RSI

Technology Advisory, Security and Compliance Services

RSI is a trusted resource to help broker dealers and financial advisors navigate today's turbulent Cybersecurity waters and deploy best-in-class security solutions. As a Preferred Partner to HD Vest, 1st Global, Cetera, and First Allied, among others, we can help you accomplish the security goals cited in the FINRA Cybersecurity checklist.

We're well suited to help you proactively plan for core business risks as well as provide incident response if needed. Our security experts can assess how your unique attack surface has evolved over time and whether your Cybersecurity planning and mitigation strategies have kept pace. Focus on the strategies and logistics that drive your future, and let us focus on keeping you secure.

Since 2008, RSI has helped organizations of all sizes achieve risk-management success and protected our customer's critical assets and reputation. Let's talk about how we can confront this evolving threat landscape together, and walk away confident you've met a business and technology partner that deeply understands your company's CyberSecurity needs.

SEC Reg S-P Cybersecurity Program
Financial service firms to have policies and procedures addressing the protection of customer information and records. This includes protecting against any anticipated threats or hazards to the security or integrity of customer records.

Managed Vulnerability Assessment
Continuously identifying, quantifying and prioritizing vulnerabilities in your IT infrastructure ensures that all resources meet or exceed risk tolerance standards.

Managed Penetration Testing
RSI can simulate real-world attacks to assess our client's external applications, network, and mobile applications vulnerabilties in addition to running independent, automated security scans encompassing the Open Web Application Security Project (OWASP) Top 10 vulnerabilities. Our network level penetration test reveals system vulnerabilities that can be easily exploited by real world attackers.

Forensics
Organizations rely on urgent and expedited resolutions after data and security breaches occur. Performing In-depth, root-cause analysis allows us to provide additional security measures to prevent future threats.

IT Asset Management
Our award-winning asset management system autonomously scans your computer's software and hardware, monitoring for needed driver updates or alerting us of unauthorized changes to system configuration. This allows you to make cost-effective decisions on purchasing, redistribution, and re-purposing of your organization's IT infrastructure.

Managed Security & Compliance
Keep up with the most advanced security technology while lowering your cost of ownership with our managed services. We customize our industry-leading managed security services to fit your needs while managing your organization's need to comply with regulations and standards.

Incident Report
Responding to a data-loss incident quickly and in an organized manner is paramount in containing a breach, limiting exposure, stemming losses and preserving evidence.

IT Support/Helpdesk
RSI provides multiple ways for customers to troubleshoot problems by offering assistance through our call center 24/7 or through our self-serve knowledge base.

RSI

858-999-3030

4370 La Jolla Village Drive, Suite 200 • San Diego, CA 92122
www.rsisecurity.com • info@rsisecurity.com

RSI Helps Broker Dealers and Financial Advisors Address FINRA Cybersecurity Checklist and Mitigate Cybersecurity Risk.

FINRA Cybersecurity Checklist	RSI Capabilities
Section 1 - Identify and Assess Risks - Inventory Identify and analyze potential dangers or risks to a firm's business that could arise through its information technology systems.	**IT Assets & Infrastructure Assessments** Regular review of your organization's existing IT infrastructure helps you identify areas of improvement, allowing for more informed and strategic business decisions to take place. Our IT Assets and infrastructure assessment analysis identifies, quantifies and prioritizes all potential hazards that might affect your systems.
Section 2 - Identify and Assess Risks - Minimize Use Limit Personally Identifiable Information (PII) collections to the least amount necessary to conduct its mission; the organization may limit potential negative consequences in the event of a data breach involving PII.	**PII Security Assessment** Our PII data security assessment includes automated scan for PII, interviews and security reviews of network security, and vulnerability assessment scan. We also assess the security controls supporting PII storage and transmission as well as results of current network and penetration tests.
Section 3 - Identify and Assess Risks - Third Party Firms should manage Cybersecurity risk that can arise across the lifecycle of vendor relationships using a risk-based approach to vendor management.	**3rd party vendor security assessment** We can help you implement a 3rd party vendor security assessment program and tools with proven methodology.
Section 4 - Protect - Information Assets Organizations should have robust malware incident handling capabilities to limit the damage that malware can cause and restore data and services efficiently.	**Robust Cyber Defenses and 24x7 Malware Monitoring Services** Your networks & computers are protected from attack, damage or unauthorized access via our threat correlation analyses, holistic application security, self-sealing BYOD protection, advanced anti-malware and more by our 24x7 Security Operations Center (SOC).
Section 5 - Protect - System Assets Identify and maintain an inventory of assets authorized to access the firm's network and critical assets that should be accorded prioritized protection.	**Identity Access Management (IAM) and Authorized Asset Identification** Our Identity Access Management (IAM) services provide control and protocols for managing cyber security. We have tools that capture, track, and compare a client's Cybersecurity asset inventory with their risk tolerance for clients of any size company.
Section 6 - Protect - Encryption Encryption protects the confidentiality of data by ensuring that only approved users can view the data. Other benefits include providing a means for ensuring information integrity and non-repudiation.	**Managed Encryption Services** We offer managed full disk encryption solutions that will install encryption and monitor your systems, giving you peace of mind that a trusted vendor partner has the ability to remotely lock, reset or "kill" the device in the event of loss or theft.
Section 7 - Protect - Employees Devices Establish, implement, and actively manage the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process to prevent attackers from exploiting vulnerable services and settings.	**Managed Endpoint Services** All the managed devices connected to your network are deployed with an award-winning agent that orchestrates the monitoring and management of policy-based hardening & security auto-configuration, offering comprehensive coverage against a vast spectrum of threats.
Section 8 - Protect- Controls and Staff Training Firms should provide cybersecurity training to determine where the skill gaps and points of risk exposure exist, and develop and deliver training in those areas.	**Deep, Wide, & Up to Date Training as a Vital Security Component** To protect the confidentiality, integrity, and availability of your systems, we've designed comprehensive on-line training programs for your employees as well as external vendors. We counter cyber-specific and cyber-enabled threat vectors every day and that field experience informs our training & security protocols.
Section 9 - Detect - Penetration Testing Penetration testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network.	**Penetration Testing Services** RSI can simulate real-world attacks to assess our client's external applications, network, and mobile applications vulnerabilities in addition to running independent, automated security scans encompassing the Open Web Application Security Project (OWASP) Top 10 vulnerabilities. Our network level penetration test reveals system vulnerabilities that can be easily exploited by real world attackers.
Section 10 - Detect - Intrusion Organizations should deploy Intrusion Detection and Prevention Systems (IDPS) to identify possible incidents, log information about them, attempt to stop them, and report them to security administrators.	**Right Sized Intrusion Detection & Prevention Solutions** We work closely with clients to understand the risk and implement an optimal Intrusion Detection & Prevention System for their needs for all business sizes ranging from cost effective software-based IDS to enterprise-grade appliances.
Section 11 - Response Plan Firms should establish policies and procedures, as well as roles and responsibilities for escalating and responding to Cybersecurity incidents to limit damage, assure external stakeholders, and reduce recovery time and costs.	**Managed Incident Response** Rely on our emergency response team to provide on-site and remote investigation of incidents, forensic analysis mitigating the impact of attacks and restoring business.
Section 12 - Recovery Organizations should have policies in place to Contain & Eradicate Cyber threats and be able to deploy a rapid Recovery plan in the event of a breach.	**Thorough Containment & Rapid Disaster Recovery Services** We respond to Cybersecurity incidents with a complete suite of Data Forensics and Incident Response (DFIR) services, quickly containing a breach, limiting exposure, stemming losses and preserving evidence while executing on business continuity and disaster recovery plan.