NAS INSURANCE CYBER CLAIMS DIGEST
2016 TRENDS AND INSIGHTS

NASinsurance.com

NAS insurance
CYBER STRONG.™

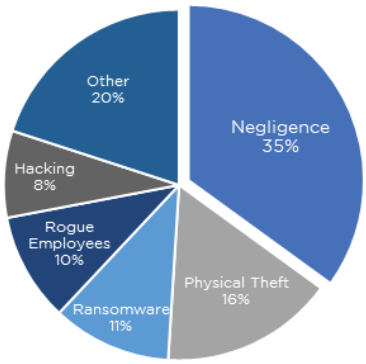
NAS INSURANCE CYBER CLAIMS DIGEST 2016 TRENDS AND INSIGHTS

The following report was developed by NAS Insurance Services' Claims Department as an effort to provide our partners and clients with insight about current cyber risks and their associated costs to commercial entities. The report is based on over 900 claims from NAS policyholders, closed in the 2016 calendar year. As there are many trends to highlight, we have noticed significant differences in claims activity between our healthcare and non-healthcare policyholders, and therefore have chosen to illustrate the findings in each of those categories.

Overview of 2016 Closed Cyber Claims

In 2016, we handled approximately one thousand cyber claims and over half involved a privacy breach. The top 5 causes of the breaches can be categorized as follows:

Healthcare



Non-Healthcare

*Other: phishing attacks, cyber extortion, malware, and wire transfer fraud

Ransomware

To say that 2016 was the year of ransomware would be an understatement. While the FBI estimated ransomware to be a $1 billion crime in 2016[1], a Kaspersky Lab research bulletin reported that ransomware attacks against businesses saw a three-fold increase in 2016, "increasing from one every two minutes, to one every 40 seconds." In addition, Kaspersky Labs highlighted that 42% of small and medium-sized businesses were hit.[2]

NAS, similarly, saw a significant increase in claims activity related to ransomware events in 2016. Healthcare-related ransomware events doubled over 2015 activity, while ransomware events among our non-healthcare policyholders showed a four-fold increase. Ransomware also became the #1 cyber claim category, surpassing "Hacking" and "Physical Theft," among our non-healthcare policyholders. In the healthcare sector, while there was a significant increase in ransomware claims, "Employee Negligence" continues to be the leading cause of a breach (e.g., healthcare records faxed to the wrong number).

SOURCE: FEDERAL BUREAU OF INVESTIGATION

[1] NBC News, January 9, 2017, http://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646

[2] Kaspersky Lab, Kaspersky Security Bulletin 2016

[3] Reuters, April 2016, http://www.reuters.com/article/us-cyber-fraud-email-idUSKCN0X505U

NAS INSURANCE CYBER DIGEST 2016 TRENDS AND INSIGHTS

In addition to the privacy breaches discussed above, cyber claims in 2016 also included a range of other cyber incidents including an increase in cyber crime, financial fraud, and regulatory investigations.

Fraudulent Transactions

In 2016, we saw a significant increase in cyber crime claims involving fraud among all categories of policyholders. As widely reported in the news and by the FBI, "Losses from these [email] scams, which are known as "business email compromise," totaled more than $2.3 billion from October 2013 through February of 2016."[3]

Financial Fraud claims by NAS policyholders increased 8x over 2015. The fraudulent wire transfer requests involved a criminal actor, posing as an employee of an insured entity, requesting a transfer of funds from the company to the criminal's bank account.

SOURCE: FEDERAL BUREAU OF INVESTIGATION

Regulatory Proceedings

In 2016, we also saw a significant uptick in government regulatory proceeding claims among our cyber policyholders in both healthcare and non-healthcare sectors. In healthcare, we recognize that the Department of Health and Human Services (and the Office of Civil Rights) has stepped up its efforts to investigate cyber incidents.

Regulatory claims outside of healthcare include investigations of cyber incidents by states' attorneys general. These include inquiries to determine whether the breached policyholder notified the attorney general's office in a timely manner, and whether they issued required notifications to affected individuals within a reasonable timeframe.

[1] NBC News, January 9, 2017, http://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646

[2] Kaspersky Lab, Kaspersky Security Bulletin 2016

[3] Reuters, April 2016, http://www.reuters.com/article/us-cyber-fraud-email-idUSKCN0X505U

Costs of Cyber Incidents

In the analysis of the costs of claims closed in 2016, it is important to understand that some of the costs pertain to near-term costs of claims opened in 2016 (e.g., costs to notify customers of a breach) as well as longer tail costs of claims opened in 2014 and 2015 (e.g., on-going legal costs, fines and penalties, etc). With that said, we continue to see the costs of customer notification as the largest cost related to a privacy or security breach. The costs do vary significantly, however, between healthcare and non-healthcare entities as follows:

Breach-related Expenses	Healthcare (% of total expense)	Non-healthcare (% of total expense)
Notification	49%	72%
Legal Fees	33%	13%
IT Forensics	15%	13%

Because most of the breach costs are associated with notification efforts, we continue to advise our clients to evaluate their cyber insurance options based on the number of customer (or patient) records they manage.

However, with ransomware and fraud activity on the rise, especially in the non-healthcare sector, we do expect IT Forensic costs to comprise a larger percentage of total breach expenses in 2017.

2016 and 2017 Open Claims Trends

The cyber claims that remain open from 2016 follow the trends of those that have closed. Ransomware events are significantly increased among both healthcare and non-healthcare insureds. In addition, as in the closed claims, costs of notification represent the highest percentage of costs among non-healthcare insureds as legal expenses are higher among the healthcare claims.

In 2017, to date, the trend in non-healthcare cyber claims has been cyber crime and ransomware events. As far as cyber crime claims are concerned, there has been an influx of fraudulent wire transfer request claims. Additionally, during the first quarter of 2017, there was a large amount of phishing attack claims involving the misappropriation of W-2 information, right before tax season. As far as healthcare cyber claims in 2017 are concerned, employee negligence remains the main cause of a breach, and we have seen a rise in ransomware and malware attacks.