Banking in focus: Your customers' attitudes to cyber security

The currency of cyber trust

Effective cyber security defences are clearly a cornerstone of every financial service. As a differentiator, cyber security extends into an integrated, well-designed customer experience.

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 and behaviours around cyber security are evolving and what this might mean for the banking sector.

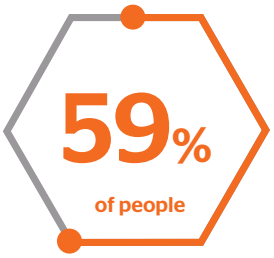
Questions of trust

No sector is more aware of the importance of cyber security than the financial services industry. Yet as the market and the broader digital landscape evolve, this research points to opportunities for leveraging cyber security as a differentiator.

Firstly, it's important to note than when respondents were asked which organisations can best protect themselves from cyber attacks, financial services was the highest-rated sector (with a mean score of 7.4 out of 10). Yet at the same time, high-profile incidents have hit public confidence, with only 13% of respondents saying their trust in organisations has increased over the last two years.

If an attack does happen, public trust can be hard to win back. In fact, only 25% of respondents say they'd trust an organisation again after it was hit, with clear implications for organisations' bottom lines. With digital channels being increasingly critical to banks' operational and marketing strategies, ensuring that customers continue to engage and share data online is essential.

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



say they're concerned that a cyber attack will have a significant impact on their life in the next 12 month

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

Helping customers to help themselves

With GDPR now in place, our research underlined the importance of good communication when it comes to building cyber trust; 82% of respondents say they expect to be informed in the wake of an attack. Today's customers want a swift and comprehensive response and they want to know that the organisation has taken the right steps to avoid more problems in future.

However, the role of communication goes much wider than recovery. When we looked at perceptions of where cyber security responsibilities lie between the organisation and the individual, we found a mixed picture. For example, 87% say individuals need to take responsibility for keeping their information safe online – yet over half (52%) don't know how to better protect themselves. As new threats emerge, 61% don't stay actively informed about the latest cyber security threats, with 15% not taking any steps at all and younger demographics less motivated to protect themselves than older people.

Such gaps and contradictions clearly present real risks; and while many banks are taking steps to educate the public about cyber security, still more can be done to inform and remind customers of why and how to stay vigilant both online and offline.

Creating stand-out customer experiences

When we looked more closely at how online services are used, the research revealed 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.

The conclusion is that customers will use digital services more if they think they are secure and they will be more tolerant of cyber security measures if they understand them. And the stand-out user experiences will be those that are well-designed enough to be seamless while incorporating security measures that reassure customers and keep data safe while not being so cumbersome that they dis-incentivise users.

To get a copy of the full report, download **The currency of cyber trust.**
atos.net/cyber-research-uk

Investing in cyber security

Customers want to see technological innovation: 59% expect financial services organisations to have data encryption in place; 67% say they would trust an organisation more to know it was investing in advanced tech; 58% want cyber security defences to be managed by a combination of human insight and automated technology.

Again, for banking organisations, this is about striking the balance between great customer experience and tight cyber security. While use of biometrics, for instance, may be convenient for customers, the ethical dimensions of retinal and facial recognition technologies cannot be ignored. 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 that means that threats can be pre-empted.

Conclusion

In the retail banking space, effective cyber security isn't only about tightening up the technological defences; it is about planning and executing cyber security as an extension of customer engagement.

Success depends on implementing a comprehensive, proportionate, end-to-end cyber security strategy that achieves the correct balance between cost and assessment of risk. And there are now real opportunities for banks to innovate in the way they communicate and design customer experiences. Getting cyber security right can help forward-thinking financial organisations to retain and win customer loyalty, strengthen wider trust and realise their digital ambitions.

56% of people are willing to compromise their user experience for better security

53% of people say the biggest reason they trust an organisation is a rigorous security process

87% say individuals need to take responsibility for keeping their information safe online

15% don't take any steps at all to stay informed about the latest cyber security threats

atos.net/cyber-research-uk

Atos