

Independent  
Community Bankers  
of Minnesota®

Partner

### Vulnerability Scanning

*“Internet perimeter scanning is not only prudent thing for all banks to do, it’s required. Assurity River’s Partner Alliance is a unique and cost effective solution for ICBM banks.”*

Doug Krukowki, COO, Independent Community Bankers of Minnesota

### Exclusive Offer

**ICBM Partner Price starting at only \$995 per year.**

## Information Security Partner Alliance

Vulnerability scanning helps secure your network and information by proactively identifying weaknesses in your security posture before hackers can exploit them.

The internet is your organization’s digital gateway to the world — and the world’s gateway to your network. Just like ensuring your doors and windows are locked, it is essential to ensure that the locks on the doors to your network are checked on a routine basis and whenever there are configuration changes, to ensure your perimeter is constantly safeguarded.

### Information Security Partner Alliance

Assurity River Group offers a comprehensive and cost-effective solution for Independent Community Bank (ICBM) members to detect security flaws in their internet perimeter. The Partner Alliance solution includes two main components: External Perimeter Scanning and Expert Analysis.

### External Perimeter Scanning




External Perimeter Scanning, sometimes referred to as “penetration testing”, is a key component to any security program. Assurity River will ensure that your perimeter is scanned on a routine basis and upon request.

- Monthly scans that tests for more than 5,000 vulnerabilities
- On-demand scans to validate configuration changes
- Findings and recommendations report
- Access to reports and history via a web portal

### Expert Analysis

Assurity River’s team of information security experts will interpret your reports and provide the advice you need to improve your bank’s security posture.

- Annual review and interpretation of reports
- Recommendations for improvement
- Security advisory services on-demand

# - 3	Severity	Protocol/Port	Vulnerability	Remediation Action
1.		udp /161	<p><b>Guessable SNMP Community String</b></p> <p>SNMP is a protocol used for remote monitoring and configuration of network devices and servers. The community string (essentially, the password) for your SNMP service was easily guessed. Although only the “read” (monitoring) string was tested, this probably means that the “write” (configuration) string is also guessable. An attacker who knows the community strings for this device will be able to monitor or reconfigure the device, potentially leading to a serious denial of service to your system or network.</p> <p><b>Evidence:</b> Community String = public</p> <p><b>CVE:</b> <a href="#">CVE-1999-0508</a></p> <p><b>CVSSv2:</b> AV:L/AC:L/Au:N/C:P/PA:P (Base Score: 4.60)</p>	At a minimum, you should change your read and write community strings to something that is hard to guess. If SNMP is not required, you should disable it. Also, SNMP (UDP/161) should not be generally accessible from the Internet.
2.		tcp /22	<p><b>OpenSSH AFS Overflow</b></p> <p>OpenSSH versions prior to 3.2.1 contain a buffer overflow if Kerberos AFS is enabled. This buffer overflow can lead to denial of service or arbitrary code execution.</p> <p><b>Service:</b> SSH-1.99-OpenSSH_3.1p1</p> <p><b>CVE:</b> <a href="#">CVE-2002-0575</a></p> <p><b>Bugtraq:</b> <a href="#">4560</a></p>	Upgrade to the latest version of OpenSSH
3.		udp /111	<p><b>Unix RPC Accessible</b></p> <p>The Unix Remote Procedure Call portmapper is accessible. This service is required for some applications, such as NFS, but is often enabled by default and is a common source of security bugs.</p> <p><b>Service:</b> RPC Portmapper vers 2 - status, nlockmgr</p>	If you do not need RPC services, turn this off.

**Vulnerabilities by Device.** Scan shows the vulnerabilities found in the system, including name, level of severity, affected service, description, and recommended remediation.

# **Assurity River Group**

*We are a leading business continuity and information security firm that helps protect your most valuable asset — your clients' trust.*

Assurity River provides business continuity and information security assessments, planning and program management to keep clients' business assets and operations secure, available and recoverable. Founded in 2003, the firm helps clients manage IT and operational risk by developing sound security and business continuity strategies and ensuring programs stay current with business and regulatory changes.

## **Information Security**

- Risk Assessment
- Penetration Testing
- Vulnerability Analysis
- Incident Response
- Forensic Analysis
- Social Engineering
- Policy Development
- IT Audit

## **Business Continuity**

- Business Impact Analysis
- Recoverability Assessment
- DR Strategic Planning
- BC Plan Development
- BC Program Assessment
- DR Testing
- Tabletop Exercises
- Plan Administration



[www.assurityriver.com](http://www.assurityriver.com)

Assurity River Group, Inc.  
4500 Park Glen Road  
Suite 120  
Minneapolis, MN 55416  
Main 952.230.6480  
Toll Free 877.753.4202  
[sales@assurityriver.com](mailto:sales@assurityriver.com)