March 21, 2022

Ransomware Risks Seen as Rising in Financial Sector, Though Industry Remains Divided on Threat Response: ACAMS Global Survey

Respondents to the ACAMS Global Ransomware Risks Survey see need for greater governmental guidance, integration of anti-financial crime teams in ransomware response

Chicago – Financial institutions and governments face the highest risk of becoming the target of ransomware attacks compared to organizations in other major economic sectors, according to nearly 400 participants in the new ACAMS Global Ransomware Risks Survey. The study—which drew responses from multinational and domestic banks, money services businesses, governmental bodies, cyber firms, and other organizations—queried participants on their perceived risks of ransomware attacks, their institutional preparedness for such cyber-incidents, and the role that anti-money laundering (AML) and sanctions compliance teams play in safeguarding their institutions. The findings indicate a prevailing view (65%) that the threat of ransomware is growing, while suggesting that private- and public-sector responses to ransomware risks have yet to fully prepare organizations for such incidents.

The study also reached the following conclusions on the nexus between the crypto-virological attacks and anti-financial crime (AFC) efforts:

- While 83% of all survey participants believe that collaboration between cybersecurity personnel and AML and sanctions teams would help shield the financial sector from ransomware attacks, fewer than 60% of financial-institution respondents say such compliance professionals actively take part in investigating ransomware incidents.
- Nearly 90% of all survey participants believe that understanding compliance red-flag indicators would help financial institutions better combat ransomware, but only 46% of financial-sector respondents say their institutions have incorporated ransomware into their AFC compliance training.
- A slim majority of respondents say their institutions have drafted incident response plans for ransomware attacks, and only 48% have policies and procedures for ransomware-related risk management.

Survey participants around the world separately indicated that governmental bodies have yet to provide adequate guidance on how private-sector organizations can shield themselves from such incidents, with 29% of all respondents saying that their national

governments have done very little to protect domestic businesses from ransomware. Nearly a third of private-sector respondents feel that the governmental guidance issued to date has been vague, the survey found.

“The survey makes clear that companies and governments alike are still finding their footing when it comes to responding to ransomware attacks,” said ACAMS CEO Scott Liles. “As the ransomware threat continues to evolve, nations and compliance professionals should expect to be called upon to play a larger role in protecting the private sector, including through greater hands-on participation in incident responses and information-sharing.”

“With the risks of ransomware and other cyber-attacks on the rise as a consequence of ongoing turmoil in Ukraine, it is critical that the compliance community and wider industry not only assess their institutional vulnerabilities but also take meaningful steps to protect themselves,” said ACAMS Sanctions and Risk Associate Sam Cousins. “The survey findings indicate that many institutions have yet to fully comprehend their risks and implement policies and procedures that can effectively respond to ransomware incidents.”

Of the 395 respondents to the survey, 64% said they work for financial institutions, with 35% of those indicating that they are employed by multinational banks, 20% by national banks,19% by regional banks, and the remainder working for money services businesses, payment service providers, cryptocurrency exchanges, insurance companies or other firms. Twelve percent of all participants said they work in the public sector while the remaining 17% said they are employed by corporates or other firms not in the financial sector. Nearly 30% of respondents said their institution was headquartered in the United States while 20% and 18% cited institutions based in Asia and Europe, respectively. To access the full survey report, please click here or visit this page :https://www.acams.org/en/media/document/global-ransomware-risks-survey-report

About ACAMS®

ACAMS is the largest international membership organization dedicated to providing opportunities for anti-financial crime (AFC) education, best practices, and peer-to-peer networking to AFC professionals globally. With over 90,000 members across 180 jurisdictions, ACAMS is committed to the mission of ending financial crime through the provision of anti-money laundering/counterterrorism-financing and sanctions knowledge-sharing, thought leadership, risk-mitigation services, ESG initiatives, and platforms for public-private dialogue. The association’s CAMS certification is the gold-standard qualification for AFC professionals, while the CGSS certification is its premier specialist qualification for sanctions professionals. ACAMS’ 60 Chapters globally further amplify the association’s mission through training and networking initiatives.
Visit acams.org for more information.

Contact:
Lashvinder Kaur
ACAMS
LKaur@acams.org
+44 7388264478