Webinar on Cybersecurity and Data Protection in Cross-border Paperless Trade

INFORMATION SECURITY
Cybersecurity and Data Protection in Single Window Systems
“Security used to be an inconvenience sometimes, but now it's a necessity all the time.”

- Martina Navratilova
Organizations face threats like Ransomware, Phishing, and Data breaches.

The European Union Agency for Cybersecurity (ENISA) Threat Landscape Report provides the fifteen top threats which PSW has included in its inventory of Cyber Threats.
WHY DATA PROTECTION IS CRUCIAL IN SINGLE WINDOW SYSTEMS

✓ **Sensitive Information Handling:**

✓ **Business Integrity and Trust:**

✓ **Operational Continuity:**

✓ **Prevention of Fraud and Cybercrime:**

✓ **Data Accuracy and Reliability:**

✓ **Supporting Digital Transformation:**
“One single vulnerability is all an attacker needs.”

Window Snyder, Chief Security Officer, Fastly
1. What PSW Does
   ❖ Centralized data exchange platform for trade facilitation.
   ❖ Streamlines trade processes and enhances efficiency for stakeholders.

2. Benefits of PSW
   ❖ Simplifies trade procedures.
   ❖ Reduces transaction costs and time.
   ❖ Enhances transparency and accountability.

3. How Do We Work
   ❖ Collaborative approach with government agencies, traders, and businesses.
   ❖ Integration of technology for seamless transactions and data exchange.

4. Data Protection
   ❖ Cybersecurity measures to safeguard sensitive trade data.
   ❖ Continuous monitoring and updates to mitigate cyber threats. (Threat Intel, Contingency, Business continuity, resilience etc.)
HOW PSW HAS ORGANIZED ITS DATA PROTECTION FUNCTIONS?

**Governance, Risk, and Compliance**
- IS Documentation (Framework, Policies, Baselines, Standards, Procedure and Guidelines)
- ISO 27001 Adoption
- Audit Compliance
- IS Awareness and Training for employee readiness
- Risk Assessments
- Information Classification
- IS Program Management

**Application Security**
- SSDLC (Secure Software Development Life Cycle)
- IS Reviews
- Checklists
- Secure Code Reviews
- SAST/DAST Assessments

**Network and Infra Security**
- CIS Benchmarking/Hardenings
- VAPTs
- Configuration Reviews
- Gap Assessments

**Security Operations Center**
- SIEM Deployment and Maturity
- Detection and Response
- Investigation and Response/Alerts
- Thread Intelligence Sharing and Collaboration
### Case Study 1: Handling a Malware Attack

**Incident:** Early signs of malware activity were detected.

**Response:**
- Activated the incident response.
- Isolated the affected systems to prevent further spread.

**Lessons Learned:**
- Emphasized the importance of timely backups.
- Highlighted the necessity of conducting regular incident response drills.

### Case Study 2: Phishing Attempt Mitigation

**Prevention:**
- Conducted comprehensive phishing awareness training for all employees.

**Outcome:**
- Achieved a significant reduction in successful phishing attempts.
- Users are now reporting suspicious emails before clicking any links, enhancing overall security awareness.
<table>
<thead>
<tr>
<th>S NO</th>
<th>CONTROL TYPE</th>
<th>CONTROL</th>
<th>STATUS</th>
<th>S NO</th>
<th>CONTROL TYPE</th>
<th>CONTROL</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IDENTIFY</td>
<td>User Training</td>
<td>Implemented</td>
<td>18</td>
<td>PROTECT</td>
<td>Disable or Remove Feature or Program</td>
<td>Implemented</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>Risk Assessments</td>
<td>Implemented/ Ongoing</td>
<td>19</td>
<td></td>
<td>Restrict File and Directory Permissions</td>
<td>Implemented</td>
</tr>
<tr>
<td>3</td>
<td>PROTECT</td>
<td>USB Blocking</td>
<td>Partially Implemented</td>
<td>20</td>
<td></td>
<td>FIM Protection</td>
<td>Planned</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>Application Isolation</td>
<td>Partially Implemented</td>
<td>21</td>
<td></td>
<td>Multi-factor Authentication</td>
<td>Partially Implemented</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>Network Segmentation</td>
<td>Implemented</td>
<td>22</td>
<td></td>
<td>Encrypt Sensitive Information</td>
<td>Partially Implemented</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>Privileged Account Management</td>
<td>Planned</td>
<td>23</td>
<td></td>
<td>Behavior Prevention on Endpoint</td>
<td>Planned</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>Update Software</td>
<td>Implemented</td>
<td>24</td>
<td></td>
<td>DLP</td>
<td>Planned</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>WAF Protection</td>
<td>Implemented</td>
<td>25</td>
<td></td>
<td>Email Security</td>
<td>Partially Implemented</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>Antivirus/Antimalware</td>
<td>Implemented</td>
<td>26</td>
<td></td>
<td>Vulnerability Scanning</td>
<td>Implemented</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>Network Intrusion Prevention</td>
<td>Implemented</td>
<td>27</td>
<td></td>
<td>Security Monitoring through SOC</td>
<td>Implemented</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>Restrict Web-Based Content</td>
<td>Implemented</td>
<td>28</td>
<td></td>
<td>SIEM</td>
<td>Implemented</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>Password Policies</td>
<td>Implemented</td>
<td>29</td>
<td></td>
<td>Threat Intelligence Program</td>
<td>Partially Implemented</td>
</tr>
<tr>
<td>13</td>
<td></td>
<td>Restrict Registry Permissions</td>
<td>Implemented</td>
<td>30</td>
<td></td>
<td>IS Incident Response Plan</td>
<td>Partially Implemented</td>
</tr>
<tr>
<td>14</td>
<td></td>
<td>Whitelisting of application</td>
<td>Partially Implemented</td>
<td>31</td>
<td></td>
<td>Tabletop Exercises</td>
<td>Planned</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td>EDR</td>
<td>Planned</td>
<td>32</td>
<td></td>
<td>SOAR</td>
<td>Planned</td>
</tr>
<tr>
<td>16</td>
<td></td>
<td>DDoS and Sandboxing</td>
<td>Implemented</td>
<td>33</td>
<td></td>
<td>XDR</td>
<td>Planned</td>
</tr>
<tr>
<td>17</td>
<td></td>
<td>Patch Management</td>
<td>Implemented</td>
<td>34</td>
<td></td>
<td>Air-gapped Data Backup and Yearly Drills</td>
<td>Partially Implemented</td>
</tr>
</tbody>
</table>
MAJOR ENHANCEMENTS

Major Project: Network Security Enhancements

- **Details:** Upgraded firewalls and implemented network segmentation.
- **Impact:** Reduced risk of lateral movement within the network.

Major Project: Implementation of SIEM

- **Objectives:** Centralized logging and monitoring.
- **Process:** Deployed SIEM, integrated with existing systems.
- **Outcomes:** Improved threat detection and response times.
FUTURE ROADMAP

Upcoming Projects

- Privilege Access Management (PAM)
- Data Loss Prevention (DLP)
- Advanced Threat Detection
- Zero Trust Architecture
- EDR/XDR (Extended Detection and Response)
- Phishing Simulation & Cyber Security Awareness Solution

Long-term Goals

- Continuous improvement and adaptation to new threats
- Improve Threat Detection and Response Capabilities
- Strengthen Data Protection and Privacy
- Foster a culture of cybersecurity awareness
- Continuously update and refine security strategies
- Enhance Cybersecurity Resilience
“It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it.”

- Stephane Nappo
TECHNOLOGIES TO IMPLEMENT ZERO TRUST

- Network Segmentation
- Next-Generation Firewalls
- Multi-Factor Authentication
- Identity and Access Management
- Secure Web Gateways
- Endpoint Protection Platforms
- Encryption
- Data Loss Prevention
- Zero Trust Network Access