Cyberattacks threaten stability of interconnected financial services

Monday, December 6, 2021 8:00 AM ET

By Peter Brennan
Market Intelligence

A cyberattack on Colonial Pipeline disrupted the supply of fuel along the U.S. East Coast earlier this year.
Source: Getty Images North America

The danger of a cyberattack capable of generating a financial crisis is growing.

Experts fear that the digital interconnectedness of the financial services industry means that a successful hack of a company could spur a domino effect. The threat is severe enough that multilateral organizations from the IMF to the Bank for International Settlements warn that financial stability is at risk. The surge in remote work during the pandemic has exposed companies' digital infrastructures even more.

"The threat landscape is changing rapidly. [Cybercriminals] are more sophisticated and better resourced," Emran Islam, senior financial

sector expert at the IMF, said in an interview. "This is almost a fait accompli. There will be cyber incidents and they will increase in size and seriousness."

The World Economic Forum has ranked cyber-related issues as the second greatest risk, after environmental ruptures such as climate change, that businesses will face over the next 10 years. Executive Chairman Klaus Schwab told the July 2020 gathering of the organization that the COVID-19 crisis was "a small disturbance in comparison to a major cyberattack," referring to such an event as a "cyber pandemic."

Companies often are wary of disclosing when they have been hit with a cyberattack so there is limited data to reveal the scale of the problem, but "there has been a huge spike, especially in the COVID period," Islam said. Two of the most notable cyberattacks this year ensnared U.S. energy group Colonial Pipeline Co. and the Brazilian meat-processing giant JBS SA.

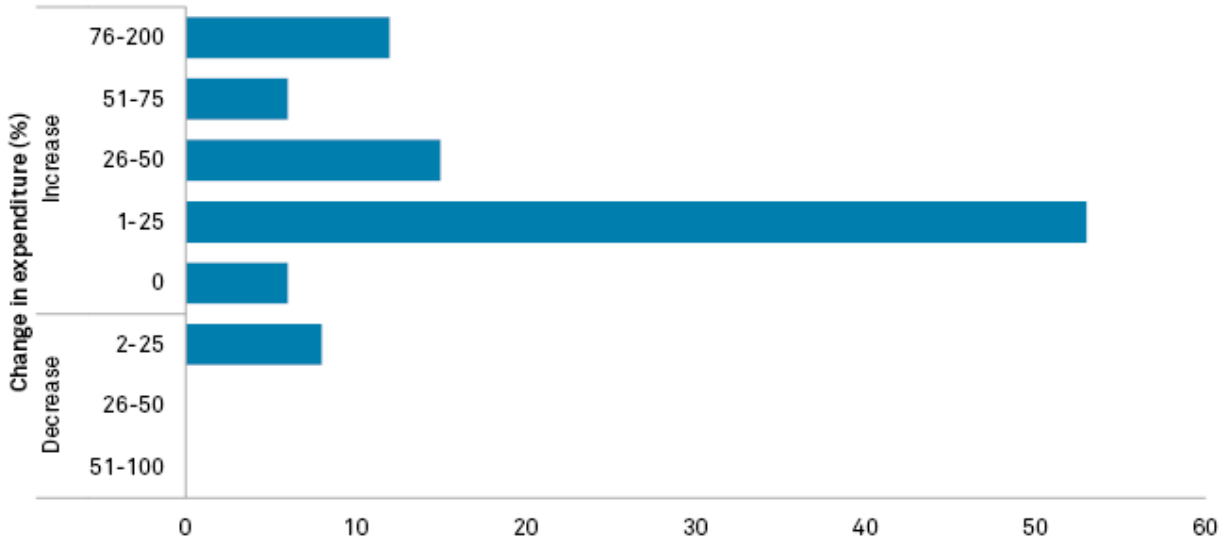
The IMF found that cyberthreats could cost banks up to 9% of their average annual net income globally, or about $100 billion, according to a 2018 study. "If a major incident crystalizes across the global economy [the cost] will be very, very substantial," Islam said.

This is the first in a series of articles examining the impact of cybercrime and strategies to combat it.

Companies are bolstering their defenses. A study of 345 companies found that 86% planned to increase their security budgets in 2021, with a median increase of 20%, according to 451 Research.

"We are in an arms race," Lance McGrath, chief security officer at Danske Bank, said in an interview. "No matter how much we in the banking sector invest there will always be the criminals investing as well because it is a low-risk, high-reward venture for them."

Study finds most companies expected to increase their security budget in 2021



Data as of June 14, 2021.

Quarterly survey completed between Oct. 29, 2020, and Jan. 21, 2021. Sample Size of 345 IT decision makers representative of small, midsize and large enterprises in private and public sectors.

Companies were asked: "By what percentage do you expect your organization's total information security budget to change in 2021 compared to 2020?"

Source: 451 Research, a part of S&P Global Market Intelligence

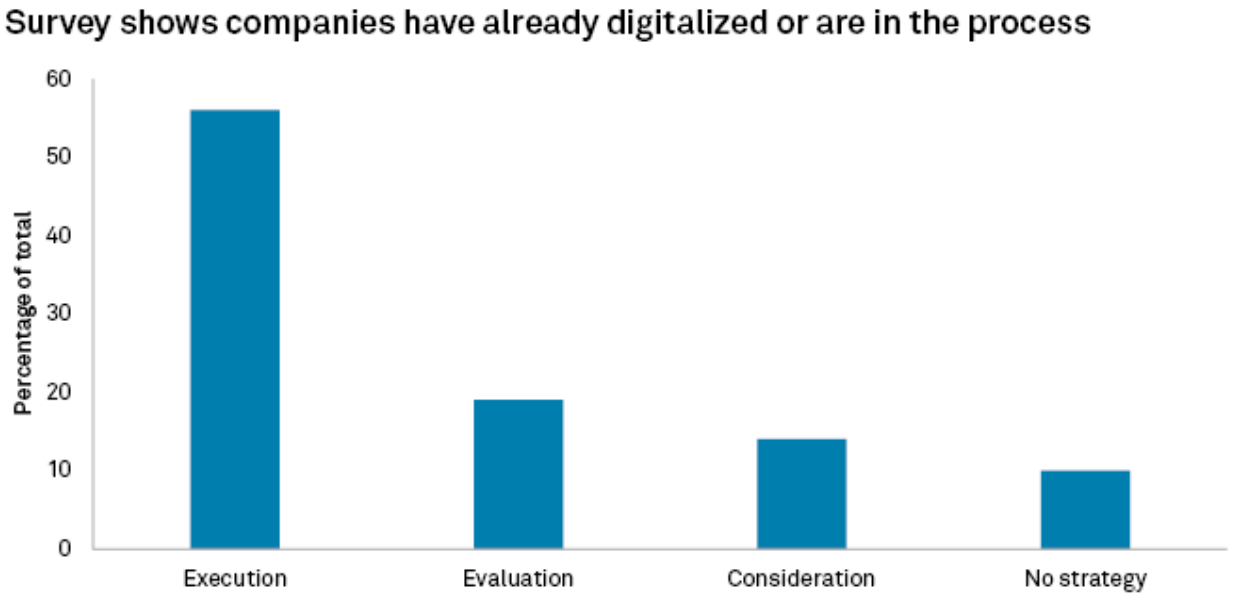
The digitalization of companies has heightened the risk of attacks, according to the Financial Services Information and Analysis Center, or FS-ISAC, an intelligence-sharing platform for financial services companies.

"With more digital services comes an expansion of the attack surface and an increase in potential vulnerabilities to cyberattacks," Teresa Walsh, global head of intelligence at FS-ISAC, said in an interview. "It is vital that the speed of new product and service offerings does not outstrip the speed of implementation of cybersecurity and anti-fraud measures, lest mass adoption result in mass risk."

> **READ MORE:** *Stay informed on how technology is reshaping the future of your sector. Get the Next newsletter delivered to your inbox every Tuesday. Sign up here.*

Crime pays

Digital heists crippled critical physical U.S. infrastructure in 2021. A ransomware attack on Colonial Pipeline shut down a 5,500-mile fuel system until the company paid a $5 million ransom. An attack on JBS, the world's largest meat-processing company, disrupted production around the world, risking higher food prices until an $11 million ransom was paid.



Data as of fourth quarter of 2020.

Execution: Company has a formal strategy and is actively digitalizing its business processes and/or assets. Evaluation: Company is planning and researching to develop a digital transformation strategy. Consideration: Company is considering it, but has no formal plans. No strategy: Company currently has no digital transformation strategy.

Extensive community of mid-level and senior IT professionals. Data completed fourth quarter 2020. All respondents (n=399). Sample is representative of small, midsize and large enterprises in private and public sectors.

Source: 451 Research, a part of S&P Global Market Intelligence

Cybercrime is a constant threat in a digital world, and companies are increasingly digitalizing. A further study by 451 Research in the fourth quarter of 2020 found that 56% of the companies surveyed had already executed a strategy to digitalize their businesses, with a further 19% planning and researching a strategy.

Phishing emails trick people into clicking on links that contain malware, enabling the attacker to then encrypt an individual or organization's IT system. The most common attack uses ransomware to disable a system or leak information until a ransom is paid.

Perpetrators of such attacks range from sinisterly named criminal gangs such as Evil Corp and DarkSide to state-sponsored groups. It is a lucrative endeavor for criminals. North Korea is estimated to have stolen some $2 billion from at least 38 countries in the past five years, according to the IMF.

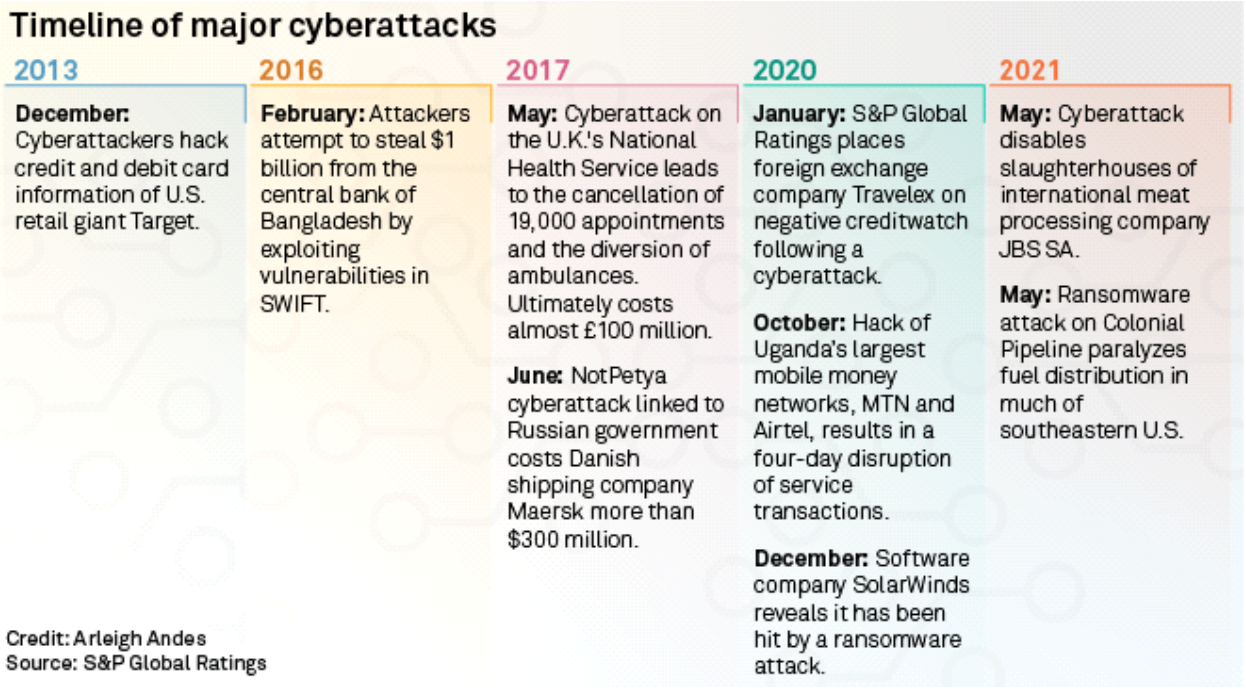
"Why would you go into a bank with a gun and try to walk away with £30,000 when you can operate safely from Russia and walk away with £50 million or £100 million?" McGrath said.

Financial services face 'Armageddon scenarios'

Most financial companies now use third-party suppliers to provide software, services, infrastructure and products to optimize their time to market, enhance their customers' experience and gain operational efficiency. But there are drawbacks in relying on opening your network to other companies.

The attack on software company SolarWinds Corp. in 2020 showed how vulnerable the digital supply chain is. The cyberattackers were able to use a SolarWinds software update to deploy malware into the networks of 18,000 SolarWinds customers, including tech giants Microsoft Corp. and Intel Corp. and federal agencies.

"There's a high dependency on technology. Any kind of cyberattack that can compromise at large scale is going to result in a massive impact for customers," McGrath said. "There are lots of Armageddon scenarios."

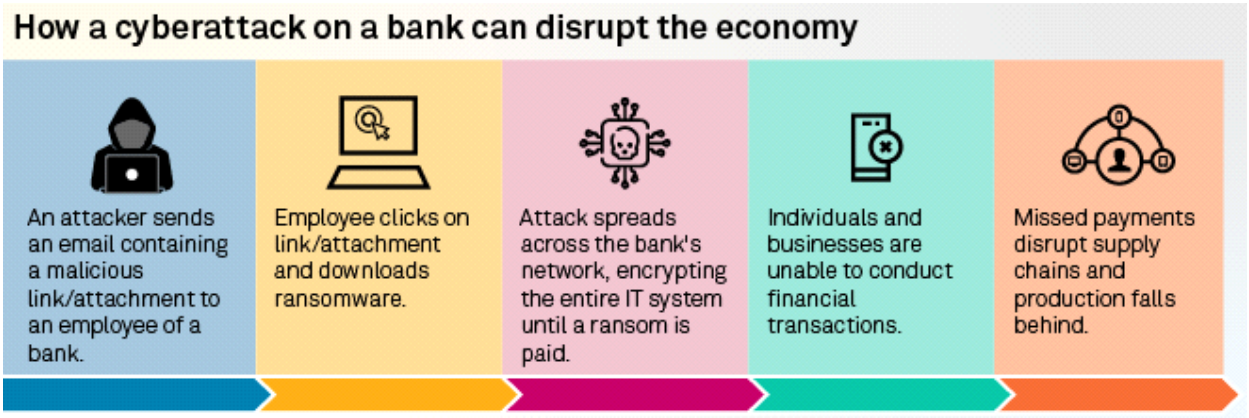


One such scenario is a hack on the financial system where transactions such as the buying or selling of a security is conducted by an intermediary.

"The interconnectedness in the financial system is a real challenge," Sanjeev Shukla, U.K. financial services security lead at Accenture, said in an interview. While a company may have adequately secured its own IT system, partners that connect on its network may not have the same standards.

Shukla gave the example of a hacker disrupting an intermediary, preventing the settlement of a security transaction. Often entities use leverage so if it is not possible to settle because the settlement provider is down, they will default on their commitment to the other side. If any intermediaries are down then there's a possibility of a cascading effect, and that could lead to some of the participants failing and the counterparties failing. "It's a domino effect," Shukla said.

An attack on a retail bank would also have serious consequences, Shukla said. Savers deposit money in a bank, expecting the bank to protect it and make the money available to them at any time. But a cyberattack that jams services, preventing savers from accessing their money, could spark a panic or a run on other banks.



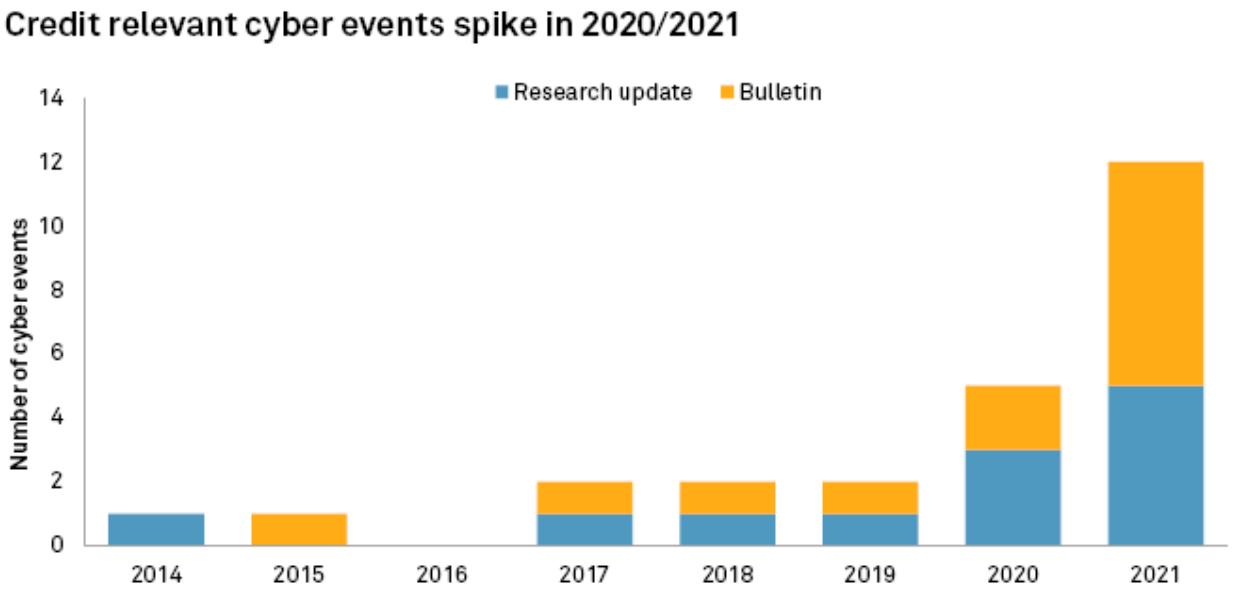
"The fact that internet banking is down, that raises the question in every depositors' mind, 'What the hell is going on?'" Shukla said.

The most serious breach of the financial system so far was the hack on the Bangladesh central bank in 2016. Cybercriminals — believed to be based in North Korea — were able to breach the bank and eventually use the international payments system SWIFT to initiate payment orders of $1 billion. While the Federal Reserve Bank of New York red-flagged many of the orders, the hackers still made off with $63 million.

Spike in credit rating events

Cybersecurity is a growing credit risk for companies, meaning their costs of borrowing could rise if an attack seriously impacts them. S&P Global Ratings has seen a spike in "credit events," whereby the rating agency either issues a bulletin, publishes research or takes a ratings action as a result of a cyberattack.

Half of all such events occurred in the past 12 months, according to Simon Ashworth, head of analytics and research at S&P Global Ratings. So far, though, there have been few changes to credit ratings.



Data as of Nov. 12, 2021.
A bulletin published by S&P Global Ratings recognizes that a cyber event has happened but is not expected to be credit material. A research update represents a ratings action taken by Ratings either directly because of a cyber event or a combination of events of which cyber was a contributor.
Source: S&P Global Ratings

SolarWinds was downgraded in April 2021 partly as a result of the cyberattack. And U.K.-based currency exchange service provider Travelex defaulted in 2020, having been downgraded earlier in the year after a cyberattack forced the company to shut down its websites.

"Governance is the key to cyberrisk management. Not just pre-attack governance, but also how you respond after an attack," Ashworth said in an interview. "Many more of those bulletins would have turned into ratings actions if governance had not been good."

Companies taking the threat more seriously

The threat to the corporate world has forced companies to invest in their cybersecurity. While the financial sector has long been worried about the security of its data, other sectors only recently have woken up to the threat.

"If you look at the last 30 to 40 years, security was an afterthought," Shukla said, noting that businesses in many nonfinancial sectors are only now realizing their dependence on third-party technology. "There's no other way. CEOs have seen how critical this technology is to their business."

Multilateral organizations, such as the Financial Stability Board, IMF and BIS, are calling for greater global collaboration between governments and companies to improve the weak links in global security.

Both SolarWinds and tech company Accellion Inc. used FS-ISAC to communicate with the financial sector following attacks. "This helped the industry act quickly to limit damage," FS-ISAC's Walsh said.

Politicians are waking up to the threat as well. After the Colonial Pipeline attack highlighted the threat to critical infrastructure, President Joe Biden issued an executive order forcing companies to report cyberattacks.

Some measures are simple and inexpensive to implement. "The single biggest step to reducing cyberattacks is multifactor identification," McGrath said. "If you have two different components to your sign-on you eliminate anywhere from 70% to 90% of all attacks."

But experts warn that the reality is that the threat is likely to persist for as long as cybercrime remains a lucrative opportunity for criminals.

"There is no solution; this will be a constant struggle. The complexity of tech means there will always be vulnerabilities, and those vulnerabilities will have to be constantly mitigated," McGrath said.

451 Research is part of S&P Global Market Intelligence