CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

WORKING PAPER

NOVEMBER 2020

Cyber Policy Initiative Working Paper Series | "Cybersecurity and the Financial System" #8

# Enduring Cyber Threats and Emerging Challenges to the Financial Sector

Adrian Nish, Saher Naumaan, and James Muir

# Enduring Cyber Threats and Emerging Challenges to the Financial Sector

Adrian Nish, Saher Naumaan, and James Muir

For your convenience, this document contains hyperlinked source notes indicated by teal-colored text.



Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

# CONTENTS

## Cybersecurity and the Financial System

Carnegie's working paper series "Cybersecurity and the Financial System" is designed to be a platform for thought-provoking studies and in-depth research focusing on this increasingly important nexus. Bridging the gap between the finance policy and cyber policy communities and tracks, contributors to this paper series include government officials, industry representatives, and other relevant experts in addition to work produced by Carnegie scholars. In light of the emerging and nascent nature of this field, these working papers are not expected to offer any silver bullets but to stimulate the debate, inject fresh (occasionally controversial) ideas, and offer interesting data.

If you are interested in this topic, we also invite you to sign up for Carnegie's FinCyber newsletter providing you with a curated regular update on latest developments regarding cybersecurity and the financial system: CarnegieEndowment.org/subscribe/fincyber.

If you would like to learn more about this paper series and Carnegie's work in this area, please contact Tim Maurer, director of the Cyber Policy Initiative, at tmaurer@ceip.org.

### Papers in this Series:

- "Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios," Jon Bateman, July 2020
- "Cyber Mapping the Financial System," Jan-Philipp Brauchle, Matthias Göbel, Jens Seiler, and Christoph von Busekist, April 2020
- "Lessons Learned and Evolving Practices of the TIBER Framework for Resilience Testing in the Netherlands," Petra Hielkema, and Raymond Kleijmeer, October 2019
- "Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment," Lincoln Kaffenberger and Emanuel Kopp, September 2019
- "Cyber Resilience and Financial Organizations: A Capacity-building Tool Box," Tim Maurer and Kathryn Taylor, July 2019
- "The Cyber Threat Landscape: Confronting Challenges to the Financial System" Adrian Nish and Saher Naumaan, March 2019
- "Protecting Financial Institutions Against Cyber Threats: A National Security Issue" Erica D. Borghard, September 2018

## Introduction

At the time of writing, several financial services firms are working to restore their networks following disruptive cyber attacks. Banks in Chile and Seychelles, as well as financial technology companies like Silverlake Axis, a supplier of core banking systems throughout the Asia-Pacific, are all reportedly victims of separate ransom and extortion attempts.[1] Elsewhere, the threat from cyber criminals triggered a suspension of automatic teller machine (ATM) transactions overnight, and hackers recently knocked websites associated with a stock exchange offline using distributed denial-of-service (DDoS) attacks.[2] Such disruptions not only impact customers of these services, but also undermine the confidence of peers in the financial services community. Regulators have been taking increasing notice of these cyber threats, and operational resilience has shot to the top of agendas around the world.

A few years ago, targeted attacks on financial services sector firms were still relatively rare. However, cases have increased in recent years as capabilities and specialisms such as network intrusion have advanced. BAE Systems in partnership with the Carnegie Endowment for International Peace has documented public examples via the Timeline of Cyber Incidents Involving Financial Institutions.[3] This timeline serves as a useful resource in tracking trends, even though public cases are just the tip of the iceberg and the true volume of incidents and near misses is much greater.

This paper provides an overview of the cyber threat landscape with respect to the financial sector (see figure 1). It is designed to complement Carnegie's International Cybersecurity Strategy for the Financial System supported by the World Economic Forum.[4] It also builds on a previous cyber threat overview published in March 2019.[5] This paper discusses the current landscape from three perspectives: enduring threats, evolving techniques, and emerging challenges. Each section also includes a focus piece describing a particular technology problem. The summary of observations and conclusions includes a review of advances in cyber resilience testing schemes.

FIGURE 1

**Cybersecurity Challenges for the Financial Services Sector Cover a Wide Range of Topics**


**SOURCE:** BAE Systems, 2020

## Enduring Threats

Only eighteen months have passed since the last Carnegie FinCyber paper on the cyber threat landscape. But a lot has happened since, most notably the largest-scale public health emergency in a century. Cyber threat actors have not stood still in this period. Many groups have been capitalizing on the turbulence in order to up their game and exploit their victims. Stepping back from this, however, the predominant motivations have not changed (see table 1).

TABLE 1
**Motivations and Capabilities of Threat Actors**

| Category | Hackers and Hacktivists | Criminals and Cheaters | States and Spies |
|---|---|---|---|
| Motives | Curiosity, attention, revenge, social justice, and/or causes | Money, more money, and even more money | National service, defense or offense against state adversaries, and/or medals and commendations |
| Capabilities | Typically low, such as re-use of off-the-shelf tools, basic scripts, or web resources | Moderate. Many attacks are simple but effective, though some groups write and deploy custom tools. | Ranges from low to very high. These are persistent adversaries with resources to try many vectors to compromise a target. |
| Response to the coronavirus pandemic | As organizations have enabled greater remote working, there has been more exposure of vulnerable, external-facing services. Nefarious actors have increased their scanning and exploitation of these for a variety of end goals. | The pandemic has created opportunities for scammers, both leveraging it as part of social engineering lures, as well as actively stealing funds such as furlough payments.[6] Organized criminal groups have doubled down on ransom and extortion tactics in particular. | Although some threat groups were impacted by the home working restrictions (for example, they were unable to access operational systems), the need for intelligence on pandemic responses created a demand to be filled. Many groups have ramped up their efforts and shifted their targeting as a result. Disinformation has also been rife, with politically motivated actors seeking to sow discord in target communities. |

The nature of these enduring threats is such that they change little over time. Actors' motivations exist outside of the cyber domain, and the internet is merely a means to an end. While their tools and techniques evolve, it is likely this rough segmentation will serve as a useful model for years to come.

One vector all of these groups use is the targeting of outdated and legacy technology within enterprise networks (see box 1).

BOX 1

**Technology Focus—Legacy Infrastructure**

Financial services firms, from central banks to retail banks and insurers, have been grappling with legacy infrastructure for many years. While this is true of many, if not all, other sectors, the problem is especially acute in finance due to the widespread reliance on core systems that are many decades old and that have often been joined together as a result of various mergers and acquisitions. The industry's reliance on software programmed in common business-oriented language (COBOL) is well-known, with the number of qualified engineers that can maintain these codebases dropping each year.

A recent report by the United Kingdom's Treasury Committee into information technology (IT) failures in the financial services sector found that not enough was being done to mitigate operational risks posed by legacy technology and that organizations must ensure that the use of legacy systems remains appropriate.[7]

Many have argued that overhaul of legacy systems should be coupled with taking advantage of cloud technology.[8] However, this requires careful planning and is not as simple as a so-called lift-and-shift. For example, legacy login credentials quickly result in current breaches if systems are inadvertently exposed to the internet. Organizations need to sort out such skeletons in the closet before migrating to the cloud.

A notable project in upgrading legacy infrastructure is the Bank of England's Real Time Gross Settlement Renewal Programme (RTGS2).[9] Many central banks around the world are monitoring this closely, with expected completion for the project around 2024. Among the main principles driving RTGS2 are higher levels of resilience and blending current needs with future-proofing—for example, retaining the financial messaging service SWIFT for connectivity and messaging services but being message-network agnostic in design.[10] Notably, the use of blockchain-type Distributed Ledger Technology (DLT) was considered for RTGS2, but it was found insufficiently mature for use.[11]

## Evolving Techniques

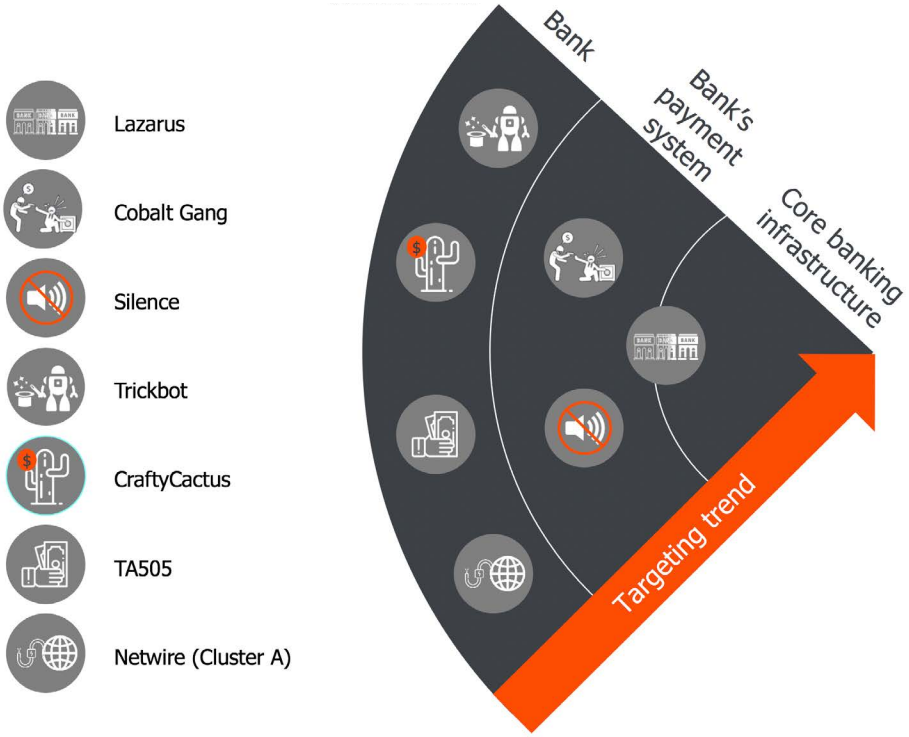
While the motivations of the various threat groups have not changed much, the techniques used to achieve their goals continue to evolve. This section highlights two areas that are key concerns to financial services sector firms today: targeted intrusions and ransom and extortion attacks.

## Targeted Intrusions

Some of the most significant threats to the financial system come from state or organized criminal groups seeking to steal funds. An overarching trend among threat actors in recent years has been their steady progression into deeper levels of financial infrastructure. Figure 2 highlights different threat groups that specifically target banks and their capability and intent to target different levels of financial infrastructure.

FIGURE 2

**Many Threat Groups Can Compromise Bank Networks but Only Some Reach Core Infrastructure**




**SOURCE:** BAE Systems, 2020

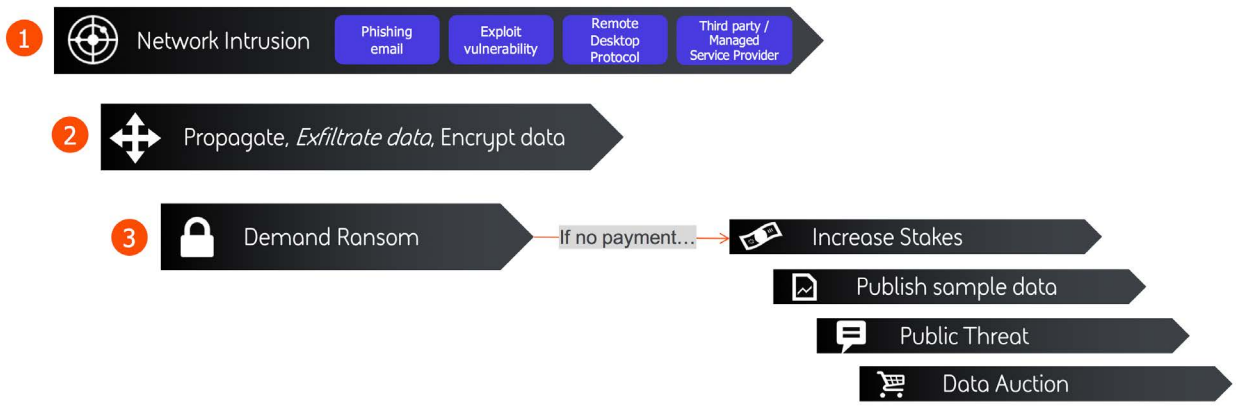
Several of these groups are expert at using sophisticated penetration testing tools, such as Cobalt Strike and PowerShell Empire.[12] These tools have advanced significantly in recent years. They contain features that make detection on enterprise networks particularly difficult. Such features include: living-off-the-land techniques, which leverage preexisting Windows tools such as PowerShell; in-memory infection, where the malware doesn't write any files to disk, in order to hamper antivirus detection; and domain name system (DNS) command-and-control modules, which can effectively evade web-proxy controls and intrusion detection tools.

## Ransom and Extortion

Ransomware has evolved from the early years of basic locker malware targeting millions of end users via phishing emails to today's sophisticated attacks against large corporations and public institutions causing millions of dollars of damages on an increasingly regular basis (see figure 3). In another recent shift in tactics, criminal groups now steal data from company networks prior to encryption and threaten to publicly release the data on their ransomware blogs if the victim does not pay up.

FIGURE 3

**Simplified Stages of a Modern Ransomware Attack with Data Theft and Extortion**



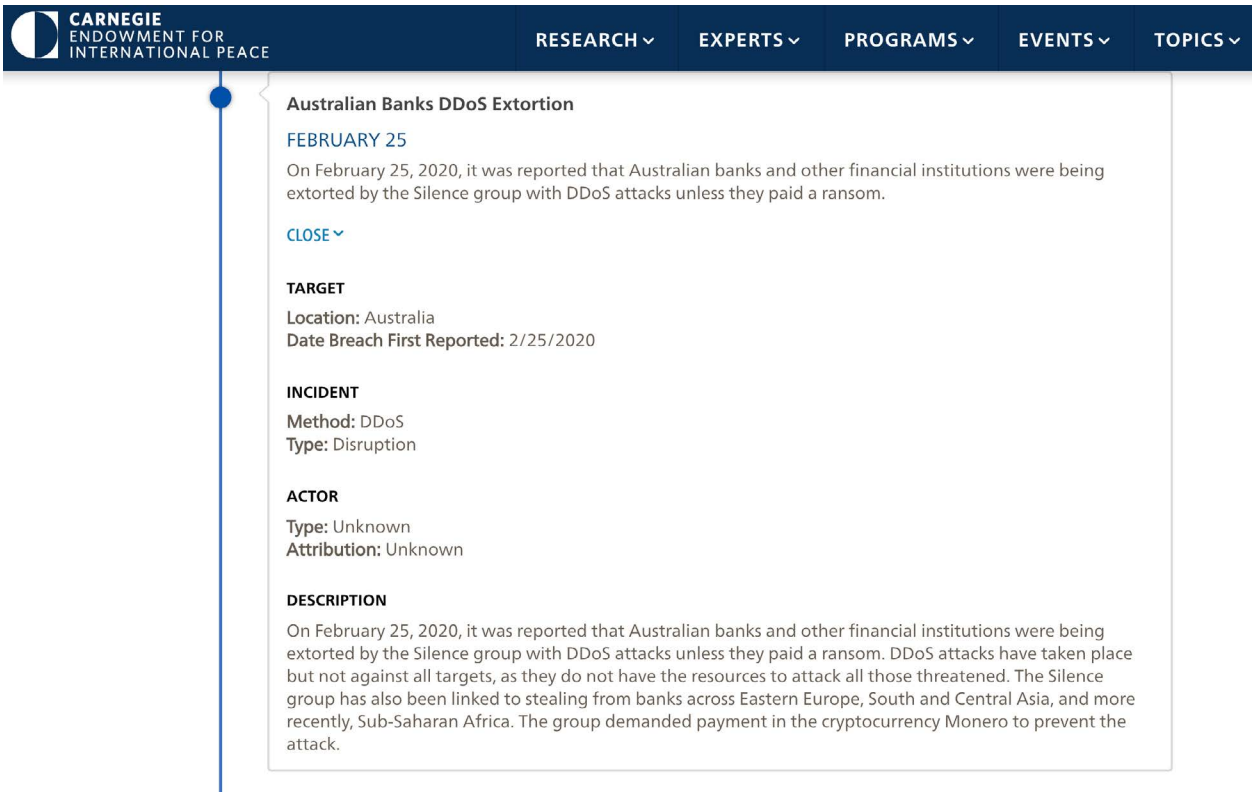

**SOURCE:** BAE Systems, 2020

The most commonly targeted sector for this type of ransomware attack is industrial and manufacturing organizations. However, as discussed in the opening section of this paper, financial services and the financial services supply chain have also been targeted recently (see figure 4). Criminals' use of new data-leaking tactics in 2020 has put increased pressure on their victims to pay, for fear that sensitive customer or commercial information will be publicly released. This could do far more damage than a traditional encryption attack, where the costs (if no ransom is paid) are purely for remediation and IT cleanup. Additional data privacy requirements (such as the European Union's General Data Protection Regulation [GDPR]) and the publicity that these attacks generate can also cause significant reputational damage to an organization.

A different twist on a ransom attack is where DDoS techniques are used to create the attack against an organization, rather than ransomware. In recent months there has been an increase in this so-called DDoS for extortion attack mode (see figure 4).

FIGURE 4

**Australian Bank DDoS Extortion**




**SOURCE:** "Timeline of Cyber Incidents Involving Financial Institutions," Carnegie Endowment for International Peace, updated August 2020, https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

The following case study demonstrates the damage a successful ransomware attack can have on a financial services organization.

## Case Study: Travelex & REvil

On December 31, 2019, the London-based foreign currency exchange Travelex was hit by a ransomware attack that crippled its network and allegedly stole five gigabytes of documents. The attackers demanded Travelex pay $6 million to restore its systems and prevent the stolen data from being leaked online. This attack had a devastating effect on Travelex, reducing their operations to pen and paper transactions and impacting a wide range of high street banks that relied upon its currency services. Reports estimated that the attack ultimately cost the firm almost $30 million and put their parent company, Finablr, under significant financial pressure, with $2.3 million reportedly paid in ransom (see figure 5).[13] Travelex subsequently filed for bankruptcy, citing the coronavirus pandemic and the cyber attack as key factors.[14]

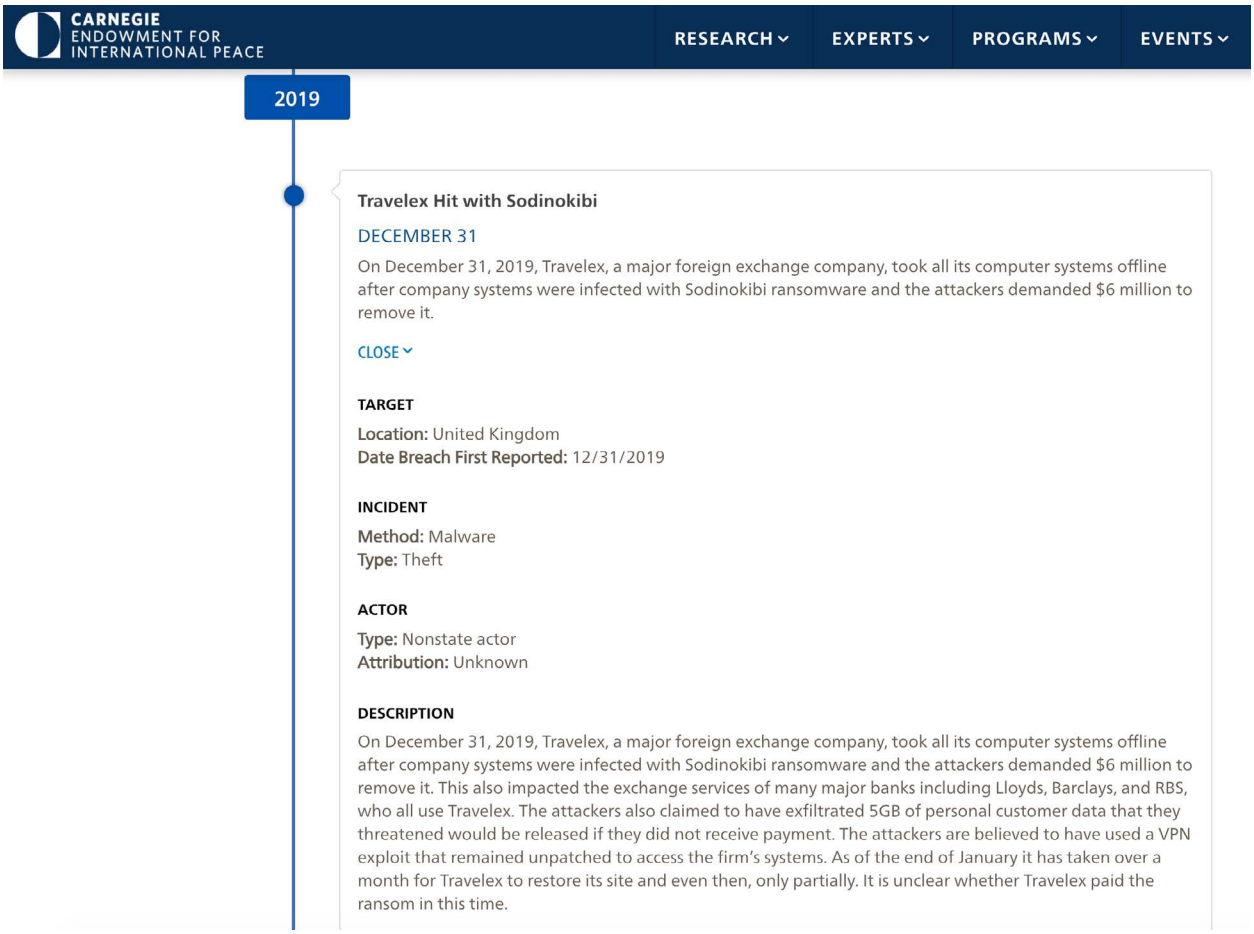
FIGURE 5
**Headlines to a Ransomware Attack Can Be as Damaging as the Intrusion**


**SOURCE:** BAE Systems, 2020

The threat actors responsible for this attack used a prolific ransomware variant called REvil, one of the pioneers in this new wave of data theft ransomware attacks. The threat group, also called REvil, has since gone on to undertake similar attacks against a wide range of victims. The attackers work on an affiliate model whereby attackers can purchase a subscription to use the malware to perform their own attacks but publish stolen data to a central blog (see figure 6). REvil affiliates predominantly favor attacks on the financial and insurance sector.

FIGURE 6

**Travelex Hit with Sodinokibi**




**SOURCE:** "Timeline of Cyber Incidents Involving Financial Institutions," Carnegie Endowment for International Peace, updated August 2020, https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

Although most ransom and extortion attacks target enterprise networks, regardless of where these services are hosted, cloud services have been specifically exploited by criminal groups.[15] This is just part of a growing concern over threats to cloud technology, another focus area for many financial services firms (see box 2).

BOX 2

## Technology Focus—Cloud

Undoubtedly the major technology trend for the finance industry in the last decade is the shift to cloud services. As more and more companies move to a cloud-first strategy or make some level of transition to the cloud and as the range of services that are available via cloud deployment continues to increase, this trend is likely to remain at the top of C-suite lists for many years to come.

Outside of the technical challenges of making this shift, there are a number of security-related concerns that consistently come into play and will feature on many internal risk registers. Each of the following concerns brings a level of complexity and a requirement for in-house expertise:

- Concerns over data residency are tangible on a backdrop of increased data regulation and a concern that businesses could—without paying attention to cloud platform terms and conditions—fall foul of data retention or privacy laws in different countries.

- The (albeit unlikely) scenario of a major cloud provider suffering a major outage that exceeds their own redundancy measures and an ability to meet customer-service-level agreements on availability has led to many companies adopting a multicloud approach, running services from Amazon Web Services, Azure, Google, and the like.

- The shared responsibility model for different cloud platforms can be a sticking point, and fully understanding which responsibilities rest with the organization, as well as how to achieve an appropriately secure configuration, can require extensive expertise. Many organizations have needed to train their staff in different cloud models, with larger organizations requiring hundreds of trained personnel in different areas.

The question of configuration remains the main security issue for cloud adoption. Examples of data breaches arising from inappropriately configured cloud storage have been seen in recent years. Despite improvements by cloud service providers trying to make it harder for these errors to occur, they are still happening. According to the 2020 Verizon Data Breach Investigations Report, 22 percent of data breaches in 2019 involved cloud assets, and misconfiguration errors (many of which are related to cloud) are now the most common type of error reported in Verizon's data.[16]

The major cloud platforms each have very high standards of security and extensive resources at their disposal. To date, their security records have been very strong. The question of whether and how a data breach at a cloud provider might occur is an interesting one, but a common viewpoint held across many industry sectors is that data and services are safer in the hands of a major cloud provider than they would be on premises. However, while that may well be correct from an individual organization's perspective, from a sector and financial services regulatory perspective, concerns around aggregation risk come to the fore, with many firms reliant on a few core IT service providers for so many critical financial services.

It is inevitable that as more and more assets are in the cloud, the threat landscape will shift to focus on technology supply chains and cloud providers—as has already begun to happen. It is highly likely that critical vulnerabilities that allow for hypervisor or virtual machine breakout (meaning that a threat actor on one public cloud instance can compromise others) will arise in the future. The arms race between these being discovered by security teams and researchers versus threat actors will be similar to that which plays out in major operating systems and software products.

## Emerging Challenges

### Threat Group Collaboration and Facilitation

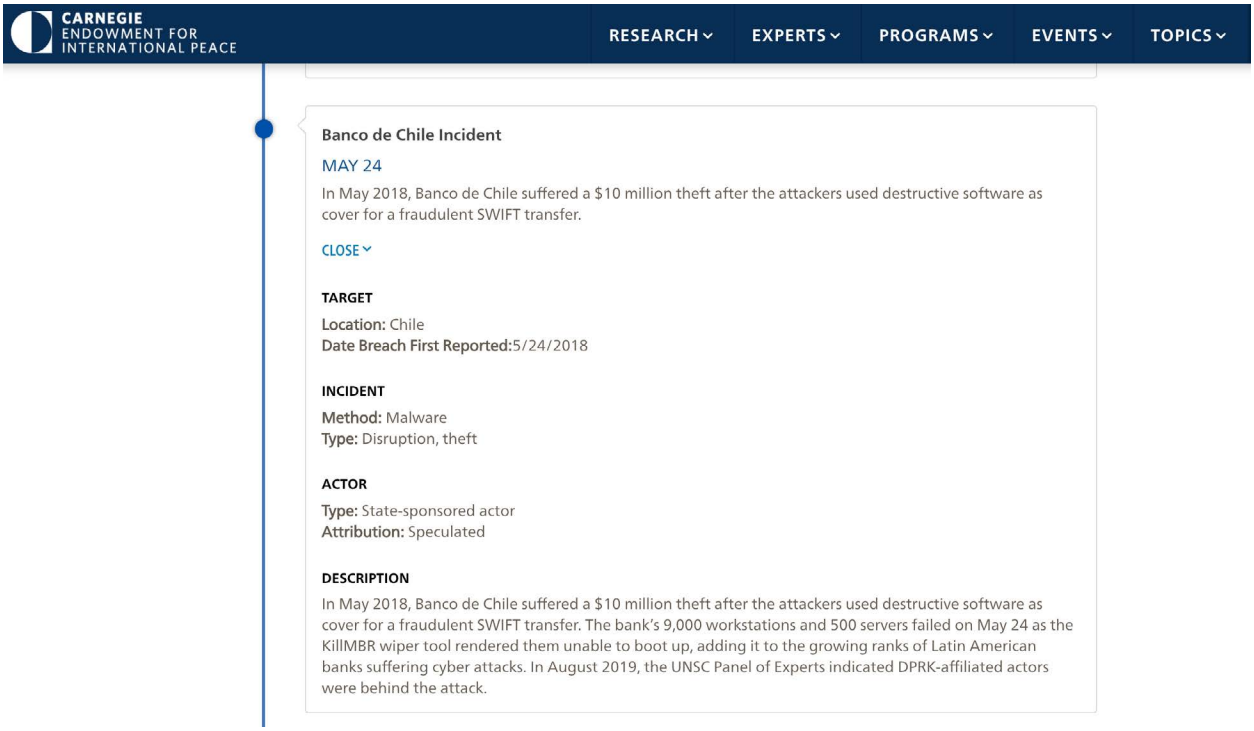
The evolution of the threat landscape features greater collaboration among threat actors. In 2018, several infections from the North Korea–based Lazarus Group coincided on networks within the same time frames as a Russian-speaking criminal group known as TA505.[17] Forensic evidence from incident response work confirmed the overlap wasn't purely coincidental; the criminal actors were found to have effectively handed over access to Lazarus. A few theories on the nature of the relationship between TA505 and Lazarus were considered, but the most likely one was a transactional relationship where TA505 sold victim network access to Lazarus.[18]

While instances of TA505 and Lazarus overlap may have subsided, overlaps between Lazarus and other criminal operations have come to light. Other incidents of transactional relationships or collaboration appeared again in 2020. Infections with the criminal malware Trickbot led to the deployment of Lazarus malware, which might indicate a similar scenario of Lazarus buying access from another party. Others have reported that a Trickbot-related framework called Anchor was also associated with Lazarus malware.[19]

TA505, meanwhile, has been busy providing access to other groups. For example, Silence, a Russian-speaking criminal group, also appears to have a relationship with TA505. During a 2019 BAE Systems investigation of a Silence intrusion against a European bank, Silence malware was deployed off the back of an initial TA505 intrusion.[20] This suggests the group also has links to other parties within the criminal underground.

Cyber criminals have created an ecosystem that is strengthened by collaboration and transactions to buy or sell products and services. They have capitalized on the intersection of cyber crime and fraud in their operation of modern criminal enterprises; an overview of how the flow between a cyber attack and cashing out and money laundering works can be found in a paper recently published by SWIFT and BAE Systems.[21] Hacking tools as well as cashing-out and money laundering services are available in criminal marketplaces to facilitate the demand (see figure 7).

FIGURE 7
**Banco de Chile Incident**




**SOURCE:** "Timeline of Cyber Incidents Involving Financial Institutions," Carnegie Endowment for International Peace, updated August 2020, https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

## Hackers-for-Hire

Hackers-for-hire is another growing trend. Malicious actors don't always carry out their own operations; they outsource them to hacker groups.[22] Paid attackers and companies are routinely hired by governments and commercial clients to infiltrate targets. There is a wide scope of these groups in capability, ranging from running information operations to selling complete malware frameworks.

Over the course of 2020, significant media attention has emerged around an alleged hackers-for-hire company operating out of New Delhi.[23] This firm had a far-reaching scope of targeting across the globe, but one of the most prominent target verticals was the financial sector.[24] Several international banks, investment firms, insurance companies, and offshore banking and finance entities were among the targets, as were hedge funds, short sellers, and financial journalists. The industry seems to have been targeted around issues of market manipulation, legal cases, and corporate espionage.[25] While the reasons for these activities may vary, parts of the financial system are increasingly caught in the crosshairs of professional hackers-for-hire.

## Disinformation and Deepfakes

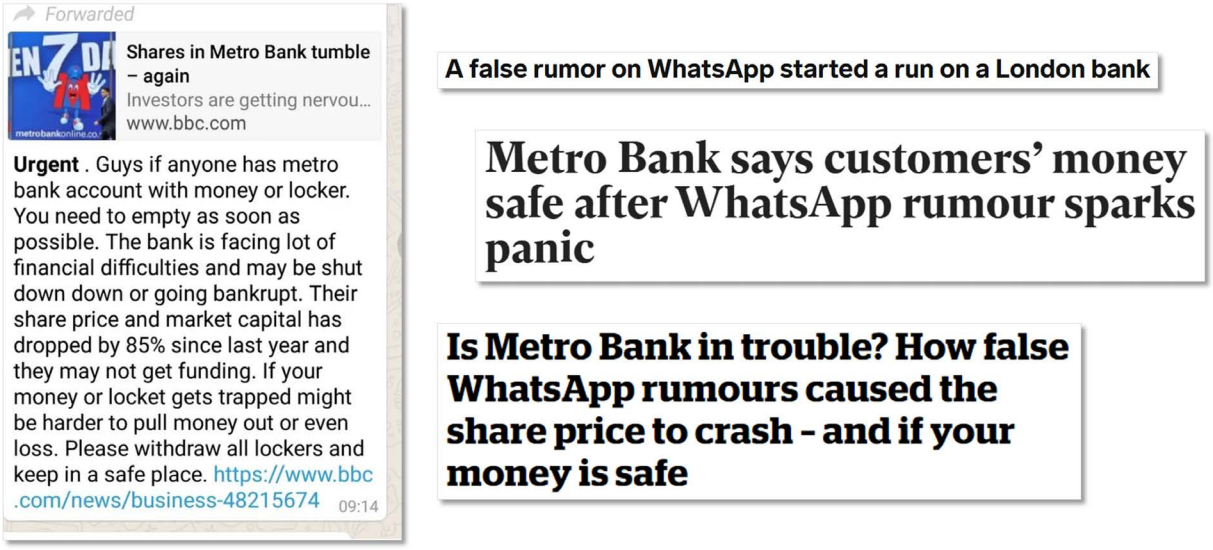
The rise of disinformation campaigns or "fake news," often spread via social media, is increasingly causing a headache for companies around the world.[26] In its 2019 Global Risks Report, the World Economic Forum found that one of the most widespread and disruptive impacts of artificial intelligence (AI) in recent years has been its role in the rise of "media echo chambers and fake news."[27]

For financial services, where transactions happen in a fraction of a second, disinformation campaigns are a significant cyber threat and often play a role in large-scale attempts at market manipulation. An example of such an attack is the January 2019 hacktivism attack on BlackRock, the world's largest asset manager. In this incident a group of environmental campaigners wrote a fake "Dear CEO" letter purporting to be from BlackRock Chief Executive Officer Larry Fink. The letter was sent to clients and media publications from an authentic-looking email address and was hosted on a website that closely resembled the official BlackRock site. The letter made numerous false claims and was picked up and published widely by various media outlets.[28] Although this incident was rooted in protest and not for financial gain, it does demonstrate the simplicity with which these campaigns can be successful. Social media and the use of troll farms and bots now means that disinformation campaigns can be incredibly complex, with intentionally misleading messages released and amplified so that they seep into mainstream consciousness and blur the line between fact and fiction. Financial markets are particularly susceptible to disinformation-driven manipulation because often, the markets are driven by perceptions relating to fears, and the resulting speculation presents opportunities for threat actors to benefit.

For example, in May 2019, Metro Bank in the United Kingdom saw its share price drop at least 9 percent after false rumors circulated on WhatsApp and Twitter that the bank was close to collapse and that customers should empty their accounts as soon as possible (see figure 8).[29]

FIGURE 8

**Fake WhatsApp Message and Resulting Headlines Around Metro Bank**




**SOURCE:** BAE Systems, 2020

An attack of this kind could be beneficial for threat actors trying to manipulate the market for financial gain, but it could also be used by states for sowing division and undermining the integrity of a country's financial infrastructure. With the world in the midst of the coronavirus pandemic, disinformation and misinformation seem to be at an all-time high, with the fear and uncertainty of the modern age feeding into the spread of rumors and fake news, often to the benefit of unseen threat actors.

In recent years, AI has generated a lot of hype around how it will change today's technologies and processes. However, as with all technology, AI can be put to malicious as well as beneficial use; a 2020 study published by the Dawes Centre for Future Crime at UCL ranked twenty ways AI could be used to facilitate crime over the next fifteen years, with fake audio and video clips called "deep-fakes"—which can be used to fraudulently obtain funds—being one of the highest concerns.[30]

Concerns around the use of AI-driven deepfake technology being used to commit fraud or gain access to confidential information should apply to all interactions that rely on voice-based authentication, including automated voice recognition authentication as well as more traditional

human-based phone calls. Cases of fraudsters seeking to use deepfake technology have been seen,[31] and with the growing development of deepfake technology and the expected ease with which such technology will become available to criminal actors, there is potential for this increasingly to be used in fraud or disruptive cyber attacks.[32] However, other new technologies also present similar risks (see box 3).

BOX 3

**Technology Focus—Quantum Computing and Cryptanalysis**

While the cloud technology paradigm is a pressing issue at present, another technological leap looms large on the horizon. Quantum computing can provide exponential improvements in processing power by taking advantage of quantum mechanical properties, and while still very much in the research and development stage, quantum computers are likely to become more readily available in decades to come.

For the finance industry, this has a number of implications. First is the question of what quantum computing can offer to improve finance applications: trading calculations and modeling and fraud detection, to start. While quantum computers are not readily available to test, proof-of-concepts have been conducted in this area using quantum-inspired computing.[33] One of the companies leading the way in commercial application of quantum computing is IBM, who highlights a number of potential applications to finance.[34]

On the flip side of this is the upheaval that a quantum computing–enabled future will bring to current cryptography. The ongoing advances in quantum computing will bring with them a major shake-up in current cryptography standards—asymmetric cryptography based on public/private keys (such as RSA and ECC) is vulnerable to attack from a quantum computer. The current expectation is that RSA-2048 will be cracked by quantum computing by 2031, with estimates for realization of so-called quantum cryptanalysis being revised down, rather than up.[35]

The timelines relevant to assessing the risk of quantum cryptanalysis involve a number of factors. Predictions from the U.S. National Institute of Standards and Technology for standardization of algorithms that can provide post–quantum cryptography give 2024 as a potential date, but complete implementation of these algorithms and integration with current technology could take twenty years.[36] Estimates of when quantum cryptanalysis may become available range between 2026 and 2031. A hypothetical financial product or system designed today may be deployed in 2025 and could be expected to have a lifetime of twenty years.

While these figures are very rough and many of these factors are case-dependent and could change in future, both demonstrate the potential for a period of time where quantum cryptanalysis is available and in which quantum-proof algorithms are not yet widely implemented (and integrated with existing technology).

The implications of this are significant for all domains and for all services on the internet. The impact on the financial system will vary on a case-by-case basis, but in general, the emergence of quantum cryptanalysis will require careful planning in mitigation.

For both of the aspects covered above, many organizations are appointing champions to keep on top of developments and to be able to plan for and react to changes in the availability of quantum computing appropriately.

## Cyber Resilience and Testing Schemes

In response to the threats outlined in this report, as well as the broader threat landscape, regulators have been increasingly concerned about cybersecurity risks to the financial services sector. Operational resilience, encompassing cyber resilience, has been toward the top of the agenda for financial services regulators including the Bank of England and the Basel Committee.[37] In a sector that is heavily reliant on trust, financial services firms that are designed to be resilient can differentiate themselves and gain competitive advantage. If organizations do not seek to minimize the occurrence of service disruptions in advance—or to at least detect, respond, and recover quickly when they do occur—there is the potential for significant harm to financial market stability, organization reputations, and consumer finances. This makes it paramount that firms consistently, methodically, and frequently assess their resilience posture and take decisive action to close any identified vulnerabilities through targeted investment decisions.

To address the topic of cyber resilience and help firms identify vulnerabilities that could be exploited by attackers to impact important business services, the Bank of England developed the CBEST framework in 2014 for financial institutions in the United Kingdom. In order to test cyber resilience, CBEST takes a threat intelligence–led approach to defining cyber attack scenarios. These are then tested, mimicking the tactics, techniques, and procedures of real-life attackers, in order to help improve the financial services firm's cyber maturity. Since then, several other schemes have emerged in other jurisdictions that seek to improve cyber aspects of operational resilience, and it is anticipated that further countries will enact similar schemes in the future.

A summary of the cyber resilience testing schemes in place currently is as follows (see table 2).

TABLE 2

**Cyber Resilience Testing Schemes in Various Countries**

| Country / region | Scheme name | Date commenced | Description |
|---|---|---|---|
| United Kingdom | CBEST | 2014 | The Bank of England developed CBEST to test firms' cyber resilience. CBEST entails that each firm conducts a realistic, simulated attack on the people, processes, and technology that comprise its cybersecurity controls, with the aim of testing not only its defenses but also its ability to detect and respond to a range of attackers.[38] |
| Hong Kong | iCAST | 2016 | As part of the Hong Kong Monetary Authority's Cyber Fortification Initiative, certain authorized institutions are required to conduct Intelligence-led Cyber Attack Simulation Testing (iCAST). This is a test of their cyber resilience by simulating real-life cyber attacks from adversaries, making use of relevant cyber intelligence.[39] |
| European Union | TIBER-EU | 2018 | The European Union developed a union-wide framework for Threat Intelligence-Based Ethical Red Teaming (TIBER-EU). Each country enacts its own implementation based on the TIBER-EU guidelines. Various EU countries have so far implemented the TIBER framework, including: Belgium (TIBER-BE), Denmark (TIBER-DK), Finland (TIBER-FI), Germany (TIBER-DE), Ireland (TIBER-IE), Italy (TIBER-IT), the Netherlands (TIBER-NL, which was developed first in 2016), and Sweden (TIBER-SE).[40] |
| Singapore | AASE | 2018 | The Association of Banks in Singapore has created the Adversarial Attack Simulation Exercises (AASE) guidelines for planned, risk-managed, and objective-driven cybersecurity assessments that simulate highly sophisticated targeted attacks against an organization.[41] |
| Saudi Arabia | Financial Entities Ethical Red Teaming | 2019 | The Saudi Arabia Monetary Authority Financial Entities Ethical Red Teaming Framework requires firms to conduct controlled attacks (for example, threat intelligence-based red-teaming tests) against their (live) production environment.[42] |
| Malaysia | Risk Management in IT | 2020 | Bank Negara Malaysia requires large financial institutions to proactively identify potential vulnerabilities, including those arising from infrastructure hosted with third-party service providers, through the simulation of sophisticated red team attacks on its current security controls.[43] |

## Conclusions

When considering threats to the resilience of the financial system, two key facets of the cyber threat landscape stand out: the actors who conduct attacks and the technology that they target. However, these are not independent variables. As new technology emerges, it opens up opportunities for attackers to exploit it—and its users. Similarly, as attackers evolve, organizations must update their technical defenses to protect against them. Nowhere is this pace as dynamic as in the financial services sector.

In many areas, the defenders are winning. For example, attacks using banking trojans against online banking are much rarer now than they were a few years ago. This is in part due to law enforcement action and disruption of large botnets, as well as improved defenses within online banking. A similar drop occurred in 2020 with respect to attacks against payment systems such as SWIFT. Improved defenses, in this case via the Customer Security Programme, have shifted the balance and now groups are turning to other techniques.[44]

In other areas defenders are losing the battle. For example, one of the most significant threats today is from network intrusions that lead to ransom and extortion. Over a dozen threat groups are using the same business model and finding it very effective. The estimated loss to victims caused by these groups in 2020 has reached hundreds of millions of dollars, with the REvil group alone claiming over $100 million in profits in one year, and the rate of attack is still accelerating.[45] At the moment it is hard to see what will slow or reverse this trend—it likely needs coordinated action from government and the private sector coming alongside the financial services community.

What the future holds for the cyber threat landscape is hard to forecast at the best of times. In a time of so much disruption to normal life, it is impossible to say what is around the corner, even for 2021. However, cyber threats will certainly remain, central motivations are unlikely to change, new technologies will gain adoption, and defending networks will continue to require significant resources and attention to detail.

## About the Authors

**Adrian Nish** is the head of Cyber Technical Services at BAE Systems' Applied Intelligence business unit. His team investigates and tracks high-end cyber threat activity for corporate and government customers around the world. Nish is a renowned expert on nation-state threats to the financial system, with firsthand experience investigating cases of complex intrusions and manipulation of payment systems. He is an associate fellow at the London-based think tank Royal United Services Institute and holds a PhD in physics from the University of Oxford.

**Saher Naumaan** is a threat intelligence analyst at BAE Systems' Applied Intelligence. Her current research is on state-sponsored cyber espionage with a focus on threat groups and activity in the Middle East. Naumaan specializes in analysis covering the intersection of geopolitics and cybersecurity and regularly speaks at events and conferences around the world. Prior to working at Applied Intelligence, she graduated from King's College London with a master's degree in intelligence and security, where she received the Barrie Paskins Award for Best MA Dissertation in War Studies.

**James Muir** leads on thematic and technology threat research at BAE Systems Applied Intelligence. His current research interests are in the ransomware threat, hackers-for-hire, and threats to operational technology. Muir is a secondee with the UK government's National Cyber Security Centre's Industry 100 scheme. Muir also holds a PhD in Neuroscience from University College London.

## Notes

1 Pierluigi Paganini, "Chilean Bank BancoEstado Hit by REvil Ransomware," Security Affairs, September 7, 2020, https://securityaffairs.co/wordpress/108014/cyber-crime/bancoestado-ransomware.html; Pierluigi Paganini, "Bank of Seychelles Hit by a Ransomware Attack," Security Affairs, September 12, 2020, https://securityaffairs.co/wordpress/108199/cyber-crime/bank-of-seychelles-ransomware-attack.html; and Leila Lai, "Silverlake Axis' IT Service Provider Hit by Ransomware Attack," Business Times, September 10, 2020, https://www.businesstimes.com.sg/companies-markets/silverlake-axis-it-service-provider-hit-by-ransomware-attack.

2 Mehedi Hasan, "Hacking Alert: Banks in Bangladesh Limit ATMs, Cards, and Online Transactions to Avoid Risks," Dhaka Tribune, September 7, 2020, https://www.dhakatribune.com/business/banks/2020/09/07/hacking-alert-banks-in-bangladesh-limit-atms-cards-and-online-transactions-to-avoid-risks; and Hanna Ziady, "New Zealand Spy Agency Investigating 'Severe' Cyberattack on Stock Exchange," CNN Business, August 28, 2020, https://edition.cnn.com/2020/08/27/investing/new-zealand-stock-exchange-cyber-attack/index.html.

3 "Timeline of Cyber Incidents Involving Financial Institutions," Carnegie Endowment for International Peace, updated August 2020, https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

4 "About the FinCyber Strategy Project," Carnegie Endowment for International Peace, https://carnegieendowment.org/specialprojects/fincyber/about.

5 Adrian Nish and Saher Naumaan, "The Cyber Threat Landscape: Confronting Challenges to the Financial System," Carnegie Endowment for International Peace, March 25, 2020, https://carnegieendowment.org/2019/03/25/cyber-threat-landscape-confronting-challenges-to-financial-system-pub-78506.

6 BAE Systems Financial Services, "COVID-19: Insights and Support for Financial Services," BAE Systems, September 28, 2020, https://www.baesystems.com/en-financialservices/covid-19; Jack Prytherch and Andy Brown, "UK: HMRC Announce Their First "Furlough Fraud" Arrest - Only a Concern for a Small Few?," Bird&Bird, July 2020, https://www.twobirds.com/en/news/articles/2020/uk/hmrc-announce-first-furlough-fraud-arrest.

7 House of Commons Treasury Committee, "IT Failures in the Financial Services Sector: Second Report of Session 2019-20," UK House of Commons, October 20, 2019, https://publications.parliament.uk/pa/cm201919/cmselect/cmtreasy/224/224.pdf.

8 Michael Woodman, "Why It's Time the Finance Sector Ditched Its Legacy Infrastructure," BT, July 19, 2018, https://www.globalservices.bt.com/en/insights/blogs/finance-sector-legacy-infrastructure; and Keith Pogson, "Why Banks Can't Delay Upgrading Core Legacy Banking Platforms," EY, June 18, 2019, https://www.ey.com/en_gl/banking-capital-markets/why-banks-can-t-delay-upgrading-core-legacy-banking-platforms.

9 "RTGS Renewal Programme," Bank of England, September 29, 2020, https://www.bankofengland.co.uk/payment-and-settlement/rtgs-renewal-programme.

10 "How the Bank of England Will Build a New RTGS System for the United Kingdom," Mi Forum, August 2020, https://www.swift.com/resource/how-bank-england-will-build-new-rtgs-system-united-kingdom.

11 "A Blueprint for a New RTGS Service for the United Kingdom," Bank of England, May, 2017, https://www.bankofengland.co.uk/-/media/boe/files/payments/a-blueprint-for-a-new-rtgs-service-for-the-uk.pdf.

12 "Cobalt Strike: Advanced Threat Tactics for Penetration Testers," https://www.cobaltstrike.com; and "Empire," published on Github, https://github.com/EmpireProject/Empire.

13 Jay Jay, "Travelex Paid $2.3m in Ransom to REvil Cyber Gang," Teiss, April 16, 2020, https://www.teiss.co.uk/travelex-ransom-revil-group.
14 Larry Jaffee, "Travelex Driven Into Financial Straits by Ransomware Attack," SC Magazine, August 10, 2020, https://www.scmagazine.com/home/security-news/travelex-driven-into-financial-straits-by-ransomware-attack.
15 Tim Maurer and Garrett Hinck, "Cloud Security: A Primer for Policymakers," Carnegie Endowment for International Peace, August 31, 2020, https://carnegieendowment.org/2020/08/31/cloud-security-primer-for-policymakers-pub-82597.
16 "2020 Data Breach Investigations Report," Verizon, https://enterprise.verizon.com/en-gb/resources/reports/dbir.
17 Based on author observation. Instances can be found at "Timeline of Cyber Incidents Involving Financial Institutions," Carnegie Endowment for International Peace, updated August 2020, https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.
18 Lily Hay Newman, "A New Breed of ATM Hackers Gets in Through a Bank's Network," Wired, September 4, 2019, https://www.wired.com/story/atm-hacks-swift-network.
19 Vitali Kremez, "The Deadly Planeswalker: How The TrickBot Group United High-Tech Crimeware & APT," SentinelOne, December 10, 2019, https://labs.sentinelone.com/the-deadly-planeswalker-how-the-trickbot-group-united-high-tech-crimeware-apt.
20 Based on author involvement in named investigation.
21 "How Cyber Attackers 'Cash Out' Following Large-Scale Heists," SWIFT, September 2, 2020, https://www.swift.com/news-events/news/how-cyber-attackers-cash-out-following-large-scale-heists.
22 Tim Maurer, "Cyber Mercenaries: The State, Hackers, and Power," Cambridge University Press, 2018, https://www.cambridge.org/core/books/cyber-mercenaries/B685B7555E1C52FBE5DFE6F6594A1C00
23 Jack Stubbs, Raphael Satter, and Christopher Bing, "Exclusive: Obscure Indian cyber firm spied on politicians, investors worldwide," Reuters, June 9, 2020, https://uk.reuters.com/article/us-india-cyber-mercenaries-exclusive/exclusive-obscure-indian-cyber-firm-spied-on-politicians-investors-worldwide-idUKKBN23G1GQ
24 John Scott-Railton, Adam Hulcoop, Bahr Abdul Razzak et al., "Dark Basin: Uncovering a Massive Hack-For-Hire Operation," The Citizen Lab, June 9, 2020, https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/
25 William Turton, "U.S. Investigating Hacker Ring Paid to Target Corporate Critics," Bloomberg, June 10, 2020, https://www.bloombergquint.com/technology/u-s-investigating-hacker-ring-paid-to-target-corporate-critics
26 Jon Bateman, "Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios," Carnegie Endowment for International Peace, July 08, 2020, https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237
27 "The Global Risks Report 2019: 14th Edition," World Economic Forum, http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
28 Jérôme Lascombe, "The BlackRock Case: Trusting Corporate and Financial Information, a New Challenge for Financial Companies and Media," Wiztopic (blog), February 4, 2019, https://news.wiztopic.com/news/the-blackrock-case-trusting-corporate-and-financial-information-a-new-challenge-for-financial-companies-and-media-e145-7e09e.html.
29 Jim Edwards, "A false rumor on WhatsApp started a run on a London bank," Business Insider, May 13, 2019, https://www.businessinsider.com/whatsapp-rumour-started-run-on-metro-bank-2019-5?r=US&IR=T

30 "'Deepfakes' ranked as most serious AI crime threat," University College London, August 04, 2020, https://www.ucl.ac.uk/news/2020/aug/deepfakes-ranked-most-serious-ai-crime-threat

31 Catherine Stupp, "Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case," The Wall Street Journal, August 30, 2019, https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

32 John Bateman, "Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios," Carnegie Endowment for International Peace, July 08, 2020, https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237; James Vincent, "This is what a deepfake voice clone used in a failed fraud attempt sounds like," The Verge, July 27, 2020, https://www.theverge.com/2020/7/27/21339898/deepfake-audio-voice-clone-scam-attempt-nisos

33 Where quantum algorithms are run on standard computing resources instead of quantum computers – see "NatWest begins testing with quantum computing power to help solve highly complex calculations," RBS, September 19, 2018, https://www.rbs.com/rbs/news/2018/09/natwest-begins-testing-with-quantum-computing-power-to-help-solv.html

34 " Exploring quantum computing use cases for financial services," IBM, https://www.ibm.com/thought-leadership/institute-business-value/report/exploring-quantum-financial

35 "The Search for Quantum Resistant Cryptography: A Whitepaper from Sectigo," Sectigo, September 2019, https://sectigo.com/uploads/resources/Quantum-Resistance-Whitepaper.pdf.

36 "NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto 'Semifinals' ," NIST, January 30, 2019, https://www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals

37 "Operational Resilience: Impact tolerances for important business services," Bank of England, December 05, 2019, https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper; "Basel Committee releases consultative documents on principles for operational risk and operational resilience," BIS, August 06, 2020, https://www.bis.org/press/p200806.htm

38 "Financial sector continuity," Bank of England, https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity

39 Sunny Yung, "Cybersecurity Fortification Initiative" (letter to the Chief Executive and all authorized institutions), Hong Kong Monetary Authority, December 21, 2016, https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161221e1.pdf.

40 "What is TIBER-EU?," European Central Bank, https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

41 "Red Team: Adversarial Attack Simulation Exercises: Guidelines for the Financial Industry in Singapore, Version 1.0" Association of Banks in Singapore, November 2018, https://abs.org.sg/docs/library/abs-red-team-adversarial-attack-simulation-exercises-guidelines-v1-06766a69f299c69658b7dff00006ed795.pdf.

42 Financial Entities Ethical Red-Teaming, Version 1.0" Saudi Arabia Monetary Authority, May 2019, http://www.sama.gov.sa/en-US/Laws/BankingRules/Financial%20Entities%20Ethical%20Red%20Teaming%20Framework.pdf.

43 Risk Management in Technology (RMiT)," Bank Negara Malaysia: Central Bank of Malaysia, June 19, 2020, https://www.bnm.gov.my/index.php?ch=57&pg=543&ac=816&bb=file.

44 "Customer Security Programme (CSP)," SWIFT, https://www.swift.com/myswift/customer-security-programme-csp

45 Based on Ionut Ilascu, "REvil Ransomware Gang Claims Over $100 Million Profit in One Year," BleepingComputer, October 29, 2020, https://www.bleepingcomputer.com/news/security/revil-ransomware-gang-claims-over-100-million-profit-in-a-year; and authors' calculations.


1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org