

# Example of a Detailed Risk Assessment Report

## *Executive Summary*

During the period of Month, Date, Year to Month, Date, Year a detailed information security risk assessment was performed on the Department XXX (code name MVROS).

The MVROS provides the ability for State vehicle owners to renew motor vehicle registration, pay renewal fees, and enter change of address information.

The assessment identified several medium risk items that should be addressed by the management team.

# DETAILED ASSESSMENT

## 1. Introduction

### 1.1 Purpose

The purpose of the risk assessment was to identify threats and vulnerabilities related to the Department of Motor Vehicles – Motor Vehicle Registration Online System (“MVROS”). The risk assessment will be utilized to identify risk mitigation plans related to MVROS. The MVROS was identified as a potential high-risk system in the Department’s annual enterprise risk assessment.

### 1.2 Scope of this risk assessment

The MVROS system comprises several components. The external (customer) interface is a series of web pages that allow the user to input data and receive information from the application. The online application is a web-based application developed and maintained by the DMV. The application is built using Microsoft’s Internet Information Server and uses Active Server Pages. The application has an interface with the motor vehicle registration database and with Paylink – an e-commerce payment engine provided by a third party vendor. DMV IT department hosts the application. The application components are physically housed in the DMV’s data center in Anytown.

The scope of this assessment includes all the components described above except for Paylink. The Paylink interface – the component managed by DMV IT – is in scope. Also in scope are the supporting systems, which include: DMZ network segment and DMZ firewalls. The web application, DMV database and operating systems supporting these components are all in scope.

## 2. Risk Assessment Approach

### 2.1 Participants

| Role                   | Participate                             |
|------------------------|---|
| System Owner           | John Smith                              |
| Security Administrator | Tom Sample                              |
| Risk Assessment Team   | Eric Johns, Susan Evans, Terry Wu       |
| Advisors               | Jason Belford, Ryan Wright, Bryan Lewis |

### 2.2 Techniques Used

| Technique                     | Description   |
|-------------------------------|---|
| Risk assessment questionnaire | The assessment team used NIST 800-30 to guide their assessment.   |
| Assessment Tools              | <p>The assessment team used several security testing tools to review system configurations and identify vulnerabilities in the application.</p> <p>The tools included nmap, nessus, AppScan</p> <p>(Not Necessary for the project)</p>  |
| Vulnerability sources         | <p>The team accessed several vulnerability sources to help identify potential threat sources. The sources consulted included:</p> <ul style="list-style-type: none"><li>• CIS Controls: <a href="https://www.cisecurity.org/controls/">https://www.cisecurity.org/controls/</a></li><li>• OWASP Top Ten: <a href="https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project">https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project</a></li><li>• NIST Vulnerability Database: <a href="https://nvd.nist.gov/">https://nvd.nist.gov/</a></li><li>• Others?</li></ul> |

| Technique               | Description   |
|-------------------------|---|
| Transaction walkthrough | The assessment team selected at least one transaction (use case) of each type and walked each transaction through the application process to gain an understanding of the data flow and control points. |
| Review of documentation | The assessment team reviewed DMV security policies, system documentation, network diagrams and operational manuals related the MVROS.   |
| Interviews              | Interviews were conducted to validate information.  |
| Site visit              | The team conducted a site visit at the Data Center and reviewed physical access and environmental controls  |

## 2.3 Risk Model

In determining risks associated with the MVROS, we utilized the following model for classifying risk:

$$\text{Risk} = \text{Threat Likelihood} \times \text{Magnitude of Impact}$$

And the following definitions:

### Threat Likelihood

| Likelihood (Weight Factor) | Definition   |
|----------------------------|--|
| High (1.0)                 | The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective                   |
| Medium (0.5)               | The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.                                  |
| Low (0.1)                  | The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised. |

*This is sample data for demonstration and discussion purposes only*

## Magnitude of Impact

| Impact (Score) | Definition   |
|----------------|--|
| High (100)     | <p>The loss of confidentiality, integrity, or availability could be expected to have a <i>severe or catastrophic</i> adverse effect on organizational operations, organizational assets, or individuals.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• A severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions</li> <li>• Major damage to organizational assets</li> <li>• Major financial loss</li> <li>• Severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.</li> </ul>                    |
| Medium (50)    | <p>The loss of confidentiality, integrity, or availability could be expected to have a <i>serious</i> adverse effect on organizational operations, organizational assets, or individuals.</p> <ul style="list-style-type: none"> <li>• Significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced</li> <li>• Significant damage to organizational assets</li> <li>• Significant financial loss</li> <li>• Significant harm to individuals that does not involve loss of life or serious life threatening injuries.</li> </ul> |
| Low (10)       | <p>The loss of confidentiality, integrity, or availability could be expected to have a <i>limited</i> adverse effect on organizational operations, organizational assets, or individuals.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced</li> <li>• Minor damage to organizational assets</li> <li>• Minor financial loss</li> <li>• Minor harm to individuals.</li> </ul>   |

*This is sample data for demonstration and discussion purposes only*

Risk was calculated as follows:

| Threat Likelihood | Impact                      |                                |                                 |
|-------------------|-----------------------------|--------------------------------|---------------------------------|
|                   | Low<br>(10)                 | Medium<br>(50)                 | High<br>(100)                   |
| High (1.0)        | Low Risk<br>(10 x 1.0 = 10) | Medium Risk<br>(50 x 1.0 = 50) | High Risk<br>(100 x 1.0 = 100)  |
| Medium (0.5)      | Low Risk<br>(10 x 0.5 = 5)  | Medium Risk<br>(50 x 0.5 = 25) | Medium Risk<br>(100 x 0.5 = 50) |
| Low (0.1)         | Low Risk<br>(10 x 0.1 = 1)  | Low Risk<br>(50 x 0.1 = 5)     | Low Risk<br>(100 x 0.1 = 10)    |

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)

### 3. System Characterization

#### 3.1 Technology components

| Component         | Description   |
|-------------------|---|
| Applications      | In-house developed uses Microsoft Active Server Pages running under Microsoft Internet Information Server 4.0 |
| Databases         | Microsoft SQL Server 2000   |
| Operating Systems | Microsoft Windows NT version 4.0 SP 2   |
| Networks          | Checkpoint Firewall<br>Cisco Routers  |
| Interconnections  | Interface to PayLink  |
| Protocols         | SSL used for transmission between client web browser and web server   |

#### 3.2 Physical Location(s)

| Location    | Description                   |
|-------------|-------------------------------|
| Data Center | 260 Somewhere Street, Anytown |
| Help Desk   | 5500 Senate Road, Anytown     |
| NOC         | 1600 Richmond Avenue, Anytown |

*This is sample data for demonstration and discussion purposes only*

### 3.3 Data Used By System

| Data                                | Description   |
|-------------------------------------|---|
| Personally identifiable information | Includes: <ul style="list-style-type: none"><li>• Name</li><li>• Address (current and previous)</li><li>• Phone Number</li><li>• SSN #</li><li>• DOB</li></ul>  |
| Vehicle information                 | Includes <ul style="list-style-type: none"><li>• Vehicle identification number</li><li>• Tag #</li><li>• Date of last emissions test</li></ul>  |
| Financial information               | <ul style="list-style-type: none"><li>• Credit card #</li><li>• Verification code</li><li>• Expiry date</li><li>• Card type</li><li>• Authorization reference</li><li>• Transaction reference</li></ul> |
| Tax                                 | Registration fee  |

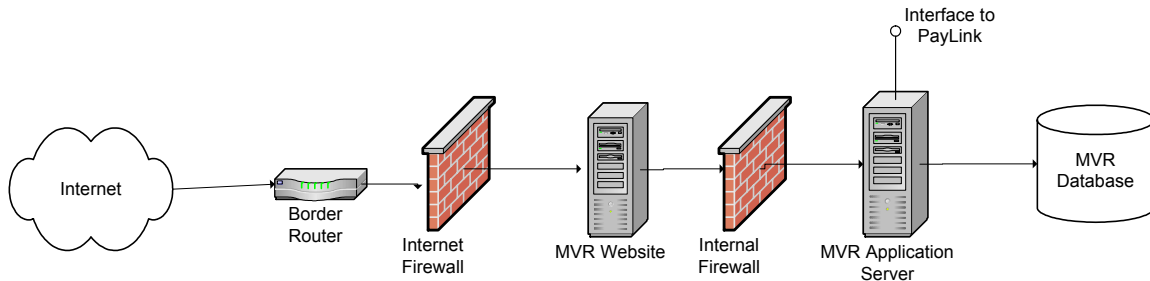
### 3.4 Users

| Users                | Description   |
|----------------------|---|
| State Vehicle Owners | Access the system via a web browser. Can renew vehicle registration provided they have a valid credit card. Can also enter change of address information. |
| DMV IT Personnel     | Manage the MVROS system including firewalls and networks. Maintain security configuration of system.  |
| DMV Operations       | Utilize information contained in the MVR database for management reporting. Generate reports and database queries.  |
| DMV Offices          | Utilize the MVR application for in-person renewals.   |

*This is sample data for demonstration and discussion purposes only*

### 3.5 Flow Diagram

The following diagram shows the in-scope technology components reviewed as part of the MVROS.



## 4. Vulnerability Statement

The following potential vulnerabilities were identified:

| Vulnerability        | Description   |
|----------------------|---|
| Cross-site scripting | The web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine, or spoof content to fool the user. |
| SQL injection        | Information from web requests is not validated before being used by a web application. Attackers can use these flaws to attack backend components through a web application.  |
| Password strength    | Passwords used by the web application are inappropriately formulated. Attackers could guess the password of a user to gain access to the system.  |
| Unnecessary services | The web server and application server have unnecessary services running such as telnet, snmp and anonymous ftp  |



| Vulnerability         | Description   |
|-----------------------|---|
| Disaster recovery     | There are no procedures to ensure the ongoing operation of the system in event of a significant business interruption or disaster |
| Lack of documentation | System specifications, design and operating processes are not documented.   |
| Integrity checks      | The system does not perform sufficient integrity checks on data input into the system.  |

## 5. Threat Statement

The team identified the following potential threat-sources and associated threat actions applicable to the MVROS:

| Threat-Source  | Threat Actions   |
|--|--|
| Hacker   | <ul style="list-style-type: none"> <li>• Web defacement</li> <li>• Social engineering</li> <li>• System intrusion, break-ins</li> <li>• Unauthorized system access</li> </ul>                            |
| Computer criminal  | <ul style="list-style-type: none"> <li>• Identity theft</li> <li>• Spoofing</li> <li>• System intrusion</li> </ul>   |
| Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees) | <ul style="list-style-type: none"> <li>• Browsing of personally identifiable information</li> <li>• Malicious code (e.g., virus)</li> <li>• System bugs</li> <li>• Unauthorized system access</li> </ul> |
| Environment  | <ul style="list-style-type: none"> <li>• Natural disaster</li> </ul>   |

*This is sample data for demonstration and discussion purposes only*

## 5. Risk Assessment Results

*{Note: Only partial list included in this example}*

| Item Number | Observation   | Threat-Source/<br>Vulnerability     | Existing controls   | Likelihood | Impact | Risk Rating | Recommended controls  |
|-------------|---|-------------------------------------|---|------------|--------|-------------|---|
| 1           | User system passwords can be guessed or cracked   | Hackers/ Password effectiveness     | Passwords must be alpha-numeric and at least 5 characters | Medium     | Medium | Medium      | Require use of special characters   |
| 2           | Cross site scripting  | Hackers/ Cross-site scripting       | None  | Medium     | Medium | Medium      | Validation of all headers, cookies, query strings, form fields, and hidden fields (i.e., all parameters) against a rigorous specification of what should be allowed   |
| 3           | Data could be inappropriately extracted/modified from DMV database by entering SQL commands into input fields | Hackers + Criminals / SQL Injection | Limited validation checks on inputs                       | High       | Medium | Medium      | Ensure that all parameters are validated before they are used. A centralized component or library is likely to be the most effective, as the code performing the checking should all be in one place. Each parameter should be checked against a strict format that specifies exactly what input will be allowed. |
| 4           | Web server and application server running unnecessary services  | All / Unnecessary Services          | None  | Medium     | Medium | Medium      | Reconfigure systems to remove unnecessary services  |

*This is sample data for demonstration and discussion purposes only*

| Item Number | Observation                                     | Threat-Source/<br>Vulnerability | Existing controls  | Likelihood | Impact | Risk Rating | Recommended controls                      |
|-------------|---|---------------------------------|--------------------|------------|--------|-------------|---|
| 5           | Disaster recovery plan has not been established | Environment / Disaster Recovery | Weekly backup only | Medium     | High   | Medium      | Develop and test a disaster recovery plan |

*This is sample data for demonstration and discussion purposes only*