



Regional Banking: Your Information  
Security Roadmap to \$10 Billion  
and Beyond



## On the road to \$10 billion

\$10 billion is a special kind of tipping point for regional banks. As you inch toward that magic number of total consolidated assets, a litany of concerns -- and ballooning costs -- arise as [Dodd-Frank Act stress test \(DFAST\)](#) requirements kick into gear. Today's heightened uncertainty surrounding regulation only adds to the scrutiny that <\$10 billion banks are under, not to mention to data security risks that develop parallel to growth.

What information security vulnerabilities do regional banks face on and off the road to \$10 billion? Here's how you can cover your regulatory bases, while enhancing controls and reducing risk:

- Identify your biggest Information security vulnerabilities
- Avoid a multi-million dollar mistake
- Map out your \$10 billion strategy
- Understand the long-term impact of effective data governance

## Is your regional bank at risk?

The headlines are rampant across industries and verticals. [Millions](#) upon millions of private data records are stolen through leaks and security breaches. Big banks and regional bank leaders alike have been targets -- an insider breach was responsible for compromising the data of over 1.5 million of [SunTrust's](#) customer data. Regional banks like SunTrust are facing information security risks across multiple fronts:

- **Trickle Down Risk:** as breaches intensify big banks are hardening their cybersecurity plans, driving hackers to prey on smaller firms. Small banks don't have the resources to hire teams of technology experts and spend millions for sophisticated software -- thus smaller banks end up being an entry point into the financial system.
- **Data Governance Failings:** unstructured data comprises the vast majority of digital business assets -- [about 85%](#) of business data. Ensuring that access is controlled and governed by business "need-to-know" is imperative; yet banks across the FinServ spectrum lack the basic infrastructure to govern identities and access management.
- **Human Error:** human error can be a major vulnerability for regional banks, who risk losing millions of dollars and invaluable data records, not to mention lasting damage to their reputations. Outdated processes, lack of training, under resourced support teams and inadequate oversight are risk drivers -- and there is always the issue of malicious intent from existing and former employees.
- **Regulatory Noncompliance:** Smaller banks face disproportionate risk with smaller scale security infrastructure and on-hand expertise; yet they face big bank requirements and regulations. The cost of noncompliance is likewise disproportionate as you edge closer to the \$10 billion threshold. Regional banks are obligated to meet the needs of their core customer base and the regulatory

world. That means proactive investment to avoid regulatory penalties, pass institutional stress tests, as well as dodge potential breaches.

## Key Milestone: The \$5 Billion Sweet Spot

Firms need to invest a year or two in prep work for increased regulation, making strategy and information security shifts to meet the growing costs of compliance.

- The \$5 billion mark is when regional banks should really start to gear up for change.
- This usually involves scouting new C-suite members from Chief Risk Officers to CISOs and staffing up with new departments and external vendors to meet a robust set of compliance and data security needs.
- Regulators will expect firms to have plans in place at the cusp of the \$10 billion mark, traditionally around \$7-8 billion in consolidated assets.
- Given the timeline and expectations, the halfway \$5 billion threshold is the ideal time to start putting the machinery in place to run like a larger financial institution.

### Avoiding a multi-million dollar mistake

The lasting effects of a data breach can reach far beyond the scope of invaluable data records lost. Lasting financial and reputational damage, litigation, regulatory penalties and more can make an average data breach cost [upwards of \\$3 million](#). What can your regional bank do to mitigate risk?

**Change your mindset:** Firms can't rely solely on error-proofing their operations. Regional banks must come to terms with the expanding costs of data protection, regulatory compliance, and the ripple effects of a breach, even if that means changing the way they do business. The opportunity cost of a potential breach that erodes market share, consumer confidence and trust over proactive security investment is often too great for firms to bear. Expanding technology and support staff as well as engaging data security providers is quickly becoming the cost of doing business for smaller banks who are seen as an easy entry point into the financial system. Some regulators, like The New York Department of Financial Services, are even [mandating](#) tighter cybersecurity rules, including increased full-time staffing of information security officers.

**Leverage security as a competitive edge:** Data security and access are only going to become larger more complex issues as firms grow and face increased regulatory scrutiny. Being able to access your regional bank's risk profile and make your data actionable is key. Banks will need more on-hand talent and technical expertise than ever before, alongside historical and centralized data, and expert analysis to make sense of it all. Bigger banks are focusing on security and you must too in order to be competitive -- that means taking stock of your unstructured data, as well as implementing Identity Access Management (IAM) and Privileged Access Management (PAM). Regional banks need to take note of big bank information security and adopt these instruments as part of their greater data governance framework.

## Shift Towards Automated Processes, IAM, and PAM

Smart Technologies and analytical tools abound to cross-check payments, govern data, perform audit trails and manage access. Here's how you can deploy identity and access management (IAM) and privilege access management (PAM) to help automate the necessary business rules for ensuring proper data governance and access:

- Understand your distributed systems, applications, platforms, and how each manages entitlements.
- Determine what privileged accounts exist, who is using them and what the existing work-flows and process surrounding them are.
- Apply automation to ensure security policies are being employed and followed according to governance rules.
- Add new users or updated access seamlessly, tightening on-and-off-boarding policies and ensure that former employees are immediately discontinued from access to your systems.

**Do more with less:** Regional banks don't have bottomless resources, yet they are particularly pressed when it comes to securing valuable data -- doing more with less is key and automation helps solve this problem. Digitization has helped replace paper-based reporting to deliver real-time data for proactive business intelligence; like root cause analyses and predictive analytics. Managing risk can be accomplished with the right visibility -- automated data tools that report on risk power a continuous cycle that constantly identifies new vulnerabilities, reevaluates and updates policies, and implements remediation to help manage the process.

**Implement proactive risk management:** Along with competent data visibility, safeguarding data networks amid the expanding threat of cybercrime is critical. Regional banks are often more vulnerable to breaches than their larger counterparts. In response, risk committees are becoming increasingly common to evaluate risk profiles from financial viability to information security risk. Data governance, remediation and access management will work to enhance cross-departmental visibility to mitigate compliance and minimize risk.

*The lasting effects of a data breach can reach far beyond the scope of invaluable data records lost. Lasting financial and reputational damage, litigation, regulatory penalties and more can make an average data breach cost upwards of \$3 million.*

## **The impact of doing nothing**

Regional firms will find the ground shifting beneath them on the road to \$10 billion. Hitting that threshold means that small scale banking strategies are no longer viable. Expenses rise within this regulatory landscape -- accounting for the cost of protecting data, monitoring systems, documenting it for regulators, hiring security vendors and staff -- and the pressure is ripe to make up for costs with increased revenue and profitability. Some smaller institutions who can't withstand the costs will be forced to merge to accomplish the big bank framework.

Enacting scalable business models and reworking data security strategies through automation and sustainable governance are part of the big bank framework regional banks can implement, without replicating complex (and costly) back office solutions.

The impact of doing nothing can lead to multi-million dollar losses for regional banks who are looking to hit the \$10 billion dollar threshold and beyond.

**Do you know where your regional bank stands?**

## **About SPHERE Technology Solutions**

SPHERE Technology Solutions is an award-winning woman-owned cybersecurity business focusing on improving security and enhancing compliance. We put controls in place to secure your most sensitive data, create the right governance processes for your systems and assets, and make sure companies are compliant with the alphabet soup of regulations surrounding this space.