



New Report Reveals How Cyber Attackers Could Target the World's Financial Markets

- Joint study examines cyber threats across global financial markets
- Securities market is one of the most at-risk areas, while trade finance is also under threat

The cyber threats faced by key financial markets across the world have been exposed by a new report published today by BAE Systems and SWIFT.

The study examines the different levels of susceptibility and threat faced by parts of the financial markets. It considers how market infrastructures and participants could be exploited by cyber criminals to penetrate organisations across the securities, trade finance, foreign exchange, and banking and payments market segments.

While the risks in banking and payments are well documented, this study reveals that the securities market is particularly vulnerable. This is due to the large number of participants and infrastructures, as well as the complex interactions involved. Weaknesses can be unknowingly introduced by traders, brokers, investors, other stakeholders – and the systems that all of these participants use. The study also shows how the foreign exchange and trade finance markets are also at risk.

The report, entitled *The Evolving Advanced Cyber Threat to Financial Markets*, analyses the changing threat landscape and explores how the financial sector is exposed to a range of emerging cyber security challenges.

Among the main recommendations proposed are:

- Securities participants should embrace the value of checks, communication and data to support pre- and post-trade activities and stave off cyber threats.
- Securities market infrastructures need to collaborate with participants to identify risks in common practices to jointly defend market operations.
- Banking and payments participants must continue to strengthen security controls while building in protection for upstream systems.
- Trade finance participants are encouraged to review and manage areas of inherent trust, which are at risk of cyber exploitation.

In an effort to help participants combat cyber fraud, SWIFT launched its Customer Security Programme (CSP) in 2016. This programme has helped its customers across the payments, securities, trade finance and foreign exchange sectors implement security controls identified as critical to defending against, detecting and recovering from cyber attacks. But with cyber threats evolving and criminals increasingly looking for ways to steal large sums of money at speed, financial organisations are being urged to be more vigilant, and take further steps to address the vulnerabilities outlined in this report.

Sanjay Samuel, Financial Services Director at BAE Systems said:

"It's all too easy to be lulled into a false sense of security, and place too much faith in



systems which cyber attackers can exploit. While the threat is greatest in the securities market, every part of the global financial services sector needs to be aware that cyber crime is evolving. Threats are becoming more intelligent, and criminals are increasingly focused on generating an ROA – return on attack – as quickly as possible.”

“There’s a wide range of cyber threats out there, and that’s why a holistic approach is becoming critical. Cyber security is no longer just a technical issue, as attackers are exploiting weaknesses in market operations, people and processes. So security needs to be embedded and coordinated across all levels and sectors of financial services organisations.”

Brett Lancaster, Managing Director, Global Head of Customer Security at SWIFT said:

“Over recent years, SWIFT has made good progress supporting financial institutions in their fight against well-organised cyber attackers – but this report shows that now is not the time to sit back and take the this progress for granted.”

“As cyber criminals become ever more innovative and agile, we need to continue to work together to build even stronger defences. Through our Customer Security Programme, we have been assisting the payments, securities, trade finance and foreign exchange sectors to better protect their immediate surroundings, and have facilitated better information sharing to help equip the industry with the tools it needs to combat cyber crimes. This report is a timely reminder that we need to go further still to keep ahead of the criminals.”

The Evolving Advanced Cyber Threat to Financial Markets report is available for financial services organisations to download now. Visit www.baesystems.com/evolvingthreat to find out more information and request your copy of the report.

ENDS

For further information, please contact:

BAE Systems

Nick Haigh, BAE Systems

M: +44 (0) 7525 390982

E: nick.haigh@baesystems.com

Bite

Bryony Alymer, Bite

M: +44 (0) 7827 917023

E: bryony.alymer@biteglobal.com

SWIFT press contact

Finsbury

+32 (0)2655 3377

SWIFT@Finsbury.com

Notes for Editors

**About BAE Systems**

At BAE Systems, we provide some of the world's most advanced technology defence, aerospace and security solutions. We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

At BAE Systems Applied Intelligence, we help nations, governments and businesses around the world defend themselves against cybercrime, reduce their risk in the connected world, comply with regulation, and transform their operations. For further information about BAE Systems Applied Intelligence, please visit www.baesystems.com/businessdefence

About SWIFT

SWIFT is a global member owned cooperative and the world's leading provider of secure financial messaging services. We provide our community with a platform for messaging and standards for communicating, and we offer products and services to facilitate access and integration, identification, analysis and regulatory compliance.

Our messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories. While SWIFT does not hold funds or manage accounts on behalf of customers, we enable our global community of users to communicate securely, exchanging standardised financial messages in a reliable way, thereby supporting global and local financial flows, as well as trade and commerce all around the world.

As their trusted provider, we relentlessly pursue operational excellence; we support our community in addressing cyber threats; and we continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies. Our products and services support our community's access and integration, business intelligence, reference data and financial crime compliance needs. SWIFT also brings the financial community together – at global, regional and local levels – to shape market practice, define standards and debate issues of mutual interest or concern. SWIFT's strategic five year plan, SWIFT2020, challenges SWIFT to continue investing in the security, reliability and growth of its core messaging platform, while making additional investments in existing services and delivering new and innovative solutions.

Headquartered in Belgium, SWIFT's international governance and oversight reinforces the neutral, global character of its cooperative structure. SWIFT's global office network ensures an active presence in all the major financial centres.