



IMPROVING OPERATIONAL RESILIENCY

Navigating the Near and Long-Term
Effects of Covid-19

Established well before the pandemic struck, the banking industry's enthusiasm for leveraging technology to improve customer experiences, streamline costs and drive growth has only accelerated over the past 18 months. As lockdowns swept the country, the ability to conduct financial transactions from anywhere shifted from a matter of mere convenience to a health and safety imperative. Suddenly, virtually everyone—not only the young and tech savvy—was eager to embrace online and mobile banking.

That spike in interest accelerated banks' pursuit of technological capabilities that can enhance the customer experience, making engagements more frictionless, personalized and cyber-secure. Yet, investing in digital initiatives can be a risky endeavor. In fact, 70 percent of digital transformation projects fall short of their goals, according to a study by Boston Consulting Group.

"That's often because they don't have the right data in the right place," Ken Watson, industry solutions director, financial services at Everbridge, told directors of financial institutions participating in a recent roundtable discussion. "It can also be due to working with poor onboarding processes, employee resistance to change and [legacy] technology."

RISING RISK

Migrating operations online during the pandemic also heightened the risk of fraud and data theft. The need to adjust to both a distributed IT landscape and the pandemic-related transition to a remote workforce during Covid prompted 96 percent of companies to increase their IT spending in 2020, according a new IDG Research Services survey. Despite that additional investment, 81 percent of senior IT and IT security leaders surveyed re-

ported viewing their organizations as lacking sufficient protection against cyberattacks.

One challenge is that threats come from all corners and take many forms. On any given day, a board might be informed that a team of hackers is attempting to mine the company's customer database, an employee accidentally downloaded malware by opening a predatory email or a ransomware perpetrator is holding its technology hostage. Some financial institutions also faced concerns

about vendors viewed as more vulnerable to cyber attack or less prepared to recover from an incident. In addition to shoring up their defenses, they needed to focus energy on helping to ensure that vendors' standards for safety measures and resiliency efforts were as high as their own.

Identifying vulnerabilities and deciding how to address them are particularly tricky for smaller financial institutions under more pressure to triage when allocating limited resources.

"There's so much going on that the emphasis is prioritizing vulnerabilities and what assets must be protected," said Ana Dutra, board member of First Internet Bank and CME Group and certified cybersecurity expert. "Boards have to ask management what kind and level of protection the company needs. The question every board needs to ask management: 'What is our value proposition when it comes down to cybersecurity and resilience?'"

It's a challenge that many boards face, agreed the director of a financial institution: "Not everyone has the resources to be cutting-edge in this space. We all have to do the best that we can with the resources we have."

A STRATEGIC APPROACH

Defining the assets that need to be protected, the threats they need to be protected from and how quickly they need

81%
of banking CEOs are
concerned about the
speed of technological
change, more than any
other industry sector.

to be recovered can help a company avoid overspending and develop a strategic approach to cybersecurity. “We’re not talking about an immaterial investment here,” said Dutra. “You need to be very clear on all of that so that you’re not unnecessarily burdening the business by investing 10 times more than you need to in certain aspects of cybersecurity.”

At the same time, appropriate investments in cybersecurity measures can pay off financially. For example, taking steps to mitigate cyber risk can lower cyber-insurance premiums. “It’s no different than putting fire safety measures in your home and receiving a deduction on your insurance premium,” explained Watson.


“The right cyber auditor can help you with that,” agreed Dutra. “They may say, ‘Take the money you’re putting in over here and shift it there where you’ll get the protection you need in a more effective and efficient manner.’”

Watson urged directors to apply a similar approach to digitization, screening potential initiatives to identify those most likely to further growth, efficiency, revenue and customer engagement goals. “It’s very important to consider digitization through the lens of opportunity,” he said, noting that one leading bank was able to streamline its branch opening process by adopting a countdown smartphone app. “They used to have two people, one would go in and the other would wait in the car and look for an [all clear] signal. Now, one person opens the branch by launching the countdown before entering. If he or she doesn’t stop the counter, it automatically notifies the security operations center.”

ON-THE-GROUND DEFENSES

Office space security practices also merit attention. “It can be easy to overlook things like entry badges and permissions that allow access to different areas and training employees to be mindful of their desktops,” said Dutra. “Maybe someone’s function changed and they should no longer have access to a certain area. Or people haven’t been instructed not to leave their desktops on and accessible when they leave.”

At a time when unanticipated events seem to regularly derail businesses, disaster preparedness is becoming a focus for many banks. Wildfires, hurricanes and infrastructure failures all disrupted lives and operations over the past year.

 **It’s very important to consider digitization through the lens of opportunity.”**

—Ken Watson, Industry Solutions Director, Financial Services, Everbridge

One regional bank experienced that firsthand, albeit in a relatively minor way, when a targeted hail-storm hit one of its branches in Texas. “Extreme weather seems to be in the news more and more often, so that is part of the plan that you need for resiliency,” said a board director.

Here, too, digitization can be leveraged to mitigate risk, said Watson, who noted that some banks use weather-monitoring systems

to gauge the likelihood of a disruptive event in their area and help position themselves to cope with and recover more swiftly from it. “Banks in areas along the Atlantic get early alerts that help them take steps like boarding up their branches, redeploying their people and having extra cash reserves to meet loan commitments on hand.”

Natural disasters, a global pandemic, cyber attacks—if 2020 taught us anything, it’s that every business is vulnerable to a wide array of unforeseen and disruptive events. As valuable as preventative measures can be, it’s equally important to weave operational resilience practices like continuity strategy, physical and cybersecurity, incident management and threat monitoring into every area of the business.

Building resilience is also a dynamic process, requiring constant vigilance about identifying ways to apply technological innovations to mitigate risks and pursue opportunities. “It doesn’t have a before, during and after,” says Watson. “It’s continuous.”

In an increasingly volatile world, the ability to prepare for, adapt to and recover from disruptions has become a competitive imperative. Banks able to make resiliency a core competency will be better equipped to mitigate risks and pursue opportunities—both today and well into the future.

Chief Executive Group

Chief Executive Group, a leading community for business leaders worldwide, exists to improve the performance of U.S. CEOs, CFOs and corporate directors. We publish *Chief Executive* magazine (since 1977), ChiefExecutive.net, *Corporate Board Member* magazine (since 1998), BoardMember.com, StrategicCFO360.com and RemoteWork360.com, as well as produce research, conferences and roundtables that enable CEOs, CFOs, board members and other members of the C-Suite to share experiences with their peers to grow companies, build communities and strengthen society. Learn more at ChiefExecutiveGroup.com.



Everbridge, Inc. (NASDAQ: EVBG) is a global software company that provides enterprise software applications that automate and accelerate organizations' operational response to critical events in order to keep people safe and businesses running. During public safety threats such as a global pandemic, active shooter situations, terrorist attacks or severe weather conditions, as well as critical business events including IT outages, cyber-attacks or other incidents such as product recalls or supply-chain interruptions, over 5,200 global customers rely on the company's Critical Event Management Platform to quickly and reliably aggregate and assess threat data, locate people at risk and responders able to assist, automate the execution of pre-defined communications processes through the secure delivery to over 100 different communication devices, and track progress on executing response plans. The company's platform sent over 3.5 billion messages in 2019 and offers the ability to reach over 550 million people in more than 200 countries and territories, including the entire mobile populations on a country-wide scale in Australia, Greece, Iceland, the Netherlands, New Zealand, Peru, Singapore, Sweden, and a number of the largest states in India. The company's critical communications and enterprise safety applications include Mass Notification and Incident Communications, Safety Connection™, IT Alerting, Visual Command Center®, Public Warning, Crisis Management, Community Engagement®, Care Converge™, and are secure, highly scalable, reliable, and easy-to-use and deploy. Everbridge is based in Boston and Los Angeles with additional offices in Lansing, San Francisco, Abu Dhabi, Beijing, Bangalore, Kolkata, London, Munich, New York, Oslo, Singapore, Stockholm and Tilburg. Learn more at Everbridge.com