2020 Cyber Digest

ANALYSIS OF 2019 CYBER CLAIMS DATA

TOKIO MARINE
HCC

Cyber & Professional Lines Group

tmhcc.com/pro

Introduction:

Throughout 2019, cyberattacks continued to be of primary concern to business leaders in all sectors. Increased sophistication of cyber criminals, a growing base of connected devices (aka, "the attack surface"), and human vulnerability all contribute to a business environment rife with cyber security risk that continues to be exploited by criminal actors.

In 2019, we saw that the activity (and expense!) of cyberattacks on our policyholders continued to shift from 'data breach' to 'cybercrime.' While phishing attacks, fraud, and ransomware are all on the rise, there was a decline in data breaches, exposure of personal information and related notification expenses.

Small to mid-sized businesses (SMB), the core of our commercial cyber business, continue to suffer from increasing attacks via email phishing and socially-engineered fraud activities. This follows broader industry trends, as well. According to Verizon's annual Data Breach Investigation Report (2019), 43% of all attacks target the small to mid-sized business sector. And these events, on average, cost small businesses $3 million *(Ponemon, State of Cybersecurity in Small & Medium Size Businesses report).*

The commercial cyber business at NAS/Tokio Marine HCC continued to expand in 2019. While we wrote approximately 12,000 individual businesses for cyber liability exposure, we also provide cyber cover as an endorsement for over 500,000 small businesses, physician's offices, and other healthcare-related facilities. With the growth of our cyber underwriting, we've also seen an increase in claims activity (as would be expected). With data on over 2,200 closed claims in 2019, we see some disturbing trends that we break out into "Healthcare" and "Non-healthcare" segments in the report that follows.

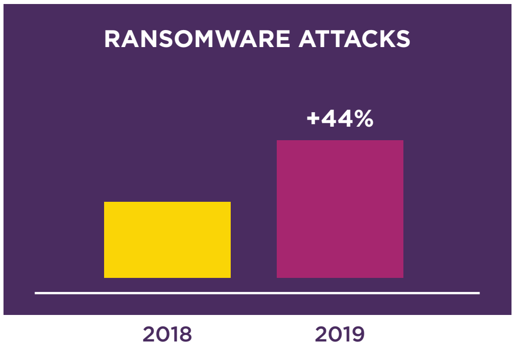
7x GROWTH IN PHISHING ATTACKS

among non-healthcare policyholders and 6X among healthcare-related businesses

If there was a theme for 2019 cyber claims, it would be the growth of phishing attacks on small to mid-size businesses. Ransomware and financial fraud claims were up across the board vs 2018 and, largely, initiated through phishing attacks. Though the larger cyber incidents at Facebook, Citrix, and Capital One grab the headlines, the rampant attacks on small and mid-sized businesses are devastating as most SMBs don't have sufficient resources to prepare nor defend themselves. A recent Fundera study reports that "3 out of 4 small businesses don't have the personnel to address IT security."

What were the top causes of cyber incidents among SMBs?

Among our non-healthcare policyholders, 2019 saw a significant 44% increase of ransomware claims vs. 2018. And, for the first time in five years of tracking, "Ransomware" is the number one cause of loss in the non-healthcare segment.


RANSOMWARE ATTACKS

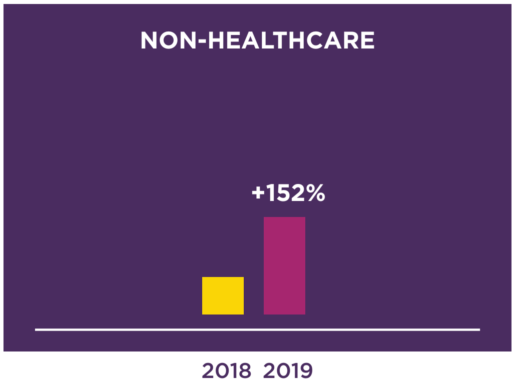
CAUSE OF CYBER LOSS
NON-HEALTHCARE

	2018	2019
Most Common Cause	Hacking Attack	Ransomware
2nd Most Common Cause	Ransomware	Hacking
3rd Most Common Cause	Phishing	Employee Negligence

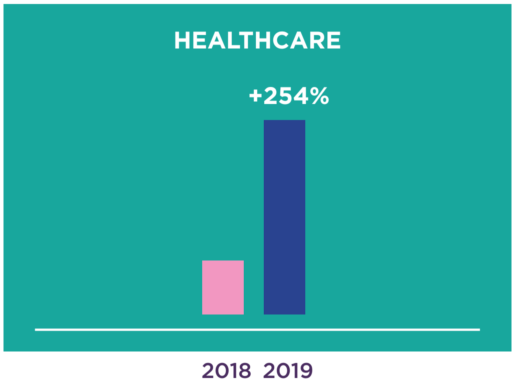
RANSOMWARE SCENARIO:
The assistant manager at a restaurant downloaded an email attachment that appeared to be a spreadsheet from her manager onto the store's computer. The file contained the 'Ryuk' virus which blocked access to the operating system and encrypted all the files on the computer. The usual desktop was covered by a message that notified him that the system and all files were encrypted and would only be unlocked if he paid a 'ransom' using BitCoin. The demands for ransom were in excess of $200,000.

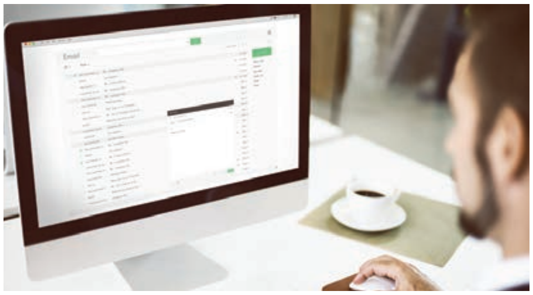
Whether through wire transfers, fraudulent payments or unauthorized access to financial accounts, cybercrime activities were up significantly on all sectors of business in 2019.

CYBERCRIME CLAIMS IN OUR NON-HEALTHCARE SEGMENT SAW A 152% INCREASE OVER 2018



CYBERCRIME CLAIMS IN OUR HEALTHCARE SEGMENT SAW A WHOPPING 254% INCREASE OVER 2018





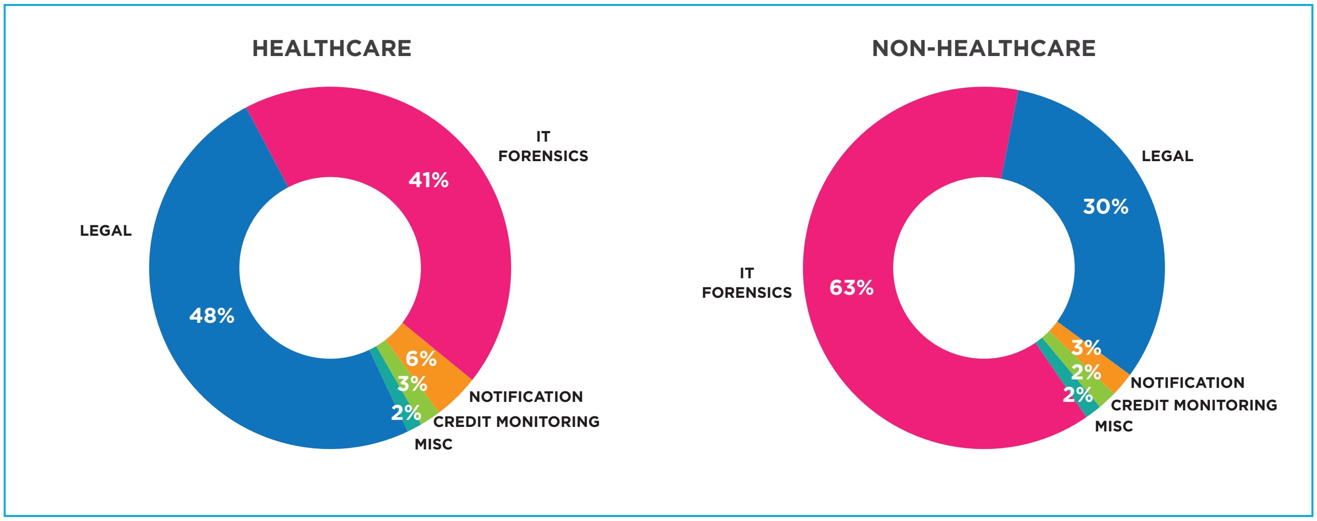
CYBERCRIME CLAIM SCENARIO

An accounts payable associate at a small manufacturer had received an email from the CFO with a few updates about several of their suppliers. In addition, there was an attached invoice with wiring instructions for one of their suppliers referenced in the email. The CFO had asked the associate to please make prompt payment. The associate, eager to please his boss, processed the payment.

Unfortunately, the email was not actually from the CFO, but a cybercriminal impersonating her and using a very similar looking email account. The attached invoice included wiring instructions and thus funds were sent to the criminal's offshore bank account.

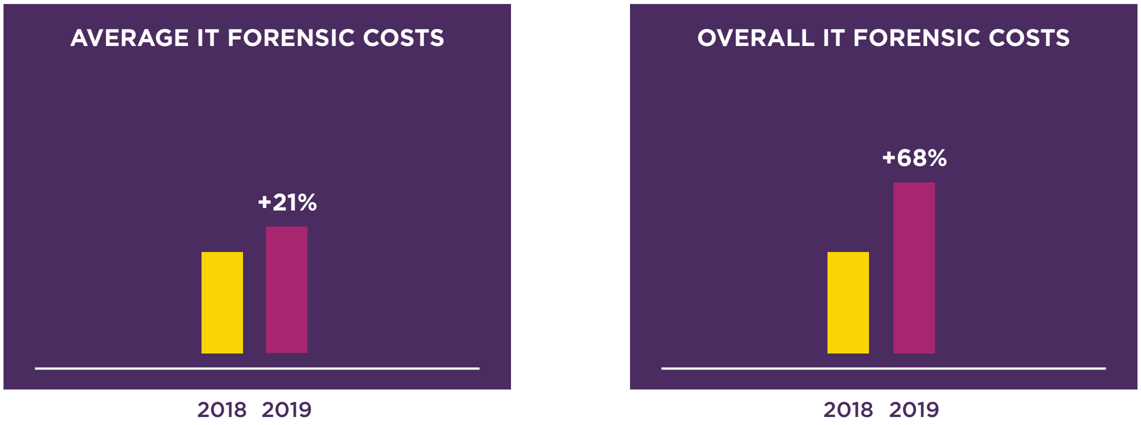
Costs of Cyber Claims 2019:
Expenses related to cyberattacks vary greatly between our "Healthcare" and "Non-healthcare" policyholders. The following illustrates how the expenses to respond to a cyberattack differ.

COSTS OF CYBER ATTACKS 2019



The expenses for IT-related services skyrocketed in 2019
Especially for our non-healthcare policyholder claims, IT Forensics costs, overall, were up 68%, while the average IT Forensic costs were up 21% vs 2018.

2019 NON-HEALTHCARE IT FORENSIC COSTS



What were the top causes of cyber incidents among healthcare-related policyholders?
For the second year in a row, employee negligence tops the causes of loss among our healthcare policyholders, with Ransomware and insider threats continuing to plague physicians, medical groups and other healthcare facilities.

CAUSE OF CYBER LOSS: HEALTHCARE

	2018	2019
Most Common Cause	Employee Negligence	Employee Negligence
2nd Most Common Cause	Ransomware	Ransomware
3rd Most Common Cause	Rogue Employee	Rogue Employee

Taking Action in 2020

While the cybercriminals continue to increase the frequency and sophistication of their attacks, business owners are also becoming more knowledgeable and prepared to defend themselves and their organizations. While cyber insurance is one effective means of mitigating risk, there are new tools, processes and technologies that small businesses can employ to protect themselves.

FIVE STEPS TO FIGHTING RANSOMWARE AND BUSINESS EMAIL COMPROMISE

1 Enforce Two-Factor Authentication For Secure Application Access

2 Implement Online Data Backups

3 Deploy Spam Filtering & Email Configuration

4 Install Next Generation Anti-Virus: Behavior-based Protection

5 Conduct Employee Anti-phishing training

For best practices to fight cybercrime, download our Ransomware & BEC Fact Sheet. For more information about this 2019 Cyber Claims Digest or about our Cyber Liability Insurance solutions, please visit us online at **tmhcc.com/cyber**