SECURITY COMPASS WHITEPAPER

Ensuring Cybersecurity in an Open Banking World

Security Compass

The move by organizations to DevOps and the digital transformation of businesses is occurring across all industries. Retail is less dependent on brick and mortar stores than ever and electronic medical records promise to make healthcare delivery more efficient. Its effect on the financial services industry has also been rapid and is accelerating.
New business models have disrupted the traditional banking industry; consumers and commercial customers are not limited to local providers, opening competition from innovative competitors.

While this has presented new challenges to traditional financial institutions, it presents many opportunities for their customers and innovative competitors. Reducing the need for physical branches lowers costs and enables organizations to offer consumer-friendly services such as lower maintenance fees, reimbursable ATM fees, higher savings, and CD yields.

Security concerns with open banking and banking-as-a-service

Earlier, regulatory restrictions presented substantial barriers to entry to the financial services industry. However, the opportunities provided by digital transformation now has encouraged regulators to open the sector to new offerings such as open banking and banking-as-a-service.

The open banking initiative in the U.K. describes itself as a "secure way to give providers access to your financial information." Likewise, the European Union's Revised Payment Service Directive (PSD2) is designed to give consumers more control over their banking data. It requires that banks give third-party providers access to a customer's payment account information (provided the customer agreed to the release). Through a well-defined set of open banking APIs, other service providers can access an individual's banking information to provide new offerings. Instead of dealing with individual banking applications, a single financial technology application can access all services across multiple institutions.

For consumers, this means more visibility and control over their financial information. For providers, open banking provides the opportunity to offer innovative products and improve the customer experience. In particular, this frees competition in the financial services market to organizations not burdened with thousands of legacy applications. The largest companies with the most insight into consumer preferences are obviously well-positioned to benefit. In 2021, Google will leverage this to offer Plex, a new mobile-first bank account integrated into Google Pay.

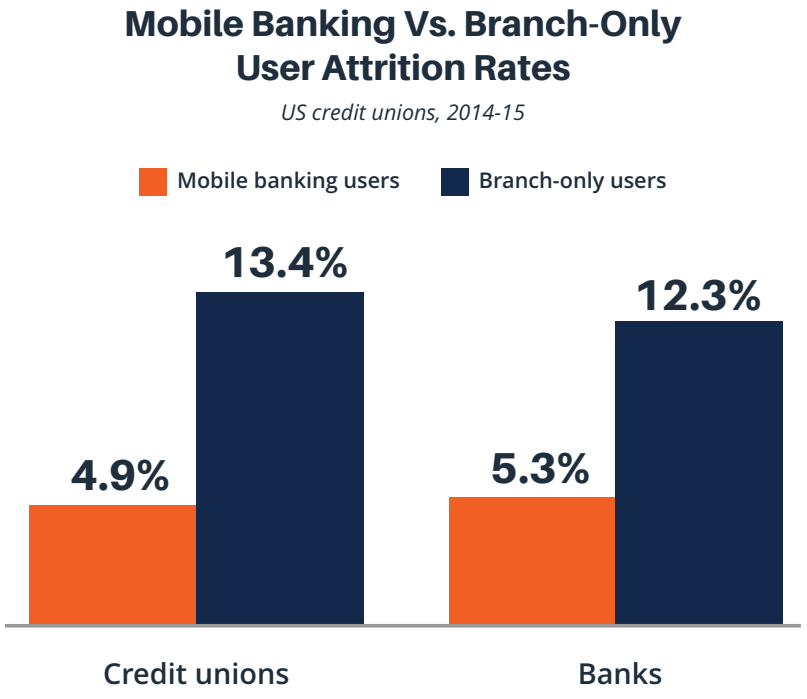
Open banking regulations are in place in much of the world, and financial institutions should anticipate similar requirements in North America. Consumers have shown a willingness to use these services — assuming adequate security is provided.

Can financial institutions thrive without innovation?

New competitors and potential partners have made it clear that financial institutions must innovate to survive and thrive. Consumers and businesses expect more from their online experience, whether that is the ability to temporarily turn-off a payment card, access a credit score, set spending limits on cards, or link debit or credit cards to smartphones.

A more convenient location or lower rates can motivate customers to leave for a competitor. By engaging consumers when they are online, you can reduce attrition.

Innovation requires financial institutions to move quickly. In today's market, web presence has become paramount, often the only presence for some firms. This means self-service account set-up for new customers, online support, mobile applications, and hyper-personalization of services.



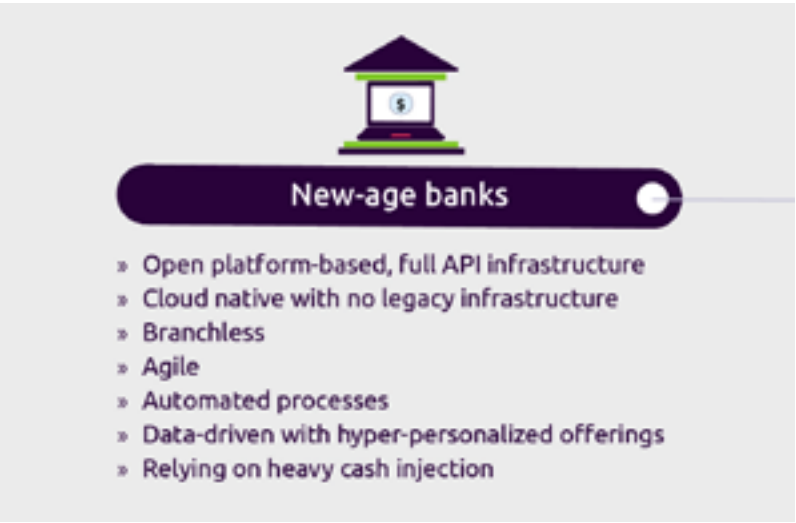
Source: Fiserv Mobile Banking Adoption White Paper

You can see the risk to banks and credit unions that are dependent on branch-only users.

New business models introduce new risks

Changing methodologies and partnerships open financial institutions to new attack vectors. Banking-as-a-service requires reliance on application programming interfaces (APIs) — both inbound and outbound. As seen in the SolarWinds breach, ensuring that assets are protected from "supply chain" attacks on vendors and partners is critical. A breach at any open banking partner can expose customer data.

Changing deployment models also introduce new challenges for security and operations. Many financial institutions have legacy systems that provide critical services. Migrating these to the cloud introduces dozens of new security challenges, including risks from insecure API calls to cloud services and managing the sensitive data in the cloud.



Source: Capgemini 2020 World Retail Banking Report

Adapting to rapid changes in the financial services sector

Software innovation requires organizations to adopt new development methodologies, including rapid development practices like agile, DevOps, and Continuous Integration/ Continuous Delivery (CI/CD). On top of this, many organizations have decided that proprietary data centers are no longer a requirement. Cloud platforms and the ability to quickly scale resources up or down allow teams to focus resources on building better software and use Cloud Service Providers (CSP). The need to adapt to this new paradigm has challenged engineering, operations, and security teams.

Gone are the days when software security could operate as a separate entity, providing testing services to development teams near the end of the development process. Using traditional testing tools like static and dynamic analysis as a first-line of defense for identifying security vulnerabilities leads to expensive code refactoring costs, delays in software releases, and friction between security and engineering teams.

Anticipate threats, rather than patching vulnerabilities

The problem with security testing is not the ability to identify vulnerabilities. Static and dynamic analysis tools easily spot many coding errors that can result in vulnerabilities. Instead, the problem is the strategy of using tools to identify vulnerabilities in lieu of anticipating threats and implementing appropriate security controls. Preventing vulnerabilities is more cost-effective than scanning for vulnerabilities later in the development lifecycle.

The process for anticipating threats and preventing vulnerabilities is not a secret. Secure coding practices help developers understand how vulnerabilities occur and more secure methods to build software. Threat modeling exercises have been used for decades to analyze a proposed application to identify potential attack vectors and apply controls to mitigate risk.

In a modern development environment, however, these can be difficult to implement. Time to market pressure prioritizes functionality and release schedules. While secure coding does not necessarily slow down a developer, remembering all of the threat scenarios, policy requirements, and mitigation controls can be difficult when customers and business owners are clamoring for new features.

New approach to threat modeling and secure coding

Threat modeling and secure coding guidelines can help, but traditional threat modeling and policy requirements do not fit well in a rapid deployment environment. Threat modeling exercises require senior security and software development resources to map out the application's architecture and trust boundaries, then map security controls from policy manuals to mitigate risk from the identified threats. This presents several challenges:

- **Scarce senior resources:**
  Traditional threat models require senior security and development resources to discuss architecture, complete questionnaires, produce data flow diagrams, and select controls. These resources are scarce and in high demand. Allocating for days or weeks of threat modeling exercises is not practical in most organizations.

- **Scalability:**
  Developing in-depth threat models is not simple. Cataloging threats and identifying appropriate controls can take weeks. Diagraming architecture and generating attack trees and DFDs require days of discussion. This investment limits in-depth threat models to an organization's most critical projects.

- **Consistency:**
  Ideally, organizations will identify threats and apply consistent controls. However, the output from manual threat models reflect the knowledge and biases of those participating in the exercise. As team members change, identified threats and controls will also change.

- **Auditability:**
  When a manual threat model is completed, the threats and controls are often maintained in a spreadsheet or shared document and updated via email. This provides poor evidence of compliance with corporate policies and regulatory standards.

Scale threat modeling to secure your financial institution

While a complete, manual threat model is required for an organization's most critical applications, security for all applications can be greatly improved by automating the process for threat modeling and applying secure coding guidelines. This is because most of the threats to an application or system are inherent to its design, purpose, and deployment environment.

For instance, if a team is deploying on AWS, there are specific tasks that must be completed to ensure only authorized users can access data buckets. Likewise, when untrusted data enters an application, controls must be in place to prevent malformed or unwanted strings from being accepted. These controls are true for any internet-facing application.

SD Elements, our flagship solution, leverages this fact to automate the threat modeling process, eliminating the manual effort significantly while delivering most of the benefits of a weeks-long manual threat modeling exercise. Through a dynamic survey, SD Elements automatically identifies the threats associated with a project's technical stack and deployment environment, translates threats and complex regulatory requirements into actionable controls, and assigns easy-to-understand tasks and test plans to DevOps teams.

Improve time to market while ensuring security

The competitive requirement to deliver new features and applications quickly requires teams to think differently about security. SD Elements ensures that threats to applications, organizational policies, and regulatory standards are met and validated. It anticipates threats and provides DevOps and security teams with actionable tasks to mitigate risk. This means that security testing is primarily validating that prescribed controls were implemented correctly instead of acting as a primary vulnerability discovery activity.

The result is a balance between speed and security. SD Elements allows companies to build products nearly as fast as if they were being built without any security or compliance at all and as safely as if they were built under the guidance of security experts.

Security Compass

Go Fast. Stay Safe.

Security Compass, a leading provider of cybersecurity solutions, enables organizations to shift left and build secure applications by design, integrated directly with existing DevSecOps tools and workflows. Its flagship product, SD Elements, allows organizations to balance the need to accelerate software time-to-market while managing risk by automating significant portions of proactive manual processes for security and compliance. SD Elements is the world's first Balanced Development Automation platform. Security Compass is the trusted solution provider to leading financial and technology organizations, the U.S. Department of Defence, government agencies, and renowned global brands across multiple industries. The company is headquartered in Toronto, with offices in the U.S. and India. For more information, please visit www.securitycompass.com.

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS

OFFICES

GLOBAL HEADQUARTERS
1 Yonge Street
Suite 1801
Toronto, Ontario
Canada M5E 1W7

TORONTO
390 Queens Quay W
2nd Floor
Toronto, Ontario
Canada M5V 3A6

NEW JERSEY
621 Shrewsbury Avenue
Suite 215
Shrewsbury, New Jersey
USA 07702

CALIFORNIA
600 California Street
San Francisco, California
USA 94108

INDIA
#4.07
4th Floor, Statesman House
Barakhamba Road, New Delhi
India 110001