Deloitte.

Planning for change

US financial leader improves cybersecurity and regulatory compliance with a technology and strategy transformation

Financial services
Industry

Cyber recovery vault
Solution

Cyber Stories

The starting point

Cyberattackers know where the money is. They relentlessly target financial institutions through increasingly sophisticated tactics—hoping to infiltrate systems, leverage data to their advantage, create chaos, and profit. Whether the end game is collecting a ransom, compromising bank accounts, or causing business disruption, there is no denying their potential to cause lasting harm.

Regulators worldwide continue to take note, vigorously establishing and enforcing rules as they seek to ensure that banks and other financial institutions remain sound and secure. For one large US financial company, the growing pressure from regulators led their leaders to take a hard look at their organization's existing and future cyber capabilities and ultimately begin charting a new path—one that would provide greater visibility into data, boost security, and improve compliance.

The combination of siloed business, risk, and technology functions and interconnected systems created challenges as the company began defining its ambition and pondering a way forward. And while company leaders wanted to improve their incident readiness with a cyber recovery vault, they quickly realized they needed to do more than install the new technology. They needed a business-centric approach to cyber that synchronized a much broader set of capabilities that ultimately drove their cyber transformation.

Factors in focus

- Growing regulatory pressure and scrutiny around cybersecurity
- Stakeholder concerns over organization's cyber readiness
- Need for broader transformation focused on business needs

The way forward

The company had already taken an important step toward greater resilience. It had selected a vendor to provide a cyber recovery vault. Such a vault can protect essential business services by storing essential backups and business data in a segregated, secured, and immutable form, preserving data almost as if it were cryogenically frozen. Through this innovative design, malware that makes its way into the vault never has a chance to deliver its payload, thus preserving the environment. By turning to a vault in the wake of a cyberattack, a company can extract, cleanse, and recertify any exposed data and applications before putting them back onto its network.

For the financial institution, the vault needed to do more. Company leaders wanted to get maximum value from the vault. They wanted to ensure that it would support evolving regulatory and reporting needs, and that it would enable future business endeavors. Leaders wanted more than a technological solution, they wanted a business-focused solution, and they enlisted Deloitte's help to begin crafting that solution.

Collaborating with Deloitte, the organization took a step back to define a more extensive cyber resilience program as part of a broader cyber transformation. Deloitte provided technical oversight for the vault's requirements, design, and architecture. Deloitte also worked closely with the financial institution to develop an operating model and governance to integrate vault operations with existing IT and cyber operations.

Insights to inspire

Do not despair (too much) over regulations. Regulatory changes can offer an opportunity to understand your data better, develop more meaningful insights into your business processes, and take steps to make your organization more resilient.

It takes more than technology to combat cyberattacks. You will also need to establish solid controls and testing procedures to help ensure your organization can use cyber technologies effectively when the time comes.

Planning for change

Next, the two organizations began crafting an enterprise-wide cyber incident response plan—one designed to help the organization quickly investigate and defend against a destructive cyberattack scenario. To make sure company leaders were aligned on challenges, opportunities, and outcomes under the program, Deloitte conducted multiple resilience labs focused on exploring the possibilities, aligning on the priorities, identifying the critical business services, and ultimately selecting the appropriate strategies.

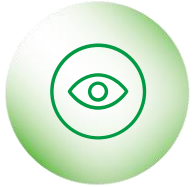
As the pieces of the broader transformation came together, Deloitte worked with the company to test processes for recovering data from the vault. And the work did not end there. The two organizations established a multiyear integrated program plan that aligned the financial institution, the technology providers, the regulatory bodies, and Deloitte on the path ahead.

Through this broader cyber transformation, the organization reduced their cyber risk, business risk, and regulatory risk, increased visibility into the essential services, processes, applications, infrastructure, and data and improved its confidence in its ability to recover from destructive cyberattacks.

The achievements

Improved technologies and controls for responding to and recovering from cyber incidents

Increased business resilience, with accelerated recovery capabilities



Greater visibility into business-critical data and processes

Improved ability to meet regulatory demands

Reduced risk and increased confidence across the enterprise

Let’s talk cyber

How will your organization stay ahead of regulatory, business, and cyber challenges? Discover how Deloitte’s worldwide team of industry-focused cyber specialists can help you create a more holistic strategy that can position your organization for future needs. Contact us to get the conversation started.

deloitte.com/cyber
deloitte.com/cir3

Contacts

Pete Renneker
Managing Director
Deloitte & Touche LLP
prenneker@deloitte.com

David Pompei
Advisory Managing Director
Deloitte & Touche LLP
dpompei@deloitte.com

Sunny Aziz
Advisory Principal
Deloitte & Touche LLP
saziz@deloitte.com

Moses Lahey
Advisory Manager
Deloitte & Touche LLP
mlahey@deloitte.com

Deloitte.

Cyber Stories