NAS insurance

2018 Cyber Claims Digest

ANALYSIS OF 2017 CYBER CLAIMS DATA

Executive Summary

The US cyber insurance market continued to expand in 2017, reaching almost $2 billion in premium and 37% growth over 2016.* NAS' cyber business grew significantly, as well, crossing over the $100 million mark in open market, program business and reinsurance cyber premium. And with the increase in premium and expansion of the number of active policies, cyber claims have also increased. Having adjusted almost 1,500 cyber claims in 2017, we identified four notable trends: (1) the number of identities impacted by a breach surged; (2) the average cost of IT forensics and call centers exploded; (3) ransomware became the second most common cause of loss for both healthcare and non-healthcare businesses; and (4) the average financial loss resulting from cybercrime (e.g., wire transfer fraud, telecommunications fraud, and phishing attacks) exceeded $100,000. Given these trends and what we have seen so far in 2018, it is likely that the number of cyber claims will continue to rise, cyber-attacks related to the Internet of Things (IoT) will grow, and ransomware will remain a serious concern.

TREND #1 Surge in the Number of Identities Impacted by a Breach

In 2017, there was an explosion of the total number of identities impacted by a breach. For healthcare, there was a 232% increase in 2017 in the number of identities impacted. For non-healthcare policyholders, there was an 85% increase from 2016 in the number of identities impacted.

TREND #2 Increase in the Average Cost of IT Forensics & Call Centers

With the increase in the number of identities impacted, trend #2 was foreseeable: larger breaches increased the average cost of remediation. Tables 1 and 2 show the average cost of each claim component as a percentage of the overall average cost of cyber claims. Notably, the average cost of IT forensic investigation fees/expenses became the largest average cost component in 2017. In 2017, the average IT forensics costs for non-healthcare businesses were up 59% as compared to 2016, and represented 44% of average non-healthcare claims costs. Likewise, in 2017, the average IT forensics costs for healthcare businesses were up 46% as compared to 2016 and represented 33% of average healthcare claims costs.

HEALTHCARE
AVERAGE COST BY COMPONENT AS PERCENT OF AVERAGE CLAIM COST, 2017

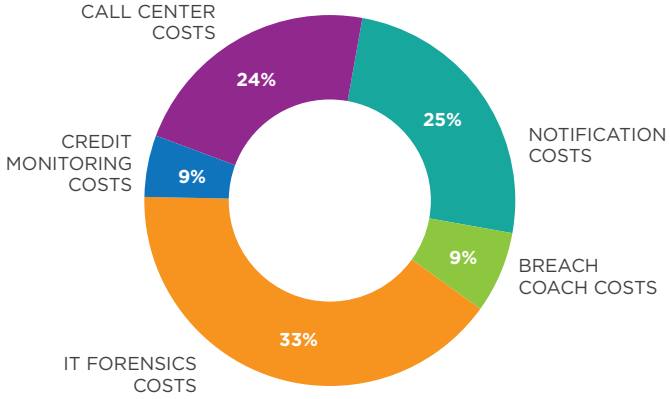


TABLE 1

NON-HEALTHCARE
AVERAGE COST BY COMPONENT AS PERCENT OF AVERAGE CLAIM COST, 2017

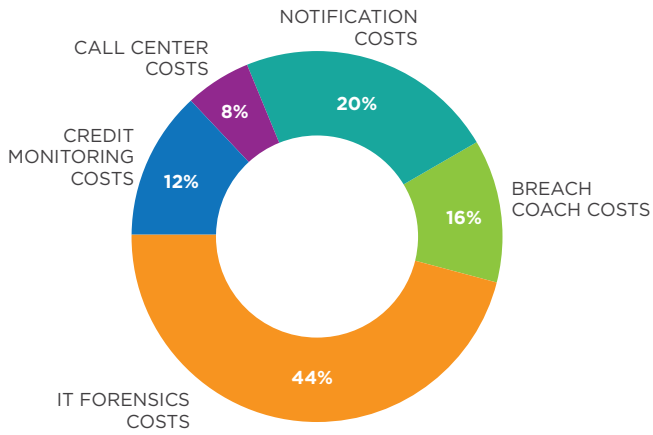
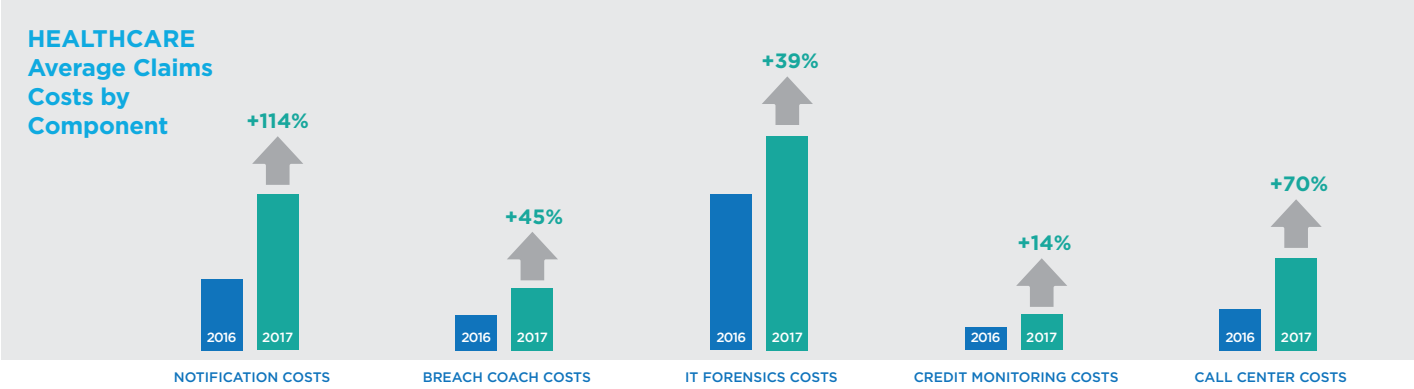


TABLE 2

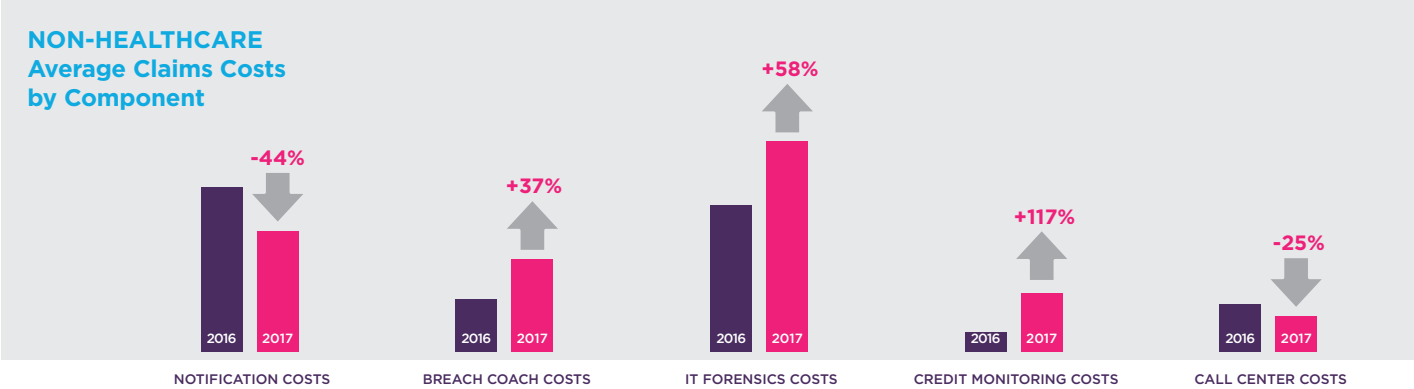
For healthcare businesses in 2017, NAS saw significant increases in the average costs of claims. Notification costs, in particular, had increased 114% over 2016 expenses as several claims involved large groups of affected individuals. Related to the increase in notification costs, is the significant 70% increase in the costs of call centers. The dramatic rise in call center costs for healthcare can be explained by the increase in identities impacted, as noted in trend #1, but unique factors within the healthcare industry also appear to have played a part. For one, healthcare businesses generally tend to access, use and store a larger volume of personal information, including sensitive health and medical information. In addition, the Health Insurance Portability and Accountability Act (HIPAA) and similar regulatory and statutory schemes contain more stringent notification requirements, making breach notifications that are required by law, far more common in the healthcare sector.

Another factor in the dramatic increase in the cost of call centers is the fact that, according to NAS data, the average age of identities impacted by a healthcare breach skewed older. Our experience has shown that individuals who are 60 years of age or older are more likely to contact a call center when a breach occurred. Also, the average length of conversations with call center representatives was longer because this demographic often requested extra assistance in understanding what the breach entailed and how it impacted them.



For non-healthcare businesses, less data was accessed, and the data was less sensitive, which meant that the breaches impacting this sector tended to be smaller (notification expenses down 44% vs 2016), and the use of call centers (down 25%) were not as significant as compared to healthcare claims.

In addition, the cost for IT Forensics in non-healthcare claims showed a sizable increase (+58% vs 2016) as a result of the increased technical complexity of many of the claims we handled.



TREND #3 Ransomware was the Second Most Common Cause of Loss

In 2017, negligence by employees or third-party service providers continued to be the most common cause of loss for the healthcare industry, while ransomware and physical theft ranked as the second and third most common causes of loss. Figure 1 and figure 2 below show the most common causes of loss in 2016 and 2017 by business sector.

For non-healthcare cyber claims in 2017, the top three causes of loss remained the same from 2016: (#1) hacking attack, (#2) ransomware and (#3) physical theft. Overall, for non-healthcare cyber claims, a hacking attack was the cause of loss 23% of the time, ransomware 20% of the time, and physical theft 9% of the time.

FIGURE 1

HEALTHCARE POLICYHOLDERS
Cause of Loss by Rank for 2016 & 2017

RANK	2016 CAUSE	2017 CAUSE
Most Common Cause	Negligence	Negligence
2nd Most Common Cause	Physical Theft	Ransomware
3rd Most Common Cause	Ransomware	Physical Theft

FIGURE 2

NON-HEALTHCARE POLICYHOLDERS
Cause of Loss by Rank for 2016 & 2017

RANK	2016 CAUSE	2017 CAUSE
Most Common Breach Cause	Hacking Attack	Hacking Attack
2nd Most Common Breach Cause	Ransomware	Ransomware
3rd Most Common Breach Cause	Physical Theft	Physical Theft

A few scenarios from claims we handled in 2017 will help to illustrate how ransomware attacks can blindside a company.

Healthcare Claim Scenario

Employees of a hospital discovered that their email accounts were not accessible. The hospital's IT department investigated and discovered that a ransomware attack infected 70 servers and 600 workstations. The hospital had to close operations for 2 business days and suffered losses in relation to the event. Cyber Insurance covered a total of $567,350, as follows:

> IT Expenses: $417,000 – Consultants were retained to immediately address the ransomware attack, secure data, investigate if any patient health information was compromised, and rebuild the hospital's network.

> Business Interruption Expenses: $65,000 – Several surgeries had to be cancelled resulting in loss of income.

> Data Recovery: $76,000 – Numerous employees had to work overtime to recreate lost data from back-ups.

> Ransom Amount: $9,350 – The hospital paid the ransom demand to regain system access.

Non-Healthcare Claims Scenario

An employment agency's server and computer system were infected with ransomware on four different dates. Though it could not immediately be determined if the attacks were related, the timing and nature of the attacks indicated that the hackers were working in concert to completely lock up the agency's system and data. Each hacker requested a ransom payment in exchange for a decryption key. The agency refused to pay the ransoms and instead shut down its system and attempted to manually recover and recreate the encrypted data. In addition, the agency rebuilt its servers to ensure that all system and network vulnerabilities were remedied. Cyber Insurance covered almost $97,000 in data recovery costs.

Ransomware Methods

The methods used for ransomware attacks are becoming more sophisticated. Spam email remains a tried and true method: one in six spam email messages comes bundled with ransomware.[i] However in 2017, criminals also tended to target specific companies.

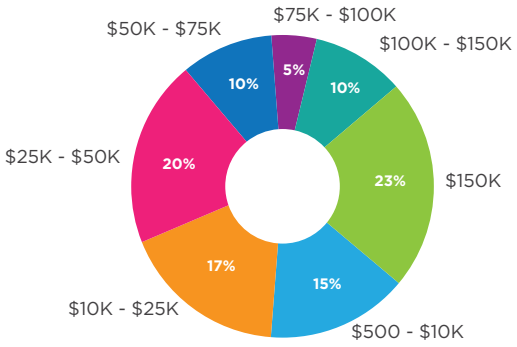
According to BitDefender, "Companies have faced extremely targeted attacks that abuse the Remote Desktop Protocol to connect to infrastructure, then manually infect computers. Ransomware has lateral movement tools to infect the organization and cover its tracks." [i]

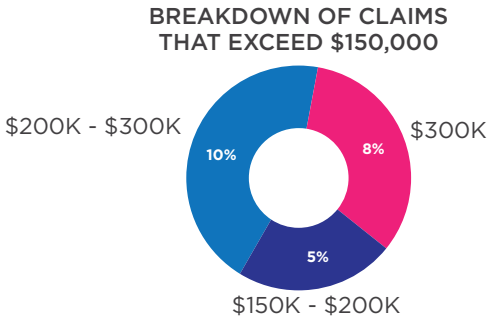
TREND #4 The Average Financial Loss Resulting from Cybercrime Exceeded $100,000

Overall, the average loss for a cybercrime claim remained consistent between 2016 and 2017. The average in 2017 was $116,697, while in 2016, the average was $117,229 – a difference of only $532. What remains significant is the fact that the average cybercrime loss in both 2016 and in 2017 was over $100,000 – a hefty sum for most small and medium size enterprises.

NAS data from 2017 shows that 23% of cybercrime claims exceeded $200,000.

2017 PERCENTAGE OF CLAIMS BY LOSS AMOUNT





NAS 2017 Claims Data.

In the following section, we focus on the top 3 types of cybercrime claims we handled during 2017. For further information on NAS cybercrime claims, please see our earlier report, "2017 Cybercrime Claims Analysis," released in June, 2018.

Focus: Ransomware

Between 2016 and 2017, there was a 152% increase in ransomware as a cause of loss for healthcare cyber claims. In this report, ransomware is a cyber-related threat with a monetary demand. The threat is typically to divulge or destroy information, to insert malicious code into a computer system, or to damage, destroy or prevent access to a computer system. The monetary demand varies in both amount and the currency; the demand might seek payment in American dollars, a foreign currency or a cryptocurrency.

Focus: Hacking Attack

Hacking attacks remained the top cause of loss for non-healthcare claims in both 2016 and 2017. In this report, a hacking attack includes unauthorized access or use of a computer system, a denial of service attack, infection of a computer system with malicious code, or an act of cyber terrorism.

The following claim scenario demonstrates how hacking attacks can impact a company.

Non-Healthcare Claim Scenario
A company's firewall was either down or not completely functional. During this time, an employee using the word "password" as his company network password had his workstation hacked. By exploiting the employee's weak password, the hacker gained remote access to the company's system on multiple occasions and downloaded the financial information of the company's clients from the past three years. A forensic investigation revealed that over 65,000 financial files were accessed or stolen. The company's clients lived in 26 different states and one U.S. territory. Notification costs, IT forensic investigation fees, and breach coach fees totaled approximately $50,000.

Focus: Phishing

A trend seen in 2016 continued in 2017: the most common method of cybercrime remains phishing. In 2017, 62% of the cybercrime claims reported to NAS were caused by phishing.

Just an extra vowel or 2...
A manufacturer of industrial products purchased items from an existing supplier. A legitimate email from the normal point of contact at the supplier was sent to the manufacturer requesting payment for the items and included wire transfer information in the email.

Unfortunately, a hacker infiltrated the supplier's email system and registered a domain very similar to the supplier's, using three E's in the supplier's name instead of two. The hacker used the spoofed email account to send an email to the manufacturer posing as the normal point of contact at the supplier. In the email, the hacker asked the recipient to ignore the prior wire transfer instructions and provided new wire transfer information.

The manufacturer did not notice the additional 'E' in the email address, and, believing the new wire instructions to be legitimate, wired $40,000 to the wrong account.

2018 Preview

Based upon trends of the existing NAS claim data, we expect cyber risks to evolve, the methods of attack to increase in sophistication, and both healthcare and non-healthcare sectors will see a significant increase in losses. In other words, no business or industry will be immune.

Figure 3: Non-Healthcare Claims, Linear Forecast

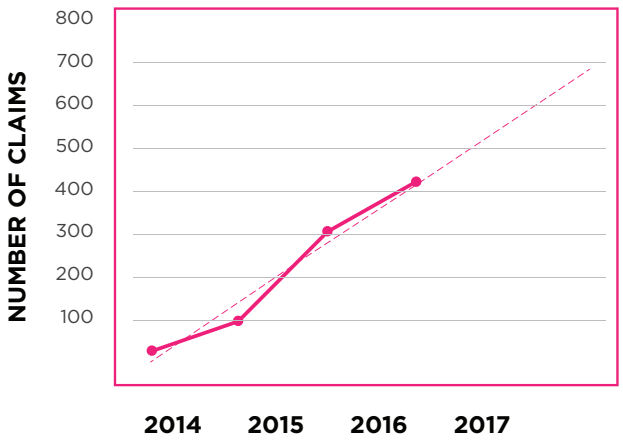
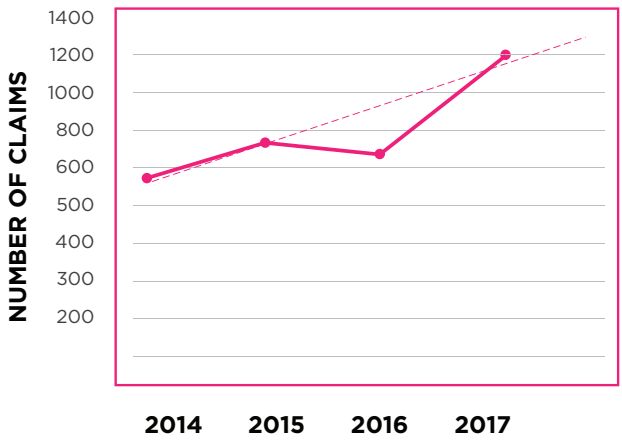


Figure 4: Healthcare Claims, Linear Forecast



We also expect that the average cost for IT forensics will continue to increase in 2018. As the methods of intrusion become more complex, it will take many more costly resources to detect a breach, determine its nature and scope, and mitigate the overall impact of a breach on an organization's business.

Another trend likely to continue in 2018 is the dramatic increase in the number of identities impacted by privacy breaches. Each identity compromised represents a potential income stream for cyber thieves.

IoT (Internet of Things) Related Cyber Attacks

Cyber-attacks related Internet of Things devices are likely to increase. According to the latest Experian Data Breach Resolution report, "In 2018, we'll see cybercriminals take this to the next level by hacking the IoT to create real-world mayhem. The interconnectedness of IoT devices make them prime targets for advanced hacks and ransomware."[iii]

Internet enabled medical devices have cyber risk too. The Healthcare Industry Cybersecurity Task Force recently wrote, "[M]edical devices and the IT networks they connect to are unique. In addition to data security and privacy impacts, patients may be physically affected (i.e., illness, injury, death) by cybersecurity threats and vulnerabilities of medical devices. .... As a result, addressing the patient safety risks posed by cyber threats are of paramount importance."[iv]

As our data shows, in 2016 and 2017, ransomware attacks continued to increase, and for 2018, we expect the number of cyber claims caused by ransomware to keep growing. James Lewis, Senior Vice President at the Center for Strategic and International Studies agrees. "One emerging trend is ransomware worms, which work their way through networks to lock out many more computers than just the initial target. New ransomware attacks are expected to gain exfiltration capabilities, stealing target files and locking the user out at the same time."[v]

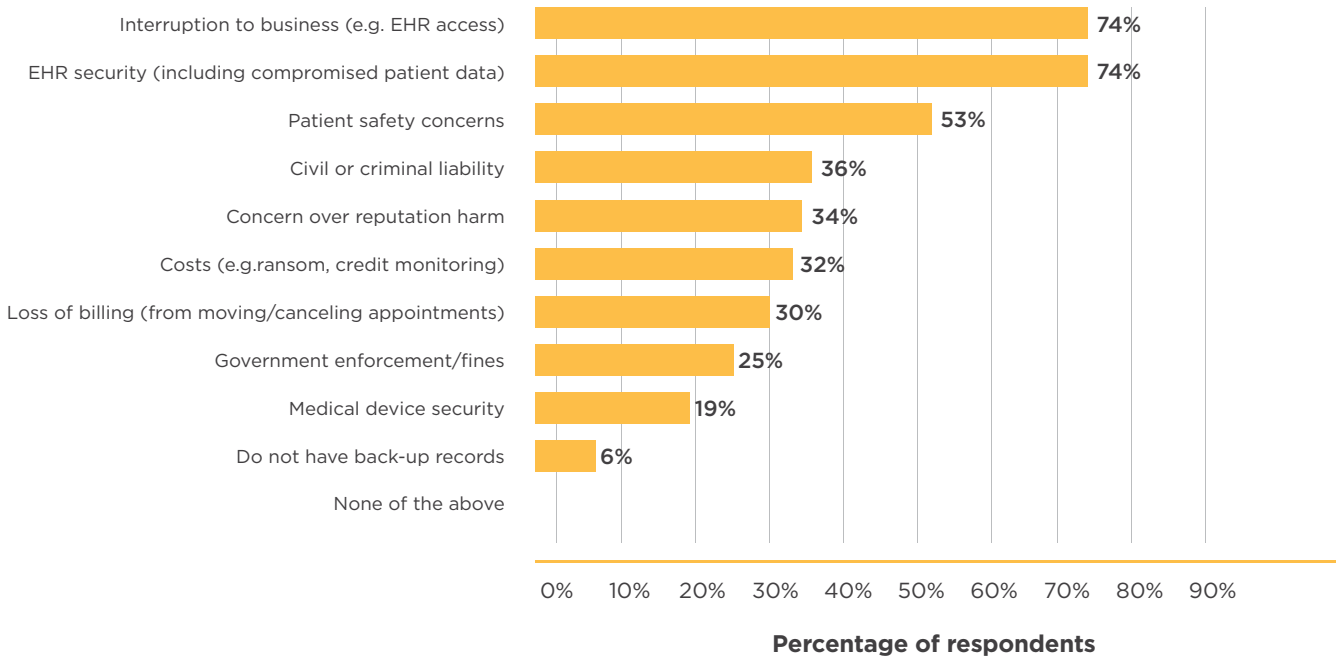
In January of 2018, Allscripts experienced a ransomware attack that impacted an estimated 1,500 clients, which Allscripts described as impacting a "limited number of applications." The ransom was 30.4 BTC (bitcoin), which was roughly equal to $325,217.07.[vii] This number may not adequately describe the impact on affected organizations. Allscripts services include record and practice management, hosting, and electronic prescription services.

After the breach occurred, "many providers [did] not have access to patient medical histories, labs, scheduling or payment applications."[viii] For a small or medium size enterprise, such a loss may severely hamper the ability to offer care.

Another trend we expect to see in 2018 claims data is an increase in business interruption claims resulting from ransomware attacks. While we predict that this trend will impact businesses across industries, a recent survey by the American Medical Association and Accenture found that business interruptions caused by cyber-attacks was the number one concern of physicians in the US.[viii]

Percentage of U.S. physicians that are concerned about select consequences of future cyber attacks as of 2017

Accenture & AMA National Physicians Cybersecurity Survey (2017)



Cyber Risk Mitigation

The most important aspect of managing cyber risk is prevention and awareness. Anyone at any level of an organization can become a target of cyber criminals, so all staff should receive training on the risks of phishing attacks, hackers' tactics, and how to avoid being a target.

Employees should always think before acting; if an email seems 'off', such as by having odd spacing or missing words, or screenshots, then employees should call the sender or initiate a separate email to confirm the suspicious email. Also, employees need to look before they click. If a link seems weird, employees should separately verify the link or email before taking any action.

EIGHT STEPS TO HELP PREVENT RANSOMWARE:[IX]

1. Segregate networks and turn off network shares to minimize the spread of a ransomware infection
2. Turn off admin rights for users who do not require them and apply least privilege policies
3. Restrict write permissions on file servers as much as possible
4. Educate users on the most common phishing and ransomware email patterns and how to respond
5. Make frequent, comprehensive backups of critical files and keep them offline
6. Protect email & web access with email & web security gateways with advanced threat protection
7. Deploy sophisticated endpoint security with behavioral & intelligent monitoring of suspicious patterns
8. Patch early & often to close known vulnerabilities in operating systems, browsers & web plugins

References

Abel, R. (2018, January 24). Allscript still recovering from SamSam ransomware attack. Retrieved from SC Media : https://www.scmagazine.com/samsam-ransomware-continues-to-wreak-havoc-on-infrastructure/article/738983/

Accenture. (2017). AMA & Accenture 2017 National Physician Cybersecurity Survey.

AON, 2017 US Cyber Market Update, July, 2018

Bitdefender. (2017). 2017 Ransomware Report. Bitdefender.

Bitdefender. (2017). The Global Threat Landscape Report - 2017.

Experian Data Breach Resolution. (2018). Data Breach Industry Forecast 2018.

Health Care Industry Cybersecurity Task Force. (2017). Report on Improving Cybersecurity in the Health Care Industry.

James Lewis. (2018). Economic Impact of Cybercrime - No Slowing Down. Santa Clara: McAfee & CSI (Center for Strategic and International Studies).

Sweeney, E. (2018, January 18). Allscripts hit with a ransomware attack affecting a 'limited number' of applications. Retrieved from Fierce Healthcare: https://www.fiercehealthcare.com/privacy-security/allscripts-ransomware-cybersecurity-ehr-applications

---

[i]AON, 2017 US Cyber Market Update, July, 2018
[ii](Bitdefender, 2017, p. 2)
[iii](Bitdefender, 2017, p. 2)
[iv](Experian Data Breach Resolution, 2018, p. 7)
[v](Health Care Industry Cybersecurity Task Force, 2017, p. 18)
[vi](James Lewis, 2018, p. 11)
[vii](Sweeney, 2018)
[viii](Abel, 2018)
[ix](Accenture, 2017)
[x](Sweeney, 2018)
[xi](Bitdefender, 2017)

For more information about this report or NAS Cyber Liability insurance, please contact:

Jeremy Barnett
Senior Vice President
NAS Insurance Services
818.382.6116
jbarnett@nasinsurance.com