

White paper

Personal cyber insurance: Protecting our digital lives



Technology comes with huge advantages for everyday life, but people should be aware that it comes also with significant risks.

Insurance has an important role to play in protecting customers against cyber threats.

We're smarter together

Introduction

As our lives become more digital, so do the risks

It is often said that smartphones are more powerful than the computers used in the NASA 1969 Moon landing mission. The 2KB memory of the Apollo 11's guidance system is tiny compared to today's Apple or Android handsets.

When coupled with always-on internet access, these devices open up a world of possibilities – but many consumers never give their sophistication a second thought.

Technology has become so ubiquitous, it is hard to live without it. It comes with huge advantages, but also risks – and there is an increasing role for insurers to play in protecting customers in the face of cyber threats.

Besides being able to shop whenever and wherever, as well as stream movies and music, the digitisation of the personal space has many other, more tangible, benefits too.

Globally, more than three quarters (76%) of account-owning adults make digital payments and rely on online banking to meet other day-to-day financial needs, such as checking balances ¹.

For millions of people in emerging markets, managing money via a mobile phone has become a lifeline. It has made it possible to send money to friends and family thousands of miles away or make payments for business transactions. These and many other everyday activities would be practically impossible for many people living in remote parts of the world, hundreds of miles away from the nearest bank.

Rapid advances in technology are enabling new services all the time. Smart doorbells let you see who is at your doorstep via an app on your phone. Smart heating and lighting controls let you change the temperature and switch lights on or off remotely. And smart energy metres help you monitor your energy usage and costs in real-time.

All such devices are part of the Internet of Things (IoT), meaning they are connected to and send information via the internet, enabling them to be controlled by phone, tablet, or PC.

By 2023, a typical UK home is expected to contain as many as 50 different IoT connected devices, including games consoles, TVs and set-top boxes, security systems, baby monitors and white goods such as smart fridges ². More than half of the world's households (53.6%) are already connected to the internet ³. In the developed world, it is even higher – 84.4%. In 2012, that figure was just 37.9%. Added to which, the number of smartphones in use is predicted to hit 3.8 billion by 2021⁴.


It may feel like we already live in an interconnected world. But the reality is we are still only in the early days of this new wave of expanded digitisation. There will be an abundance of opportunities to come, but that will also mean a greater need for risk awareness and mitigation.

1 Forbes: Technology Is Delivering Better Access To Financial Services. Here's How
<https://www.forbes.com/sites/worldeconomicforum/2018/04/21/global-findings/#5124c85b1fa0>

2 Total Telecom: EE: Average UK Smart Home will have 50 connected devices by 2023
<https://www.totaltele.com/500103/EE-Average-UK-Smart-Home-will-have-50-connected-devices-by-2023>

3 ICT: Facts and Figures 2017
<https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf>

4 Newzoo: Global mobile market report 2018
https://resources.newzoo.com/hubfs/Reports/Newzoo_2018_Global_Mobile_Market_Report_Free.pdf?submissionGuid=95946481-bfac-478b-bfe5-672a48f72385



Cyber risks
have real
repercussions
for individuals

Emerging cyber risks for individuals

There is always an element of risk in all everyday online activities. But the manner in which individuals conduct themselves online can determine whether they expose them to active threats. That might relate to storing credit card details on a retailer's website or sharing sensitive personal data via an unprotected wireless network, or nonencrypted websites.

But in our increasingly connected world, the risk does not stop just because you switch off your computer or put down your smartphone. It has been predicted that by 2030 there will be around 125 billion IoT devices globally⁵, which represents a huge potential for cyberattacks.

The chances of your smart doorbell or connected fridge being targeted by hackers are relatively slim. However, the more commonplace devices like these are, the greater the inherent risk becomes too. Partly, this could be down to a lack of awareness and understanding of what smart devices are and how they function – does everyone with a connected device stop to think about how secure or otherwise that might be?

In recent years, the phenomenon of ransomware⁶ has become a particularly high profile cyberthreat. Such attacks follow a broadly similar pattern, whereby a website or other online system will be taken over by an attacker who locks the legitimate owner out and demands a ransom. Although it is typically attacks on businesses that have made the headlines, anyone can be a ransomware target.

5 HIS Markit: Number of Connected IoT Devices Will Surge to 125 Billion by 2030
<https://technology.ihs.com/596542/number-of-connected-iot-devices-will-surge-to-125-billion-by-2030-ihs-markit-says>

6 Sophos: After SamSam, Ryuk shows targeted ransomware is still evolving
<https://nakedsecurity.sophos.com/2018/12/18/after-samsam-ryuk-shows-targeted-ransomware-is-still-evolving/>

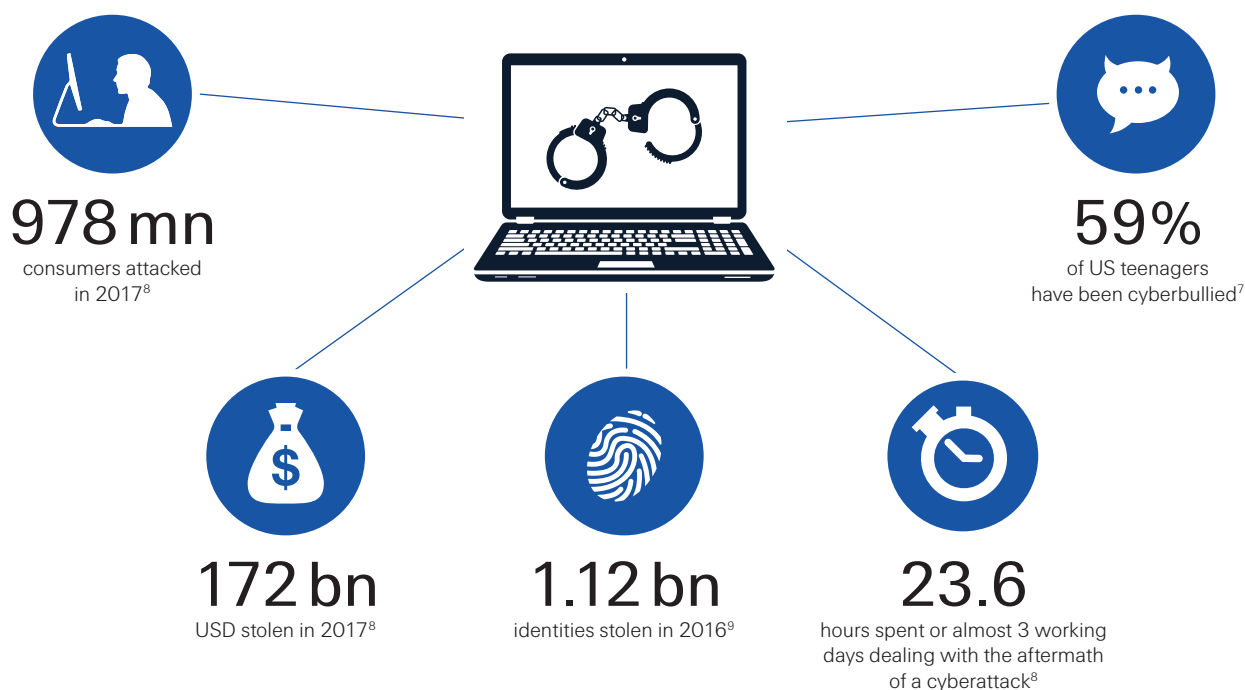
There are other attacks that target individuals more specifically, and which can have profound and distressing consequences.

If a person's bank details are compromised or stolen it can be the start of a series of problems that go far beyond unlawful withdrawal of funds: identity theft. In addition to possibly clearing your accounts out, crooks may use your personal information to open bank accounts or take out loans in your name. While fraudsters abscond with their ill-gotten gains, the individual whose identity has been cloned will be left with the fallout. Frequently this will involve payment default notices and a damaged credit record all of which may only come to light several months after the fraud was perpetrated.

The emotional and psychological harm of falling victim to identity theft can be profound and is not the only example of how our digital lives can start to impact on our overall wellbeing. Cyberbullying and stalking have become all too common parts of everyday life for far too many people, with more than half of US teenagers saying they have been bullied or harassed online⁷.

From identity theft, to hacking of subscription services and IoT home devices, the list of cyber risks people, and not just organisations, are facing is growing all the time as the cyber threat landscape metastasizes rapidly.

Cyber risks have real repercussions for individuals



7 Pew Research: Majority of Teens Have Experienced Some Form of Cyberbullying
<http://www.pewinternet.org/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/>

8 Symantec: Norton Cyber Security Insights Report 2017
<https://us.norton.com/cyber-security-insights-2017>

9 Symantec: Internet Security Threat Report Government
<https://www.symantec.com/content/dam/symantec/docs/reports/gistr22-government-report.pdf>

How consumers can respond to these threats

There are steps every individual can take to protect themselves from these risks. Taking responsibility for one's personal cybersecurity and learning good habits are critical first steps, as are:

- Using unique passwords for every account and choosing passwords that are difficult to guess
- Having up-to-date security software as well as running automated software updates
- Ensuring home IoT devices have security in place
- Banking and shopping via websites with extra security in place like 'https://'
- Only opening email attachments if they come from recognised contacts, and never giving out personal information, logins or passwords in response to emails purporting to come from banks or other organisations
- Regularly backing up valuable data like work files, music, photos and storing it safely



Personal cyber hygiene practices for individuals

There are several useful resources with information and tips and tricks on how individuals can safeguard themselves. Here are a few examples:

HM Government

<https://www.cyberaware.gov.uk/>

BSI für Bürger

https://www.bsi-fuer-buerger.de/BSIFB/DE/Home/home_node.html

SISA

<https://www.swiss-isa.ch/en/>

Stop. Think. Connect.

<https://www.stophinkconnect.org/>

People can respond to cyber threats by implementing personal cyber hygiene

But even the most vigilant and online-savvy people will never be entirely risk-free. This is where personal cyber insurance can help mitigate the risk and transfer the potential for loss from that residual risk. Although not yet widely available, personal cyber insurance is expected to become a fast-growing market segment in the near future due to the rapidly increasing exposures consumers face today.

The benefits of such an insurance product to individuals and families can range from support in improving people's cyber security posture to financial compensation and expert help in the aftermath of a cyber incident. But for insurance companies making the most of the growth opportunity requires developing products that meet the needs of a new generation of digital, connected consumers.

Personal cyber insurance

Where is the consumer cyber insurance need?

Assessing the market opportunity for personal cyber insurance calls for an analysis of many factors. The key one is identifying the customer need.

To that end, Swiss Re conducted a global survey. Here is a summary of the results:

Most feared cyber risk scenarios and coverage needs

The top four cyber risk scenarios that people worry about most are:

- 1 illicit access of financial credentials (a hacker gets access to your online banking details and might therefore be able to steal money)
- 2 identity theft (an attacker steals your digital identity to purchase goods or services online in your name)
- 3 data loss due to a technical issue (your personal data gets deleted by a virus or software glitch)
- 4 illicit publication of personal data (somebody else publishes your private pictures online)

These are the four main areas where customers are receptive to the idea of a cyber insurance policy that will cover them against some of the consequences of these fears coming true.

Most feared scenarios in %



Product characteristics

When we asked people how they would be most likely to buy a cyber insurance policy, there was a rough 60:40 split.

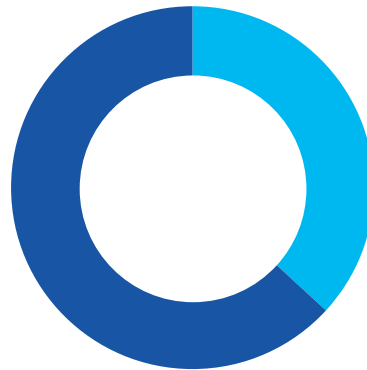
A clear majority of respondents (63%) said they would prefer to buy personal cyber insurance in combination with other products. Natural partners for this kind of bundle would include their home insurance or – if they have one – their private liability policy. Just over a third (37%) would also be interested in looking at standalone personal cyber insurance products.

Preferred structure of cyber insurance in %



63

Add-on to other insurance



37

Standalone cyber insurance

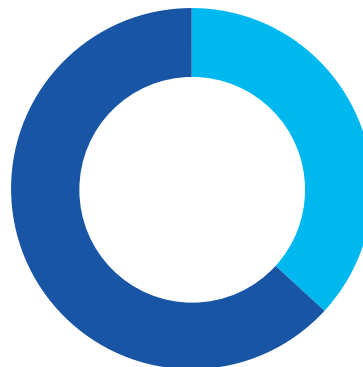
When Swiss Re asked consumers if they would want to choose specific coverage elements for their own insurance policy, a similar split became evident. Those favouring the all-in-one cyber insurance product approach made up 62% of respondents, with 38% expressing an interest in being able to tailor a product to suit their circumstances.

Preferred type of cyber insurance in %



62

All-in-one cyber insurance



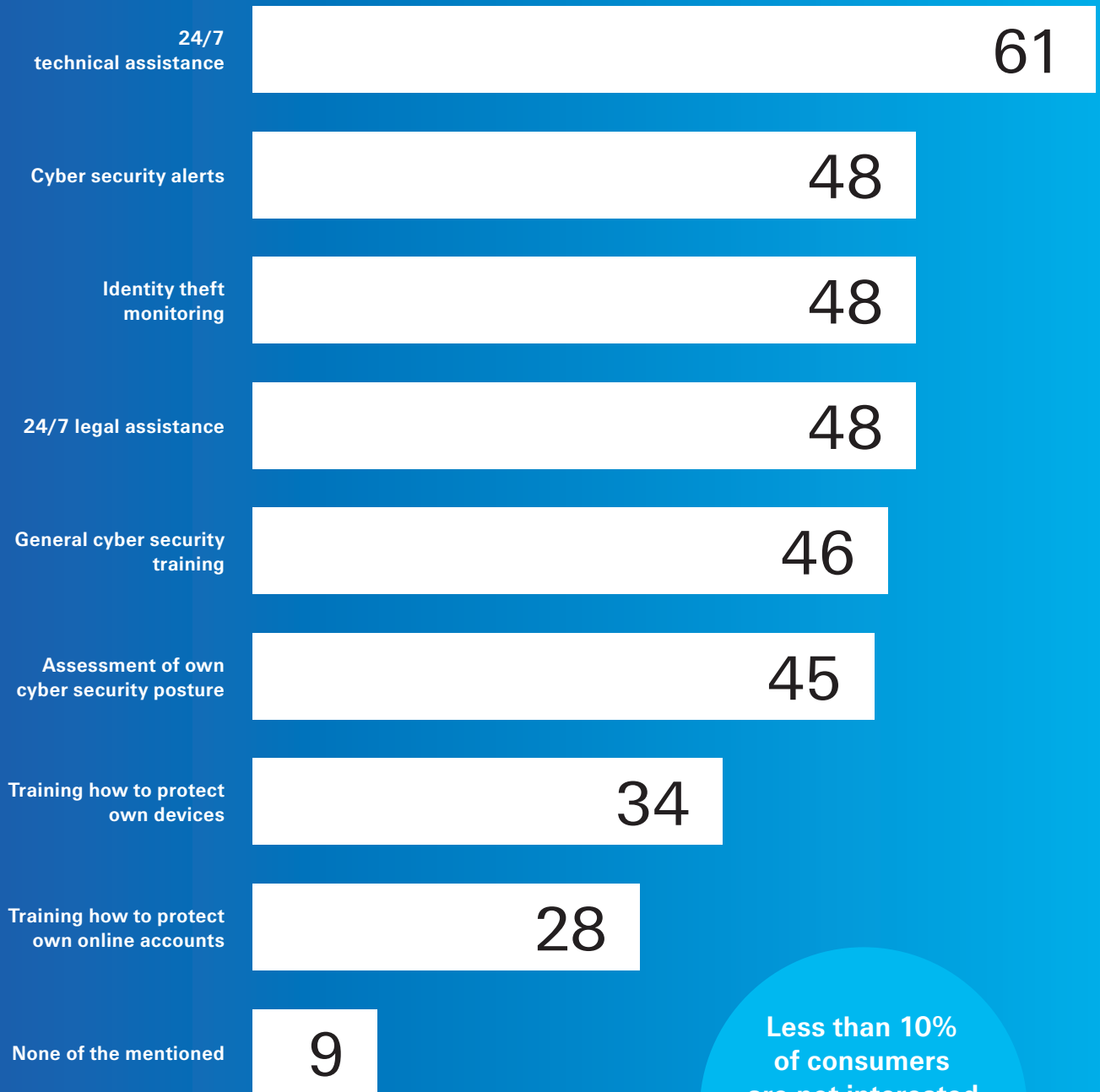
38

Ability to modularly choose cyber insurance coverage

Respondents to Swiss Re's survey also expressed a desire for additional features within cyber insurance products, including 24/7 access to technical assistance, a hotline for legal advice or identity theft monitoring.

Consumer interest in additional services in %

Would you be interested in having additional services offered by a cyber insurance provider aside from financial reimbursement?



Less than 10% of consumers are not interested in assistance and risk management services

More than half of the survey respondents said they would buy personal cyber insurance

Willingness to buy

Overall, when asked if survey respondents would buy personal cyber insurance, 56% of people said they would. As awareness of cybersecurity risk increases, a corresponding increase in interest in cyber insurance could easily be seen in the near future.

When respondents' answers were split along gender lines, a clear difference began to emerge. Almost two-thirds of women said they would buy cyber insurance, whereas just over half of men said they would. There were no age-related attitudinal differences revealed.

Asked why they thought it was unlikely they would buy such a product, respondents' answers centred around two main observations. The first was that the perceived risk of being a victim of a cyberattack is small. The second is that they were not aware of any such products on the market. While the second of those objections will ultimately be overcome by growing availability and better visibility of cyber insurance products for individuals, the former demonstrates the need for further market education.

One well-orchestrated attack on a large business or service provider has the potential to implicate huge numbers of people, significantly amplifying an individual's risk of being harmed by an attack they are not even the specific target of. For example:

2016

Yahoo¹⁰: A series of data breaches dating back to 2013 and 2014 affected the company's entire user base – some three billion accounts.

2017

Aadhaar¹¹: The world's largest biometric database containing the personal information of more than 1 billion people was hacked into. Many of the records were then sold online.

2018

Marriott International¹²: Since 2014, the guest reservation database of its Starwood Hotel subsidiary had been accessed by an unauthorised party. Around 500 million customers were affected.

In an increasingly connected world, is it reasonable to assume you are isolated from risk simply because you are too small to be directly targeted? The answer is clear, but it is yet to be widely recognised by the public at large.

10 BBC: Yahoo 2013 data breach hit 'all three billion accounts'
<https://www.bbc.co.uk/news/business-41493494>

11 Hindu Business: 1bn records compromised in Aadhaar breach since January
<https://www.thehindubusinessline.com/news/1-bn-records-compromised-in-aadhaar-breach-since-january-gemalto/article25224758.ece>

12 New York Times: Marriott Hacking Exposes Data of Up to 500 Million Guests
<https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html>



Username

Password

LOGIN

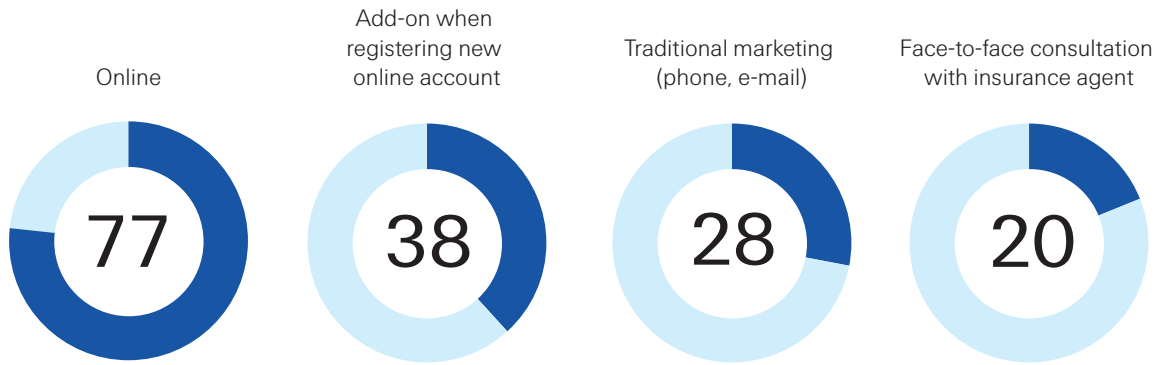
Distribution channels

Perhaps unsurprisingly, the most likely way in which surveyed consumers said they would buy cyber insurance is online. This is a target demographic that uses digital technology, after all. Consequently, 77% of respondents told Swiss Re their preferred channel would be direct online purchase, while 38% said they would prefer to select personal cyber insurance as an optional add-on when registering their new online accounts such as e-banking, mail service or social media.

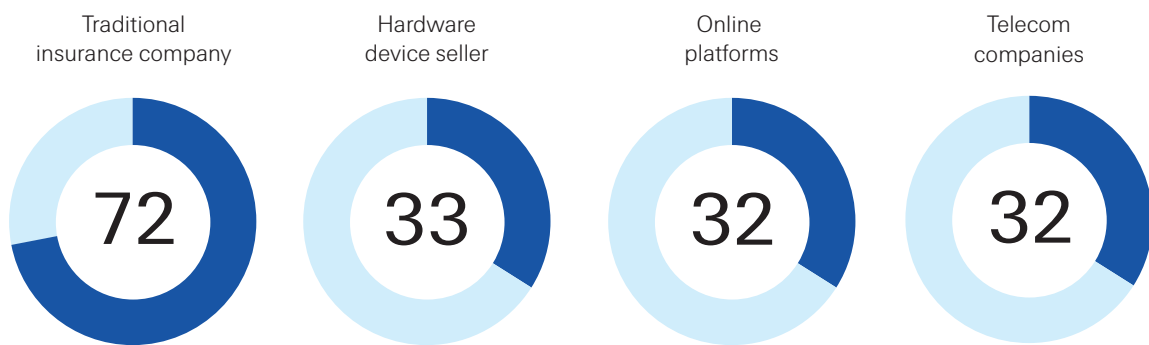
Only one-in-five would prefer a face-to-face consultation with their insurance agent.

The traditional insurance company was named as the most preferred provider (72%) for personal cyber insurance, while roughly one third indicated they would be equally interested in buying their insurance policy via other providers such as hardware device sellers, online platforms or telecom companies.

Preferred way of buying personal cyber insurance in %



Preferred providers of personal cyber insurance in %



Available personal cyber insurance products in the market

While personal cyber insurance is slowly becoming increasingly common, it is still a very long way from being a mass market product, especially when compared with more standard offerings like motor, household or even health insurance.

For the most part, existing personal cyber insurance policies tend to offer first-party covers, to mitigate against financial loss in the event of a cybersecurity problem. Few products provide cyber third-party coverage to protect individuals against liability claims, which they might be exposed to because of their actions or inactions in the digital world. This might include inadvertently forwarding a contaminated email and infecting somebody else's computer with malware.

Anyone caught up in a cyberattack that has involved some sort of financial loss will want their cover to reimburse them. That level of cover is probably going to be regarded as the bare minimum. However, many people will not be able to deal with the complexity of the fallout from a cyberattack alone but need hands-on assistance. Conceivably, that could include the provision of technical help, access to legal support, and possibly psychological counselling too. The addition of features such as this will not only enhance the levels of cover, but will really help illustrate the value such personal cyber insurance policies represent.



Access
to assistance and
services are
key value drivers of
cyber insurance
for individuals

Potential additional services to enrich the risk transfer element

- Access to 24/7 expert hotline who helps policyholders recover quickly from a cyber incident
- Support from IT specialists to clean devices and restore compromised data
- Legal advice and consultation
- Psychological counselling to help with cyberbullying
- Online training where policyholders can learn about how to improve their own cyber security posture

Non-exhaustive list detailing the main and most common features and benefits of personal cyber insurance

Cyber cover	Coverage description	Example scenarios
Financial fraud	<ul style="list-style-type: none"> Reimbursement of financial loss due to unauthorised use of your online payment services. Cover for costs related to blocking and reissuing your payment cards. 	<ul style="list-style-type: none"> You become the victim of an email phishing attack where you voluntarily disclose your e-banking login credentials. This data is used to transfer and steal funds from your online bank account.
Online shopping	<ul style="list-style-type: none"> Reimbursement of the purchase price of goods you bought online but which are not delivered, are damaged during delivery or wrongly delivered. 	<ul style="list-style-type: none"> You place an order on a fake webshop with an identical look and feel to a known retailer. The order you place will never be fulfilled as the entire enterprise is a sham designed to part you from your money.
Identity theft	<ul style="list-style-type: none"> Reimbursement of the cost of rectifying records with banks/authorities and of unpaid leave when you take time off from work to meet with banks/authorities. Costs for a consultant to restore credit records and personal identity. 	<ul style="list-style-type: none"> Your credit card details are stolen and sold on the dark web, following a retailer data breach. This data is then used to fraudulently buy goods in your name. You need to take time off from work in order to rectify the situation.
Data restoration	<ul style="list-style-type: none"> Costs for IT specialist to clean your hardware device of any malware and restore your compromised data. 	<ul style="list-style-type: none"> An infected memory stick transfers malware to your computer leading to loss of or damage to your data. You require the services of an IT specialist to help you isolate and erase the virus and then upload the data from a secure backup.
Cyberbullying	<ul style="list-style-type: none"> Costs to reduce and mitigate the impact of unlawful harassment and/or defamation of you or a family member via online media such as: <ul style="list-style-type: none"> Psychological consultation Legal advice Relocation costs Online reputation restoration where IT specialist tries to remove or suppress the personal content Parent's liability for claims brought against them due to their children's cyberbullying activities. 	<ul style="list-style-type: none"> Your child becomes a victim of a social media cyberbullying campaign, which puts your family under stress. Your child needs professional aid from a psychologist to better deal with the situation. From the discussion, it becomes clear that only moving the family to a new location and school would reduce the stress level. Your child harasses a schoolmate over social media. You risk being the subject of legal action relating to a perceived failure of your duty of supervision.
Cyber extortion	<ul style="list-style-type: none"> Reimbursement of a ransom payment. Costs for IT specialist to mitigate cyber extortion attempt. 	<ul style="list-style-type: none"> By clicking on a malicious link on a website you inadvertently infect your computer with ransomware which encrypts all your data. A demand for ransom money is then received (often asking for Bitcoins) in order to get the key that unlocks your data.
Cyber liability	<ul style="list-style-type: none"> Liability for claims brought against you in connection with your exchange or transfer of electronic data or use of your own IT systems. Liability for claims brought against you in connection with a breach of personal rights and copyrights. 	<ul style="list-style-type: none"> One of your smart home devices has been infected with malware and used as part of an orchestrated cyberattack without your knowledge. You use a copyright protected company logo on your personal blog.

Above cyber covers for individuals are either bundled and sold as standalone cyber insurance policies or combined with other coverages such as homeowner's, private liability or legal protection insurance.

Personal cyber insurance market size

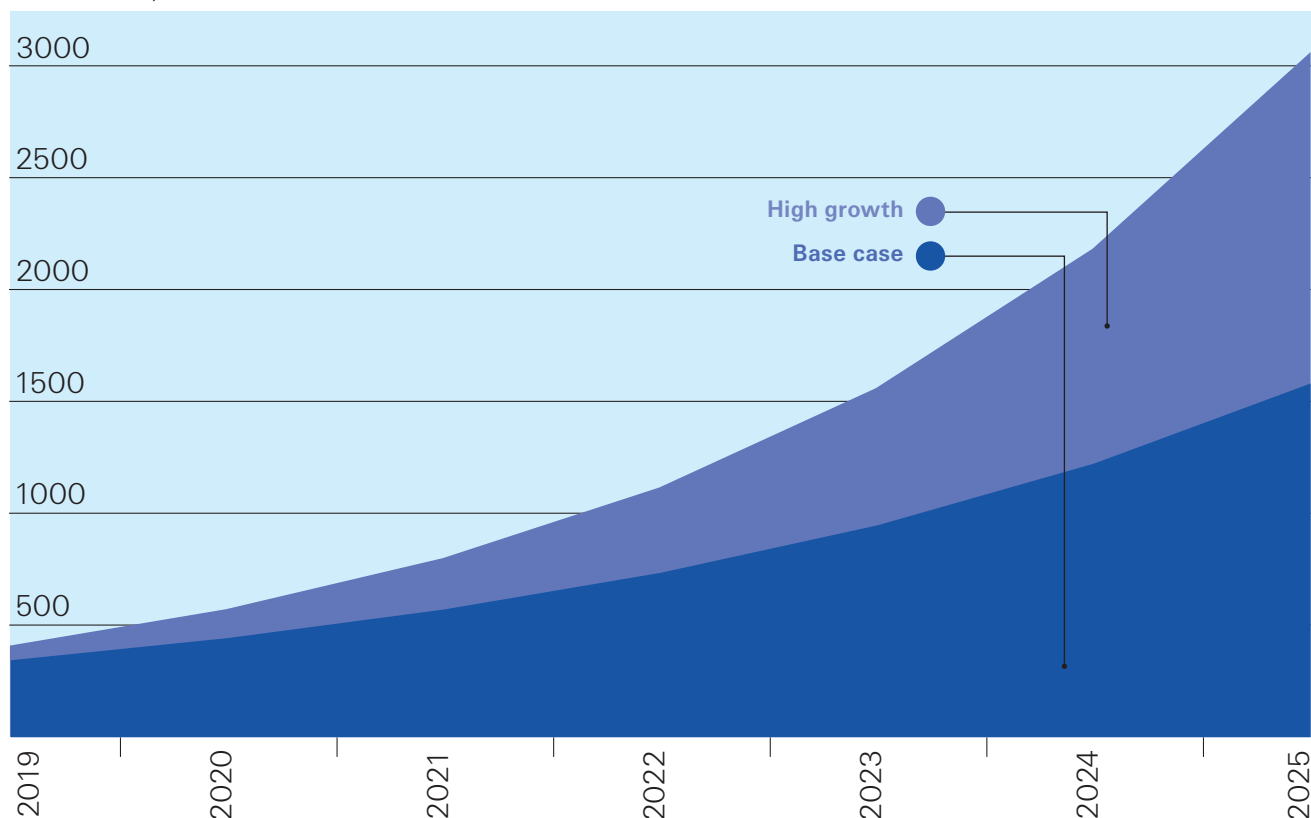
As the global market for personal cyber insurance is still in the early stages of development, there is little data to call upon when discussing its likely growth. However, we can look toward the commercial cyber cover sector for a comparison.

In 2018, the worldwide market for standalone commercial cyber insurance is estimated to be around USD 4 billion to USD 4.5 billion. There is widespread industry consensus that the market will grow with annualised double-digit rates to between USD 7.5 billion and USD 10 billion by 2020¹³.


While its development is lagging that of the commercial sector, we would expect a similar growth trajectory in time as products achieve more maturity and become more widely available. Although the size of the market is hard to estimate, our analysis leads us to believe the worldwide market for personal lines cyber insurance could reach between USD 1.6 billion and USD 3.1 billion by 2025.

Personal cyber insurance market size estimation

Gross written premium in million USD



¹³ Swiss Re: Cyber getting to grips with a complex risk
<https://www.swissre.com/institute/research/sigma-research/sigma-2017-01.html>



**Personal
cyber hygiene
is essential**

**For increased
customer value
insurers need
to provide the right
insurance-service
package**

**The personal
cyber insurance
market
is estimated
to grow up to
USD 3.1 billion
by 2025**

Conclusion

Almost every facet of modern life is dependent on technology working in harmony with us. It does not take much to illustrate the extent of that dependency. A few hours without email or internet access is more than enough to cause consternation to any workplace, after all. These are concerns that might once have been the preserve of the business world, but which have entered the realm of people's personal lives, too.

The dependency on technology will not be reversed and will only grow in size, scale, and significance. Along with that, there is the inevitable increasing risk of individuals becoming the victim of a cyber incident – whether directly or indirectly.

In the same way as washing hands is frequent routine, personal cyber hygiene needs to become an everyday behaviour of people.

Although the current market for personal cyber insurance is not yet developed, customers seem to ask for insurance products that help them mitigate their personal cyber risk. Thus, Swiss Re estimates the personal cyber insurance market to grow to between USD 1.6 billion and USD 3.1 billion by 2025.

Going beyond a simple financial loss recovery approach and combining personal cyber insurance with value-adding services could be the factor that ignites interest from customers and really starts to open the market up. Those insurers who are able to find innovative routes to partner with service providers who can add value to the product could find themselves with a clear advantage.

Appendix

Survey details:

Swiss Re conducted a global survey via an online questionnaire collecting answers from 886 respondents across different professions and in different industry sectors.

Gender split of survey respondents was 35% women and 65% men. The majority of respondents fall into the following age bands: 18–24 years: 17%, 25–34 years: 32%, 35–44 years: 22%, 45–54 years: 20%.

Survey participants answered 26 questions in respect of their digital affinity, cyber risks awareness, preferred personal cyber insurance product features and willingness to buy.

This white paper shows a selection of key findings from the survey.

Market size estimation assumptions:

Swiss Re estimated the worldwide personal cyber insurance market size following a four-step approach:

- 1** Number of households were estimated using total population and average household size per country assuming that many personal cyber products will be designed and bought as family policies.
- 2** Country internet penetration rates were applied to derive the number of households with internet access. Assumption is that households without internet access have very low exposure to cyber risks and hence have limited needs for personal cyber insurance.
- 3** Country-specific conversion rates were estimated to approximate the number of households with internet access, which are willing to buy personal cyber insurance resulting in the potential addressable market for such insurance.
- 4** Average annual premium of available personal cyber insurance products in a country was applied to the potential addressable market in order to deduct the total market premium. For countries where personal cyber insurance is not yet offered, annual average premium levels from a reference country were indexed by means of per capita GDP purchasing power parity rates.

The high growth scenario assumes higher conversion rates and more pronounced annual growth for the period 2019 to 2025 compared to the base case.

Contact



Fabian Willi
Senior Cyber Solutions Manager
Fabian_Willi@swissre.com



Dr. Maya Bundt
Head Cyber & Digital Solutions
Maya_Bundt@swissre.com

© 2019 Swiss Re. All rights reserved.

Title

Personal cyber insurance:
Protecting our digital lives

Authors:

Fabian Willi
Dr. Maya Bundt

Graphic design and production:

Swiss Re Corporate Real Estate & Services/
Media Production, Zurich

Disclaimer

The content of this white paper is subject to copyright with all rights reserved. The information may be used for private or internal purposes, provided that any copyright or other proprietary notices are not removed. Electronic reuse of the content of this white paper is prohibited. Reproduction in whole or in part or use for any public purpose is only permitted with the prior written approval of Swiss Re, and if the source reference is indicated. Courtesy copies are appreciated.

Although all the information discussed herein was taken from reliable sources, Swiss Re does not accept any responsibility for the accuracy or comprehensiveness of the information given or forward looking statements made. The information provided and forward looking statements made are for informational purposes only and in no way constitute or should be taken to reflect Swiss Re's position, in particular in relation to any ongoing or future dispute. In no event shall Swiss Re be liable for any financial or consequential loss or damage arising in connection with the use of this information and readers are cautioned not to place undue reliance on forward- looking statements. Swiss Re undertakes no obligation to publicly revise or update any forward-looking statements, whether as a result of new information, future events or otherwise.

Swiss Reinsurance Company Ltd
Mythenquai 50/60
P.O. Box
8022 Zurich
Switzerland

Telephone +41 43 285 2121
Fax +41 43 282 2999
www.swissre.com