

Insurance in focus: Your customers' attitudes to cyber security

The currency of cyber trust

Effective cyber security is not only essential to insurance companies' ability to innovate through technology, it's now an important element of customer engagement.

Cyber security in the UK today

As cyber crime rises and everyday services are increasingly digitalised, public opinions on cyber security are changing. Citizens are becoming more careful about how they share their information and more aware of organisations who might fail to protect it. To find out more, we surveyed over 3,000 UK citizens to explore how attitudes to and behaviours relating to cyber security are evolving and what this might mean for firms whose services they use.

A question of trust

Whether it's people's family and relationship information, financial details or medical records, insurance companies hold some of our most sensitive personal data. There is, therefore, a clear responsibility on insurers, and a high expectation from customers that this data will be fully protected.

Yet recent high-profile data breaches have taken their toll on public trust in organisations. In fact, only 13% of respondents to our survey said their trust in organisations has increased over the last two years and almost half (48%) rated insurance companies at high risk of cyber attack.

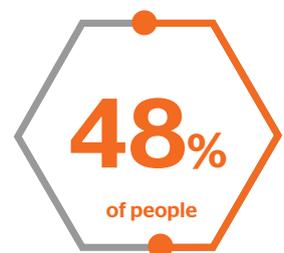
Since the introduction of GDPR, the financial implications of a data breach are serious given the scale of the possible penalties. Our research also underlined important reputational risks, with only 25% of respondents saying they would trust an organisation again after it was hit.

Assessing the cyber security risk

It is vital that insurers understand their cyber security risks in order to manage them effectively. The risk landscape is evolving fast as insurance companies introduce emergent technologies such as cloud, automation and new digital channels to increase operational efficiency and improve customer service. This more connected digital environment together with the predicted surge in smart devices in customers' cars and homes - will inevitably create more potential vulnerabilities.



say that recent attacks have made them more aware of cyber security



that insurance companies are at high risk of a cyber attack



say they would still trust an organisation after an attack

Your report into cyber security in the UK today and the data behind our Digital Vision for Cyber Security

atos.net/cyber-research-uk

Atos

Assessing the cyber security risk (contd.)

One consequence is that cyber security risks are increasingly shared between organisations and customers who use digital channels and connected devices. The respondents to our survey are aware of this dual accountability, with 87% saying that individuals need to take responsibility for keeping their information safe online. Yet when we looked more closely at how people protect themselves, we found a very mixed picture. Over half (52%) don't know how to better protect themselves; as new threats emerge, 61% don't actively stay informed about the latest cyber security threats and 15% don't take any steps at all. These gaps and contradictions present real risks to consumer and insurers alike.

Cyber security as a differentiator

What's clear from our survey is that communication is as important as technology when it comes to public trust. As insurers seek to build closer relationships with their customers, especially through digital channels, there will be more touchpoints through which to communicate about the cyber security measures they are taking and to inform and remind customers about how to remain cyber vigilant.

In fact, the research points to significant opportunities for companies to differentiate themselves by communicating more effectively with their customers about cyber security. 58% say cyber security is a deciding factor when choosing which organisations to interact with and 53% of our respondents said that the biggest reason they trust an organisation is a rigorous security process.

Investing in cyber security

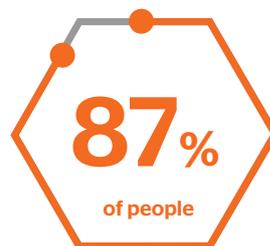
The other good news is that we found a willingness, as far as financial or personal information is concerned, to go through more cyber security steps in exchange for better security. 56% of respondents are willing to compromise their user experience for increased protection; 66% are happy to compromise on the speed of a service; and 59% are happy to compromise on the complexity of logging in.

Customers say they want to see technological innovation across the board: 49% expect the insurance industry to have data encryption in place; 67% say they would trust an organisation more to know it was investing in advanced tech; and 58% want cyber security defences to be managed by a combination of human insight and automated technology. Threat monitoring is critical and as cyber threats evolve, so must organisations' capabilities. Advanced analytics, in combination with automation, speed up the detection of anomalies and will help organisations on their journey to predictive and prescriptive security.

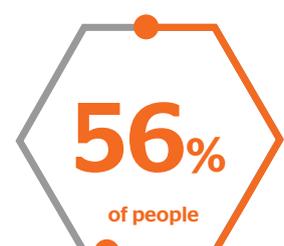
Conclusion

It is vital that cyber security becomes and remains an enabler – not a blocker – to digital transformation if insurance companies are to safely achieve the speed and efficiency they are looking for. And with today's digitally savvy customers wanting information and communication, a transparent approach to cyber security will help to retain public confidence in digital channels and wider trust in a company's brand.

The first step is for insurers to fully understand and assess their cyber security risks. Success then depends on implementing a comprehensive, proportionate, end-to-end cyber security strategy that achieves the correct balance between cost and assessment of risk. There are now real opportunities for insurers to gain competitive edge in the way they design convenient, secure and reassuring customer experiences. Getting cyber security right can help forward-thinking companies to retain and win customer loyalty and realise their digital ambitions.



say individuals need to take responsibility for keeping their information safe online - yet 15% don't take any steps at all to stay informed about the latest cyber security threats



are willing to compromise their experience for better cyber security



say cyber security is a deciding factor when choosing which organisations to interact with



To get a copy of the full report, download **The currency of cyber trust**.

atos.net/cyber-research-uk