Chair, GFIA cyber risks working group
Stephen Simchak
American Property Casualty Insurance Association

Making a drama out of a crisis

Cyber crime is increasing as criminals exploit the COVID-19 pandemic

It has become a truism to say that we are in unprecedented times because of the COVID-19 pandemic, but GFIA's cyber risks working group has responded to the new challenges with aplomb.

GFIA recognised early on that the work-from-home environment is amplifying and changing the nature of cyber risks. Cybercriminals quickly realised that the unexpected changes to work environments have created opportunities to obtain sensitive information, eavesdrop on conference calls or virtual meetings, or conduct other malicious activities. Amid an extraordinary rise in cyber attacks and rapid evolutions in the methods of cybercriminals (see Figure 1), many industry watchers have predicted that demand for cyber insurance will increase rapidly.

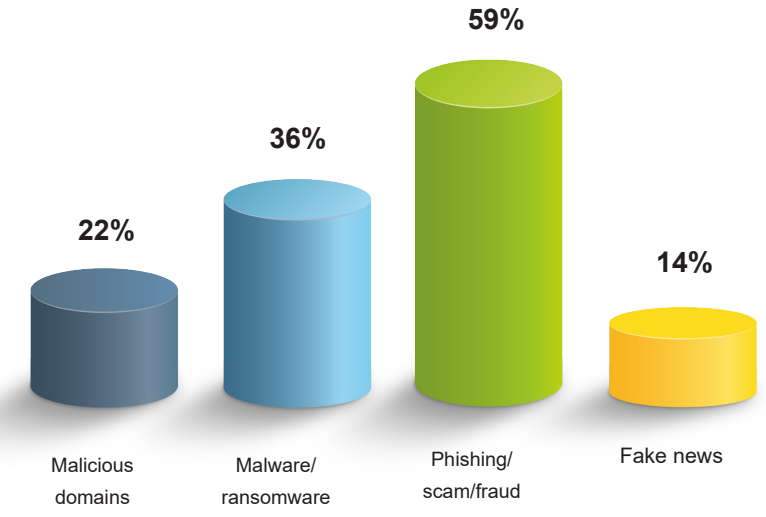
This is unsurprising, as a September 2020 report by S&P Global Ratings estimated that annual cyber insurance premiums globally currently stand at around $5bn, but the yearly costs of cyber crime already exceed $700bn (see Figure 2).

While the actual effects on demand have yet to be seen, there are clear signs that underwriters are tightening underwriting criteria and creating more detailed underwriting processes in response to the growth in cyber

"Annual cyber insurance premiums globally currently stand at around $5bn, but the yearly costs of cyber crime already exceed $700bn."

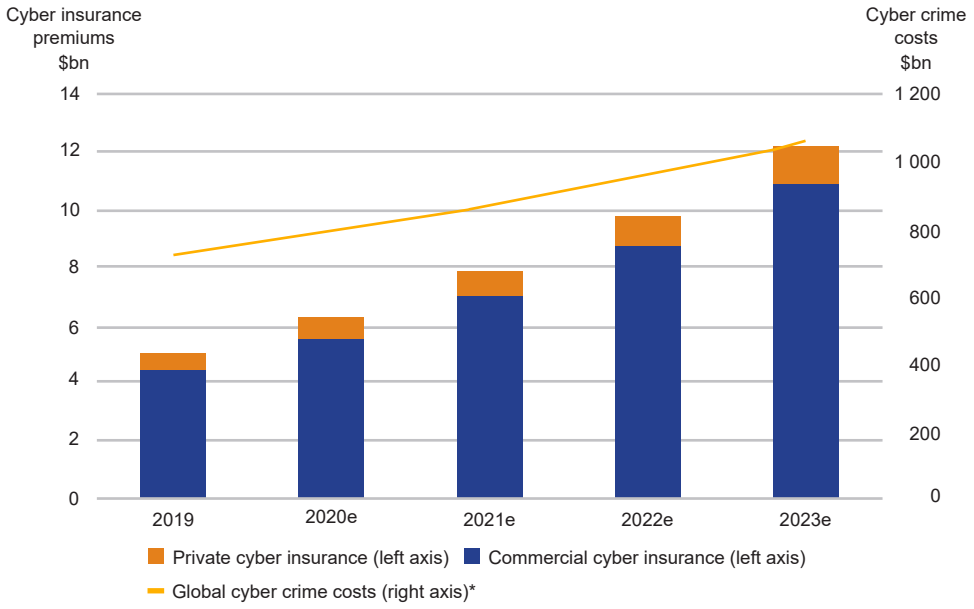
attacks. An increased focus on cyber risks is likely to lead to additional action by governmental authorities, which could have implications for cyber underwriters. GFIA is considering what the pandemic will mean for the supervision of cyber underwriting in the face of increased risks, and whether it will lead to more scrutiny and calls from governments for artificial standardisation.

Figure 1: Percentage of Interpol countries reporting COVID-19-related cyber threats



Source: "COVID-19 Cybercrime Analysis Report", Interpol, August 2020

Figure 2: Forecast growth in cyber crime costs and cyber insurance premiums



* Starting point: $600bn estimate in 2017 by Centre for Strategic and International Studies + 10% growth a year = around $726bn for 2019

e = estimate

Source: "Cyber Risk in a New Era", © Standard & Poor's Financial Services LLC, September 2020

"There are clear signs that underwriters are tightening underwriting criteria and creating more detailed underwriting processes in response to the growth in cyber attacks."

Rethinking awareness campaigns

The new reality of cybersecurity also means that the insurance industry and governments may need to consider changes to cyber education and awareness campaigns as the risks and weak points evolve.

GFIA's cyber risks working group has first-hand experience of this with its study of the different cyber-awareness campaigns that are being conducted around to world. It had planned to release a report on this in 2020. However, since the pandemic hit, GFIA is considering whether the report needs to be updated to reflect the recent evolution of cyber risks and changes in awareness campaigns. It now hopes to release the report by the end of 2020 or early in 2021.

Liaising with international bodies

Beyond COVID-19, this year GFIA has continued its extensive outreach to international bodies that set cyber-related standards. In January, it commented on a draft report by the OECD entitled "The role of public policy in encouraging clarity in cyber insurance coverage".

Among its comments, GFIA pointed out that while alignment of the terminology of risks may be beneficial to help customers better understand cyber insurance, the context of those efforts matters and should not be an opportunity for government regulators to "write the product" or force standardisation.

Recommendations sent to the FSB

In addition, in July 2020, GFIA submitted comments to the FSB on its Consultation Report, "Effective Practices for Cyber Incident Response and Recovery". While GFIA believes that the report offers helpful observations to enhance cyber incident response and recovery, it recommended that the FSB:

- recognises and provides tools for scaling the identified practices;
- takes into account existing regulation by which financial institutions must abide;
- reflects a more appropriate role for the Board; and,
- strengthens the emphasis on cross-border coordination and incident sharing.

GFIA also expects that the IAIS will still release a delayed paper on issues related to cyber underwriting before the end of 2020. The cyber risks working group will be ready to respond when it does.