



THE GLOBAL CYBER THREAT

Cyber threats to the financial system are growing,
and the global community must cooperate to protect it

Tim Maurer and Arthur Nelson

In February 2016, hackers targeted the central bank of Bangladesh and exploited vulnerabilities in SWIFT, the global financial system's main electronic payment messaging system, trying to steal \$1 billion. While most transactions were blocked, \$101 million still disappeared. The heist was a wake-up call for the finance world that systemic cyber risks in the financial system had been severely underestimated.

Today, the assessment that a major cyberattack poses a threat to financial stability is axiomatic— not a question of *if*, but *when*. Yet the world's governments and companies continue to struggle to contain the threat because it remains unclear who is responsible for protecting the system. Increasingly concerned, key voices are sounding the alarm. In February 2020, Christine Lagarde, president of the European Central Bank and former head of the International Monetary Fund, warned that a cyberattack could trigger a

The assessment that a major cyberattack poses a threat to financial stability is axiomatic—not a question of *if*, but *when*.

serious financial crisis. In April 2020, the Financial Stability Board (FSB) warned that “a major cyber incident, if not properly contained, could seriously disrupt financial systems, including critical financial infrastructure, leading to broader financial stability implications.” The potential economic costs of such events can be immense and the damage to public trust and confidence significant.

Two ongoing trends exacerbate this risk. First, the global financial system is going through an unprecedented digital transformation, which is being accelerated by the COVID-19 pandemic. Banks compete with technology companies; technology companies compete with banks. Meanwhile, the pandemic has heightened demand for online financial services and made work-from-home arrangements the norm. Central banks around the globe are considering throwing their weight behind digital currencies and modernizing payment systems. In this time of transformation, when an incident could easily undermine trust and derail such innovations, cybersecurity is more essential than ever.

Second, malicious actors are taking advantage of this digital transformation and pose a growing threat to the global financial system, financial stability, and confidence in the integrity of the system. The pandemic has even supplied fresh targets for hackers. The financial sector is experiencing the second-largest share of COVID-19–related cyberattacks, behind only the health sector, according to the Bank for International Settlements.

Who is behind the threat?

More dangerous attacks and ensuing shocks should be expected in the future. Most worrisome are incidents that corrupt the integrity of financial data, such as records, algorithms, and transactions; few technical solutions are currently available for such attacks, which have the potential to undermine trust and confidence more broadly. The malicious actors behind these attacks include not only increasingly daring criminals—such as the Carbanak group, which targeted financial institutions to steal more than \$1 billion during 2013–18—but also states and state-sponsored attackers (see table). North Korea,

for example, has stolen some \$2 billion from at least 38 countries in the past five years.




This is a global problem. While cyberattacks in high-income countries tend to make headlines, less attention is paid to the growing number of attacks on softer targets in low- and lower-middle-income countries. Yet it is in those countries where the push toward greater financial inclusion has been most pronounced, leading many to leapfrog to digital financial services such as mobile payment systems. Although they do advance financial inclusion, digital financial services also offer a target-rich environment for hackers. The October 2020 hack of Uganda’s largest mobile money networks, MTN and Airtel, for example, resulted in a major four-day disruption of service transactions.

The responsibility gap

Despite the global financial system’s increasing reliance on digital infrastructure, it is unclear who is

A closer look at cyberattacks

The actors behind these incidents include not only increasingly daring criminals but also states and state-sponsored groups, with diverse goals and motivations.

THREAT ACTOR	MOTIVATIONS	GOALS	EXAMPLES
 <p>Nation-states, state-sponsored groups</p>	Geopolitical, ideological	Disruption, destruction, damage, theft, espionage, financial gain	Permanent data corruption, targeted physical damage, power grid disruption, payment system disruption, fraudulent transfers, espionage
 <p>Cybercriminals</p>	Enrichment	Theft/financial gain	Cash theft, fraudulent transfers, credential theft
 <p>Terrorist groups, hacktivists, insider threats</p>	Ideological, discontent	Disruption	Leaks, defamation, distributed denial-of-service attacks

Source: European Systemic Risk Board. 2020. “Systemic Cyber Risk.” https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemicyberrisk~101a09685e.en.pdf

Without dedicated action, the global financial system will only become more vulnerable as innovation, competition, and the pandemic further fuel the digital revolution.

responsible for protecting the system against cyberattacks. In part, this is because the environment is changing so quickly. Without dedicated action, the global financial system will only become more vulnerable as innovation, competition, and the pandemic further fuel the digital revolution. Although many threat actors are focused on making money, the number of purely disruptive and destructive attacks has been increasing; furthermore, those who learn how to steal also learn about the financial system's networks and operations, which allows them to launch more disruptive or destructive attacks in the future (or sell such knowledge and capabilities to others). This rapid evolution of the risk landscape is taxing the responsiveness of an otherwise mature and well-regulated system.

Better protecting the global financial system is primarily an organizational challenge. Efforts to harden defenses and toughen regulation are important but are not enough to outpace the growing risks. Unlike many sectors, most of the financial services community does not lack resources or the ability to implement technical solutions. The main issue is a collective action problem: how best to organize the system's protection across governments, financial authorities, and industry and how to leverage these resources effectively and efficiently.

The current fragmentation among stakeholders and initiatives partly stems from the unique aspects and evolving nature of cyber risk. Different communities operate in silos and tackle the issue through their respective mandates. The financial supervisory community focuses on resilience, diplomats on norms of state behavior, national security agencies on trying to deter malicious activity, and industry executives on firm-specific rather than sector-specific risks. As lines between financial services firms and tech companies become ever more fuzzy, the lines of responsibility for security are likewise increasingly blurred.

The disconnect between the finance, the national security, and the diplomatic communities is particularly pronounced. Financial authorities face

unique risks from cyber threats, yet their relationships with national security agencies, whose involvement is necessary to effectively tackle those threats, remain tenuous. This responsibility gap and continued uncertainty about roles and mandates to protect the global financial system fuel risks. Part of this uncertainty is due to the current geopolitical climate and high levels of mistrust, which hinder collaboration among the international community. Cooperation on cybersecurity has been hampered, fragmented, and often limited to the smallest circles of trust because it touches on sensitive national security equities. International and multi-stakeholder cooperation is not a "nice-to-have" but a "need-to-have."

An international strategy

To achieve more effective protection of the global financial system against cyber threats, the Carnegie Endowment for International Peace released a report in November 2020 titled "International Strategy to Better Protect the Global Financial System against Cyber Threats." Developed in collaboration with the World Economic Forum, the report recommends specific actions to reduce fragmentation by fostering more collaboration, both internationally and among government agencies, financial firms, and tech companies.

The strategy is based on four principles: first, *greater clarity about roles and responsibilities is required*. Only a handful of countries have built effective domestic relationships among their financial authorities, law enforcement, diplomats, other relevant government actors, and industry. Existing fragmentation hampers international cooperation and weakens the international system's collective resilience, recovery, and response capabilities.

Second, *international collaboration is necessary and urgent*. Given the scale of the threat and the system's globally interdependent nature, individual governments, financial firms, and tech companies cannot effectively protect against cyber threats if they work alone.

Third, *reducing fragmentation will free up capacity to tackle the problem*. Many initiatives are underway to better protect financial institutions, but they remain siloed. Some of these efforts duplicate each other, increasing transaction costs. Several of these initiatives are mature enough to be shared, better coordinated, and further internationalized.

Fourth, *protecting the international financial system can be a model for other sectors*. The financial system is one of the few areas in which countries have a clear shared interest in cooperation, even when geopolitical tensions are high. Focusing on the financial sector provides a starting point and could pave the way to better protection of other sectors in the future.

Among actions for strengthening cyber resilience, the report recommends that the FSB develop a basic framework for supervising cyber risk management at financial institutions. Governments and industry should strengthen security by sharing information on threats and by creating financial computer emergency response teams (CERTs), modeled on Israel's FinCERT.

Financial authorities should also prioritize increasing the financial sector's resilience against attacks targeting data and algorithms. This should include secure, encrypted data vaulting that allows members to securely back up customer account data overnight. Regular exercises to simulate cyberattacks should be employed to identify weaknesses and develop action plans.

To reinforce international norms, the report recommends that governments make clear how they will apply international law to cyberspace and strengthen norms to protect the integrity of the financial system. The governments of Australia, The Netherlands, and the United Kingdom have already taken a first step with statements indicating that cyberattacks from abroad may be regarded as illegal use of force or intervention in the domestic affairs of another state.

Cyber resilience and strengthened international norms can facilitate collective response through law enforcement actions or multilateral reaction with industry. Responses can include sanctions, arrests, and asset seizures.

Governments can support these efforts by establishing entities to assist in assessing threats and coordinating responses. Intelligence gathering should include a focus on threats to the financial system, and governments should share such intelligence with allies and like-minded countries.

Building capacity

The comprehensive strategy outlined in the Carnegie report depends in turn on building the cybersecurity workforce, expanding the financial sector's cybersecurity capacity, and safeguarding gains in financial inclusion that have resulted from the digital transformation.

Elevated unemployment due to the pandemic provides an important opportunity for training and hiring talented people to strengthen the cybersecurity workforce. Financial services firms should invest in initiatives to build the talent pipeline, including high school, apprenticeship, and university programs.

Building cybersecurity capacity means focusing on providing assistance where it is needed. The IMF and other international organizations received many requests for cybersecurity assistance from member states, particularly following the 2016 Bangladesh incident. G20 governments and central banks could create an international mechanism to build cybersecurity capacity for the financial sector, with an international agency such as the IMF designated to coordinate the effort. The Organisation for Economic Co-operation and Development and international financial institutions should make cybersecurity capacity building an element of development assistance packages and should significantly increase assistance to countries in need.

Finally, maintaining progress in financial inclusion requires strengthening connections between financial inclusion and cybersecurity. This is particularly urgent in Africa, with many countries on the continent experiencing a significant transformation of their financial sectors as they extend financial inclusion and move to digital financial services. A network of experts should be created to focus specifically on cybersecurity in Africa.

The time has come for the international community—including governments, central banks, supervisors, industry, and other relevant stakeholders—to come together to address this urgent and important challenge. A well-thought-out strategy, such as the one above, provides a blueprint for turning words into action. **FD**

TIM MAURER is the director of the Cyber Policy Initiative and a senior fellow in the Carnegie Institute of International Peace's Technology and International Affairs Program.

ARTHUR NELSON is a research analyst in Carnegie's Cyber Policy Initiative.