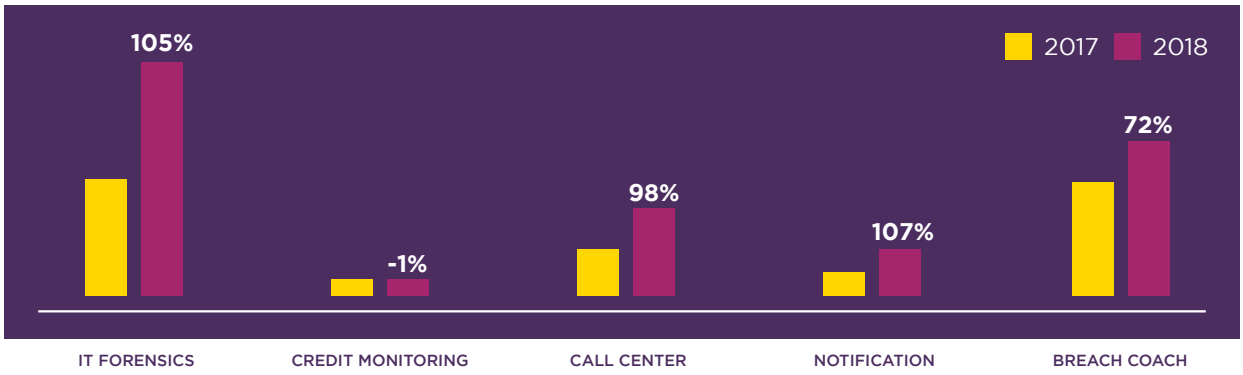
In 2018, the costs of cyber claims among our healthcare segment were lower than 2017 in each category. We believe that 2017 claims incurred extraordinary costs due to the size of several breaches that affected hundreds of thousands of patients, thereby increasing costs for areas such as notification, call centers and credit monitoring. In 2018, while the number of breaches increased, the universe of affected individuals decreased 34%.

COSTS OF CYBER CLAIMS: HEALTHCARE



Among non-healthcare businesses, the overall number of cyber incidents grew 38%. This sharp uptick also led to significant increases in the costs of responding to the incidents, in every category, with the greatest increase in Notification and IT forensics costs.

COSTS OF CYBER CLAIMS: NON-HEALTHCARE



Causes of Loss

In 2018, cyber losses among non-healthcare businesses were attributed to Hacking, Ransomware and Phishing Attacks. "Hacking," in many cases, led to data exposure and data theft and thus policyholders incurred substantial cyber breach response costs. The phishing attacks, at times led to a data breach, however, often led to some type of fraudulent financial transaction (e.g., wire transfer to a fraudulent account). Among healthcare insureds, financial fraud incidents increased 29% and among non-healthcare entities, the increase was 89% over 2017 claims.

CYBER CRIME CLAIMS: FINANCIAL FRAUD INCIDENTS

CYBER CRIME CLAIMS SCENARIO: Financial Fraud

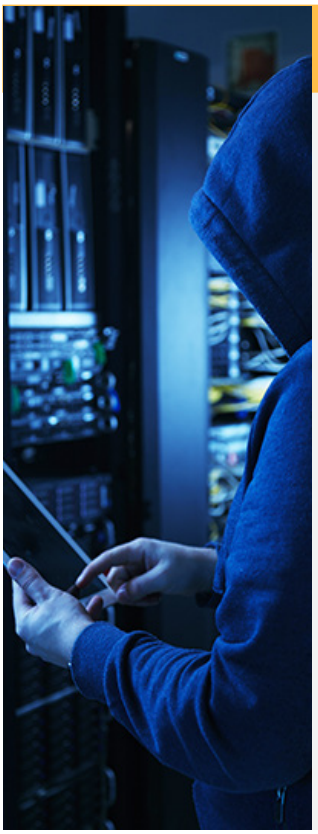
Our insured, an investment advisory firm, received a routine email request to transfer $480,000 from someone purporting to be their client. An authorized employee at the advisory firm, presuming the request was legitimate, processed the transfer. When the insured's client was notified of the completed transaction, he immediately contacted the firm about the fraudulent transaction. It was determined that funds were sent to a cybercriminal. The Insured had cybercrime limits of $1 million, subject to a $5K retention. The insured's IT team conducted an investigation and confirmed that the email was a phishing email by a bad actor impersonating the insured's client. Insurance did cover the costs of funds lost, outside of the $5,000 retention.

Though phishing schemes, financial fraud and automated ransomware attacks get a lot of attention, **human error** is still the number one cause of loss among our healthcare insureds. According to our 2018 cyber claims data, cyber incidents caused by Employee Negligence are up 25% over 2017.

NEGLIGENCE CLAIMS SCENARIO: Violation of Confidential Medical Information

A patient of an insured medical clinic alleged that a nurse accessed her medical records and disclosed her medical and personal information to third parties without her authorization. The patient alleged that the nurse, a former girlfriend of the patient's current boyfriend, also (falsely) stated that the patient had a sexually transmitted disease, made comments about the patient's current relationship, shared how many times she was pregnant, and commented on the patient's appearance during medical visits.

The medical clinic's defense was that it adhered to strict policies with regards to HIPAA, and that its employee failed to follow protocol. The matter settled out of court for a five-figure settlement that was covered by the Security and Privacy Liability insuring agreement.



Growth of Ransomware Extortion Demands

In 2017 and 2018, ransomware events were front and center as an area of great concern for our insureds and remained the second-most cause of loss among all of our cyber claims in each year. Over the past 2 years, we resolved over 90 ransomware incidents among a broad range of businesses and with various ransom demands. Payment demands were wide-ranging and topped out over $30,000 (and in a variety of currencies). In addition to the actual ransom payments, the technical and legal expenses associated with negotiating and paying the cryptocurrency demands often tripled or quadrupled the cost of resolving the issue with expenses often soaring over $70,000.

Looking across both segments, healthcare ransomware costs were significantly higher than non-healthcare. In 2017, the average ransom payment to healthcare insureds was 106% greater than non-healthcare. In, 2018, the gap was smaller, with healthcare ransom payments only 18% greater than non-healthcare.

In early 2019, we have already seen a huge shift. In 3 separate events, ransom demands have ranged from $100,000 to $1.2 Million. And, according to a broader study by the NetDiligence Insurance Industry Cybercrime Task Force, other carriers are seeing this trend of much higher ransom demands. We will continue to monitor and report on this activity over the course of the year ahead.

Preventing and Mitigating Losses From A Cyber Attack

We are often asked for suggestions or guidance on how to reduce the risk of a cyber incident. Given the complexity of 'cyber incidents' and the wide range of types of attacks, there are no easy answers. However, we have found that the more prepared an organization is to respond, the faster they recover.

Resources like NAS' CyberNET – an online training platform and call center with cyber security experts, can help organizations educate their employees about cyber risks as well as provide guidance on an effective "Cyber Incident Response Plan."

As a means of 'first response' to a suspected incident, here's a helpful guide of what to do in various situations to help mitigate the impact:

Cyber Event	Immediate Mitigation Steps
Ransomware infection	• Isolate infected computer from all networks (by unplugging network cable and/or turning off Wi-Fi) • Take picture of ransomware message (if possible) • Do not immediately rebuild your system (you might destroy important forensic evidence) • Regularly backup all critical data and store offsite
Phishing email attack	• Change password (strong and unique passphrase) • Forward email to IT • Enable Multi Factor Authentication • Learn how to recognize a phishing email
Malware infection	• Remove malware • Scan network for any other unauthorized files and user accounts • Install anti-virus software and keep updated
Email compromise	• Change passwords (strong and unique passphrase) • Enable Multi Factor Authentication
Unauthorized files or user accounts on server or client	• Close Remote Desktop Protocol (RDP) ports • Change passwords (strong and unique passphrase) • Enable Multi Factor Authentication • Use VPN for remote access
Mistaken wire transfer	• Call bank and report details • Attempt to halt transfer