Deloitte.

FINANCIAL SERVICES INDUSTRY
JUNE 2023

Five ways banks can mitigate a catastrophic cybersecurity event

Contents

Over the past few years, financial institutions around the globe have faced more intense cybersecurity threats than ever.

In 2021 alone, ransomware attacks against banks rose by an astonishing 1,318%.[1] This is at least partly due to the pandemic, which spurred a rapid transition to remote work and accelerated the move towards digital transformation. As a result of these unplanned initiatives, many banks are now struggling to address the vulnerabilities introduced by a wider attack surface.

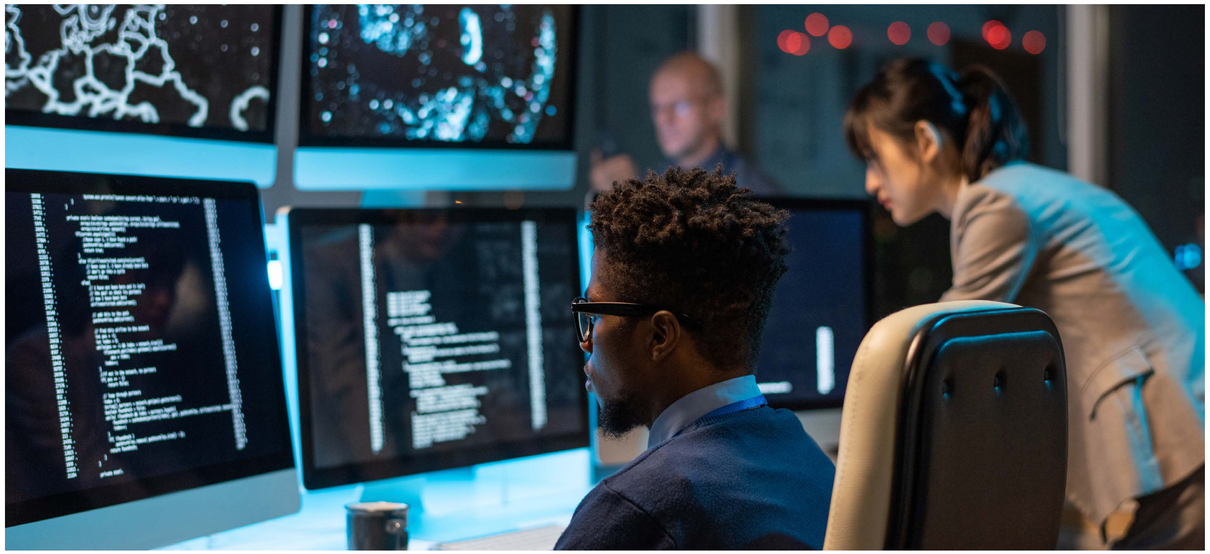
At the same time, mounting geopolitical uncertainty is putting financial institutions under greater pressure to mitigate against unexpected loss events.

This isn't simply to forestall the increasingly sophisticated cybersecurity attacks made possible by the interconnectivity of systems. It is also in response to more stringent regulations. The US and Europe are now required to take action to minimize customer harm – this includes understanding your critical third party providers to reduce your concentration risk. Similarly, regulatory trends in Europe, Asia, and North America are urging local and global banks to enhance their enterprise resilience.

To keep pace, most financial institutions are hardening their controls and looking for ways to strengthen their cyber maturity. Despite this, many banks have still to demonstrate adequate risk mitigation against a catastrophic cybersecurity event.

What is a catastrophic cybersecurity event?

To understand what's at stake, it's helpful to define what a catastrophic cybersecurity event entails.



For instance, events in scope could include:

1. An organized cyberattack that results in the simultaneous loss of both production and backup data
2. A service degradation that makes infrastructure, applications, and corresponding services inoperable, locks clients out of their accounts, and leads to a loss of trust – and ultimately lost customers
3. A cybersecurity event aided and abetted by either malicious or unwitting insiders that trickles across the enterprise to bring down the entire IT infrastructure
4. An IT outage that restricts access to recovery systems, making it impossible to maintain core business operations
5. A systemic market disruption that prevents accessibility to a broad swath of bank products

Although financial institution executives are assessing and sponsoring activities to understand how to recover from a scenario that restricts their access to their data and/or infrastructure, only a few have active capability.

Recovery from cyber attacks that disable systems require a different approach to standard disaster recovery planning. Disaster recovery assumes systems and backup are available, so even if systems go down for a few hours, they can be recovered quickly from dedicated backup facilities. In the most advanced financial institutions, paired or active-active data centers enable continuity of service even if one location were to fail.

In a catastrophic scenario, however, connection between data centers and or backup sites designed to replicate data also replicates malware across technology at the speed of light. This outcome is not lost on attackers. As a result, institutions that face these kinds of real-world situations may find themselves unable to manage their liquidity in the market, settle transactions, or support customer withdrawals without business workarounds.

Greater resilience requires new protocols

The cruel irony is that the very technologies that organizations have put in place to streamline operations and better serve customers can be used by attackers for financial gain. Financial institutions, and their regulators, are aware of the limitations of current disaster recovery plans, recognizing that new protocols are needed to counter today's complex threat environment.

While there is no one-size-fits-all solution to guard against catastrophic cybersecurity events, there are certain leading practices financial institutions may want to explore:

- **Plan for destructive scenarios.** Regulators require that extreme but plausible scenarios be considered. By gaining a better understanding of the impact of these types of crises, financial institutions can determine the data and systems they need to recover quickly as a minimum viable business, establish their baseline capabilities, and identify critical gaps they need to close. It is key to maintain a perspective and balance the spend on resilience against the risk reduction achieved. Re-use of existing technology, re-shaping process, and business workarounds can play a major part.
- **Develop a plan to recover a minimum viable business to maintain core services.** At a bare minimum, financial institutions must assess which key services are required to maintain core operations. The answer to this question is not as straightforward as you'd imagine. A triage process needs to be applied to consider the prioritization of fundamental requirements such as managing liquidity and settling in the market, customer accounts, payments, and balancing the books, among a host of other services. As a first step, internal teams will need to resolve these conflicting priorities so that IT teams can pinpoint the specific applications and systems that must be recovered first.
- **Protect foundational systems.** Once critical business functions are identified, they should be mapped to underlying applications, data, and infrastructure to uncover interdependencies that enable recovery. In addition to supporting efforts to establish a minimum viable technical operating environment, this process can help organizations enhance awareness of risk across the business.
- **Build a critical materials vault.** To prevent catastrophic losses, leading organizations are now building isolated, immutable, intelligent materials vaults to store critical data, applications, and core infrastructure services. By creating immutable recovery zones, clean rooms, and preconfigured workflows, financial institutions can gain the ability to reconstruct damaged environments and recover minimal viable operational capacity quickly.
- **Strengthen recovery processes.** To enhance institutional resilience, banks will need to strengthen their recovery playbooks, carefully documenting the recovery processes to recover critical services. Optimization of recovery speed can only be achieved through conducting tests to verify that their solutions work as designed.

Greater resilience requires new protocols

"While cybersecurity might be the domain of the CISO, cyber recovery requires cross-functional collaboration from technology, business resilience, and risk, as well as the CISO and COO."

To be effective in catastrophic cybersecurity events, banks must build muscle memory in a multifunctional team that is both drilled in the processes and capable of working in an agile manner. While cybersecurity might be the domain of the CISO, cyber recovery requires cross-functional collaboration from technology, business resilience, and risk, as well as the CISO and COO. This explains why accountability for cyber recovery tends to sit at the CIO or COO level within business functions where the risk is most acute.

Beyond the compliance imperative, planning for recovery from severe scenarios can also have day-to-day operational benefits. For instance, it often drives simplification of core banking processes, reducing cost while enabling technology transformation (e.g., cloud migration). By applying an organizational survivability lens to development and business change programs, organizations can futureproof supporting technology and remain within their stated risk appetite.

Connect with us

Endnote

1 *https://www.zdnet.com/article/the-state-of-ransomwarenational-emergencies-and-million-dollar-blackmail/*

Nick Seaver
Partner – London
Cyber and Strategic Risk

nseaver@deloitte.co.uk

Jay Choi
Partner – Copenhagen
Cyber and Strategic Risk

jaychoi@deloitte.dk

William McLeod-Scott
Partner – London
Cyber and Strategic Risk

wmcleodscott@deloitte.co.uk

Kristian Skotte
Partner – Copenhagen
Cyber and Strategic Risk

kskotte@deloitte.dk

Pete Renneker
Managing Director – Cincinnati
Cyber and Strategic Risk

prenneker@deloitte.com

Melissa Valdes
Senior Manager – London
Cyber and Strategic Risk

mevaldes@deloitte.co.uk

Deloitte.

J30970