

FINANCIAL INDUSTRY

Are You Prepared For A Cyberattack?



The growing dependence on technology has brought a similar upsurge in cyberattacks, particularly in the financial industry. Whether a bank, credit union, or insurance, financial institutions are a key target for attackers. Similarly, the traditional culture of financial institutions often leaves IT behind the times – and vulnerable to attack.

COMPLIANCE REQUIREMENTS

Compliance is central to many areas of financial services and information security is no exception. Many financial institutions are subject to Gramm-Leach Bliley Act (GLBA) security requirements, but that's only the first of many. Those firms handling credit card data are also subject to PCI-DSS, and public corporations to SOX. In many cases, ISO 27001 is a necessity in the financial industry to demonstrate proper controls to customers and investors.

Rhino Security Labs provides the technical expertise and guidance to help financial institutions through these security requirements.

POTENTIAL IMPACTS






- Service Downtime / Financial Losses
- Reputation Loss
- Negative Press
- Breach Lawsuits / Legal Fees

ATTRACTIVE AND READY TARGETS

With large, sensitive databases and applications, the financial industry faces a number of security adversaries. But outside threats aren't the only security concern to IT. Legacy banking applications, poor development practices, and network complexities all provide weaknesses to be exploited by attackers. Even the largest financial firms aren't immune to such issues – as shown with breaches at JPMorgan and Citi.



FINANCE TARGETS

-  Card Data Warehouse
-  Sensitive backups
-  Banking App Environments
-  End User Databases
-  Critical Financial Systems

RELATED ASSESSMENT SERVICES

To support the security needs of the industry, we have a range of penetration testing services. Below are a few of these recommendations, customized around your business business and technology needs.



1. Penetration Testing

Our world-class penetration testing and research has been covered in Wired, Forbes, CNN and other outlets, showcasing our comprehensive assessment package. Identify the weaknesses– and strengths – of your security infrastructure before attackers do.



2. Social Engineering

While security assessments are typically focused on technology, many attacks begin with a phishing email or phone call. Test employee education, security policies, and technical controls to identify gaps in phishing prevention.



3. Application Assessment

Each application assessment starts with the OWASP Top 10 risks, but includes more advanced vulnerabilities to ensure all attack vectors have been identified. Whether web, mobile, or IoT, we have the experience to address the unique security challenges you face.



4. Secure Code Review

Identify and remediate software vulnerabilities early and often. With a hybrid approach, we use both automated code scanners and hands on, manual analysis to conduct a thorough security review of your application.

PAST ATTACKS



JUNE 2011

CITIBANK
360,000 users' card data stolen

OCTOBER 2014

JP MORGAN
76 million users in banking breach

MARCH 2015

SMCF CU
Montana Credit Union hacked by ISIS

SEPTEMBER 2015

EXCELLIUS INSURANCE
10.5 Million customers affected

OCTOBER 2015

SCOTTRADE
4.6 million users compromised

ABOUT RHINO SECURITY LABS

Rhino Security Labs is a top penetration testing and security assessment firm, with a focus on web applications, cloud/AWS, network, mobile apps and phishing testing. With manual, deep-dive engagements, we identify and demonstrate security vulnerabilities which put clients at risk.

Endorsed by industry leaders, Rhino Security Labs is a trusted security advisor to the Fortune 500.