MARSH JLT SPECIALTY

INSIGHTS | JUNE 2020

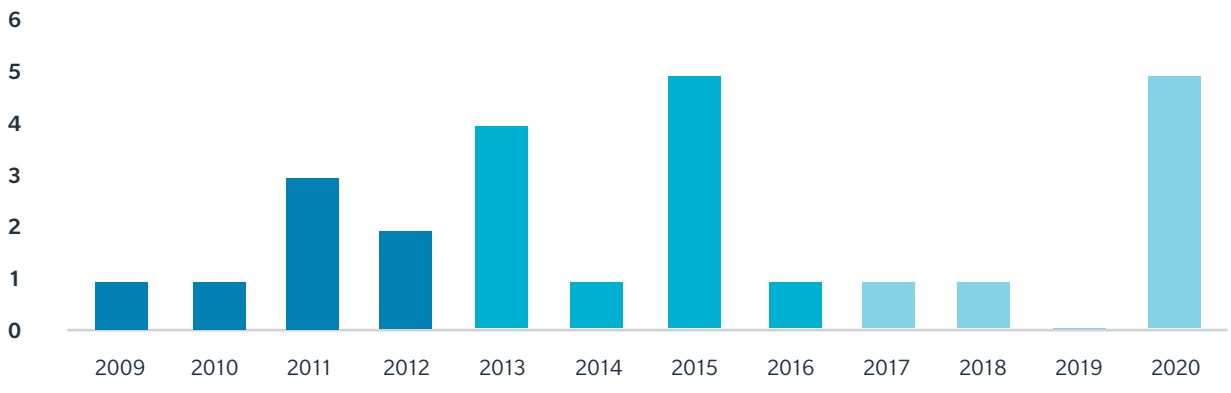
Crime claims on the rise — what to do about it

We are living in the cybercrime era — from phishing scams, fraudulent bank transfers, to impersonation scams, companies are facing increased threats from known and unknown actors. In this report, Marsh-JLT Specialty focuses on Cyber-related crime, its growth over the last five years, and (more importantly) how to mitigate the risks faced by businesses.

Volume of Crime claims have increased

By analyzing notifications filed with insurers under Singapore-placed Commercial Crime Policies over the last decade, we have found that the rate of notification for 2020 (January to May) has already matched 2015's high of five notifications for the opening half of a year. This is a sizeable shift in the trend from the last four years — from 2016 to 2018, we only recorded one claim in the first half of each year, and we reported no claims in the same period for 2019. A vast majority of this year's notifications were in relation to Cyber-related crimes.

FIGURE 1 No. of crime notifications filed in the opening half of a year



MARSH

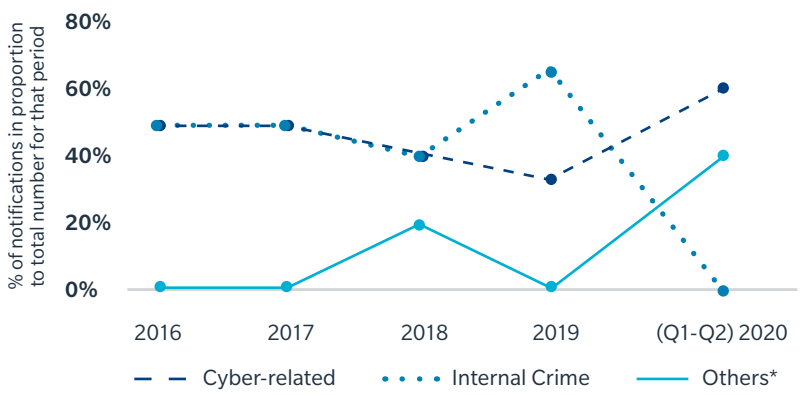
Cyber-related crimes on the rise in 2020

There is a distinction between Cyber-related activities, which would be covered under a Cyber Policy (e.g. theft of data, rectification of network breaches, etc.), and crime activities resulting in loss of funds which would be covered under a Commercial Crime Policy. For the avoidance of doubt, this document exclusively discusses "Cyber-related crime". Such crimes include "Computer Fraud" (e.g. fraudulent electronic transfers) and "Social Engineering Fraud" (e.g. impersonation fraud).

In the first five months of 2020 alone, there has been an almost 30% increase in the number of Cyber-related crimes compared to 2019 — forming 60% of all notifications filed in 2020 year to date. Similarly, clients should also be aware that the rate of employee-perpetrated crime ("Internal Crime") remains high — with the number of Internal Crime notifications reaching an all-time high in 2019.

FIGURE 2

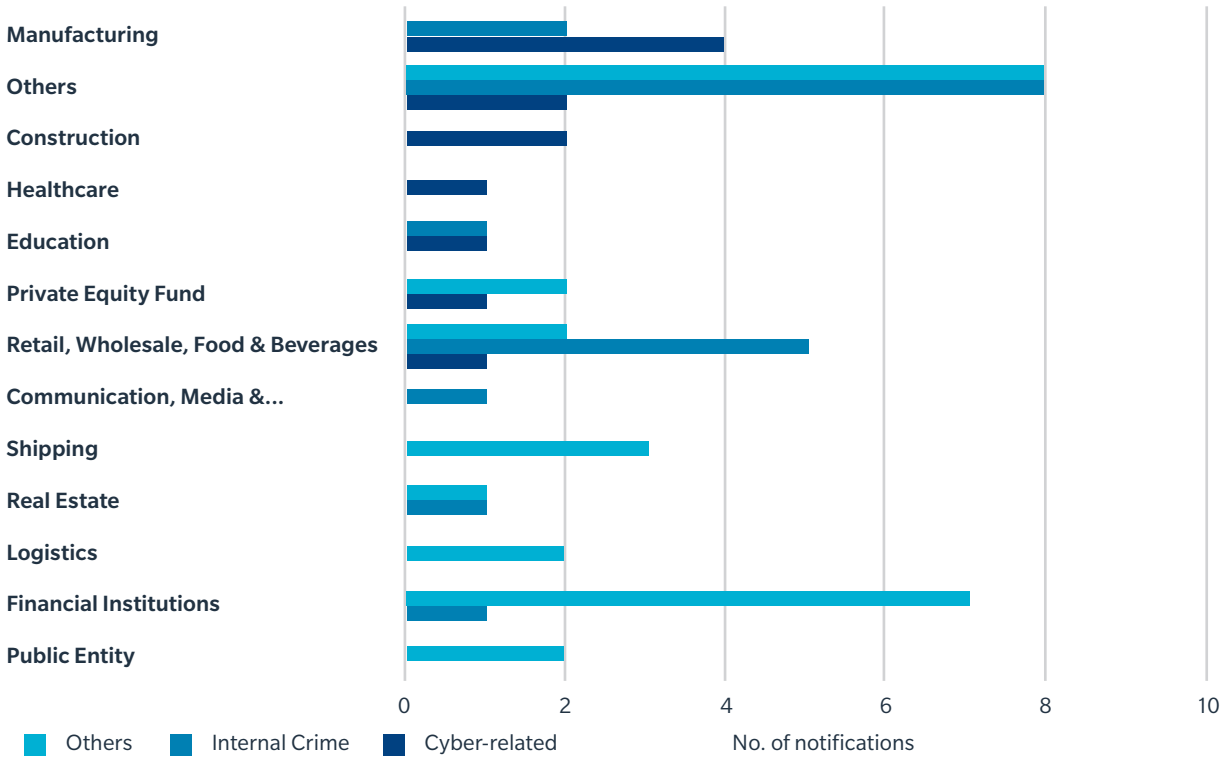
Type of crime notifications over the last 5 years



*This category includes crimes like theft, damage to property, forgery, and/or fraudulent alteration.

FIGURE 3

Types of crime claims by industry



Operations with less focus on internal compliance processes enable a higher rate of Internal Crime

Clients in Retail, Wholesale, and Food & Beverages reported the highest number of Internal Crime. The common thread for the above-identified sectors was that these companies tend to be business-to-consumer entities, with more employees on the ground handling cash. It is arguably harder in these cases to monitor internal controls and maintain record-keeping, allowing criminals to abuse the loopholes from within these companies.

Manufacturing clients suffer the most Cyber-related crimes

Based on our statistics, we found that the Manufacturing industry reported the highest number of Cyber-related crime by far. It is probably due to companies in this sector having several vendors across the world (as they source for raw materials across a varied number of suppliers) as well as having broad base of international customers, which make them more susceptible to such crime.

Listed companies vs. Private companies

It is interesting to note that Private companies reported an overwhelming majority, i.e. 77%, of Cyber-related crime. Public companies plausibly employed more sophisticated IT security infrastructure than the former. That being said, greater vigilance does not necessarily translate to less crime — we discovered that reports of Internal Crime are actually more prevalent in Public companies than Private companies. One reason for this could be that Public companies are consistently performing internal audits as mandated by the listing authorities' regulations. This does contribute to an increase in the number of reports of suspicious activity within the company, as it could allow for a greater proportion of crime committed to be uncovered.

FIGURE 4 No. of notifications by company type

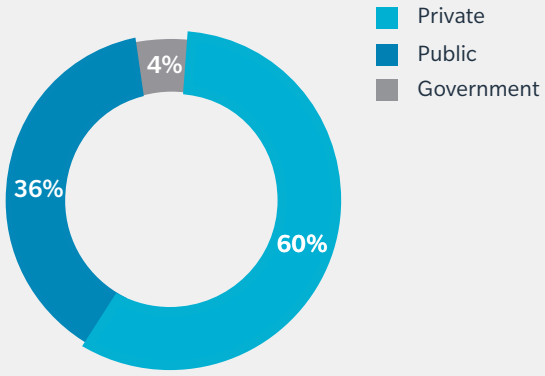
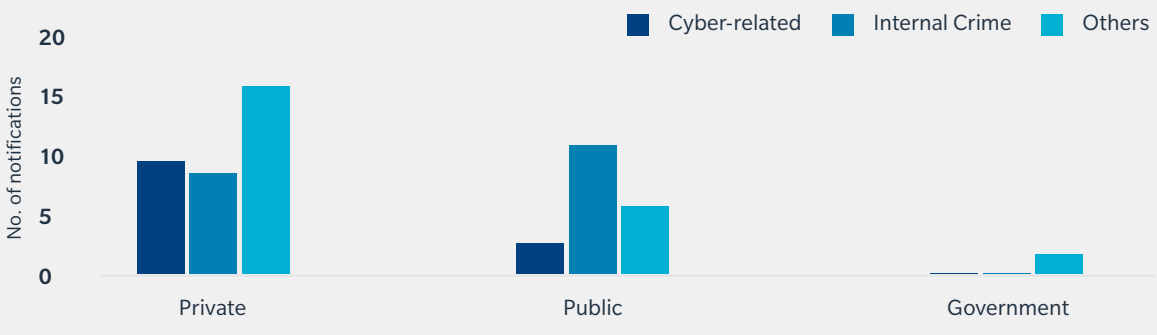


FIGURE 5 Composition of notifications by type of crime



What can a Commercial Crime Policy do for your business?

While strong internal protocols can help a company in reducing the probability of fraud, dishonest employees and external fraudsters can still circumvent the security of even the most well-regulated companies or the most robust controls, leading to potentially substantial financial losses. This can be financially devastating for companies and/or cause severe reputational harm, making Commercial Crime insurance an essential part of a company's defense.

In the event that you require an Investigative Specialist to establish the facts and quantum of the loss, insurers would typically reimburse you for such expenses, provided that the fraud is established. Most policies would also reimburse you for any legal expenses incurred in recovering the fraud loss from known perpetrators.

Non-Employees

Usually cover for losses caused by non-employees is more perils based, including:

"Theft", "Damage", and/or "Disappearance"

- Theft, physical loss, damage or actual destruction, or disappearance of the company's money, securities, and/or other property, both on its premises or elsewhere (for example, while in transit).

"Forgery" and/or "Fraudulent Alteration"

- Forgery or alteration of negotiable instruments, including forging an authorized personnel's signature on business checks.
- Receipt of counterfeit currency.

"Computer Fraud"

- Fraudulent manipulation of the computer's computer system, leading to a hacker transferring funds to an outside account.
- Fraudulent electronic funds transfer instructions sent to the company's bank purporting to be from the company, leading to a fraudulent bank transfer.

"Social Engineering Fraud" (as an extension)

- Fraudulent impersonation of an employee/vendor, deceiving and manipulating victims into transferring funds.

Employees

Most Commercial Crime Policies cover the losses caused by any acts of fraud or dishonesty committed by an employee. There is often a coverage requirement for the act to be for personal gain or have an intent to cause a loss to the Company.

Social-Engineering Fraud

This type of fraud refers to fraudulent impersonations of employees (often senior employees) or vendors requesting the company to wire funds or to change the bank account details of a vendor. These fraudsters tend to conduct extensive research on their victims before making the request in order to increase their credibility — often altering legitimate payment instructions to avoid suspicion. Since the perpetrators of social engineering fraud are able to create plausible scenarios, their schemes may not be detected until funds have been wired to overseas bank accounts, limiting the possibility of recovery.

Fraudsters have also for some while been targeting newly-acquired businesses in different countries by impersonating the new parent company "head office" because controls and reporting lines are often changing or not fully formed.

This area is obviously of particular relevance to the private equity and mergers and acquisitions segment.

Insurers in Asia only started offering Social Engineering Fraud cover as an extension approximately 5 to 10 years ago. Prior to that, the Commercial Crime Policy in Asia would not typically be triggered by Social Engineering or Payment Diversion Frauds. As insurers see increasing losses in the recent couple of years, they have begun to expressly exclude these areas, or impose more restrictive sub-limits as a default. We have, however, seen that in some cases (albeit not all), these sub-limits are negotiable subject to the fulfillment of certain conditions. These can include top-up of premiums, or if the organization is able to demonstrate robust preventive measures, for example.

FIGURE 6

Majority of payments are made within 12 months of the date(s) of notification

	<6 months	7-12 months	13-24 months	>24 months
Fraud Loss	29%	29%	33%	9%
Investigation/Recovery Fees	43%	14%	29%	14%

In respect of covered claims, 58% of fraud losses were paid within 12 months of the date of notification. 57% of all costs and expenses (Investigation/Recovery fees) were also paid in that same time frame.

Crime Case Study

Background

A wealth management company, which manages a Private Equity fund, purchased a Commercial Crime insurance policy. The company manages a fund.

The Fraud

Monitoring the way the company instructed its administrators to make legitimate payments, the fraudsters mimicked those and sent fraudulent payment instructions to the administrators. This was not picked up and the administrators emptied the bank accounts of the company, in favor of the fraudsters.

The Phishing Link

Several employees clicked on a phishing link sent by fraudsters to their corporate email inboxes. This allowed the fraudsters to gain access to the computer systems — and monitor it.

The Commercial Crime Insurance Policy

Marsh successfully convinced the insurer that this incident qualified as a Computer Fraud, allowing the company to recover the full amount of loss and also Investigative Specialists' fees.

Check list for filing Claims	
What is the nature of the suggested loss?	Internal Crime? Social Engineering Fraud?
Please provide copies of all relevant documents.	1. Internal investigation reports (e.g. employee statements, findings). 2. Documents related to the incident (e.g. emails, bank transfer receipts). 3. Police Reports (If the incident was reported). 4. External Investigative Specialist report(s) / lawyers' legal advice*. 5. Curriculum vitae and charge out rates for said Investigative Specialists / lawyers*.
What is the chronology of the matter?	1. Date of discovery of the alleged loss. 2. Details of the alleged loss (e.g. location, parties involved, any suspects).
Any potential for recovery?	If you have a suspect in mind, what is the likely outcome/strategy for this? (e.g. Mareva Injunction)

**IMPORTANT: Please be sure to inform us prior to such an appointment so that Marsh can request for the Insurer's written consent. "Prior written consent" is a strict term and condition of the Policy and failing to do so may jeopardize potential coverage of the claim.*

For more information about Commercial Crime insurance and other solutions from Marsh, visit www.marsh.com, or contact the following Financial Lines (FINPRO) / Private Equity and M&A Practice (PEMA) representatives.

AI LING CHEOW
PEMA Practice Leader, Asia
AiLing.Cheow@marsh.com

DANNY WONG
Assistant Vice-President, PEMA
Danny.Wong@marsh.com

GARY CHUA
FINPRO Leader, Singapore
Gary.Chua@marsh.com

PIN LI LIM
Senior Claims Advocate, PEMA / FINPRO
PinLi.Lim@marsh.com

PH20-0989