NAS Cybercrime: 2017 Claims Analysis

NAS insurance

Cybercrime: Hype or Real Threat to Businesses?

Cybercrime has become front-page news because the threat to businesses and individuals continues to grow, and the attacks are seemingly indiscriminate, keeping everyone on edge. Cybercrime, like most crimes, has a victim, but the perpetrator is often unknown and leaves few, if any, clues about who committed the crime.

For companies of all sizes, the possibility of cybercrime lurks among the many risks businesses face, but remains mysterious because of the complexity and anonymity that surrounds it. While cybercrime is global, the United States is the top target country for web application attacks, with 238,643,360 attacks being targeted at the United States in the fourth quarter of 2017 alone.

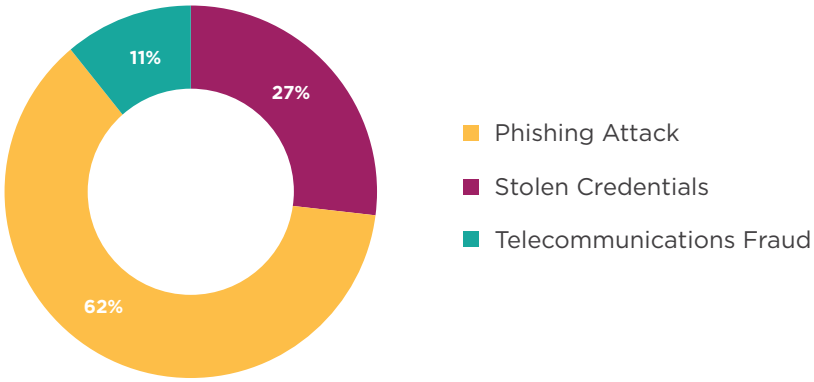
NAS Insurance: Cybercrime Claims in 2017

As used in this report, the term "cybercrime" refers to the theft of money, securities or tangible property by hacking or phishing, as well as losses resulting from telecommunications fraud.

(NOTE: Ransomware, also a significant cyber threat to businesses and one of the leading cyber claims among NAS policyholders will be covered in our broader 2017 Cyber Claims Digest).

In 2017, cybercrime continues to be an expensive loss for our insureds, with 1 in 4 claims exceeding $200,000. Significant losses have been reported across healthcare, manufacturing, education, and technology services companies. We are also seeing an expansion of the types of cybercrime tactics including phishing attacks, stolen credentials and telecommunications fraud.

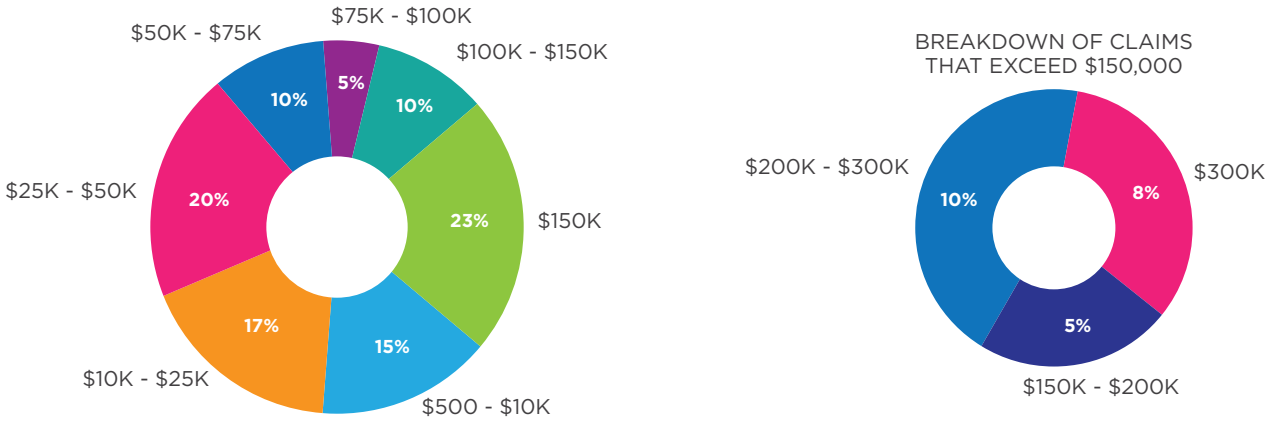
Percentage of Cybercrime Claims by Method of Attack



Cybercrime Loss Amounts

NAS data from 2017 shows that 23% of cybercrime claims exceeded $200,000. The average cybercrime loss amount in 2017 was $116,697. For a small or medium size business, an unexpected expense upward of $100,000 can have devastating consequences. The following chart provides details on the percentage of cybercrime claims by amount of loss:

2017 PERCENTAGE OF CLAIMS BY LOSS AMOUNT

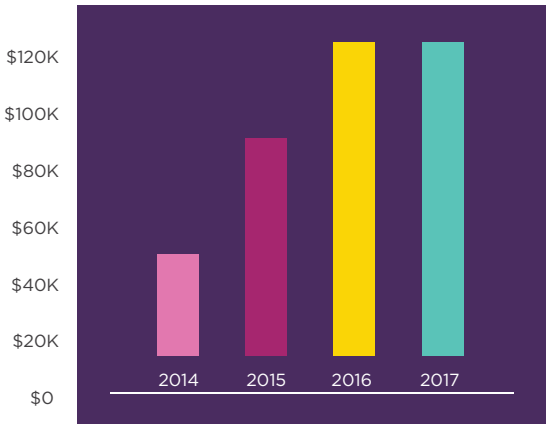


NAS 2017 Claims Data.

In 2017, the average cybercrime claim cost businesses over $100K

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.

Average Cybercrime Loss by Year



Cybercrime Focus – Phishing

Phishing involves a criminal actor who fraudulently uses electronic communications, like email or a malicious website, to impersonate a business, a representative of the business, or its brand, products or services to steal private information or money. The average loss for a claim caused by phishing was $96,270.

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.

Why does phishing remain the #1 method of cybercrime? Criminals have had success at exploiting a very common business practice, wiring money to a third party, to siphon funds to their own accounts.

Below are examples of the more common types of phishing attack cybercrime claims seen by NAS in 2017.

NAS CLAIM FILE: PHISHING SCENARIOS

Four Hours on a Friday ....

An unknown person obtained corporate email credentials and began impersonating a company executive. The hacker sent an email to the finance department asking for a wire transfer of approximately $50,000. The finance department responded with questions to confirm the request, such as how the request should be codified in the internal accounting system. The hacker used the executive's email to respond, and in the response referenced another expense (likely gleaned from reading the executive's earlier emails) as an example of how to handle the transfer which further appeared to legitimize the wire transfer request.

The money was wired. The entire situation happened between 10:30 am and 2:30 pm on a Friday.

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.

Phishing remains the most popular and easiest way to commit cybercrime.[iii]

More than 90% of successful hacks and data breaches stem from phishing— emails crafted to lure their recipients to click a link, open a document or forward information to someone they shouldn't. [iv]

With such a high success rate, it is clear why phishing remains the number one way cyber criminals steal money and sensitive information. In terms of how phishing occurs, the most common methods are[v]:

- **Domain squatting:** Domains named to look like valid domains
- **Domain shadowing:** Subdomains added under a valid domain without the owner's knowledge
- **Maliciously registered domains:** A domain created to serve malicious purposes
- **URL shorteners:** A malicious URL disguised with a URL shortener
- **Subdomain services:** A site created under a subdomain server

In November of 2017, Akamai (a leading web content delivery network) found that of the 8.3 billion login attempts on its platform, "a whopping 3.6 billion were determined … to be malicious login attempts. In terms of industries, Akamai's data showed that the targeted verticals (from highest to lowest) were: Retail, Hotel & Travel, High Tech, Media & Entertainment, Financial Services, and Consumer Goods[vi].

Cybercrime Focus – Stolen Credentials

The theft of money using stolen credentials was the second most common method of cybercrime in 2017, according to NAS data. The average loss caused by stolen credentials was $90,950.

NAS CLAIM FILE: STOLEN CREDENTIAL SCENARIO

Inspection or Inspection?

A bank provided a loan to a business for an office space and improvements to the office space. The practice of the bank was to inspect the improvements before distributing any of the loan proceeds to the construction company performing the work. While the bank was conducting the inspection, an executive at the construction company checked his email, clicked on an errant link that requested his email login information, and entered his login information. A hacker used the login information to look at emails between the executive and the bank.

The assailant created a fake domain that was off by only one letter – an 'i' [as in iodine] and an 'l' [as in lemon] were swapped – just like the title of this scenario, can you tell the difference?[1]

The assailant copied the text of a prior email between the construction executive and the financial institution, pasted it into an email from the spoofed domain name, and submitted new wiring instructions to the bank. The financial institution wired more than $300,000 to the fraudulent account.

[1]The first word is Inspection with a capital 'I' and the second word is inspection with a lowercase "l".

Cybercrime Focus – Telecommunications Fraud

Companies of all sizes use auto-attendant features in their phone systems to save time and money, and ideally to route customers and vendors to the company representative best suited to assist them. However, auto attendants and other features of modern phone systems are vulnerable to cybercrime.

NAS' 2017 claims data reveals that the average loss due to telecommunications fraud was $315,097. The range had a low of $3,340, and a high of approximately $1,200,000. The median loss was $148,159. For a small to medium size company, a phone bill that is three times (or more) higher than normal is very problematic.

NAS CLAIM FILE: TELECOMMUNICATIONS FRAUD SCENARIO

Thanksgiving Greetings to the World

During the long Thanksgiving weekend, attackers determined that calling a company's toll-free number, and interacting with the auto-attendant in a particular manner would allow anyone to use the company's phone line to call anywhere in the world. Thousands of calls were made during the long Thanksgiving weekend around the world using the company's phone system.

The company's telecom provider alerted the company about the unusual activity, and put an end to it. However, the company's phone bill for the illicit calls was about $48,000: $40,000 for phone calls, plus $7,500 for the FUSF (Federal Universal Service Fund Surcharge).

The True Cost of Cybercrime

It is important to note that NAS' loss data only measures the amount of money lost by the insured and does not necessarily reflect amounts paid under insurance. Additionally, the indirect costs and potential reputational harm associated with cybercrime is not taken into account in this data, but they can be significant. Employees' time and attention may be diverted to deal with the impact of cybercrime. Whether an enterprise is small or medium, having employees devote unexpected time to cleaning up a cybercrime event is both disruptive and costly. Also, customers lose confidence in a company's ability to keep business transactions and sensitive information secure after a company is victimized by cybercrime, which can lead to customer attrition and the loss of future business opportunities.

Cost by Industry Sector

The cost of cybercrime varies by size and sector. "[O]rganizational size, as measured by the number of enterprise seats or nodes, is positively correlated to annualized cyber crime cost." In other words, the larger the company, the higher the cybercrime cost. Likewise, cybercrime is more expensive for certain sectors than others. "The cost of cyber crime for companies in financial services and utilities and energy [has] the highest annualized cost. In contrast, companies in life science, education and hospitality incurred a much lower cost on average."[viii]

Key Finding #3 from the 2017 Cost of Cybercrime Report[ix]

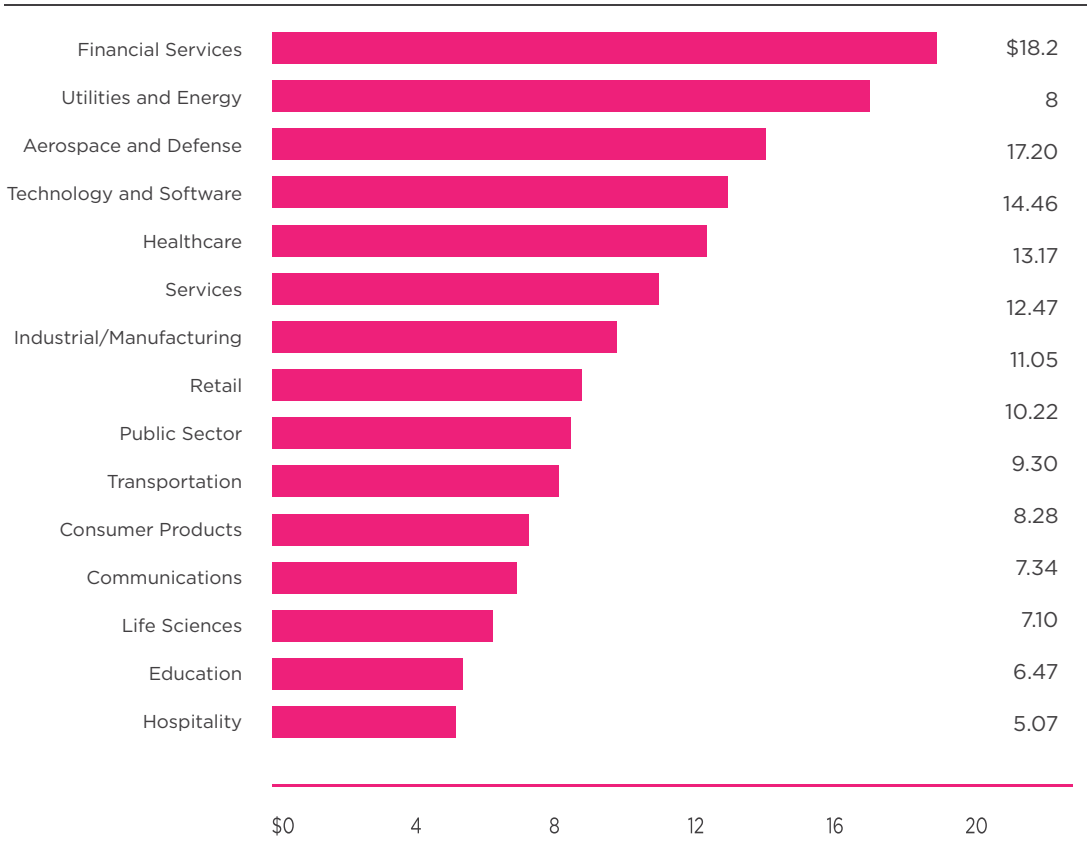


Figure 7
Average annualized cost by industry sector
US$ millions

Legend
Consolidated view
n = 254 companies

Total annualized cost ($1 million omitted)

Potential Trend for 2018: Manufacturing Sector

As noted in this report, the manufacturing sector was the second most common target of cybercrime in 2017 according to NAS claims data. While this was surprising, industry experts predict that this trend is likely to continue. "We will see more and more traction next year in … 'traditional industries'. Particularly in the manufacturing space … in 2018."[xvi]

The manufacturing industry has become a target for cybercrime because the schemes often involve the theft of a physical product that can be easily resold. For example, a 2017 NAS claim involved a manufacturer of high-tech accessories. The company received an email from a spoofed email address that attached a realistic looking, but fake, purchase order for $24,000. An additional $27,000 was later added to the order for a total exceeding $51,000. The goods were shipped, and the manufacturer never received payment.

AVERAGE PHISHING CLAIM COST IN 2017

$96K

We expect that this type of phishing attack to steal goods and products will remain a primary method of cybercrime. Again, the fact that the average NAS phishing claim in 2017 was over $96,000, and that phishing tends to be an easy, lucrative business likely means that we will continue to see more claims and higher losses resulting from cybercrime in 2018.

In addition, the use of stolen credentials to steal money or gain access to sensitive data will continue to be a common cause of cybercrime in 2018. Here, companies are vulnerable as long as employees use simple passwords or habitually use the same password to login to multiple systems or devices.

Cybercrime Mitigation

The most important aspect of managing the risk of cybercrime is prevention. As noted above, wire fraud initiated via phishing is a common cause of claims, and we expect this to continue. However, there are steps a company can take to avoid it.

Cyber Security Best Practices

Multi-factor Authentication

One critical security measure against phishing schemes is the implementation of a multi-factor authentication protocol for wire transfer requests. In other words, using a phone call, text message, fax, or another method of confirming a user's identity before processing a wire transfer request or a request to change account information is an essential tool in the prevention of cybercrime.

Software Updates

Companies should always keep software up to date, including antivirus software, application software (especially web browsers) and operating systems. In addition, companies should stay up to date on informational advisories and formal notices from service providers, including SaaS, PaaS and IaaS providers, and act accordingly. Notably, in 2017, Amazon Web Services issued twelve security bulletins – which is essentially one per month. Access to data and systems should be limited to those who need it to perform essential job duties. Companies should have policies on what employees can and cannot keep or install on work computers. Spam filters and firewalls are essential, as is scanning all new devices, like USB drives, prior to connecting to a company network.

Employee Training

Also, education of all employees – whether it is the CEO or the receptionist – about phishing is important. Anyone can become a victim, so everyone within an organization 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.

Password Management

Enforcing a strong, effective password policy is critical to cybersecurity. Employees are often told not to reuse passwords, but the practice remains prevalent. Passwords should be complex, have at least eight characters, and include capital and lower case letters, number(s) and symbol(s). A password should not contain birthdays, phone numbers, or names of friends, pets, or TV characters.

At least every four months, passwords should be changed. Also, passwords should not be revealed to anyone, including assistants or managers. If a password is written down, it should not be stored near a device. Also, employees should not use the "remember password" feature of web browsers.

10 STEPS TO REDUCING CYBERCRIME

- Require two-factor authentication for access to email from the internet
- Prepend a marker (e.g., "Subject: [External] ... ") to the subject line denoting externally originated emails
- Require Virtual Private Network (VPN) access for telecommuters
- Monitor corporate and guest network activity
- Keep tabs on sensitive data & regularly monitor events and logs
- Establish a Data Classification Policy and limit printing copies
- Provide employees with travel devices that can be rebuilt upon return, limit access from these devices
- Encourage traveling employees to note travel device usage times and locations
- Do not grant employees administrative access to their devices

Verizon. (2017). *Data Breach Digest.*

References

Amazon Web Services . (2018, 04 16). Latest Bulletins. Retrieved from Amazon Web Services (AWS): https://aws.amazon.com/security/security-bulletins/

Anti-Phishing Working Group. (2017). *Phishing Activity Trends Report 3rd Quarter 2017.*

CISCO. (2018). *CISCO 2018 Annual Cybersecurity Report.*

Experian Data Breach Resolution. (2018). *Data Breach Industry Forecase 2018.*

Insiders, C. R. (2017). *Ransomware 2017 Report*. Sponsored by Bitdefender.

Kubecka, C. (Q4 2017). *State of the Internet - Security.* Akamai.

Lewis, J. (February 2018). *Economic Impact of Cybercrime - No Slowing Down.* McAfee & CSIS (Center for Strategic and International Studies).

Palmer, D. (2017, September 22). *1.4 million phishing websites are created every month: Here's who the scammers are pretending to be.* Retrieved from ZDNet: http://www.zdnet.com/article/1-4-million-phishing-websites-are-created-every-month-heres-who-the-scammers-are-pretending-to-be/

Poneman Institute and Accenture. (2017). *2017 Cost of Cybercrime Study, Insights on the Security Investments that Make a Difference.*

Steve Morgan, Cybersecurity Ventures. (2017). *2017 Cybercrime Report.* Herjavec Group.

Telecoms.com. (n.d.). *Telecoms.com Intelligence Annual Industry Survey 2017.* telecoms.com Intelligence in partnership with Heavy Reading.

The Council of Economic Advisers. (2018). *The Cost of Malicious Cyber Activity to the U.S. Economy.*

Verizon. (2017). *Data Breach Digest.*

---

[i](Lewis, February 2018, p. 4)
[ii](Kubecka, Q4 2017, p. 18)
[iii](Lewis, February 2018, p. 4)
[iv](Steve Morgan, Cybersecurity Ventures, 2017, p. 9)
[v](CISCO, 2018, p. 21)
[vi](Kubecka, Q4 2017, p. 25)
[vii](Poneman Institute and Accenture, 2017, p. 17)
[viii](Poneman Institute and Accenture, 2017, p. 20)
[ix](Poneman Institute and Accenture, 2017, p. 20)
[x](Steve Morgan, Cybersecurity Ventures, 2017, p. 10)
[xi](Amazon Web Services , 2018)