

# NIST CYBERSECURITY FRAMEWORK ASSESSMENT

Tuberous Sclerosis Alliance

December 18, 2020

# Table of Contents



Executive summary

3



Detailed findings and recommendations

8



Cyber Threat Intelligence

20



Future state roadmap

33



Appendix

36



# EXECUTIVE SUMMARY

# Assessment Overview

## Overview

As the leading Tuberous Sclerosis Complex (TSC) advocacy and research funding entity in the United States and beyond, the Tuberous Sclerosis Alliance (TS Alliance) engaged RSM US LLP (RSM) to assess the organization’s current state information security program maturity.

Within this document are the results of our assessment, along with recommendations to reduce overall risk from the findings we identified.

## Methodology

Our assessment was executed along three key components of analysis:

- **Interviews:** we walked through critical IT controls with personnel at the TS Alliance to gain an understanding of current security practices.
- **Analysis:** received and analyzed relevant documentation on processes.
- **Reporting:** providing you a detailed report on observations and actionable recommendations.

## Summary of Results

The TS Alliance has attained the **partial** tier based on the National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF) which considers security, risk and compliance. As a result of this assessment, we identified several opportunities for improvement.

Detailed findings and recommendations can be found starting on pg. 8. Additional information on our analysis can be found in the Appendix on pg. 36

### Analysis Inputs

For this cybersecurity assessment, RSM reviewed and assessed more than...

**15+** documents

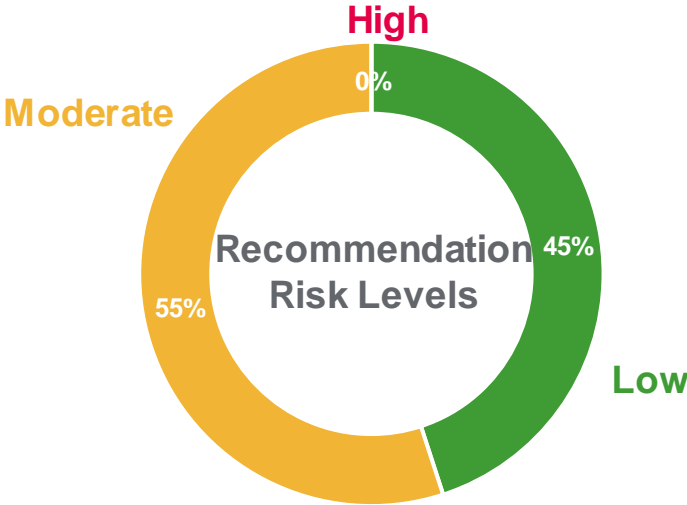
This included TS Alliance policies and procedures, network diagrams, and other documentation.

### Recommendations

As a result of the cybersecurity assessment, RSM noted...

**20** recommendations

When adopted across the network environment, this should address the identified NIST CSF control gaps.



| Risk Level | # of Risks |
|------------|------------|
| High       | 0          |
| Moderate   | 11         |
| Low        | 9          |

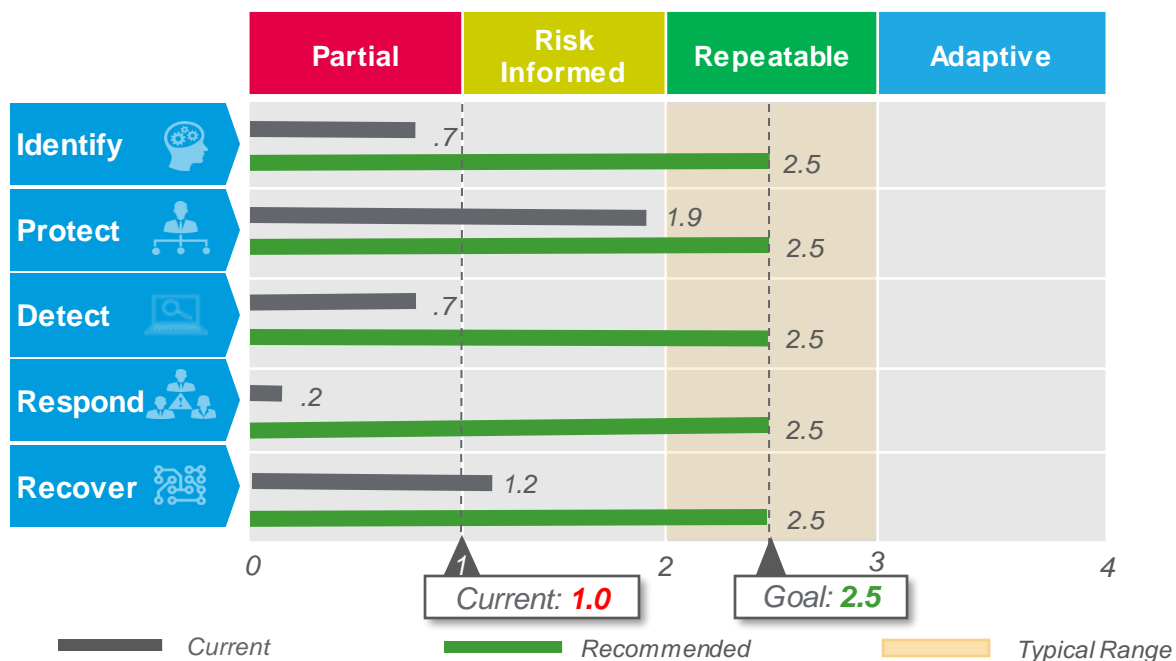


# Assessment Overview

## Summary Evaluation

Based on the methodology (noted to the right), TS Alliance has attained the level **partial** with an average tier score of **1.0** when evaluated against the NIST CSF's implementation tiers.

As a result, TS Alliance has opportunities for improvement within its cybersecurity program. We have noted several high-level weaknesses were identified during the assessment. Full detailed observations can be found in the detailed section on page 7.



**Note:** It is not appropriate or cost effective for most companies to achieve the highest levels of maturity

## Methodology Framework

Our assessment was conducted in alignment with the NIST CSF. The NIST CSF provides a common language for understanding, managing and expressing cybersecurity risk to critical stakeholders. It can be leveraged to help identify the organizations current cybersecurity posture and prioritize actions for areas of improvement to reduce cybersecurity risk. The NIST CSF is broken down into 5 core areas that were the focus of our assessment.

|   |  |
|---|--|
| <b>Identify</b><br>  | <p><b>Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities. Includes:</b><br/>                     Asset Management (ID.AM), Business Environment (ID.BE), Governance (ID.GV) Risk Assessment (ID.RA), Risk Management Strategy (ID.RM)</p>   |
| <b>Protect</b><br>   | <p><b>Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. Includes:</b><br/>                     Access Control (PR.AC), Awareness and Training (PR.AT), Data Security (PR.DS), Information Protection Processes and Procedures (PR.IP), Maintenance (PR.MA), Protective Technology (PR.PT)</p> |
| <b>Detect</b><br>    | <p><b>Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. Includes:</b><br/>                     Anomalies and Events (DE.AE), Security Continuous Monitoring (DE.CM) Detection Processes (DE.DP)</p>  |
| <b>Respond</b><br> | <p><b>Develop and implement the appropriate activities to act regarding a detected cybersecurity event. Includes:</b><br/>                     Response Planning (RS.RP), Communications (RS.CO), Analysis (RS.AN), Mitigation (RS.MI), Improvements (RS.IM)</p>   |
| <b>Recover</b><br> | <p><b>Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. Includes:</b><br/>                     Recovery Planning (RC.RP), Improvements (RC.IM), Communications (RC.CO)</p>  |

# SWOT Analysis

Based on the interviews and documentation, RSM team has produced a SWOT analysis to develop an understanding of the key issues and summarize TS Alliance's cybersecurity posture.



## Strengths

- Protection capabilities through with an outsourced Managed Service Provider
- Backups deployed for critical systems
- Secure protocols for Remote Access



## Weaknesses

- Foundational access controls, phishing, training and communications processes are not well defined
- Incident response plan
- Vulnerability management activities
- Vendor risk management



## Opportunities

- User access review enhancements
- Governance strategy development
- Data privacy assessment/program
- Cyber incident identification and management
- Asset management practices



## Threats

- Social engineering and phishing
- Unsecured peripherals and removable devices
- Lost or stolen devices
- Insider threat (malicious or accidental)
- Internet access to business systems

# Cybersecurity Assessment – Summary Overview by NIST Domains

| Overall: 1.0                                    | Sub-Categories Maturity Ratings  | Category Summary  |
|---|--|---|
| <b>Identify</b><br>● 0.7<br><i>Partial</i>      | <ul style="list-style-type: none"> <li>● Asset management</li> <li>● Business environment</li> <li>● Governance</li> <li>● Risk assessment</li> <li>● Risk management strategy</li> <li>● Supply chain risk management</li> </ul>                | <p><b>Overview:</b> IT understands the business and their general requirements, however, information security lacks structure and there is limited documentation to drive consistent execution of security activities.</p> <p><b>Strengths:</b> An IT managed services provider has been contracted to assist in IT asset management, including configuring and maintaining endpoints.</p> <p><b>Challenges:</b> A risk management program is not in place. Ad-hoc processes are not aligned to any defined regulatory or compliance-based policies. TS Alliance does not have a formal Information Security strategy or policy.</p>  |
| <b>Protect</b><br>● 1.9<br><i>Risk Informed</i> | <ul style="list-style-type: none"> <li>● Access control</li> <li>● Awareness and training</li> <li>● Data security</li> <li>● Information protection processes and procedures</li> <li>● Maintenance</li> <li>● Protective technology</li> </ul> | <p><b>Overview:</b> This is TS Alliance's strongest domain. There are strong environment protections, but weak user training threatens to undermine organizational security.</p> <p><b>Strengths:</b> Access control process in place. Maintenance processes managed by Optimal Networks and in-place.</p> <p><b>Challenges:</b> Information protection strategy should be created and reviewed. End user cybersecurity training should be implemented.</p>   |
| <b>Detect</b><br>● 0.7<br><i>Partial</i>        | <ul style="list-style-type: none"> <li>● Anomalies and events</li> <li>● Detection processes</li> <li>● Security continuous monitoring</li> </ul>  | <p><b>Overview:</b> Despite a network firewall, there are very few logging or monitoring processes in place.</p> <p><b>Strengths:</b> A network firewall is configured and in place, so detection and monitoring capabilities are ready to be implemented.</p> <p><b>Challenges:</b> Developing and implementing stronger controls for removable media and information at rest and implementing firewall monitoring.</p>  |
| <b>Respond</b><br>● 0.2<br><i>Partial</i>       | <ul style="list-style-type: none"> <li>● Analysis</li> <li>● Communications</li> <li>● Improvements</li> <li>● Mitigation</li> <li>● Response planning</li> </ul>  | <p><b>Overview:</b> This is TS Alliance's weakest domain. Logging management and monitoring strategy needs to be recorded and reviewed; mitigations for other monitoring controls are not yet in place.</p> <p><b>Strengths:</b> External managed service providers can monitor security event logging processes on TS Alliance's behalf.</p> <p><b>Challenges:</b> Monitoring system logs and building out formal network intrusion detection procedures and controls.</p>   |
| <b>Recover</b><br>● 1.2<br><i>Risk Informed</i> | <ul style="list-style-type: none"> <li>● Communications</li> <li>● Improvements</li> <li>● Recovery planning</li> </ul>  | <p><b>Overview:</b> TS Alliance has a general understanding of their critical assets and the recovery activities that would need to occur. They do not have a formalized plan in place to define all activities, prioritization based on system or business process, and delegated responsibilities.</p> <p><b>Strengths:</b> There is a general understanding of the critical applications in the environment and ownership of those applications, however formal rankings have not been evaluated and assigned. Communication appears to include all necessary stakeholders and information sharing is provided on an as needed basis.</p> <p><b>Challenges:</b> There is no formal plan in place to follow in the event of a wide-spread disaster, so recovery activities may be impacted and delayed. Additionally, recovery capability testing is informal and unvetted.</p> |

● Low Risk      ● Moderate Risk      ● High Risk





# DETAILED FINDINGS AND RECOMMENDATIONS



# Background

The NIST Cybersecurity Framework (CSF) provides a common language for understanding, managing, and expressing cybersecurity risk, as well as providing guidance for how private sector organizations can assess and improve their ability to prevent, detect and respond to cyber attacks

The NIST CSF consists of three main components, as listed below:

| Component                      | Description  |
|--------------------------------|--|
| <b>1. Framework Core</b>       | This is a set of cybersecurity outcomes, organized into five categories, that translates cybersecurity activities into cross-functional groups to facilitate analysis. |
| <b>2. Implementation Tiers</b> | Tiers describe the degree to which an organization’s cybersecurity management activities demonstrate the characteristics described within the framework.               |
| <b>3. Profiles</b>             | Profiles summarize the alignment of the organization’s overall cybersecurity posture in a “current” profile, compared to a “target” profile.                           |

Within the next page, we began our objective review of the cybersecurity processes in place at TS Alliance and performed an analysis using the implementation tiers to assist in risk-rating each of the five categories (and the 23 individual subcategories) to an observed implementation tier.

We assessed processes within the five categories (and 23 subcategories) to determine which implementation tiers could be summarized to create TS Alliance’s current state profile. Using this information, we then developed a target profile along with a roadmap to achieve those outcomes.

| Framework Core  |  |
|-----------------|--|
| <b>Identify</b> | Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities  |
| <b>Protect</b>  | Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.   |
| <b>Detect</b>   | Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.  |
| <b>Respond</b>  | Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.  |
| <b>Recover</b>  | Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. |

| Implementation Tiers           |  |
|--------------------------------|--|
| Rating                         | Description  |
| <b>Tier 1</b><br>Partial       | No policy exists for the control, and it has not been implemented on any systems. The controls indicate that several key elements of data security are not in place.                                       |
| <b>Tier 2</b><br>Risk Informed | The control has an informal policy, and only parts of the control have been implemented. The controls indicate an ability to sustain some security efforts, though key controls and programs are lacking.  |
| <b>Tier 3</b><br>Repeatable    | The control has been implemented on most systems and has a formalized policy. A few key controls may not be implemented effectively.   |
| <b>Tier 4</b><br>Adaptive      | The control has an approved written policy and has been implemented on all systems. The organization has implemented consistent monitoring and analysis of the security program for continual improvement. |

# Category #1 – Identify

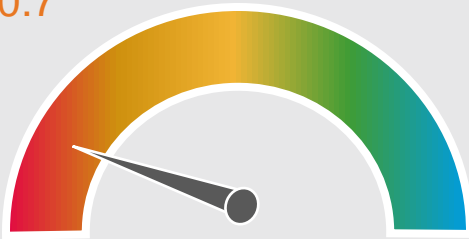
## Findings and Recommendations

**Overview**  
Basic security practices in place, but lack of baseline internal and external assessment to inform risk management processes.

**Strengths**  
Understanding of the business environment and leveraging a third-party to maintain endpoints.

**Opportunities**  
Developing and implementing more formal IT and vendor governance practices.

0.7



**Tier: Partial**

- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy
- Supply chain risk management

| Detailed Finding   | Risk       | Recommendation   |
|--|------------|--|
| <p><b>#1 – Vendor inventory and vendor risk management program have not been formally established</b></p> <p>The TS Alliance could determine a population of vendors via the accounts payable system; however, a succinct inventory is not maintained to catalogue each vendor relationship, business relationship owner, nature of business conducted, data transferred, data transfer channels, criticality of relationship and other key factors required to determine vendor risks. Additionally, while there may be some ad-hoc due diligence procedures, such as multiple approvals for contracts over a certain threshold, formal vendor management procedures have not been established to provide critical insight into the effectiveness of third-party controls, specifically for vendors processing and/or storing company data.</p> | ● Moderate | <ul style="list-style-type: none"> <li>• Document a population of vendors with attributes such as services provided, types of data shared, system connections and connection type</li> <li>• Establish and perform due diligence processes including information security questionnaires, attestation report reviews, ongoing concern, etc.</li> </ul>   |
| <p><b>#2 – Informal risk management program</b></p> <p>The TS Alliance has an established board of directors and audit committee to oversee and provide input on organizational risk. However, RSM noted that there are opportunities for improvement in a formal risk management program that allows TS Alliance to identify its risk profile, risk appetite and threat vectors. A business impact analysis has not been performed to document all potential risks to organizational systems, processes and data with associated risk probabilities and level of impact. Additionally, processes have not been established to centrally document and track risk management efforts of threats identified (i.e., tracking compliance to mitigation controls for an identified risk).</p>   | ● Moderate | <ul style="list-style-type: none"> <li>• Periodically perform an information security risk assessment (leveraging external partners, as necessary).</li> <li>• Key security functions and risks enterprise-wide should be evaluated, even if at a high level.</li> <li>• Re-evaluation should occur using a risk-based approach, accounting for criticality of assets and changes to the environment.</li> </ul> |
| <p><b>#3 – Business impacts not assessed</b></p> <p>TS Alliance has not completed a formal business impact analysis. This analysis would support further development of the risk management program and IT disaster recovery plan, as well as establish priorities and recovery order of systems, in addition to recovery time objectives (RTO) and recovery point objectives (RPO). Additionally, a business impact analysis will allow the organization to strategically manage risk, categorize systems and processes to determine appropriate protections and track compliance to the established standards.</p>   | ● Moderate | <ul style="list-style-type: none"> <li>• IT assets (hardware, software and services) should be classified according to business impact to aid in response/recovery activities, aligned with business priorities.</li> </ul>  |

● Low Risk      ● Moderate Risk      ● High Risk

# Category #1 – Identify

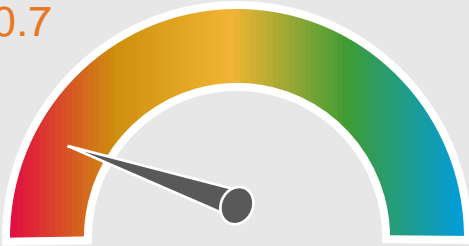
## Findings and Recommendations

**Overview**  
Basic security practices in place, but lack of baseline internal and external assessment to inform risk management processes.

**Strengths**  
Understanding of the business environment and leveraging a third-party to maintain endpoints.

**Opportunities**  
Developing and implementing more formal IT and vendor governance practices.

0.7



**Tier: Partial**

- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy
- Supply chain risk management

| Detailed Finding   | Risk   | Recommendation  |
|--|--|---|
| <p><b>#4 – Domain policies not in line with Microsoft’s standards</b></p> <p>In reviewing TS Alliance’s active directory password policy, it was noted that settings for password expiry and length were established. However, these, along with several other password settings deviated from Microsoft recommendations, including the following:</p> <ul style="list-style-type: none"> <li>• The current password minimum length is set to six characters. A minimum password length determines the least number of characters for a user account. Permitting shorter passwords reduces security because they can be easily broken with tools that can brute force password guesses.</li> <li>• The current minimum password age is 0 days. With no minimum time requirement between password changes, a user can repeatedly change their password until the password history requirement is met, effectively negating the password history requirement and re-using the original password again.</li> <li>• The current maximum password age is 180 days. The maximum password age is the number of days that a password can be used before the system requires the user to change it. The longer a password exists, the higher the likelihood that it will be compromised by a brute force attack, by an attacker gaining general knowledge about the user, or by the user sharing the password with other personal accounts. Additionally, any accounts that may have been compromised remain exploitable for as long as the password is left unchanged.</li> <li>• The current setting is to reset account lockout counter after 10 minutes. The account lockout feature, when enabled, prevents brute-force password attacks on the system. This parameter specifies the period that must pass after failed logon attempts before the counter is reset to 0. The smaller this value is, the less effective the account lockout feature will be in protecting the local system.</li> <li>• The current setting for password complexity is not enabled. This policy setting enabled, combined with a minimum password length of 8, ensures that there are at least 218,340,105,584,896 different possibilities for a single password making a brute force attack much more difficult. Passwords that contain only alphanumeric characters are easy to compromise by using publicly available tools.</li> </ul> | <ul style="list-style-type: none"> <li>● Moderate</li> </ul> | <p>TS Alliance should consider revising the following domain policies following guidance from Microsoft:</p> <ul style="list-style-type: none"> <li>• Increase the minimum password length requirement for standard user accounts to at least eight characters. In enterprise environments, the ideal value for the minimum password length setting is 14 characters, however this should be adjusted to meet the organization’s business requirements.</li> <li>• It is recommended to set the minimum password age to at least one day.</li> <li>• It is recommended the maximum password age is set between 30 and 90 days.</li> <li>• The Secure Technical Implementation Guide for Windows 10 suggests the reset account lockout counter to be at least 15 minutes.</li> <li>• Passwords should contain additional characters and meet complexity requirements, enforced by setting password complexity to enabled.</li> </ul> |

● Low Risk      ● Moderate Risk      ● High Risk



# Category #1 – Identify

## Findings and Recommendations

**Overview**  
Basic security practices in place, but lack of baseline internal and external assessment to inform risk management processes.

**Strengths**  
Understanding of the business environment and leveraging a third-party to maintain endpoints.

**Opportunities**  
Developing and implementing more formal IT and vendor governance practices.

0.7



**Tier: Partial**

- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy
- Supply chain risk management

| Detailed Finding   | Risk   | Recommendation   |
|--|--|--|
| <p><b>#5 – Numerous accounts violate principles of least privilege</b></p> <p>TS Alliance works with Optimal Networks to assign users access rights to applicable files, folders, or drives via active directory groups and organizational units based on department and responsibilities. However, RSM inspected the active directory user listing and noted there are many active accounts that do not follow security best practices, including:</p> <ul style="list-style-type: none"> <li>• 38 accounts that have not logged in in the past 90 days, 35 of which have not logged in greater than two years with some last logon dates dating 10 years and more.</li> <li>• 41 accounts are set so the password does not expire and have had a password reset in greater than 180 days, violating the set domain policy.</li> <li>• 37 of these have not been reset in greater than 1000 days, or roughly three years, and several greater than 5,000 days, or more than 13 years.</li> <li>• Many of these were also high-privilege accounts, including three enterprise admin accounts, two domain admin accounts, eight administrators accounts and one remote desktop user's account.</li> <li>• High privileged accounts may not be restricted to individuals and/or system accounts that absolutely require the assigned privileges.</li> <li>• The four active domain admin accounts include the CEO and senior associate director, as well as two service accounts. As TS Alliance has outsourced day-to-day IT operations, the two user domain admin accounts may not be necessary unless actively managing the network. Service accounts should not be granted domain admin rights as this typically goes beyond the principle of least privilege, providing more access than needed and for a time period longer than needed.</li> <li>• Roughly eight privileged accounts granted enterprise admin or administrators are generic or shared accounts that do not provide accountability to an individual.</li> </ul> <p>These issues further highlight the observation that TS Alliance does not perform regular, periodic reviews of privileges and access levels of all user and system/service accounts to determine whether access rights remain appropriate.</p> | <ul style="list-style-type: none"> <li>● Moderate</li> </ul> | <p>TS Alliance should consider the following:</p> <ul style="list-style-type: none"> <li>• Setting policies to disable accounts after a defined period of inactivity.</li> <li>• Enforcing the periodic rotation of passwords via the maximum password age policy and allowing account passwords to expire.</li> <li>• Restrict privileged access on an as-needed basis when necessary for job responsibilities or actions to be taken.</li> <li>• Perform a periodic user access review to confirm the appropriateness of active accounts and access right assigned.</li> <li>• Review the appropriateness of executives having domain admin privileges. Since they are frequent targets of phishing attacks, their credentials pose greater risk of loss.</li> <li>• Review procedures for granting domain admin privileges. domain admin rights allow an account to have full ownership rights to the entire domain, including all domain workstations and servers. Microsoft recommends this access to only be enabled temporarily as needed, and then removed once the work is done.</li> </ul> |

● Low Risk      ● Moderate Risk      ● High Risk



# Category #1 – Identify

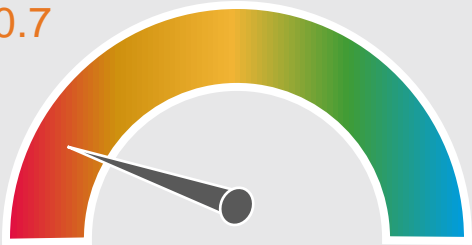
## Findings and Recommendations

**Overview**  
Basic security practices in place, but lack of baseline internal and external assessment to inform risk management processes.

**Strengths**  
Understanding of the business environment and leveraging a third-party to maintain endpoints.

**Opportunities**  
Developing and implementing more formal IT and vendor governance practices.

0.7



**Tier: Partial**

- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy
- Supply chain risk management

| Detailed Finding   | Risk   | Recommendation  |
|--|--|---|
| <p><b>#6 – Penetration testing on critical, risk-weighted networks has not been performed</b><br/>The TS Alliance’s internal and external network has not been tested to validate their security and stability. Penetration testing allows for insight into the capabilities and weak points in TS Alliance’s network to harden the TS Alliance cybersecurity posture.</p>   | <ul style="list-style-type: none"> <li>● Moderate</li> </ul> | <p>Establish a methodology incorporating penetration testing into the risk assessment and management program.</p> <ul style="list-style-type: none"> <li>• Procure services to perform penetration testing on the internal, external and wireless networks</li> </ul>   |
| <p><b>#7 – Cybersecurity situational awareness and cyber threat intelligence</b><br/>The TS Alliance receives ad-hoc security notices from supporting vendors in relation to technologies in use. However, these notices come second-hand at the discretion of the service provider and what they believe their clients may want to know. The TS Alliance does not currently conduct or acquire targeted threat intelligence services to support its cybersecurity governance processes. It is important for the TS Alliance to understand the threats against the organization to be able to respond appropriately. Furthermore, threat intelligence allows the company to align security resources where attacks are most likely to occur. Employees need to know their role in the protection of the company, but very few know the actual threat vectors nefarious actors use to compromise systems like that of TS Alliance. A full deep and dark web sweep allows for insight into the company’s criminal interest and take steps to prevent it in the future.</p> | <ul style="list-style-type: none"> <li>● Moderate</li> </ul> | <p>Procure third-party services to periodically perform cybersecurity situational awareness testing along with cyber threat intelligence reviews.</p> <ul style="list-style-type: none"> <li>• Re-evaluation should occur using a risk-based approach considering criticality of assets and processes and any changes to the environment</li> </ul> |

● Low Risk      ● Moderate Risk      ● High Risk

# Category #1 – Identify

## Findings and Recommendations

**Overview**  
Basic security practices in place, but lack of baseline internal and external assessment to inform risk management processes.

**Strengths**  
Understanding of the business environment and leveraging a third-party to maintain endpoints.

**Opportunities**  
Developing and implementing more formal IT and vendor governance practices.

0.7



**Tier: Partial**

- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy
- Supply chain risk management

| Detailed Finding  | Risk  | Recommendation   |
|---|---|--|
| <p><b>#8 – Governance materials are not maintained</b></p> <p>The TS Alliance has several policies and procedures, such as the Internal Control document, Whistleblower Policy, and a financial Crisis Management Policy. However, many policies, including roles and responsibilities, that contribute to an information security program have not been formally defined. These informal policies, procedures and standards include but are not limited to:</p> <ul style="list-style-type: none"> <li>• Access control, including separation of duties, the principle of least privilege, periodic user access reviews and data flow diagrams</li> <li>• Awareness and training, including role-based and cybersecurity awareness training programs</li> <li>• Configuration management, including configuration standards and baselining</li> <li>• Audit record management, including logging, monitoring, alerting, retention and review of suspicious activity</li> <li>• Asset management program including the asset lifecycle, risk categorization, marking, flow and inventory. This includes physical assets (i.e., PCs, monitors, hard drives) and software assets (i.e., executables, web applications, authorized external systems)</li> <li>• Secure configuration, including restrictions on end user software, mobile code usage restrictions and implementation guidance</li> <li>• Backup and recovery, including appropriate objectives for system recoverability</li> <li>• Physical security expectations, including visitor management</li> <li>• Risk management program, including appropriate governance, risk and compliance (GRC) implications</li> </ul> | <ul style="list-style-type: none"> <li>● Low</li> </ul> | <p>TS Alliance should initiate the formal development of policies and standard operating procedures (SOPs).</p> <ul style="list-style-type: none"> <li>• These should provide standardized guidance to TS Alliance employees and management taking into consideration appropriate compliance measures</li> <li>• Although external services may be leveraged to develop and execute these standards, TS Alliance should establish a means of governance over roles and tasks to be outsourced</li> </ul> |

● Low Risk      ● Moderate Risk      ● High Risk

# Category #2 – Protect

## Findings and Recommendations

**Overview**  
There are strong environment protections, but weak user training threatens to undermine organizational security.

**Strengths**  
Access control process in place.  
Maintenance processes managed by Optimal Networks and in-place.

**Opportunities**  
Information protection strategy should be created and reviewed. End user cybersecurity training should be implemented.



- Access control
- Awareness training
- Data security
- Info protection process and procedures
- Maintenance
- Protective technology

| Detailed Finding   | Risk   | Recommendation  |
|--|--|---|
| <p><b>#9 – Undefined end user cybersecurity training strategy</b><br/>Despite intermittent trainings held by Optimal Networks, the TS Alliance has not established security and privacy training standards for employees. Users are the key to a strong information security program. Without consistent, effective hands-on training, and phishing and vishing testing, people are the greatest liability to the security of TS Alliance’s assets and data. A formal awareness and training program should be established and include role-based information security training on an ongoing basis. Training materials should be updated to reflect changes to the environment. As an augmentation of user training, advanced preparation for access to sensitive data and systems will enable TS Alliance to protect its reputation, as well as client data.</p> | <ul style="list-style-type: none"> <li>● Moderate</li> </ul> | <p>Establish a methodology to provide consistent cybersecurity training and testing of employees. This can be obtained through a Learning Management System (LMS) with applicable material, or through an external vendor to conduct.</p> <ul style="list-style-type: none"> <li>• Training can be in person, or through a subscription to readymade content.</li> <li>• Testing can be through follow up quizzes, phishing, vishing, etc.</li> </ul> |
| <p><b>#10 – Formal change management procedures and responsibilities have not been defined</b><br/>The TS Alliance relies on supporting vendors to makes changes to its IT infrastructure on an as-needed basis. However, this process has not been formally established to consider whether certain level of changes require management’s review and approval and/or end-user testing prior to implementing the change. Change testing and approval should be consistently tracked and documented following a standard methodology so the appropriate stakeholders follow the process to completion; safeguarding both the content and the security of the assets.</p>  | <ul style="list-style-type: none"> <li>● Low</li> </ul>      | <p>Changes to TS Alliance’s network should undergo a consistent process before implementation</p> <ul style="list-style-type: none"> <li>• Contract your MSP to formalize the process through which updates and reconfigurations are vetted, tested, approved, and pushed onto TS Alliance systems</li> </ul>   |

- Low Risk
- Moderate Risk
- High Risk

# Category #2 – Protect

## Findings and Recommendations

### Overview

There are strong environment protections, but weak user training threatens to undermine organizational security.

### Strengths

Access control process in place.  
Maintenance processes managed by Optimal Networks and in-place.

### Opportunities

Information protection strategy should be created and reviewed. End user cybersecurity training should be implemented.

1.9



**Tier: Repeatable**

- Access control
- Awareness training
- Data security
- Info protection process and procedures
- Maintenance
- Protective technology

### Detailed Finding

#### #11 – Shared identifiers for suite access inhibits traceability of records

TS Alliance employees currently badge into the building and elevator but use a standard PIN code for suite doors. Using a shared identifier doesn't allow for an audit trail with respect to suite access. It also poses a security risk if the code is shared with nefarious actors or not changed in a timely manner following an employee termination. Transferring all doors to individual badge access would allow for logging of individuals entering the suite, and for individual access control management.

### Risk

● Low

### Recommendation

Establish methods to account for individual access to organization owned office spaces and IT assets.

● Low Risk

● Moderate Risk

● High Risk



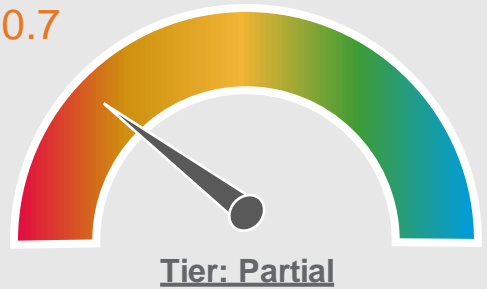
# Category #3 – Detect

## Findings and Recommendations

**Overview**  
Despite a network firewall, there are very few logging or monitoring processes in place.

**Strengths**  
A network firewall is configured and in place, so detection and monitoring capabilities are ready to be implemented.

**Opportunities**  
Developing and implementing stronger controls for removable media and information at rest and implementing firewall monitoring.



- Anomalies and events
- Security continuous monitoring
- Detection processes

| Detailed Finding   | Risk   | Recommendation  |
|--|--|---|
| <p><b>#12 – Lack of centralized logging and monitoring processes</b><br/>The TS Alliance does not have formally defined internal standards for system activity logging and monitoring. While the TS Alliance employs a managed IT service provider among other IT vendors, processes have not been established to monitor the internal network, nor gain comfort over logging and monitoring processes within hosted environments. These should be implemented to allow for logging of activity in TS Alliance’s environment and proactive identification of potential security incidents.</p> | <ul style="list-style-type: none"> <li>● Moderate</li> </ul> | <p>Establish logging and monitoring processes throughout the organization to protect against destructive cyber events.</p> <ul style="list-style-type: none"> <li>• Request a regular report on your MSPs logging and monitoring processes</li> </ul> |

- Low Risk
- Moderate Risk
- High Risk

# Category #4 – Respond

## Findings and Recommendations

**Overview**  
 Logging management and monitoring strategy needs to be recorded and reviewed; mitigations for other monitoring controls are not yet in place.

**Strengths**  
 External Managed Service Providers can monitor security event logging processes on TS Alliance’s behalf.

**Opportunities**  
 Monitoring system logs and building out formal network intrusion detection procedures and controls.



**Tier: Partial**

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

| Detailed Finding   | Risk  | Recommendation   |
|--|---|--|
| <p><b>#13 - Lack of infrastructure vulnerability management program</b></p> <p>The TS Alliance has anti-virus software installed on workstations, and vulnerability scans are performed on servers by the hosting vendor, however formal vulnerability management processes have not been established to consistently identify, document, evaluate (impact and likelihood), prioritize and respond to identified threats in the environment.</p> <p>A vulnerability management program is not in place to ensure scope and coverage of all information assets and to prioritize and measure vulnerability management efforts (e.g., mitigating high risk vulnerabilities within 2 to 14 days).</p> | <ul style="list-style-type: none"> <li>● Low</li> </ul> | <p>Develop and document a vulnerability management program.</p> <ul style="list-style-type: none"> <li>• This vulnerability management program should include regular assessment to identify vulnerabilities and standard practices, guidelines, and metrics to evaluate, prioritize, remediate and report on identified threats</li> <li>• This program be reviewed regularly to ensure alignment with business units and third parties that are relied upon</li> </ul> |

● Low Risk      ● Moderate Risk      ● High Risk

# Category #5 – Recover

## Findings and Recommendations

### Overview

There is a general understanding of critical assets and accompanying recovery activities. However, no formalized plan documents prioritization based on system, business process or responsibilities.

### Strengths

Communication includes necessary stakeholders and information sharing is provided on an as needed basis.

### Opportunities

Incident response and disaster recovery plans need to be defined. CTI processes should be explored and implemented.

1.2



**Tier: Risk Informed**

- Communications
- Improvements
- Recovery planning

### Detailed Finding

#### #14 – Lack of formalized and tested incident response plan

RSM reviewed the COVID-19 Preparedness and Staff Back-up Plans, along with documentation following a recent data breach that occurred at a vendor. Despite these plans, the TS Alliance handles cyber incidents on an ad hoc basis, and thus, an incident response plan is not formally documented. This plan is critical in the event of a declared cyber event. Without a documented, socialized and rehearsed plan, the incident response time and risk of severity and impact of an incident increases significantly.

Strategies should include preparations for additional risk implications as the organization and its clients grow and mature. Several strategic and technical scenarios could be considered, such as:

- Breach and/or exfiltration of organizational data (including physical loss of data or resources at headquarters)
- Outages of critical applications or cloud infrastructure
- Economic threats and risks (such as price fluctuations in critical commodities)
- Human errors or failures
- Regulatory compliance failures (such as fines, mandated shutdowns or reporting obligations)

### Risk

- Low

### Recommendation

- Document an incident response plan to establish roles and responsibilities (internal and external), prioritization and rating of incidents, reporting and contact information, strategies and goals, metrics for measuring success and effectiveness, and processes to review and improve.
- The incident response plan should consider various incidents, such as malware infection, ransomware, and physical breach or loss of assets (laptops or paper information)
  - A comprehensive incident response plan should the above scenarios and capabilities to detect, analyze, prioritize, report-on and resolve cybersecurity incidents in a consistent manner

- Low Risk
- Moderate Risk
- High Risk



# CYBER THREAT INTELLIGENCE ASSESSMENT RESULTS

# Cyber Threat Intelligence Assessment Results

| Overview  | Detailed Finding  | Risk   | Recommendation  |
|---|---|--|---|
| <p><b>Overview</b><br/>Overall, there is not a direct threat targeting the TS Alliance.</p> <p>We believe that in the future if there were an attack against the company, it would stem from opportunistic threat actor activity, or threat actors seeking to gain information about donors which could be used for financial gain.</p> <p>Please see the observations for more information on specific activities noted.</p> | <p><b>High volume of Dark Web chatter about Blackbaud post-cyber incident</b></p> <p>We discovered a high volume of Dark Web activity surrounding Blackbaud, its Raiser's Edge product, and the recent cybersecurity incident that impacted Blackbaud data. Most of the identified conversations were threat actors discussing the cybersecurity incident and the payment of the associated ransom.</p> <p>We did not find specific instances of data stolen from Blackbaud being sold on the Dark Web. Several Russian language forums, including Korovka and Maza, re-posted news articles discussing the incident.</p> | <ul style="list-style-type: none"> <li>Moderate</li> </ul> | <p>We recommend ongoing monitoring to ensure that any TS Alliance data affected in the Blackbaud breach does not appear for sale on the Dark Web. If data does appear, we recommend conducting a takedown service by working with a threat intelligence vendor and law enforcement to remove any potentially affected data. Additionally, we recommend notifying the Blackbaud team of this information to ensure they are monitoring the situation and conducting due diligence in the event new information is posted online.</p> |

● Low Risk     
 ● Moderate Risk     
 ● High Risk

# Cyber Threat Intelligence Assessment Results

| Overview  | Detailed Finding   | Risk   | Recommendation   |
|---|--|--|--|
| <p><b>Overview</b><br/>Overall, there is not a direct threat targeting the TS Alliance.</p> <p>We believe that in the future if there were an attack against the company, it would stem from opportunistic threat actor activity, or threat actors seeking to gain information about donors which could be used for financial gain.</p> <p>Please see the observations for more information on specific activities noted.</p> | <p><b>Accounts for Blackbaud domain sold on Dark Web</b></p> <p>We discovered a high volume of portal accounts sold in association with myschoolapp.com which appears to be a Blackbaud domain. These domains were for-sale on Genesis Store.</p> <p>The Genesis Store is a predominantly Russian-speaking, invitation-only Dark Web marketplace. This marketplace sells targeted combinations of accounts, session cookies, browser fingerprints and other system information, which threat actors can purchase and upload into a custom Chromium plugin called "Genesis Security." With this plugin, a buyer can use the purchased account information for full "identity takeover" through a single browser session.</p> <p>None of the accounts sold were associated with TS Alliance.</p> | <ul style="list-style-type: none"> <li>Moderate</li> </ul> | <p>We recommend ensuring that multi-factor authentication is enabled organization wide at TS Alliance, to combat attacks such as those possible when such information is purchased on the Genesis Store.</p> <p>Furthermore, we recommend establishing vendor risk management procedures that require existing vendors, as well as future vendors, to be assessed through the entire vendor risk management lifecycle.</p> |

● Low Risk     
 ● Moderate Risk     
 ● High Risk

# Cyber Threat Intelligence Assessment Results

## Overview

Overall, there is not a direct threat targeting the TS Alliance.

We believe that in the future if there were an attack against the company, it would stem from opportunistic threat actor activity, or threat actors seeking to gain information about donors which could be used for financial gain.

Please see the observations for more information on specific activities noted.

| Detailed Finding   | Risk  | Recommendation  |
|--|-------|---|
| <b>Leaked credentials from third-party breaches</b><br><br>We discovered 16 instances of leaked credentials. These credentials likely were exposed as a result of third-party data dumps – there is no reason to believe these credentials were exposed a result of unauthorized access to TS Alliance systems. Please see the next slide for a list of the exposed credentials. | ● Low | These credentials could have been used for password reuse attacks, which are commonly used by threat actors attempting to gain access to a company's network. We recommend that passwords for these accounts be reset in case employees are using the same passwords between platforms. Additionally, employees should be trained about the risk of using the same passwords between platforms and that the TS Alliance enforce password complexity requirements per industry best practice |

● Low Risk

● Moderate Risk

● High Risk

# Cyber Threat Intelligence Assessment Results

| Credentials*                               | Date       | Data Dump                 |
|--|------------|---------------------------|
| jjsham@tsalliance.org: [REDACTED]          | 12/2/2020  | GoNitro – Data Dumps      |
| sroberds@tsalliance.org: [REDACTED]        | 11/21/2020 | Crawled/Unknown           |
| whittemore@tsalliance.org: [REDACTED]      | 11/21/2020 | Crawled/Unknown           |
| p.crino@tsalliance.org: [REDACTED]         | 11/21/2020 | Crawled/Unknown           |
| onda@tsalliance.org: [REDACTED]            | 11/21/2020 | Crawled/Unknown           |
| wtolentino@tsalliance.org: [REDACTED]      | 1/17/2019  | Collection 1 – Data Dumps |
| linda.creighton@tsalliance.org: [REDACTED] | 1/17/2019  | Collection 1 – Data Dumps |
| wtolentino@tsalliance.org: [REDACTED]      | 1/17/2019  | Collection 1 – Data Dumps |
| whittemore@tsalliance.org: [REDACTED]      | 1/17/2019  | Collection 1 – Data Dumps |
| linda.creighton@tsalliance.org: [REDACTED] | 1/17/2019  | Collection 1 – Data Dumps |
| jdotson@tsalliance.org: [REDACTED]         | 10/1/2016  | Exploit.in – Data Dumps   |
| kcarlson@tsalliance.org: [REDACTED]        | 10/1/2016  | Exploit.in – Data Dumps   |
| dhook@tsalliance.org: [REDACTED]           | 8/31/2016  | Dropbox – Data Dumps      |
| jjsham@tsalliance.org: [REDACTED]          | 8/31/2016  | Dropbox – Data Dumps      |
| jdotson@tsalliance.org: [REDACTED]         | 5/31/2016  | Myspace – Data Dumps      |
| sroberds@tsalliance.org: [REDACTED]        | 5/1/2016   | LinkedIn – Data Dumps     |
| mperraut@tsalliance.org: [REDACTED]        | 5/1/2016   | LinkedIn – Data Dumps     |

● Low Risk      ● Moderate Risk      ● High Risk

\*Redacted passwords available upon request



# Cyber Threat Intelligence Assessment Results

## Overview

Overall, there is not a direct threat targeting the TS Alliance.

We believe that in the future if there were an attack against the company, it would stem from opportunistic threat actor activity, or threat actors seeking to gain information about donors which could be used for financial gain.

Please see the observations for more information on specific activities noted.

| Detailed Finding   | Risk  | Recommendation  |
|--|---|---|
| <p><b>Phishing email follow-up</b></p> <p>We discovered the following compromised credentials associated with the phishing emails provided:</p> <ul style="list-style-type: none"> <li>lvkathyk@gmail.com: [REDACTED] (Exploit.in, October 2016)</li> <li>lvkathyk@gmail.com: [REDACTED] (LinkedIn, May 2016)</li> </ul> <p>These credentials could have been used to compromise and impersonate Kathy Kingston, leading to the purchase of \$515 in gift cards by Chelsea Holman. However, we cannot verify that these credentials were used to take over the account and according to the evidence provided by TS Alliance, it appears the email was spoofed. Further information related to the phishing emails was not discovered and it is unclear whether all the incidents are related.</p> | <ul style="list-style-type: none"> <li>Low</li> </ul> | <p>We recommend that Kathy Kingston reset her personal and corporate passwords as soon as possible.</p> |

● Low Risk

● Moderate Risk

● High Risk

\*Redacted passwords available upon request

# Cyber Threat Intelligence Assessment Results

## Overview

Overall, there is not a direct threat targeting the TS Alliance.

We believe that in the future if there were an attack against the company, it would stem from opportunistic threat actor activity, or threat actors seeking to gain information about donors which could be used for financial gain.

Please see the observations for more information on specific activities noted.

| Detailed Finding   | Risk  | Recommendation  |
|--|---|---|
| <p><b>Potentially typosquatted domains</b></p> <p>We identified 15 potentially typosquatted domains related to the TS Alliance domain. Please see a list of the domains on the next slide.</p> <p>Typosquatting attacks attempt to duplicate legitimate URLs through typos or spelling similarities to convince users to navigate to a malicious site or spoof a legitimate certificate. These malicious sites can be used to collect personal information about users, such as credentials or to infect users' machines with malware.</p> | <ul style="list-style-type: none"><li>● Low</li></ul> | <p>We recommend reviewing the attached domains/certificates to determine whether these domains are legitimately associated with TS Alliance. If these domains are not legitimately affiliated with TS Alliance, we recommend ongoing monitoring of the domains to ensure they do not begin to host content. A domain hosting spoofed TS Alliance content could be used to trick TS Alliance employees and/or customers into giving up personal information, such as login credentials and/or financial information.</p> |

● Low Risk

● Moderate Risk

● High Risk

# Cyber Threat Intelligence Assessment Results

| Domains         | Change        | IP Address     |
|-----------------|---------------|----------------|
| usalliance.org  | Bitsquatting  | 199.60.103.31  |
| dsalliance.org  | Bitsquatting  | 23.236.62.147  |
| tralliance.org  | Bitsquatting  | 192.185.134.34 |
| tcalliance.org  | Bitsquatting  | 104.31.70.216  |
| t3alliance.org  | Bitsquatting  | 209.87.159.177 |
| ts-alliance.org | Hyphenation   | 216.21.239.197 |
| tesalliance.org | Insertion     | 162.144.22.76  |
| fsalliance.org  | Replacement   | 160.153.32.39  |
| txalliance.org  | Replacement   | 209.99.64.76   |
| taalliance.org  | Replacement   | 116.203.1.227  |
| gsalliance.org  | Replacement   | 203.245.44.39  |
| tsalli.ance.org | Subdomain     | 91.195.241.137 |
| tsallian.ce.org | Subdomain     | 216.83.206.108 |
| tsallianc.e.org | Subdomain     | 51.140.127.152 |
| stalliance.org  | Transposition | 77.72.0.142    |

● Low Risk
 ● Moderate Risk
 ● High Risk

# Cyber Threat Intelligence Assessment Results

## Overview

Overall, there is not a direct threat targeting the TS Alliance.

We believe that in the future if there were an attack against the company, it would stem from opportunistic threat actor activity, or threat actors seeking to gain information about donors which could be used for financial gain.

Please see the observations for more information on specific activities noted.

| Detailed Finding   | Risk  | Recommendation   |
|--|---|--|
| <p><b>Paycor, Inc. data breach and vulnerabilities</b></p> <p>On February 16, 2018, TS Alliance's payroll provider, Paycor, Inc. (Paycor), suffered a data breach, when an employee accidentally mailed employee's Internal Revenue Service W-2 information to an unauthorized third-party. This data breach was disclosed to the state of California and based on information listed on the state of California Department of Justice website, Paycor notified all affected individuals.</p> <p>Additionally, in 2015 and 2016, the Paycor website and a Paycor subdomain were affected by cross-site scripting (XSS) vulnerabilities. Based on the information available, it is unclear whether these vulnerabilities have been patched.</p> | <ul style="list-style-type: none"> <li>● Low</li> </ul> | <p>We recommend establishing vendor risk management procedures that require existing vendors, as well as future vendors, to be assessed through the entire vendor risk management lifecycle.</p> |

● Low Risk

● Moderate Risk

● High Risk

# Cyber Threat Intelligence Assessment Results

## Overview

Overall, there is not a direct threat targeting the TS Alliance.

We believe that in the future if there were an attack against the company, it would stem from opportunistic threat actor activity, or threat actors seeking to gain information about donors which could be used for financial gain.

Please see the observations for more information on specific activities noted.

| Detailed Finding  | Risk  | Recommendation   |
|---|---|--|
| <p><b>Cvent vulnerability</b></p> <p>On October 13, 2020, information about a XSS vulnerability that affects the login.cvent.com subdomain was posted on the OpenBugBounty website. Based on the information available, the status of the patching effort is currently "on hold."</p> <p>Two other XSS vulnerabilities affecting the cvent.com domain were disclosed on OpenBugBounty in 2015, 2016 and 2018. Both vulnerabilities are currently listed as patched.</p> | <ul style="list-style-type: none"><li>● Low</li></ul> | <p>We recommend establishing vendor risk management procedures that require existing vendors, as well as future vendors, to be assessed through the entire vendor risk management lifecycle.</p> |

● Low Risk

● Moderate Risk

● High Risk

# Cyber Threat Intelligence Assessment Results

## Overview

Overall, there is not a direct threat targeting the TS Alliance.

We believe that in the future if there were an attack against the company, it would stem from opportunistic threat actor activity, or threat actors seeking to gain information about donors which could be used for financial gain.

Please see the observations for more information on specific activities noted.

| Detailed Finding  | Risk  | Recommendation  |
|---|---|---|
| <b>Recent Certificate Registration</b><br><br>We discovered a recent certificate registered in November 2019 pertaining to TS Alliance. This certificate was give.tsalliance.org. CTI analysts reviewed this certificate and determined it was a legitimate registration associated with TS Alliance. We review these types of registrations for potential typosquatting attacks. Typosquatting attacks attempt to duplicate legitimate URLs through typos or spelling similarities to convince users to navigate to a malicious site or spoof a legitimate certificate. These malicious sites can be used to collect personal information about users, such as credentials, or to infect users' machines with malware. | <ul style="list-style-type: none"><li>● Low</li></ul> | No action needs to be taken at this time. This information is provided for situational awareness. |

● Low Risk

● Moderate Risk

● High Risk

# Cyber Threat Intelligence Assessment Results

## Overview

Overall, there is not a direct threat targeting the TS Alliance.

We believe that in the future if there were an attack against the company, it would stem from opportunistic threat actor activity, or threat actors seeking to gain information about donors which could be used for financial gain.

Please see the observations for more information on specific activities noted.

| Detailed Finding   | Risk  | Recommendation  |
|--|-------|---|
| <b>High volume of Dark Web chatter about Blackbaud pre-cyber incident</b><br><br>We discovered a high volume of Dark Web chatter and activity regarding Blackbaud before the cybersecurity incident occurred. In August 2019 on CodeBy Forum, Russian actors discussed what happens when you try to "hack" a database protected by Blackbaud OnMessage Shield (a web application firewall) and how the database can remain secured. Additionally, in October 2019, an actor posted an advertisement to test and fingerprint WAF products, including OnMessage Shield on the Verified Carder Forum. | ● Low | This finding is provided for situational awareness. No action can be taken on this chatter, as the cybersecurity incident it relates to already occurred. |

● Low Risk

● Moderate Risk

● High Risk

# Cyber Threat Intelligence Assessment Results

## Overview

Overall, there is not a direct threat targeting the TS Alliance.

We believe that in the future if there were an attack against the company, it would stem from opportunistic threat actor activity, or threat actors seeking to gain information about donors which could be used for financial gain.

Please see the observations for more information on specific activities noted.



| Detailed Finding   | Risk  | Recommendation   |
|--|---|--|
| <p><b>Strong social media presence</b></p> <p>During our review, we noted that TS Alliance had a strong social media presence (including references made to the entity by other individuals/accounts) on Twitter. All the information reviewed was noted as benign and containing no malicious content.</p> <p>We also noted that social media references increased in the April to December 2020 period. The biggest spike in social media references occurred in April 2020, when a virtual event was promoted by the TS Alliance – please see screenshot below.</p> | <ul style="list-style-type: none"> <li>● Low</li> </ul> | <p>This finding is provided for situational awareness, as social media is often used in malicious attacks against entities that may result in brand damaging information. Given the increasing nature of social media usage for marketing purposes, we believe that TS Alliance should continue to utilize Twitter for promoting the organization.</p> |

● Low Risk      ● Moderate Risk      ● High Risk





# FUTURE STATE ROADMAP

# Target Profile Strategic Roadmap

| Overall: <b>1.0</b>                   | Recommendations   | 2021 |    |    |    | 2022 |    |    |    | Potential Owner |
|---------------------------------------|---|------|----|----|----|------|----|----|----|-----------------|
|                                       |   | Q1   | Q2 | Q3 | Q4 | Q1   | Q2 | Q3 | Q4 |                 |
| <b>Identify</b><br>● 0.7 Partial      | Establish vendor inventory and vendor risk management program     |      |    |    | ●  | ●    |    |    |    | TS Alliance     |
|                                       | Formalize risk management program                                 |      |    |    | ●  | ●    | ●  | ●  |    | MSP             |
|                                       | Business Impact Assessment and BCP/DR                             |      |    | ●  | ●  | ●    |    |    |    | TS Alliance     |
|                                       | Domain policies not in line with Microsoft's standards            | ●    | ●  |    |    |      |    |    |    | MSP             |
|                                       | Numerous accounts violate principles of least privilege           | ●    | ●  |    |    |      |    |    |    | MSP             |
|                                       | Perform penetration testing on critical, risk-weighted networks   |      | ●  | ●  | ●  | ●    | ●  |    |    | MSP             |
|                                       | Cybersecurity situational awareness and cyber threat intelligence |      |    | ●  | ●  | ●    |    |    |    | MSP             |
|                                       | Maintain governance materials                                     |      |    | ●  | ●  | ●    |    |    |    | MSP             |
| <b>Protect</b><br>● 1.9 Risk Informed | Develop end user cybersecurity training strategy                  |      | ●  | ●  |    |      |    |    |    | MSP             |
|                                       | Define formal change management procedures and responsibilities   |      |    | ●  | ●  | ●    | ●  |    |    | MSP             |
|                                       | Implement unique identifiers for suite access                     |      |    |    |    | ●    | ●  | ●  | ●  | TS Alliance     |

Note: The timeline shown above is based on the average time that RSM has seen organizations be able to implement such programs and do not include variables such as budget, resources or other prioritized projects that may hinder the ability to implement such programs.

# Target Profile Strategic Roadmap

| Overall: <b>1.0</b>                   | Recommendations   | 2021 |        |    |        | 2022 |        |    |    | Potential Owner   |
|---------------------------------------|---|------|--------|----|--------|------|--------|----|----|-------------------|
|                                       |   | Q1   | Q2     | Q3 | Q4     | Q1   | Q2     | Q3 | Q4 |                   |
| <b>Detect</b><br>● 0.7 Partial        | Centralize logging and monitoring processes             |      | ●————● |    |        |      |        |    |    | MSP               |
| <b>Respond</b><br>● 0.2 Partial       | Develop infrastructure vulnerability management program |      |        |    | ●————● |      |        |    |    | MSP               |
| <b>Recover</b><br>● 1.2 Risk Informed | Formalize and test incident response plan               |      |        |    |        |      | ●————● |    |    | TS Alliance & MSP |

Note: The timeline shown above is based on the average time that RSM has seen organizations be able to implement such programs and do not include variables such as budget, resources or other prioritized projects that may hinder the ability to implement such programs.








# APPENDIX

# Assessment Approach

## Key Objectives

Our assessment was conducted in alignment with the NIST CSF. The NIST CSF provides a common language for understanding, managing and expressing cybersecurity risk to critical stakeholders. It can be leveraged to help identify the organizations current cybersecurity posture and prioritize actions for areas of improvement in an effort to reduce cybersecurity risk.

The NIST CSF is broken down into five core areas that were the focus of our assessment. We then assessed the relevant processes within each area using the scale to the right to calculate relevant maturity scores:

|   |  |
|---|--|
| <b>Identify</b><br>  | Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities  |
| <b>Protect</b><br>   | Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.   |
| <b>Detect</b><br>    | Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.  |
| <b>Respond</b><br> | Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.  |
| <b>Recover</b><br> | Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. |

## Maturity Scale

| Rating                           | Description   |
|----------------------------------|---|
| <b>1</b><br><b>Partial</b>       | No policy exists for the control, and it has not been implemented on any systems. This maturity rating indicates that several key elements of data security are not in place.   |
| <b>2</b><br><b>Risk Informed</b> | The control has an informal policy, and only parts of the control have been implemented. This maturity rating indicates an ability to sustain some security efforts, though key controls and programs are lacking.  |
| <b>3</b><br><b>Repeatable</b>    | The control has been implemented on most systems and has a formalized policy. This maturity rating indicates an ability to define and meet several security objectives. A few key controls may not be implemented effectively.  |
| <b>4</b><br><b>Adaptive</b>      | The control has an approved written policy and has been implemented on all systems. This maturity rating indicates a mature security program has been integrated into company culture. The organization has implemented consistent monitoring and analysis of the security program for continual improvement. |

## RSM US LLP

1861 International Drive  
Suite 400  
McLean, VA 22102

+1 703 336 6310  
rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit [rsmus.com/aboutus](http://rsmus.com/aboutus) for more information regarding RSM US LLP and RSM International.

RSM, the RSM logo and *the power of being understood* are registered trademarks of RSM International Association.

© 2020 RSM US LLP. All Rights Reserved.