FUTUREMATTERS™
CENTRE OF EXCELLENCE

GFTN
GLOBAL FINANCE & TECHNOLOGY NETWORK

Synergy In Cybersecurity

May 2025

Contents

Introduction 03

Section 1:
Cybersecurity Threats and Financial Stability 03

- The Growing Cybersecurity Threat
- Emerging Cyber Threats
- Insights on Cybersecurity Challenges
  - 1. Technological Complexities
  - 2. Global Impact of Cyber Incidents
  - 3. Tech Debt and Cybersecurity 04

Section 2:
Key Cybersecurity Strategies 04

- Adopting Zero Trust for Enhanced Cybersecurity Resilience
- Building Security by Design to Mitigate Risks
- Transparency and Open-Source Approaches in Cybersecurity
- Cybersecurity's Growing Importance in Financial Transactions and Payments
- Managing Third-Party Risks and Supply Chain Vulnerabilities
- Focusing on Cyber Resilience to Recover from Attacks 05
- Collaboration and Intelligence Sharing to Stay Ahead of Threats

Incident Reporting and Handling: Striking the Right Balance 05

- The Need for Streamlined Incident Reporting
- The Value of Cyber Incident Notification
- Challenges of Meeting Diverse Reporting Requirements
- Improving the Reporting Framework
- The Need for Preparedness in Incident Response 06
- Addressing the Skills Gap During Cyber Incidents

Reactions and Recommendations on Incident Reporting 06

- Harmonized Data for Systemic Risk Monitoring
- Agreement on a Two-Stage Approach
- Flexibility in Incident Reporting Timelines
- Industry Feedback and Tailored Approaches

Conclusion 06

Section 3:
Strategic Approaches to Mitigating Quantum Computing Risks and Enhancing Cryptography Agility 07

- 1. Introduction
- 2. Update to Cryptography and Crypto Agility Implementation
- 3. Understanding the Quantum Computing Threat
- 4. The Role of AI in Cybersecurity and Quantum Risk Management
- 5. Case Study: Integrating Quantum and AI for Strategic Advantage
- 6. Collaboration and Knowledge Sharing
- 7. Conclusion 08

Contributors 09

References 10

Introduction

In a rapidly evolving technological landscape, organisations face unprecedented challenges in cybersecurity and resilience, given the integration of emerging technologies such as AI, and cloud computing within our daily lives. While quantum computing remains a largely nascent technology, it remains a fast-growing space, with quantum investments by governments estimated to be around US$42 billion as of June 2024.[1]

As organisations increasingly adopt these new technologies, new vulnerabilities are emerging that cybersecurity leaders have to pay attention to. The shift to commercial cloud environments has introduced new challenges in safeguarding sensitive data and critical systems. During a roundtable held at the Insights Forum 2024 at the Singapore Fintech Festival, cybersecurity leaders, policymakers, and regulators gathered to discuss the changing landscape of cybersecurity amidst emerging technological developments.

Section 1:

Cybersecurity Threats and Financial Stability

The Growing Cybersecurity Threat

One of the central themes of the forum was the escalating scale of cybersecurity risks. A report by Cybersecurity Ventures, noted that global cybersecurity damages in 2024 are expected to reach US$9.5 trillion[2]**.** Measured as a country, that number would make cybercrime the third-largest economy globally, after the United States and China. This figure serves as a stark reminder of the massive financial threat posed by cyber incidents. Additionally, the average cost of a data breach in 2023, according to IBM, was reported to be US$4.5 million per incident, marking an all-time high[3].

Emerging Cyber Threats

The main focus of the roundtable was the emerging cybersecurity risks that organisations face, particularly those stemming from vulnerabilities within the supply chain. Participants discussed a global financial stability report [4], which highlighted the increasing frequency of cyberattacks since the onset of the COVID-19 pandemic, and their escalating threats to financial stability.

The report revealed that while the direct financial losses from most cyber incidents are relatively small, rare but extreme incidents can cause significant damage. For instance, events that occur once per decade, but result in massive financial losses—sometimes as high as US$2.5 billion—are becoming more common. While no cyber event has yet triggered systemic consequences for global financial stability, the potential for such incidents to occur is rising, especially with the advancement of technologies like quantum computing and increasing digitalisation.

The report also highlighted the vulnerability of the financial sector, noting that around 20% of all cyber incidents occur within financial institutions. The interconnectedness of financial systems increases the risk of these incidents affecting multiple organisations simultaneously. For example, many financial institutions rely on third-party IT service providers, which increases the possibility of a cyber event spreading across various firms and even across borders. The shared dependence on these service providers creates vulnerabilities that can have far-reaching consequences. One speaker stressed the importance of monitoring third-party risks and mapping out technological and financial linkages to understand and mitigate exposure to systemic shocks.

Insights on Cybersecurity Challenges

Additional insights from the forum centred on several key challenges that businesses face in safeguarding their operations:

1. **Technological Complexities**

   Advancements in technology introduce new challenges for cybersecurity. For example, cybersecurity software systems, such as privileged access management (PAM), that access sensitive systems at a granular level can create complexities in managing cybersecurity at scale. As technologies evolve and require constant updates, organisations face increasing difficulties in maintaining effective security controls. Businesses must adapt their security frameworks to keep pace with emerging threats.

2. **Global Impact of Cyber Incidents**

   Incidents like WannaCry[5] and SolarWinds demonstrate the global consequences of cyber vulnerabilities. The virtual blast radius of such attacks extends far beyond the affected organisations, with ripple effects throughout industries, governments, and nations. This highlights the critical need for organisations to

© 2025 GFTN Limited, All Rights Reserved. Reproduction Prohibited.

understand the software supply chain and to manage vulnerabilities that can spread across interconnected entities.

3. **Tech Debt and Cybersecurity**

   Another significant issue is tech debt, where cybersecurity is often treated as an afterthought, with organisations simply meeting compliance requirements rather than addressing long-term vulnerabilities. This tech debt grows over time as tech systems accrue, increasing the potential impact of any incident. To mitigate this risk, businesses must move beyond mere compliance and focus on building resilience into their systems, ensuring they are secure by design and capable of withstanding disruptions.

Cybersecurity threats are evolving rapidly, and organisations must adapt to these new risks. Discussants emphasised the importance of adopting a proactive and resilient approach to securing digital infrastructures. Businesses must not only focus on preventing cyberattacks but also prioritise building resilient systems capable of mitigating the impacts of potential incidents.

Section 2:

Key Cybersecurity Strategies

Adopting Zero Trust for Enhanced Cybersecurity Resilience

The importance of adopting zero-trust security models was underscored as a crucial strategy for defending against sophisticated cyber threats. Zero trust operates on the assumption that breaches will occur, making it essential to verify every access request. As one expert stated, ***"We were the only hyperscaler unaffected by [the SolarWinds attack]. This is not a boasting statement, this is simply an engineering one."*** By adopting zero-trust, organisations can significantly reduce the likelihood of successful attacks through stringent access verification and continuous monitoring.

Building Security by Design to Mitigate Risks

The forum highlighted the need for a shift toward security by design to mitigate risks from the outset. This approach involves integrating secure development practices into the lifecycle of projects, preventing certain types of cyber threats such as phishing. One speaker shared that their organisation successfully implemented FIDO authentication, which eliminated phishing attempts and account takeovers since 2017. Additionally, the adoption of memory-safe programming languages has helped mitigate vulnerabilities related to remote code execution.

Transparency and Open-Source Approaches in Cybersecurity

Another key theme discussed was the role of transparency and open-source approaches in fostering collaboration across the cybersecurity community. By sharing security methodologies openly, organisations can contribute to a larger knowledge base, helping others improve their cybersecurity practices. One speaker remarked, ***"This engineering is also open-source, public, and free to the world,"*** demonstrating how sharing knowledge can strengthen the entire ecosystem.

Cybersecurity's Growing Importance in Financial Transactions and Payments

As financial services become increasingly interconnected and operate in real time, the need for robust cybersecurity has never been more critical. Financial institutions must protect not just against data theft but also broader risks to assets and reputation. As one participant observed, ***"The number one priority for CEOs in the next three to five years is cyber and risk management."***

Managing Third-Party Risks and Supply Chain Vulnerabilities

The importance of managing third-party risks was a recurring topic, particularly in the context of supply chain vulnerabilities. With organisations depending on external vendors and service providers, it is essential to ensure that partners maintain strong cybersecurity hygiene. One speaker posed the question, ***"How do you make sure that every one of them is having good cyber hygiene?"***

Focusing on Cyber Resilience to Recover from Attacks

While preventing all cyberattacks is unrealistic, organisations can focus on building cyber resilience to ensure rapid recovery after an incident. By implementing cybersecurity controls and enhancing visibility, organisations can detect and disrupt adversary activities,

© 2025 GFTN Limited, All Rights Reserved. Reproduction Prohibited.

minimizing the attack's impact. As one expert noted, ***"You cannot stop all attacks, but what you can do is to make sure that you disrupt when the attack path is happening."***

Collaboration and Intelligence Sharing to Stay Ahead of Threats

Finally, staying ahead of cyber threats requires collaboration and intelligence sharing across industries. By understanding the tactics of cybercriminals, organisations can better anticipate emerging risks and bolster their defences. One participant concluded, ***"We need to acknowledge the fact that anybody who operates in today's business is obviously in a network. They have partners, they have vendors, they have suppliers who are all connected to the network."***

A holistic approach that combines strong security practices, strategic risk management, and collaboration across sectors is essential for addressing the complex and evolving challenges of cybersecurity. Organisations must remain proactive, transparent, and forward-thinking to build trust and maintain secure digital operations. By focusing on both prevention and resilience, businesses can effectively navigate the increasingly complex cybersecurity landscape.

Incident Reporting and Handling: Striking the Right Balance

The Need for Streamlined Incident Reporting

Incident reporting is a crucial part of cybersecurity after a cyber-attack. However, the variety of reporting requirements across regions and industries can be counterproductive, diverting resources away from the critical task of managing the incident itself. The complexity of these fragmented regulations can overwhelm organisations, leading to inefficiencies. As one expert noted, ***"If you want me to report all of those, I would literally be doing nothing else."***

The Value of Cyber Incident Notification

While challenging, incident reporting provides significant value, particularly in sharing attack details, identifying vulnerabilities, and improving overall cybersecurity. Early detection and swift response can prevent further damage, and sharing incident data helps other organisations strengthen their defences. One panelist explained, ***"As incidents are reported... that can provide others an opportunity to review their own controls and ensure that they are not vulnerable to a similar sort of incident or attack."***

Challenges of Meeting Diverse Reporting Requirements

Organisations often face difficulties navigating the complex and diverse reporting requirements in different jurisdictions. Multinational companies, in particular, struggle to meet varying timelines and reporting standards in countries such as the U.S., China, and Singapore [6].

One expert remarked, ***"It becomes extremely complex for any CISO... to operate in such a diverse regulatory environment."*** The diversity of regulations adds unnecessary complexity, hindering a swift and coordinated response.

Improving the Reporting Framework

To improve the reporting framework, it is necessary to focus on streamlining the criteria for reportable incidents. For example, incidents that involve attempted attacks without malicious intent or significant impact should not be subject to mandatory reporting. As one panelist pointed out, ***"How do you even define an attempted attack? Is it a blocked phishing email or a scan against your perimeter?"*** By prioritising incidents with malicious intent and substantial impact, organisations can make the reporting process more efficient and effective.

The Need for Preparedness in Incident Response

Swift reporting is essential for effective incident management, but many organisations still struggle with preparedness. Lack of readiness can result in delayed reporting, hindering response efforts. One expert emphasised, ***"My first and foremost wish list from incident reporting perspective is for organisations to be ready...to make a conclusion and disclose their position on that in a swift manner."*** Preparedness is key to ensuring that incidents are handled effectively and timely.

© 2025 GFTN Limited, All Rights Reserved. Reproduction Prohibited.

Addressing the Skills Gap During Cyber Incidents

A critical challenge in incident response is the shortage of skilled professionals who can manage the crisis. Experts stressed that during an attack, response teams should be focused on addressing the issue, not bogged down by excessive reporting. As one noted, ***"We wouldn't want those groups or those specialists to be distracted by overly burdensome or fragmented reporting requirements...we really want those teams focused on responding to that incident."*** Standardised reporting guidelines would allow experts to concentrate on recovery efforts without being overwhelmed by administrative tasks.

Recommendations for Incident Reporting

Harmonised Data for Systemic Risk Monitoring

One of the key recommendations was the need for high-quality, harmonised data for effective monitoring of systemic cyber risk. While efforts to improve data collection have made progress, variability in reporting standards across countries remains a challenge. The need for consistent, comparable data is crucial for regulators and industry players to better assess risks and respond accordingly. Improved reporting would also benefit sectors such as cyber insurance, which relies heavily on incident data.

Agreement on a Two-Stage Approach

A two-stage incident reporting process was proposed as an effective solution. The first stage would involve early notification of the incident and an assessment of its potential impact on critical infrastructure. This would allow organisations to prepare and plan their response. The second stage would provide more detailed information once the incident is understood. Flexibility in this process is essential, with the approach tailored to the unique needs of each sector.

Flexibility in Incident Reporting Timelines

The difficulty of meeting varying incident reporting timelines across jurisdictions was acknowledged. Disparate timelines make comparisons challenging, and efforts to harmonise them are needed. Although reasonable response times have been established, there should be an openness to revising them based on feedback from industry stakeholders.

Industry Feedback and Tailored Approaches

The need for sector-specific responses was emphasised. Different industries face different challenges when it comes to incident reporting, and tailored approaches are essential for effective coordination. It was agreed that feedback from industry stakeholders is crucial for refining the process and improving coordination between regulators and the industry.

Conclusion

The discussions around incident reporting and handling underscored the challenges of harmonising data, defining reportable incidents, and accommodating varying timelines. While progress has been made, the need for streamlined, standardised, and flexible incident reporting remains. Feedback from industry stakeholders is essential to ensure a more coordinated and effective response, allowing organisations to balance reporting requirements with timely and efficient crisis management.

© 2025 GFTN Limited, All Rights Reserved. Reproduction Prohibited.

Section 3:

Strategic Approaches to Mitigating Quantum Computing Risks and Enhancing Cryptography Agility

1. Introduction

As cybersecurity faces increasing challenges from emerging technologies, particularly quantum computing, organisations must prioritise enhancing their cryptographic practices.

This report outlines two key strategies to mitigate the risks posed by quantum computing: updating current cryptographic standards to post-quantum cryptography (PQC) and implementing a crypto agility framework. These approaches will help organisations manage evolving cryptographic needs as quantum computing advances and secure their data from future quantum threats.

2. Update to Cryptography and Crypto Agility Implementation

Organisations must prepare for the transition to quantum-safe cryptography by updating existing systems to align with new, anticipated standards. The concept of *crypto agility* is crucial in this context—enabling organisations to quickly adapt to new cryptographic standards as they emerge. This is vital given the potential threat quantum computers pose to current encryption methods. A robust cryptography and key management strategy is essential, focusing on:

- **Cryptographic Research Investment**: Allocating resources to research and development ensures preparedness for quantum challenges.
- **Cryptography Inventory and Risk Assessment**: Assessing existing cryptographic systems to identify key assets, such as customer data and intellectual property, helps prioritize efforts in securing sensitive data.

3. Understanding the Quantum Computing Threat

Quantum computing has the potential to disrupt current encryption systems, such as RSA and AES, which are based on mathematical problems that quantum computers can solve more efficiently than classical computers. The risk is significant, as quantum computing could render much of today's encrypted data vulnerable. To mitigate this, organisations need to conduct thorough risk assessments to identify systems and assets at high risk of quantum attacks and take steps to secure them.

4. The Role of AI in Cybersecurity and Quantum Risk Management

AI is playing an increasingly vital role in cybersecurity by helping organisations proactively address vulnerabilities and secure systems, including those at risk from quantum computing. Key AI applications in cybersecurity include:

- **Fraud Detection**: AI can analyse large volumes of transaction data in real-time, identifying fraud patterns and anomalies.
- **Security Automation**: AI enables automation of security processes, improving threat detection speed and reducing workload for cybersecurity professionals.

However, the growing reliance on AI introduces new risks, such as adversarial attacks that manipulate AI models. Organisations must balance the benefits of AI-driven security with strategies to secure AI systems themselves.

5. Integrating Quantum and AI for Strategic Advantage

Although quantum computing poses risks, it also offers opportunities. Some organisations are exploring how AI and quantum technologies can be integrated to create competitive advantages:

- **Quantum-Resistant Security**: Companies are developing technologies to ensure secure transactions in a post-quantum world, such as contactless technologies designed to withstand quantum attacks.
- **AI for Liquidity Management**: Financial institutions are investigating the potential of integrating AI with quantum computing to enhance liquidity management. For instance, HSBC has been exploring quantum computing applications, including portfolio optimization and risk assessment to enhance both security and operational efficiency[7].
- **Real-Time Analytics**: AI combined with quantum computing could be used to improve real-time analytics for customer transactions, enabling better security and customer service.

6. Collaboration and Knowledge Sharing

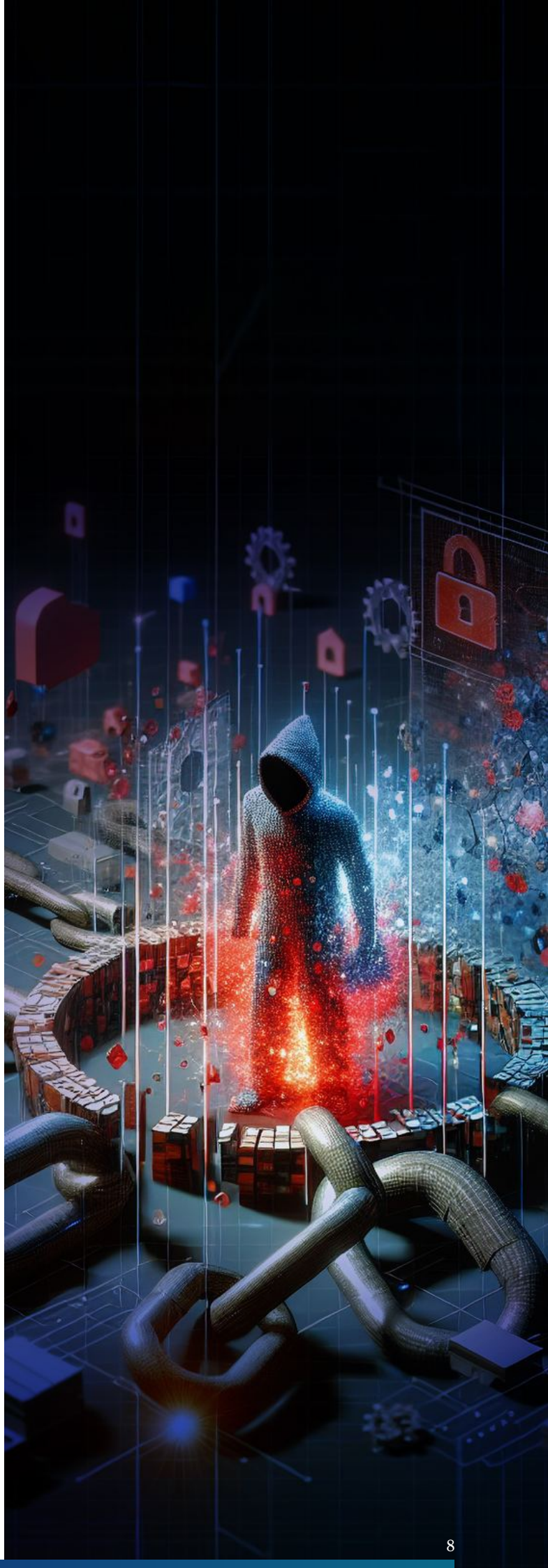
Collaboration is key to addressing the challenges posed by quantum computing and AI. Many companies are forming

© 2025 GFTN Limited, All Rights Reserved. Reproduction Prohibited.

partnerships with academic institutions and government agencies to drive research and innovation in both fields. For instance, collaborations with universities like Nanyang Technological University (NTU) in Singapore are helping businesses stay ahead in quantum computing and AI research[8]. Additionally, industry consortiums are essential for sharing insights, best practices, and research, enabling a unified approach to quantum risks and AI security.

7. Conclusion

The ongoing advancements in quantum computing present significant risks, particularly to cryptographic systems. Organisations must take proactive steps to prepare for a quantum-enabled future, focusing on updating cryptographic systems, implementing crypto agility, and leveraging AI to enhance cybersecurity. Collaboration across industries, academia, and governments will be crucial in addressing these challenges and ensuring secure, resilient infrastructures. By adopting quantum-resistant technologies and AI-powered security solutions, organisations can not only mitigate quantum computing risks but also unlock new opportunities for operational efficiency and customer differentiation.



© 2025 GFTN Limited, All Rights Reserved. Reproduction Prohibited.

Authors

Laurence Van der Loo

Sebastian Jerome Chin
Student, St. Joseph's Institution

Contributor

Yogesh Hirdaramani
Content Manager, GFTN

Production

Sachin Kharchane
Graphic Designer

© 2025 GFTN Limited, All Rights Reserved. Reproduction Prohibited.

References

1. Carr, B., Harper, J., Oppong, K., Clarke, et al. Programmable compliance – the future of integrating policy and regulation into tokenized assets and money. (n.d.). https://fintechfestival.sg/hubfs/SFF%202024/website/Agenda%20Booklet/Insights-Forum-Agenda-2024-10-04.pdf?hsLang=en

2. Cybersecurity Ventures. Cybercrime to cost the world $10.5 trillion annually by 2025. Cybercrime Magazine. (2024). https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

3. IBM. What is a cyberattack? . (n.d.). https://www.ibm.com/topics/cyber-attack

4. International Monetary Fund. Global Financial Stability Report. In World Economic and Financial Surveys [Report]. (2024). https://www.astrid-online.it/static/upload/imf_/0000/imf_gfsr-4-24.pdf.

5. National Audit Office. Investigation: WannaCry cyber attack and the NHS. (2018). https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

6. BankInfoSecurity. India to set 6-Hour breach reporting requirement. (n.d.). https://www.bankinfosecurity.com/india-to-set-6-hour-breach-reporting-requirement-a-18996

7. Bowers, R. Preparing for a quantum future: What's next for quantum computing in financial services? Fintech Futures. (2024) https://www.fintechfutures.com/2024/12/preparing-for-a-quantum-future-whats-next-for-quantum-computing-in-financial-services/

8. Singapore Inks MoU with Quantinuum, Enabling Access to their Advanced Quantum Computer. (n.d.). https://www.quantinuum.com/press-releases/singapore-inks-mou-with-quantinuum-enabling-access-to-their-advanced-quantum-computer

© 2025 GFTN Limited, All Rights Reserved. Reproduction Prohibited.

Global Finance &
Technology Network (GFTN)

6 Battery Road, #28-01, Singapore 049909
gftn.co | hello@gftn.com

Disclaimer: This document is published by Global Finance & Technology Network Limited (GFTN) as part of its FutureMatters insights platform. The findings, interpretations and conclusions expressed in GFTN Reports are the views of the author(s) and do not necessarily represent the views of the organisation, its Board, management or its stakeholders.

© 2025 Global Finance & Technology Network Limited, All Rights Reserved. Reproduction Prohibited.

© 2025 GFTN Limited, All Rights Reserved. Reproduction Prohibited.