Your students' attitudes towards cyber security

The currency of cyber trust

Effective cyber security is essential - not only to safeguard students and staff, but to enable universities to compete.

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 educational institutions.

It has always been the responsibility of every university to safeguard the data it holds on behalf of students and staff. What's changed is universities' exposure to risk and students' awareness of how their data is being managed.

Questions of trust

Since the introduction of the General Data Protection Regulation (GDPR), the potential costs of a cyber attack are significant. As well as the larger financial penalties, there are serious reputational impacts if data falls into the wrong hands, as recently experienced by one London university. Yet with competition becoming more fierce, trust and credibility are important assets, both to attract students and preserve the value of the education that universities offer.

Perhaps unsurprisingly, our research found that 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, trust can be hard to win back; 25% of younger respondents didn't use an organisation again once it had been attacked. All this makes cyber security and 'cyber trust' a business priority for any university.

Shared responsibilities?

Educational institutions have a duty of care to their students, many of whom are away from home for the first time and expect to be protected. At the same time, students themselves, like anyone online, are surely accountable to an extent for their own cyber security. Our survey respondents certainly think so: 87% claim that individuals need to take responsibility for keeping their information safe online. Yet when we took a closer look at how people protect themselves, we found a very mixed picture.

63% of people say that recent attacks have made them more aware of cyber security

25% of 16-24 year olds didn't use an organisation again once it had been attacked

75% of university students are in the age group most often affected by cyber attacks (aged 16-24)

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

Educational institutions have a duty of care to their students, many of whom are away from home for the first time and expect to be protected. At the same time, students themselves, like anyone online, are surely accountable to an extent for their own cyber security. Our survey respondents certainly think so: 87% claim that individuals need to take responsibility for keeping their information safe online. Yet when we took a closer look at how people protect themselves, we found a very mixed picture.

50% of 16-24-year-olds admit they don't take any practical steps to stay safe online (compared to 40% of +55-year-olds). What's more, over half (52%) of our respondents don't know how to better protect themselves and 61% don't actively stay informed about the latest cyber security threats. These findings underline the importance of universities taking active steps to protect potentially vulnerable students.

Transparency and accountability

Our survey found that cyber security is increasingly important to UK citizens, with 58% saying it's a deciding factor when choosing which organisations to interact with. While cyber security in itself is unlikely to be the key factor in choice of university, having an innovative digital strategy might well be. Cyber security, therefore, is an essential 'hygiene' factor for students and parents while also being a vital enabler in institutions' successful digital-innovation.

So, what can universities do to win and retain 'cyber trust'? Given the risky gaps in students' knowledge and online behaviours, there is value in awareness-raising about how to stay cyber secure. Making responsibilities transparent, with clear agreements around data governance (based on GDPR compliance), will both inform and reassure. A balanced approach is needed to provide the required safeguards while not raising unnecessary challenges or concerns. Interestingly, our research highlights opportunities to make this kind of information integral to users' online experience, given that 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 if they knew their data will be better protected.

Investing in cyber security technology

It is vital that universities understand their cyber security risks in order to manage them effectively. With many institutions moving more and more of their content and interactions to digital channels, they will collect more data and the 'attack surface' (open to hackers) will in turn expand.

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

As a result, universities' end-to-end cyber security strategies need to evolve and make use of advancing security technologies. Our survey respondents agree: 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. Using advanced analytics (in combination with automation) will speed up the detection of anomalies and enable institutions to use cyber security capabilities that better predict attacks, and even stop them from happening in the first place.

Conclusion

As the threat landscape evolves and universities expand their use of digital tools and channels, cyber security responses must also evolve. Universities need access to the right cyber security expertise and technologies, with a strategy for clear communication and data governance.

The first step is for institutions 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 universities to differentiate themselves through convenient, secure and reassuring online experiences for students. Getting cyber security right is a critical part of wider trust in institutions, protecting reputations and helping universities to realise their digital ambitions.

50%
of 16-24 year olds
say they don't take any practical steps to stay safe online

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

70%
believe organisations need more technology to help fight cyber crime