

Almost Two-Thirds of Financial Services Firms Have Suffered a Cyber-attack in the Last 12 Months

Submitted by: Rise PR

Thursday, 5 November 2020

- Research with CISOs and CIOs reveals 45% of FS firms have seen increased cybersecurity attacks since Covid-19
- 42% say securing the remote workforce has become a main cybersecurity objective, 47% have increased investment in secure collaboration tools
- Almost half say weakness in the supply chain has most potential to cause damage over next 12 months

5 November 2020, Theale, UK – 65% of large Financial Services (FS) firms have suffered a cyber-attack in the last 12 months, according to new research today from data security provider HelpSystems.

The research with 250 CISOs and CIOs in global FS firms also showed the impact that Covid-19 is having on FS firms' cybersecurity, with 45% of respondents reporting an increase in cyber-attacks since the pandemic first emerged. Securing the remote workforce has become a key objective for 42% of FS firms, while almost half (47%) have already increased their investment in secure collaboration tools.

92% of FS organisations have increased their cybersecurity investment over the previous 12 months, 26% significantly so. The main investment priorities for CISOs over the next 12 months include secure file transfer (64%), protecting the remote workforce (63%) and cloud/Office365 (56%).

"It's a highly challenging cybersecurity landscape for the financial services sector, with many CISOs focused on battling day-to-day threats alongside trying to achieve broader strategic objectives," said Kate Bolseth, CEO, HelpSystems. "Technology is a key part of cybersecurity of course, and no organisation will ever be secure without the right security solutions to protect the organisation here and now. But of equal importance, especially for longer-term strategic goals, is ensuring the right processes are in place and educating and training employees."

The research, *Cybersecurity Challenges in Financial Services* (<https://www.clearswift.com/cta/financial-services-cybersecurity-report>), revealed that the two threats with most potential to cause damage were cybersecurity weaknesses in the supply chain (46%) and increased working from home due to Covid-19 (36%). The extent to which Covid-19 has impacted cybersecurity strategies in FS firms around the world was clear. Around one-third of respondents had reacted quickly to update their regulatory best practices and 46% had re-evaluated their cybersecurity training and policies to better reflect the increased home working.

Almost half of respondents felt that Covid-19 has accelerated changes that were already in discussions, such as a move to Office 365. Such changes form part of broader digital transformation strategies, which was seen as the main challenge facing FS, both now and in three years' time.

"FS is such an important sector, the backbone of the global economy, so keeping it secure and operational is a major priority," continued Kate Bolseth. "Cyber-attacks are growing in volume and severity, so FS firms need to not only protect the organisation against day-to-day threats, but also make the transition to digital, meet regulatory demands, and secure a remote workforce in the light of

Covid-19. It's really tough and there's no silver bullet, just constant evolution in the face of the changing threatscape."

The HelpSystems report – 'Cybersecurity Challenges in Financial Services' – is available to download here (<https://www.clearswift.com/cta/financial-services-cybersecurity-report>).

-ends-

About the research

This research was conducted by technology research firm, Vanson Bourne, on behalf of HelpSystems in August and September 2020. A total of 250 senior cybersecurity and IT decision-makers (209 CISOs, 41 CIOs) in large global FS organisations were polled – 50 in the US, UK, The Netherlands, Germany and Australia.

For further information, please contact:
Paul Allen / Rise PR (<http://risepr.co.uk>)
07515 199 487 / paul@risepr.co.uk

Or visit www.helpsystems.com