It's not a matter of if — it's when

PAYMENT RESILIENCY

Network disruptions are as disastrous as they are inevitable. Building resiliency into your payments ecosystem can't be a "We'll get to it tomorrow" scenario.

AI-armed hackers are intent on attacking your payments ecosystem. Geopolitical risks and environmental disasters can be catastrophic to your operations. And tech issues are just waiting to sideswipe you at any moment. Any of these would wreak havoc on both your revenue and reputation. Often with devastating repercussions.

Those are just facts. And ignoring them isn't a strategy.

Among Chief Information Security Officers (CISOs) surveyed

51%

see operational (including payments) resiliency as a high-priority investment area[1]

Imagine your worst-case scenario. Now multiply it by a factor of ten or more. Because that's the number of ways an unforeseen network outage can strike. And if you don't have a payment resiliency plan in place — *if you thought about it but didn't act on it* — the unimaginable will become inevitable.

While 51% represents a majority, it's still a concerning figure. That means nearly half of CISOs aren't prioritizing payment resiliency. That said, astute CISOs are proactively working to defend their organizations. 20% are planning to increase their cybersecurity total cost of ownership by more than 10%, with 25% excited about emerging solutions in payment continuity.[1]

But what's most encouraging is that 44% of CISOs have stated interest in receiving outside assistance in finding payment resiliency solutions.[1] Realizing you can't necessarily achieve payment resiliency on your own is a critical first step in ensuring your organization can confidently protect itself when disaster does happen.

Network disasters

Being prepared for a crisis event is critical

So, we've mentioned worst-case scenarios. There's more out there than you can imagine, but they tend to fall into four categories — all that can be defended against through an effective payment resiliency plan.

Knowing the dangers is key to determining your solutions. The greatest threats to your payments ecosystem are:

Cyberattacks and data breaches

System failures

Climate disasters

Geopolitical risk

Even the strongest networks are susceptible. What is critical to keep in mind is you can't prevent the above. You can only protect your systems and mitigate, or at least minimize, any damage. In many situations other banks may be similarly impacted by third-party threats; having a strong payment resiliency strategy in place will give you an advantage over your less proactive peers.

Cyberattacks keep

10 out of 13

resiliency managers up at night[2]

Cyberattacks

Can you pay the price of a cyberattack?

Since 2004, the financial sector has suffered more than 20,000 cyberattacks causing $12 billion in losses.[3] Meanwhile, ransomware attacks on the sector leapt from 55% in 2022 to 64% in 2023.[4] Imagine such an attack on your organization. IT teams are caught off guard and customer service representatives are overwhelmed with calls from angry customers and merchants. Each passing hour results in lost revenue and goodwill. Cards drop to bottom-of-wallet — or worse, they're cancelled. As your situation becomes front-page news, lawyers and law enforcement rush in to help. But, even if you meet the extortionists' demands, unlocking your systems could take days. By that point, the damage is done.

Could you survive 10 days of digital downtime?

In 2023, a global hospitality and entertainment company suffered $110 million in losses after a hack shut down their systems.[5] While $110 million is a staggering number, what was truly staggering were the repercussions of the attack. For 10 disastrous days, the organization had to kick into "manual" mode to keep their business running — something they were ill-equipped to do. Cash-only transactions at some of their venues, reservations system offline, and dead key cards leading to long check-in queues were just some of the frustrating impacts that cost the company considerable goodwill, trust and loyalty.

System failures keep

9 out of 13

resiliency managers up at night[2]

System failures

What happens when 30 minutes turns into 18 hours?

Routine network maintenance is critical to smooth, uninterrupted payments processing, and best done during low-traffic hours. But suppose your scheduled 3:00–3:30 a.m. Sunday maintenance doesn't restart your systems after the planned 30 minutes. Emergency action kicks into gear and your system finally blinks back to life at 9:00 p.m. Monday night. That's 18 hours of downtime defined by declined transactions, missed payments, and frustrated cardholders — and making you yet another contributor to the $152 million cost of downtime to financial institutions globally per year.[6]

Climate disasters keep

6 out of 13

resiliency managers up at night[2]

Climate disasters

Can your data center take the heat?

A record heat wave has hit a city thousands of miles away — where your network's data center resides. 19% of data center outages are due to cooling system failure[7] and, in this instance, yours is one of them. As the center's supercomputers suffer a literal meltdown, payments can't be processed, and transactions in your region plummet by half. While the root cause may have been an act of nature, that's little comfort to your customers who might just start considering other banking options.

Geopolitical risk keeps

6 out of 13

resiliency managers up at night[2]

Geopolitical risk

Will your data center be a wartime target?

Hostilities between nations put your banking capabilities at risk in specific regions. A targeted attack creates the loss of vital financial data, processing systems are out of commission, and the simplest financial transaction becomes impossible. Financial turmoil is further intensified by cyberattackers on both sides, looking to destabilize their adversary's economic security. While the conflict is regional, these actions can impact any organization connected to the global payments ecosystem.

Ever-changing regulations

The importance of regulatory compliance

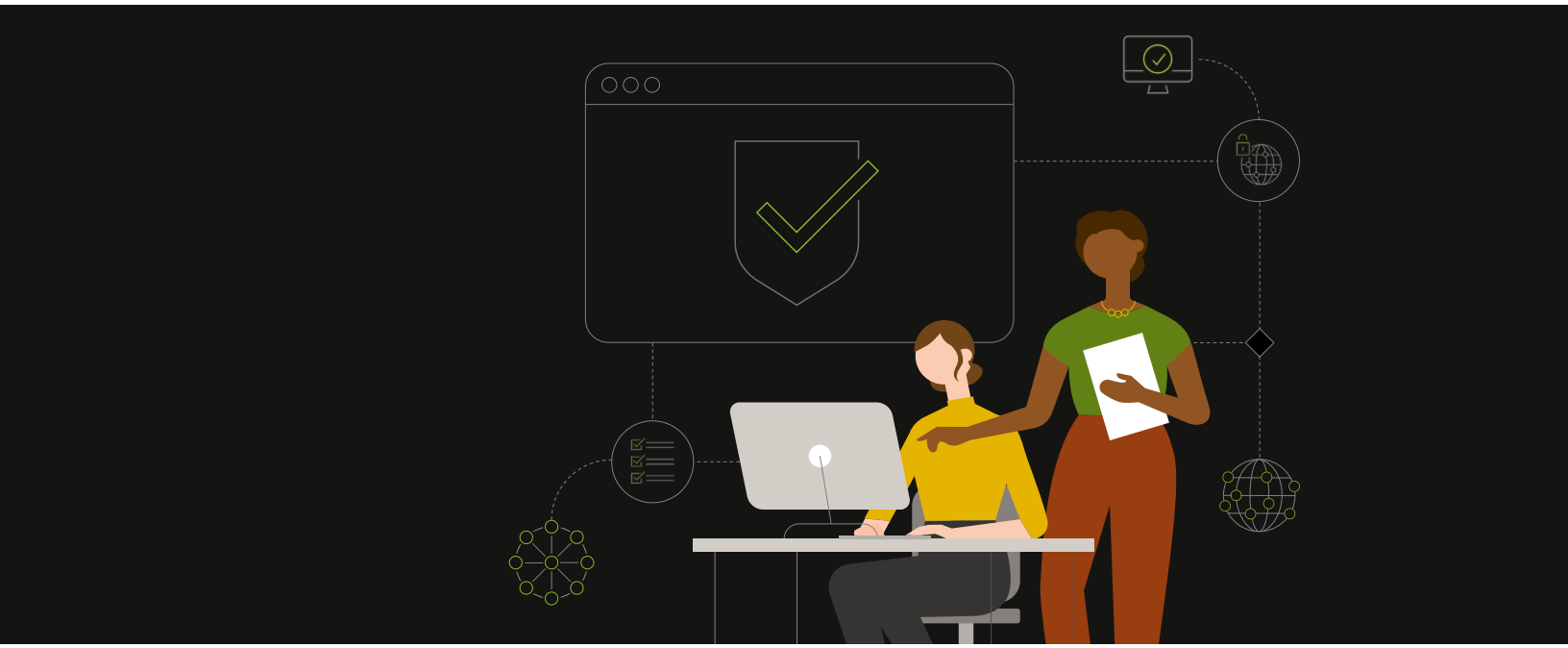
As digital technology — and the risks it brings — advances, so do regulations designed to strengthen the security of banks and other financial players. The ever evolving and complex regulatory landscape saw the financial industry spend over $115 billion globally in 2023 on regulatory technology to comply with various regulations and protect against digital threats and financial crimes.[8]

This has led to the introduction of the Digital Operational Resiliency Act (DORA) in the European Union, which requires that the operational resiliency of all financial institutions be fully compliant with the Act by January 17, 2025. The purpose of DORA is to harmonize the rules relating to operational resiliency to ensure the financial sector can stay resilient in the event of an operational disruption.

In other markets like the U.S., U.K., Australia and Japan, similar regulatory changes are in the works.[9] The overall objective for enacting these new regulations is to bolster operational resilience and ensure the impact of any disruptions on payment ecosystems is minimized.

These regulatory changes present a new challenge for the financial industry, as a failure to comply could not only result in significant fines, but reputational loss and, in extreme instances, license revocation.

Click here to learn more about DORA.



The rise of AI

72%
of CEOs

interviewed aren't comfortable making cybersecurity-related decisions[10]

Keeping your AI technology ahead of their AI technology

The upsurge of AI is fundamentally changing the world around us right before our eyes — and unsurprisingly, cyberattackers have embraced this phenomenon as their perfect partner-in-crime.

"In 2023, technological advancements surged. Artificial intelligence and ransomware-as-a-service platforms have streamlined hackers' ability to execute ransomware attacks."[10]

Pure Storage. Lifecycle of a Ransomware attack.

As AI evolves and advances, so do unlawful ways to exploit it. Getting smarter and smarter, artificial intelligence is even learning to adopt human behavior for malicious intent. Like the technology itself, criminal strategies involving AI can prove impossible to keep up with.

One way to outsmart criminal use of AI — or any emerging tech — is to outsource a third-party expert. No organization can be expected to know and do everything, and trying to be "master of all" isn't a risk worth taking. Engaging an external partner who's an authority on AI, network ecosystems and payment resiliency brings a level of expertise and impact-minimization you could never achieve on your own, no matter how tech-savvy you are.

"With the accelerating digitalization of business models comes vulnerability to cyberattacks. Even the largest and most technologically advanced companies are not immune."

Istari | The CEO Report of Cyber Resiliency

continued next page →

66%
of FIs

that use Machine Learning or AI experienced a decrease in overall fraud rates[11]

"In today's world where the payment ecosystem is highly distributed and increasingly complex, it's vital banks get the support they need to ensure card payments run seamlessly."

Laura Quevedo, EVP, Financial Crime & Resiliency, Mastercard Services

But like two sides of a coin, AI has positive advantages to bring to your payment resiliency. Machine learning and predictive analytics are effectively helping banks optimize decisioning and pinpoint and prevent the most subtle or sophisticated fraud attempts.

According to Laura Quevedo, EVP, Financial Crime & Resiliency, Mastercard Services, "With an increased focus on resiliency, we are harnessing the latest AI technology to advance our solutions and make it even easier to 'stand in' for our customers to keep payments flowing. This improves consumer experience and protects trust across the ecosystem."

In the arena of payment resiliency, Mastercard is making major strides in the use of AI through our Dynamic Decisioning service. If an outage occurs for any reason, Dynamic Decisioning steps in, employing AI technology to evaluate more than 200 dynamic variables to make informed authorization decisions on the bank's behalf. AI modeling leverages learnings from historical decision patterns, allowing it to imitate the issuer's decision.

Further reading

McKinsey & Company. The future of the payments industry: How managing risk can drive growth | February 2024

GoCardless. AI Payments: How is AI affecting the payment industry? | June 2023

Why zero downtime matters

Security concerns

34%

of consumers are very concerned with the level of cybercrime[12]

11%

are extremely concerned and have been impacted by it[12]

Reputational damage

45%

learn about data breaches, cyberattacks, and scams happening in their country and around the world through mainstream news media[12]

When every payment just works, people trust you more

Why does payment resiliency matter? Think of it this way. You're driving on the highway late at night and you're running on empty. You find the last station for the next 100 miles, but your card is declined at the pump. Now what? Or this: Hot tickets for a popular concert just went on sale — and the best seats will sell out in minutes. Your card is on file with the ticket seller, you've picked your seats, you hit BUY and .... Error. Those seats are gone. Outages impact merchants, too. If a customer has issues with their card at the point-of-sale, whether it's an online retailer or a local food truck, the impact can be potentially lost revenue and loyalty for merchants. Think of the frustration across the payments value chain.

Now imagine a million or more of "you". Everyday people who rely on their financial institutions every single day for every single transaction.

When payments systems are down, whether it's for eight hours or 12 days, the cost can be incalculable. The service that you provide is simplicity itself — a consumer buys something with a tap, swipe or click. It's a no-brainer decision that takes seconds. Fail to deliver on that simple expectation (and the reason why doesn't matter), and trust is lost. Your reputation and customer relationship plummet.

As consumer awareness of data breaches, scams and cybercrime escalates, so does their expectation of a consistently seamless, problem-free payment experience.

What's more, they expect their payment provider will protect — and reimburse — them when fraud occurs.

But, in the end, why is payment resiliency so important? Because the people who count on you are.

Become risk-ready

Payment resiliency is too big to take on alone

Effective payment resiliency demands strategic collaboration. Enhancements made on an ad hoc basis to close gaps may work as an immediate fix, but they don't necessarily add up to a long-term risk-management solution. With advancing technology, heightened consumer expectations, rising geopolitical and cybercriminal threats and intensifying regulatory scrutiny, your payment resiliency strategy needs to be looked at holistically and systematically — with the right partner. This is where Mastercard can step in.

Read our latest article on how to best prepare and protect your payments ecosystem.

How we can help

Every outage damages both your bottom line and reputation. Mastercard offers a comprehensive suite of payment resiliency solutions ready to be tailored to your strategic needs.

To find out more, and to contact us, visit our Payment Resiliency webpage.

Sources

1 Aite-Novarica 2023, Study of FIs and Merchants on Cybersecurity

2 Aite-Novarica 2022, Payment Processing Resiliency: A study on strategies and experiences

3 IMF Blog: Rising Cyber Threats Pose Serious Concerns for Financial Stability

4 Packetlabs: The History of Financial Sector Cybersecurity: Statistics to Know

5 SecurityWeek Network: MGM Resorts Says Ransomware Hack Cost $110 Million

6 Splunk: The Hidden Costs of Downtime in Financial Services

7 Data Center Knowledge: Top Data Center Outage Trends and Strategies for Reducing Risk

8 Latest trends in regulatory compliance, 2023

9 Changes on the horizon to U.S. operational resilience regulations?, 2024

10 Istari, The CEO Report on Cyber Resilience

11 PYMNTS. Mastercard: AI Lets Us Prevent Payment Disruptions

12 Aite-Novarica & Mastercard Consumer Study on Cybersecurity, 2022

Legal disclaimer