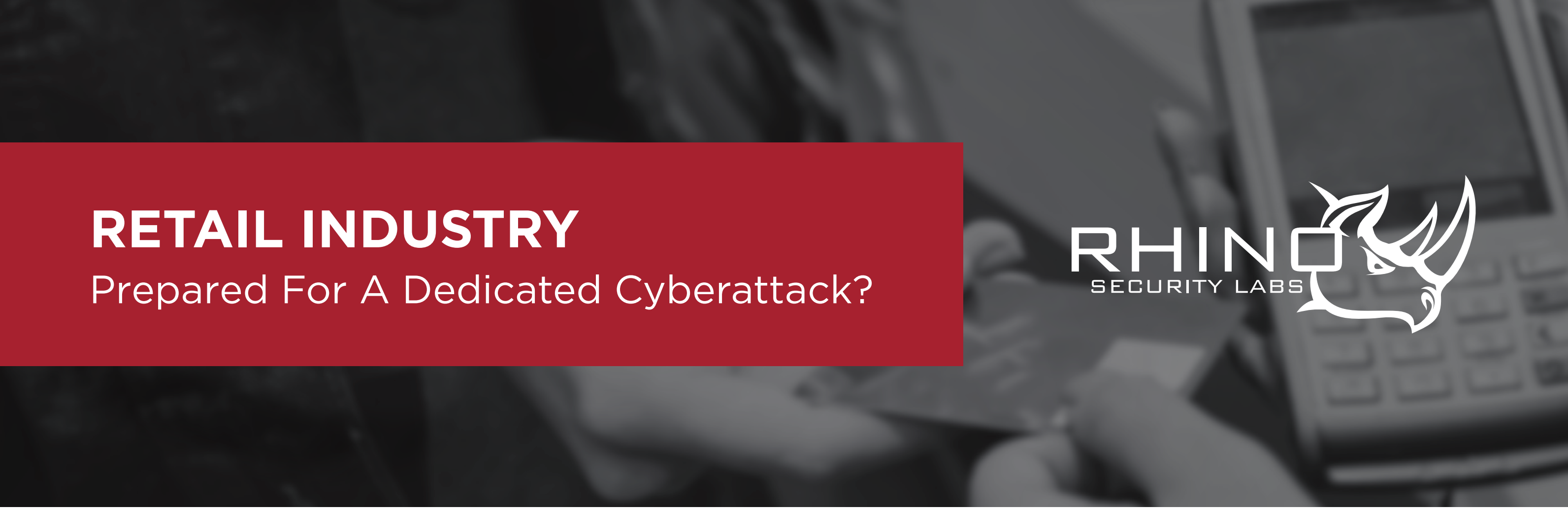
RETAIL INDUSTRY

Prepared For A Dedicated Cyberattack?



The growing dependence on technology has brought an upsurge in cyberattacks, particularly in the Retail industry. With a high reliance on point-of-sale (POS) terminals and the potential for credit card theft, the retail industry is at a particularly high risk.

COMPLIANCE REQUIREMENTS

Compliance is central to the retail industry, with PCI-DSS regulation requiring all companies who handle card data to be compliant. Public retail corporations are also subject to SOX compliance, requiring further checks and balances to ensure data security is implemented properly. In many cases, ISO 27001 is required to demonstrate proper controls to customers and investors.

POTENTIAL IMPACTS

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

ATTRACTIVE AND READY TARGETS

With client information, credit card databases, and point of sale terminals, the retail industry faces a series of threats.   But valuable data isn’t the only security concern to IT. Legacy POS applications and poor development practices provide weaknesses for attackers to exploit.

Even the largest retailers aren’t immune these attacks—as shown with breaches at Target and Home Depot.

RETAIL TARGETS

- Point of Sale Systems
- End User Databases
- Critical Financial Systems
- Sensitive backups
- Card Data Warehouses

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 ⚠

OCTOBER 2013

NEIMAN MARCUS

1.1 million customers affected

FEBRUARY 2014

EBAY

Class action lawsuit filed after massive breach

AUGUST 2014

ALBERTSONS

Card info for unknown number of customers lost

SEPTEMBER 2014

HOME DEPOT56

million credit cards stolen in POS breach

DECEMBER 2014

TARGET

Infamous POS hack steals over 40 million cards

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.