

Towards a safer cybersecurity environment

Insurance industry cyber-awareness initiatives

January 2021



Introduction

The research that underpins this report was started by the GFIA Cyber Risks Working Group in September 2019 after we realised that there is limited information available publicly on “best practices” in cyber-risk and cyber-insurance awareness efforts around the world.

We therefore set out to catalogue the efforts that insurance industry associations in various countries have undertaken, including information on their goals, communication methods, target audiences and partnerships, and to offer observations on similarities between them. Our hope is that learning about the types of approaches will inspire others to launch or expand their own cyber-awareness efforts and that in doing so we can help make our society safer than it is today.

We initially completed our research in January 2020 but, before we could publish the report, the global COVID-19 pandemic struck. Recognising that the pandemic and the “work from home” environment would have significant implications for cybersecurity and cyber underwriting, we decided to delay publication so that we could conduct additional inquiries into how the insurance industry has adjusted its awareness campaigns.

While it is still too early to know the full implications of the pandemic for cyber-awareness efforts, we have added some initial updates based on an additional survey. Further research on the effects of the pandemic on cyber-awareness campaigns is warranted, however.

Though much more research could be done on how to raise awareness about cyber risks and the role that cyber insurance can play in responding to them, we hope that this will serve as a conversation starter within the industry, in government agencies and in civil society groups around the world.

One conclusion we can draw with near certainty is that cyber-awareness efforts will continue to grow in importance as the size and nature of cyber risks continues to evolve rapidly.

Stephen Simchak
Chair, GFIA Cyber Risks Working Group
January 2021

Contents

Examples of cyber-education and cyber-awareness initiatives

- 4 **Canadian Life and Health Insurance Association**
- 5 **Dutch Association of Insurers (VVD)**
- 6 **General Insurance Association of Japan**
- 7 **General Insurance Association of Korea**
- 8 **Insurance Bureau of Canada**
- 10 **Insurance Council of New Zealand**
- 11 **Insurance Europe**
- 13 **Portuguese Association of Insurers (APS)**
- 14 **Observations on the initiatives**

Canadian Life and Health Insurance Association



The Canadian Life and Health Insurance Association (CLHIA) started its cyber-education work in 2013. The work on cybersecurity at the CLHIA is focused on bringing its member companies together to share threat-level information and keeping members informed of new cybersecurity initiatives by different levels of government.

To support this effort, the CLHIA had formed a Committee on Information Security, which includes key cybersecurity representatives from its member companies. The Committee monitors, discusses and advises on best practices for the industry regarding cybersecurity. In addition, the CLHIA holds monthly security information-sharing calls with member companies to communicate information on best practices and approaches to addressing cybersecurity risks.

Further, as part of the CLHIA's role to assist its member companies in their preparedness for responding to an industry-wide cyber-breach incident, the CLHIA held its first ever industry tabletop exercise in March 2018. The tabletop exercise included representation from a number of its member companies and simulated an industry-wide cyber incident. Following the exercise, the CLHIA and its members developed an industry cyber playbook, which is a framework that provides guidance on how the life and health insurance industry can evaluate and respond to an industry-wide cybersecurity incident.

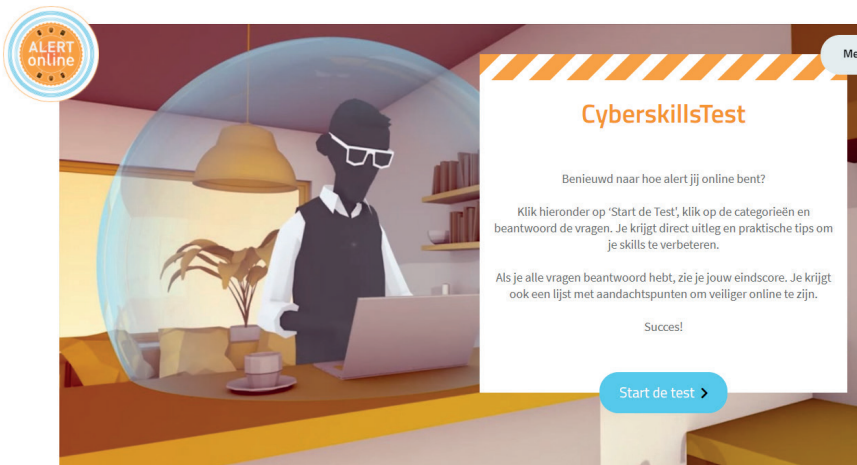


Dutch insurers, together with other stakeholders, take part in “Alert Online”¹, an annual awareness campaign by stakeholders from the public, academic and private sectors to make the Netherlands safer online. Over 170 stakeholders promote cyber-secure behaviour among Dutch consumers, the national and regional governments, small and medium-sized enterprises (SMEs) and other companies, institutions and non-governmental organisations.



Stakeholders organise events throughout the year, but the main activities of the campaign take place in October during European Cyber Security Month. “Alert Online” also publishes the results of its yearly cybersecurity awareness survey² in October. The Dutch Association of Insurers (VVD) has been a partner in that campaign.

While “Alert Online” is mainly focused on addressing cyber risks, through the participation of insurance companies it also touches on the role that cyber insurance can play in responding to these risks.



1 <https://www.alertonline.nl/en/home>

2 <https://www.alertonline.nl/media/Cybersecurity-Bewustzijnsonderzoek-Alert-Online-2018-2.pdf>

General Insurance Association of Japan



The General Insurance Association of Japan (GiAJ) conducted a survey of businesses in Japan in 2018 to measure their understanding of cyber risks, and it used the findings of that survey to present information on a special educational website on cyber insurance³. Using the survey results, the GiAJ was able to target particular shortcomings in the understanding of cyber risks in the business community.

In addition to developing that website, the GiAJ also produces and distributes to businesses leaflets entitled “Cyber Insurance Story”⁴, which contain information about cyber risks and how cyber insurance can help address them.

In early October 2020, the GiAJ launched a survey on “Cyber Risk Awareness and Countermeasures for Domestic Companies”, which aims to understand changes in corporate awareness and behaviour related to cyber risks during the COVID-19 pandemic.

While the GiAJ’s efforts are intended to increase awareness in companies of any size, it has particularly targeted SMEs due to their perceived lower levels of understanding of cyber risks and the relative slowness with which they have taken up cyber insurance.

The Tokyo Metropolitan Police Department partners with the GiAJ in its cyber efforts and the GiAJ tracks the increase in the uptake of cyber insurance policies through its member companies in order to measure the success of its cyber-education efforts.



動画
「サイバースリスクと保険による備え」
を公開中！

動画をみる

³ <https://www.sonpo.or.jp/cyber-hoken/>

⁴ <https://www.sonpo.or.jp/news/notice/2019/ctuevu000000mmq-att/flyer.pdf>

General Insurance Association of Korea

The General Insurance Association of Korea (GIAK) is seeking to raise awareness of cyber risks and the cyber insurance industry by executing a wide range of projects in cooperation with the government, academia and other groups.

While its efforts also include awareness of voluntary cyber insurance, many of its projects are in the context of Korea's compulsory cyber liability insurance mandates. Korean law has required financial institutions to purchase cyber liability insurance policies since 2005. This requirement was extended to credit information companies in 2015 and to certain types of information and communication service providers (eg telecommunications companies and web portal service providers) in 2019.



The GIAK's educational efforts include discussions and seminars with the Korean National Assembly, the Korea Communications Commission (KCC) and the Financial Services Commission (FSC). The information sessions with the KCC and the FSC are intended to update companies of all sizes — from conglomerates to SMEs — about data breach liability coverage and cyber insurance.

The GIAK has supported several renowned professors' research projects on cyber risk. Its work with academia has focused on the introduction of the mandatory data breach liability coverage. Its views are presented to other scholars and the National Assembly.

In addition, educational leaflets (approximately 20 000 copies), posters and video clips were created and distributed in cooperation with the Korea Internet & Security Agency and the Korea Association for ICT Promotion to promote and boost the uptake of cyber insurance.

These projects have been taking place since 2017.

The Insurance Bureau of Canada (IBC) launched a significant public awareness campaign⁵ in October 2019 to educate the SME business sector, given the sector's vulnerabilities to cyber threats as well as the fact that SME businesses make up a significant portion of the Canadian economy. The IBC's communication campaign is specifically geared towards educating SMEs about the risks of cyber attacks, their impact on businesses and risk-mitigation measures.

To prepare for the public awareness campaign, the IBC commissioned a poll in July 2019 to examine how members of Canada's SME community feel about cyber risk as a growing threat. As part of the cyber communications campaign, the poll canvassed several SMEs to gauge their cyber readiness, awareness and interest in risk management. Among other findings, the poll found that of SMEs with fewer than 500 employees, 44% did not have any defences against possible cyber attacks and 60% had no insurance to help them recover from an attack.

Questions about insurance? Call us.

Insurance Bureau of Canada
Toll-free: 1-844-224-IBC (1-844-227-5422)

ibc.ca

- [@insurancebureau](#)
- [facebook.com/insurancebureau](#)
- [youtube.com/insurancebureau](#)

Insurance Bureau of Canada is the national trade association for Canada's private home, car and business insurers.



© 2018 Insurance Bureau of Canada. All rights reserved.
The information provided in this document is a service for informational and educational purposes only. Please consult the appropriate qualified professional to determine if this information is applicable to your circumstances.

10/18

FACTS ABOUT CYBER CRIME



Cyber crime typically involves an attack on an organization's electronic infrastructure and/or gaining unauthorized access to data with the intent of stealing it. These attacks are not only inconvenient and expensive, they can present an existential threat to a business or organization.

Criminal hackers are working around the clock to find new ways of compromising the security systems of organizations regardless of their size. Individuals, complex cyber criminal networks and even foreign governments are engaging in cyber crimes. **No one is immune.**

How big is the problem?

Cyber crime creates problems that are significant and costly.

- ▶ Worldwide, incidents of cyber crime cause **almost \$600 billion in losses every year.**
- ▶ Cyber attacks can be fatal to businesses. **Approximately 60% of small businesses go out of business within six months of a cyber attack.¹**
- ▶ In Canada, the **average cost of a data breach is \$4.74 million.²**
- ▶ Every year, Canada loses 0.17% of its gross domestic product to cyber crime – the **equivalent of \$3.12 billion per year.**

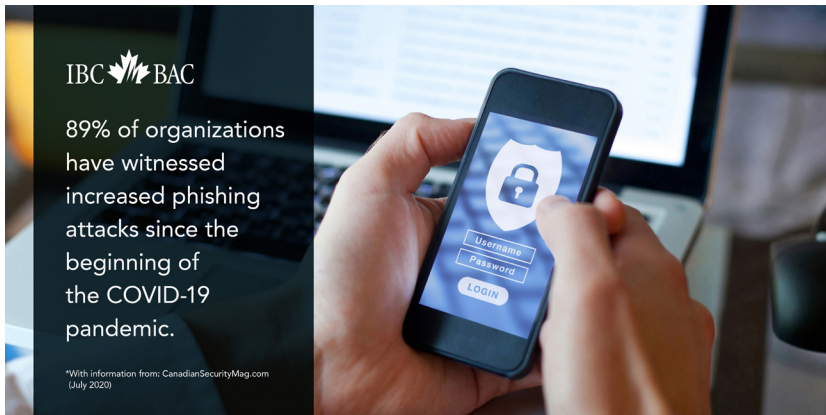
- ▶ In 2016, **fraud accounted for 47.5% of cyber crimes** reported by Canadian police services.³
- ▶ Identity theft and identity fraud accounted for **1.1% and 3.5%** respectively, of cyber crimes in 2016.³
- ▶ The average **data breach detection and escalation cost** in Canada – which include forensic and investigative activities, assessment and audit services, crisis team management and communications and credit monitoring – is **\$1.78 million.⁴**



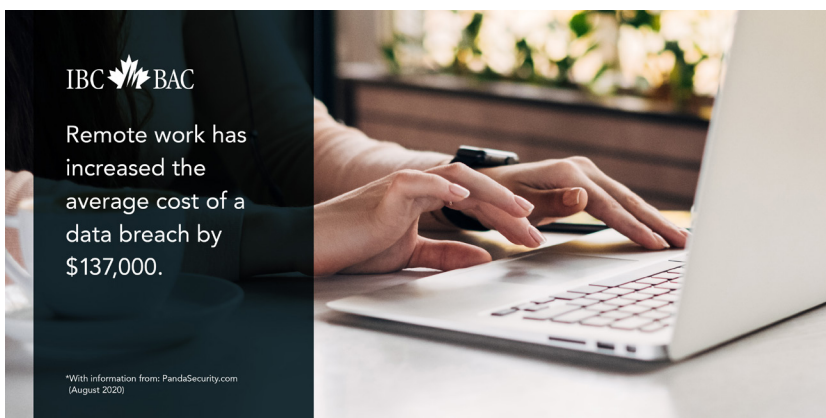
In addition to releasing the results of the SME poll, the cyber communications campaign includes videos and infographics on social media and on the IBC website to provide helpful information to those inquiring about cyber risk and security.

⁵ <http://www.ibc.ca/on/business/risk-management/cyber-risk/cyber-security>

The IBC's campaign also includes substantial media outreach. Since it was launched, the campaign has received a significant amount of traditional and social media attention. The IBC will continue to track and monitor the campaign's reach.



In October 2020, the IBC launched another campaign⁶, again focused on educating SMEs about cyber risk and the benefits of cyber insurance. Because the IBC's resources are now dedicated to COVID-19 issues, the campaign is smaller than the 2019 version.



⁶ <http://www.ibr.ca/on/business/risk-management/cyber-risk/an-increased-threat-during-covid-19>

The Insurance Council of New Zealand (ICNZ) launched an extended effort four years ago to raise awareness of cyber risks and to advocate the benefits of cyber insurance to the business sector. Its main target audiences include boards of directors, SMEs and brokers. Additionally, the ICNZ has engaged in outreach to IT professionals.

As part of its efforts to reach boards of directors, the ICNZ has partnered with the Institute of Directors and provides it with articles on cyber-related issues for its member publications.

Regarding outreach to SMEs and brokers, the ICNZ has held seminars for members of business organisations and brokers and has provided material to both in order to further disseminate information about cyber risks and cyber insurance cover. Having strong connections with brokers is critical because all insurance policies for businesses in New Zealand are brokered, and broker contracts prohibit direct contact between the underwriter and the insured.

Outreach to SMEs is essential because 95% of New Zealand's businesses are SMEs, which in New Zealand are defined as employing 20 or fewer individuals. New Zealand SMEs often lack the dedicated risk management or IT roles of larger companies, which makes cyber preparedness both challenging and critical. Cyber support for New Zealand's SMEs is very often outsourced, which creates the illusion of protection and an impression that little needs to be done. The ICNZ's seminars focused on SMEs seek to dispel those false impressions.

The final group that the ICNZ targets is IT professionals. Members and brokers have informed the ICNZ that there is resistance to insurance at an IT level because they see cyber insurance as a threat to their role within companies. The ICNZ works to dispel this view and instead help IT professionals to understand that insurance is part of effective IT management.

The ICNZ also uses traditional media and social media to convey its messages to a broader audience.



Insurance Europe



In October 2019, Insurance Europe published “Insurers’ role in EU cyber resilience”⁷, which highlights the key role insurers play in assisting the EU in its efforts to increase cyber resilience and competitiveness. The European federation’s publication includes examples of cyber-resilience initiatives by its member associations. Several national associations published cyber insurance guides for SMEs and ran public awareness campaigns for SMEs and brokers to raise awareness of cyber risks and insurance services that mitigate these risks. Some members of Insurance Europe also participate in national cybersecurity centres, where information on cyber threats and intelligence is shared among participants, with other members participating in financial sector-specific information-sharing initiatives.



With the entry into force of the European Union’s General Data Protection Regulation (GDPR) requirements in 2018, Insurance Europe launched efforts to raise awareness among data protection authorities and interested policymakers of the benefits of allowing insurers access to the incident data collected under the GDPR to enable insurers to better understand and quantify cyber risks. To this end, a template for data breach notifications⁸ was developed, with a particular focus on easing the reporting process for SMEs.



Insurance Europe also partners with other groups, including industry groups, at European level to raise awareness of the services offered by cyber insurers, most notably by working on the October 2018 report “Preparing for cyber insurance”⁹. The report was co-authored with the Federation of European Risk Management Associations (FERMA) and the European Federation of Insurance Intermediaries (BIPAR), with contributions from brokers Marsh and Aon, and aims to help organisations that are considering cyber insurance by providing guidance on some of the important questions they need to ask to assess their cybersecurity and insurance needs.

⁷ <https://insuranceeurope.eu/insurers-role-eu-cyber-resilience>

⁸ <https://www.insuranceeurope.eu/template-data-breach-notifications>

⁹ <https://www.insuranceeurope.eu/sites/default/files/attachments/Preparing%20for%20cyber%20insurance.pdf>

During the COVID-19 pandemic, Insurance Europe's members have been active in raising awareness of the cyber risks associated with remote work, including the increased vulnerability of businesses due to the use of private home networks and computers. Several European associations launched campaigns during this period, highlighting the importance of cyber resilience for all businesses, as well as the key role to be played by insurers in the prevention, mitigation and transfer of cyber risk.


Insurance Europe's website¹⁰ carries resources on cyber risks and insurance.

CYBER RISK

Insurers' key role in increasing cyber resilience

Although increased digitalisation has obvious benefits to society, it also brings risks. The potential for serious economic and commercial repercussions, illustrated by events such as the WannaCry ransomware attack, means that increasing the cyber resilience of businesses and society is vital. The COVID-19 pandemic has also demonstrated the importance of digitalisation for societies to be able to operate and the need for this environment to be safe.

Insurers have a key role to play, not only in providing insurance cover, but also in helping their clients prevent these risks and mitigate their impact when they materialise. Their advice on prevention and mitigation builds on many years of insuring other large and multifaceted events, such as natural catastrophes.




CYBER RISKS
"A challenge & an opportunity"
by Nicolas Jeanmart
Insurance Europe Annual Report 2019-2020

Insurers' own cybersecurity

However, as insurers, too, embrace the digital transformation, they must also make sure that they do so in a safe way. To strengthen the cyber resilience of the industry, Insurance Europe calls for a risk-based set of rules that insurers can tailor to the risks to which they are exposed and the systems and services that need to be protected and maintained. In the same way that insurers' use of information and communications technology (ICT) is proportionate to their needs, so too must be the rules addressing their security.

PUBLICATION



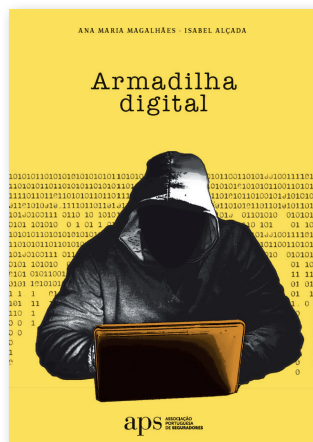
INSURERS' ROLE IN EU CYBER RESILIENCE

- Development of the cyber insurance market ✓
- National insurance association initiatives ✓
- Data breach notification template ✓

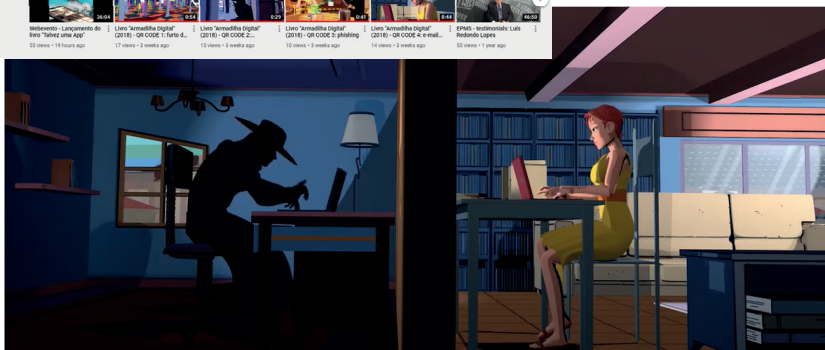
¹⁰ <https://www.insuranceeurope.eu/cyber-risk>

Portuguese Association of Insurers

The Portuguese Association of Insurers (APS) launched a programme for young students (12–16 years) to raise awareness of cyber risks. The Association edited a book entitled “Digital Trap” (“Ardilha digital”), which revolves around the Ventura family: Abel, the father, is the owner of a travel agency; daughter Beatriz is a student; and Aunt Aline, owns a ticketing company. Characters from the National Unit for Fighting Cybercrime and Technological Crime of the Portuguese Criminal Police also appear, presenting many concepts and risks from the digital world. The “Digital Trap” includes a leaflet with 4 QR codes linking to videos¹¹ on specific cyber crimes: identity theft, card cloning, phishing and email scams.



The book is part of a larger collection of financial education books, “Insurance and Citizenship”, that is edited and distributed by the APS as part of its efforts to educate the public on key insurance issues.



11 See <https://youtu.be/vaHBr2t7378> (identity theft); https://youtu.be/Ld_oClpUrFQ (card cloning); <https://youtu.be/xDl4p4f4R60> (phishing); https://youtu.be/j_xPHQu6P4c (email scam)

Observations on the initiatives

- While all the associations had a range of target audiences for their efforts, they shared a focus on SMEs. Because they are smaller, SMEs often lack in-house cyber expertise, which leaves them without a full understanding of cyber risks and, therefore, particularly vulnerable. As a result, they stand to benefit most from cyber-awareness/education campaigns.
- Several associations noted the importance of their outreach to brokers, which are an important link in reaching SMEs. In some cases, GFIA members had formal relationships with brokers to produce written reports and information that would benefit SMEs in considering their cyber insurance needs (for instance the report authored in part by Insurance Europe). As well as partnerships with brokers, some GFIA members focused aspects of their educational campaigns on brokers.
- In addition to efforts to raise awareness within government agencies, partnerships with government agencies are also a feature of some cyber-awareness efforts. For example, the ICNZ co-hosted a seminar with New Zealand government agencies and supported its Cyber Emergency Response Team (CERT) in conducting a “cyber awareness month”. Similarly, in Korea, the GIAK has strong partnerships with the National Assembly and government agencies to raise awareness of cyber insurance in the context of Korea’s mandatory cyber insurance.
- While traditional media, including press releases and interviews, is part of the overall effort, social media and the publication of materials on websites are increasingly seen as cost-effective and efficient communication tools.
- The month of October, which is a “cyber security awareness month” in many jurisdictions, features heavily in the plans of GFIA members’ cyber-education efforts.
- Many of the activities that insurance associations have undertaken did not require substantial additional funds beyond existing employee salaries and resources. An exception is the poll commissioned in Canada by the IBC.

- The most common metrics for measuring the success of these efforts are to track new purchases of cyber insurance and direct polling. One topic for further research could be to identify and analyse the most effective metrics.
- Most cyber-education efforts undertaken by GFIA members are relatively new, generally having been launched within the past five years.
- COVID-19 has changed cyber-education efforts to some degree because of the increased risks associated with the “work from home” environment. At this point, GFIA members that have pivoted their cyber-education campaigns to pandemic-related cyber risks are focused on understanding the increased risk and the degree of awareness of those risks in the remote work environment. The full effects of COVID-19 on cyber-awareness campaigns is not likely to be known for some time, however. This evolving area will be an important area for further research.

© GFIA

Brussels, January 2021

All rights reserved

Design: GFIA

The booklet “Towards a safer cybersecurity environment” is subject to copyright with all rights reserved. Reproduction in part is permitted if the source reference “Towards a safer cybersecurity environment”, GFIA, January 2021” is indicated. Courtesy copies are appreciated. Reproduction, distribution, transmission or sale of this publication as a whole is prohibited without the prior authorisation of GFIA.

Although all the information used in this publication was taken carefully from reliable sources, GFIA does not accept any responsibility for the accuracy or the comprehensiveness of the information given. The information provided is for information purposes only and in no event shall GFIA be liable for any loss or damage arising from the use of this information.



 www.GFIAinsurance.org

 [@GFIAinsurance](https://twitter.com/GFIAinsurance)

 [Global Federation of Insurance Associations](https://www.linkedin.com/company/global-federation-of-insurance-associations)