HOW A CYBERATTACK COULD CAUSE THE NEXT FINANCIAL CRISIS

Frozen ATMs. Halted payments. Widespread panic.
Here's what governments need to do to prevent catastrophe.

Paul Mee and Til Schuermann

EVER SINCE THE forced bankruptcy of the investment bank Lehman Brothers triggered the financial crisis 10 years ago, regulators, risk managers, and central bankers around the globe have focused on shoring up banks' ability to withstand financial shocks.

But the next crisis might not come from a financial shock at all. The more likely culprit: a cyberattack that causes disruption to financial services capabilities, especially payments systems, around the world.

Criminals have always sought ways to infiltrate financial technology systems. Now, the financial system faces the added risk of becoming collateral damage in a wider attack on critical national infrastructure. Such an attack could shake confidence in the global financial services system, causing banks, businesses, and consumers to be stymied, confused, or panicked, which in turn could have a major negative impact on economic activity.

Cybercrime alone costs nations more than $1 trillion globally, far more than the record $300 billion of damage due to natural disasters in 2017, according to a recent analysis our firm performed. We ranked cyberattacks as the biggest threat facing the business world today – ahead of terrorism, asset bubbles, and other risks.

An attack on a computer processing or communications network could cause $50 billion to $120 billion of economic damage, a loss ranking somewhere between those of hurricanes Sandy and Katrina, according to recent estimates. Yet a much broader and more debilitating attack isn't farfetched. Just last month, the Federal Bureau of Investigation issued a warning to banks about a pending large-scale attack known as an ATM "cash-out" strike, in which waves of synchronized fraudulent withdrawals drain bank accounts. In July, meanwhile, it was revealed that hackers working for Russia had easily penetrated the control rooms of US electric utilities and could have caused blackouts.

$1 trillion

How much cybercrime costs nations globally

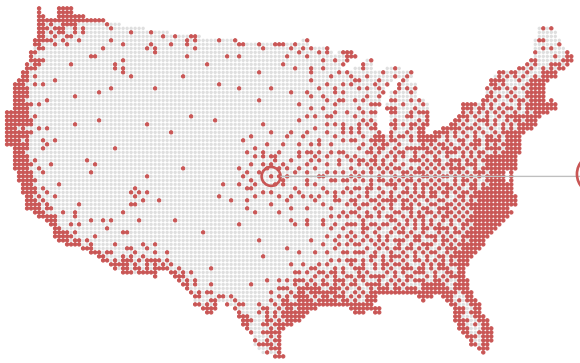
CYBERATTACK SCENARIOS

How might a financial crisis triggered by a cyberattack unfold? A likely scenario would be an attack by a rogue nation or terrorist group on financial institutions or major infrastructure. Inside North Korea, for example, the Lazarus Group, also known as Hidden Cobra, routinely looks for ways to compromise banks and exploit cryptocurrencies. An attack on a bank, investment fund, custodian firm, ATM network, the interbank messaging network known as SWIFT, or the Federal Reserve itself would represent a direct hit on the financial services system.

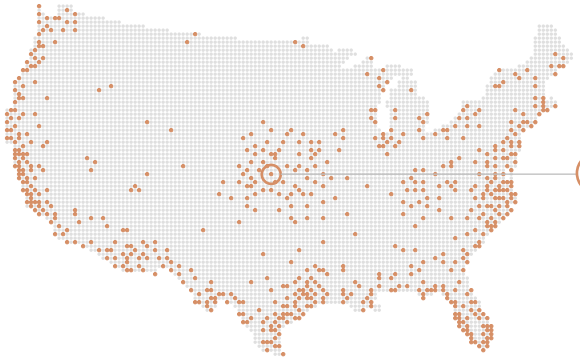
Another possibility would be if a so-called hacktivist or "script kiddy" amateur were to use malicious programs to launch a cyberattack without due consideration of the consequences. Such an attack could have a chain reaction, causing damage way beyond the original intent, because rules, battle norms, and principles that are conventional wisdom in most warfare situations but don't exist in a meaningful way in the digital arena. For example, in 2016 a script kiddie sparked a broad denial-of-service attack impacting Twitter, Spotify, and other well-known internet services as amateurs joined in for mischief purposes.

EXHIBIT 1: HOW A CYBERATTACK SPREADS

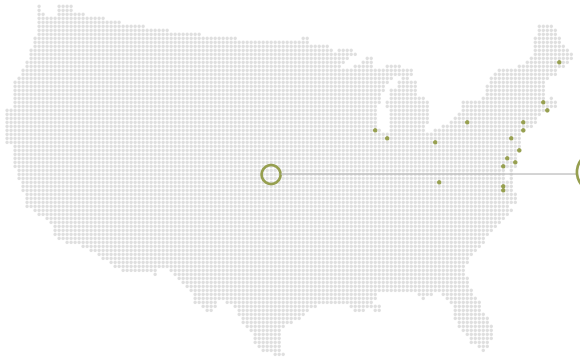
How fast cyberattacks will spread depends on what controls are in place to prevent them. Below we explore how far a cyberattack virus could spread in 60 hours under four different scenarios.



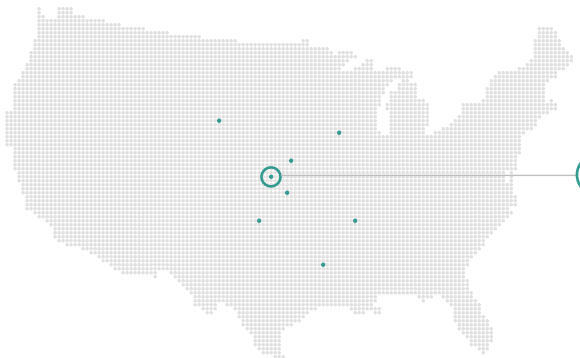
NO CONTROLS
Virus spreads quickly throughout all populated areas of the United States



DETECTION CONTROLS
Virus spreads at a slower pace



PROTECTION CONTROLS
Virus spreads no further than half of the country, by hour 52, spread lessens and the virus is eliminated from some areas



IDENTIFICATION CONTROLS
Virus spreads at much slower pace and stays close to point of origin

SIXTY HOURS

Four scenarios of possible virus spread after 60 hours

VIRUS POINT OF ORIGIN
A virus is spread through use of a Point-of-sale device

Source: Oliver Wyman analysis

Whether a major cyberattack is deliberate or somewhat accidental, the damage could be substantial. Most of the ATM networks across North America could freeze. Credit card and other payment systems could fail across entire nations. Online banking could become inaccessible: no cash, no payments, no reliable information about bank accounts. Banks could lose the ability to transact with one another during a critical period of uncertainty. There could be widespread panic, albeit temporary.

Such an outcome might not cause the sort of long-simmering financial crisis that sparked the Great Recession, because money would likely be restored to banks and payments providers once systems were back online. At the same time, it isn't clear how a central bank, the traditional financial crisis firefighter, could respond to this type of crisis on short notice. After the problem is fixed and the crisis halted, a daunting task of recovery would loom. It would be even more difficult if data were corrupted, manipulated, or rendered inaccessible.

STOPPING THE CONTAGION

How can we prevent such a scenario? Companies must implement systems that enable them to stop the spread of a cyberattack contagion, and to resume operations as rapidly and smoothly as possible. The financial services industry needs to fully agree on, and be prepared to practice, coordinated response and recovery strategies to prevent systemic breakdowns. Regulators in many nations have been working diligently to prepare for and curtail cyberattacks, but they need to look beyond their own borders and introduce regulations, laws, and cooperative frameworks in unison, such as the European Union's Network and Information Security Directive, which is designed to protect an ever-growing list of critical infrastructure, from banking and healthcare systems to online marketplaces and cloud services.

Many of these steps are being undertaken to varying degrees. But more needs to be done. An attack that undermines confidence in those very machines could have debilitating consequences on the flow of money between consumers, businesses, and financial institutions around the world.

Paul Mee is a New York-based partner in Oliver Wyman's Digital practice and leads the firm's Cyber Risk Management practice.
Til Schuermann is a New York-based partner in Oliver Wyman's Financial Services practice and was a senior vice president at the Federal Reserve Bank of New York during the financial crisis.

This article first appeared in Harvard Business Review.