

# Cybersecurity for Main Street America



## 3 Step Cybersecurity Plan

Presented by



### Point of Contact

Raymond Gonzalez

(202) 792-8757

[raymond.gonzalez@j2rvets.com](mailto:raymond.gonzalez@j2rvets.com)

Washington, DC

## Overview

### Cybersecurity by a Veteran Owned Business

“Government Contractors must implement cybersecurity standards described in NIST Special Publication 800-171, full compliance is required.” - Multiple Agencies

J2R VETS provides Cybersecurity for Government, Commercial and our Residential clients. Cybersecurity is a necessary and expensive practice that is tedious and time consuming. Our teams can service all of your cybersecurity needs including CMMC, SOC, MSSP, Forensic Audits, Regulatory Risk Assessments and more.

Our services meet the highest standards including the required reporting needed for contract compliance. The following outlines a three step process to protect your networks from online threats and gain peace of mind.

### *3 Step Cybersecurity Plan*

#### **1. Vulnerability Scanning**

Def. Vulnerability scanning is an inspection of the potential points of exploitation on a network to identify security holes. A vulnerability scan detects and classifies system weaknesses in computers, networks and communications equipment and predicts the effectiveness of countermeasures. Vulnerability scanning your computer network is a vital part of your obligatory organizational security and IT risk management approach for several reasons:

- Vulnerability scanning lets you take a proactive approach to close any gaps and maintain strong security for your systems, data, employees, and customers. Data breaches are often the result of unpatched vulnerabilities. Identifying and eliminating security gaps lowers your risk
- Cybersecurity compliance and regulations demand secure systems. NIST, PCI DSS, CMMC, and HIPAA all emphasize vulnerability scanning to protect sensitive data
- Cyber criminals have access to vulnerability scanning tools. It is vital to carry out scans and take restorative actions before hackers can exploit any security vulnerabilities

## 2. Penetration Testing

Def. Penetration testing is a type of security testing used to uncover vulnerabilities, threats and risks that an attacker could exploit in networks, software or web applications. Common vulnerabilities include network design errors, configuration errors and software bugs.

Our Penetration Testing service tests your network often so you can stay compliant and prove diligence in securing your online presence.

- Detect and safely exploit vulnerabilities
- Identify paths attackers can use to breach your network
- Quantify the risk to your systems
- Manage your network resources more efficiently to better defend data and equipment
- Continually combat the existence of critical vulnerabilities throughout your network
- Use the most up-to-date cyber security library of multi-platform exploits to defend your network

## 3. Social Engineering Testing

Def. Social engineering is the art of exploiting human psychology and the manipulation of people, rather than technical hacking techniques, to gain access to buildings, computer systems, devices and your data.

Bad actors are brazenly targeting organizations through highly complex official looking and sounding communications.

Organized hackers invest in significant amounts of research to target specific people and many of their targets are falling prey to these false requests.

- Our Social Engineering services tests your employees to see if they take our network compromising bait
- We identify who in your organization needs basic Social Engineering security training

# Pricing and Options

## Cybersecurity Package Includes:




1. Up to 20 internal and/or external IP’s and targets per client location
2. Lightweight agent can be installed on all internal targets
3. Weekly internal **Vulnerability Scanning** reports (full or compliance scan)
4. Monthly external **Penetration Test** reports (full or compliance scan)
5. Monthly **Social Engineering** reports

**Pricing: \$Call per month per location**

### Value Pricing:

- No setup and consult fees with pre-paid three month trial (\$1200 savings)
- Discounted pre-paid three month trial
- Cancel at any time with 30 days notice after first three months of service

## Additional Options

<p><b>PCI ASV Certified Scanning</b></p> <ul style="list-style-type: none"> <li>○ Managed PCI ASV Scanning on the schedule of your choosing.</li> <li>○ Quarterly Attestation of Compliance Reports are delivered.</li> <li>○ Up to 5 re-scans per month are included.</li> </ul>	<p><b>Internal Scanning Appliance</b></p> <ul style="list-style-type: none"> <li>○ Required for scanning internal networks</li> <li>○ Devices for internal scanning will require on-site hands/eyes support for cabling and setup.</li> <li>○ Provide support and guidance to designated on-site personnel.</li> </ul>
<p><b>Additional IP Targets Per Site</b></p> <ul style="list-style-type: none"> <li>○ Add additional targets if your sites have more than 20 targets to scan.</li> <li>○ Headquarters locations with a large footprint may qualify for additional discounting</li> </ul>	<p><b>Additional Compliance Scan Reports Available</b></p> <p>NERC CIP - OWASP - HIPAA - SOX CMMC - FISMA - FINRA - PCI (non-ASV)</p> <div style="display: flex; justify-content: space-around; align-items: center;">    </div>