TOPEKA METROPOLITAN TRANSIT AUTHORITY

Board of Directors Meeting – Agenda Item

ITEM	At-Bay Security Scan
CONTACT	Richard Appelhanz
RECOMMENDATION	Approve
SUMMARY	Review Security Scan provided by our Cyber Insurance Carrier At-Bay.
FISCAL IMPACT (Current and Future)	N/A
PRIORITY/GOAL	N/A
ATTACHMENTS	Yes

Security Report

Prepared for	Topeka Metropolitan Transit Authority
Website	topekametro.org
Date	October 19, 2023

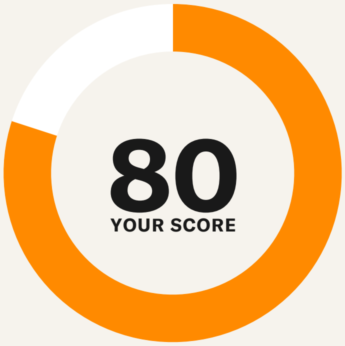
Security Summary

TOPEKA METROPOLITAN TRANSIT AUTHORITY

Transportation and Warehousing - topekametro.org

Scanned on October 17, 2023

Resolve issues to unlock best rates and coverages.



▲ 2% above industry average

Required to Bind

0 Critical issue(s)

No issues detected.

May Impact Premium or Terms

1 Important issue(s)

Implement a recommended SEG to protect against email-based attacks
This issue is important and may impact your premium or coverage.

Action Recommended

2 Moderate issue(s)

Strengthen Microsoft 365 security settings to avoid email compromise.
This issue is moderate and should be resolved to improve security.

Implement a strong password policy to avoid email compromise.
This issue is moderate and should be resolved to improve security.

WHAT AM I AT RISK FOR?

Ransomware - Low

Data Breach - Low

Business Interruption - Low

Financial Fraud - Low

RANSOMWARE COST ESTIMATE

$162K

Calculation based on industry, revenue, and At-Bay data. Try our Ransomware Cost Calculator to estimate the cost of an attack.

at-bay.com/ransomware-calculator

Top Security Issues

❗ Implement a recommended SEG to protect against email-based attacks

A secure email gateway (SEG) is software that protects against phishing and other email-based attacks. Phishing is among the most common methods to initiate a ransomware attack, and an SEG can protect your business by reviewing and blocking malicious emails.

We discovered your organization does not use an SEG on all domains.

Example Domain: topekametro.org, MX Record: topekametro-org.mail.protection.outlook.com.

At-Bay recommendation: Implement a recommended SEG on all email domains to protect against email-based attacks.

For more information, see Email Security.

⬍ Strengthen Microsoft 365 security settings to avoid email compromise.

Due to its popularity, Microsoft 365 is one of the most frequently attacked business technologies. An estimated 13% of all cyber insurance claims result from Microsoft 365 compromises. However, the default security settings on Microsoft 365 can be enhanced by following Microsoft's list of security best practices.

We discovered your email service provider is Microsoft 365.

Example Domain: topekametro.org

At-Bay recommendation: Strengthen your business' security settings for Microsoft 365 to avoid email compromise. We also recommend you review the security configuration on a regular basis to ensure it is always up to date.

For more information, see Email Security.

⬍ Implement a strong password policy to avoid email compromise.

A password policy is an effective way to enforce email password guidelines and keep a business secure. Attackers often use lost or stolen credentials to gain unauthorized access to systems and launch cyber attacks, as more than 50% of all cyber attacks originate from an email-based compromise.

At-Bay recommendation: Implement a strong password policy to prevent attackers from gaining unauthorized access to your employees' email accounts.

For more information, see Access Controls.

HOW SERIOUS IS THE ISSUE?

⛔ **Critical**
Critical issues must be resolved to bind your policy.

❗ **Important**
Important issues may impact your premium or coverage.

⬍ **Moderate**
Moderate issues should be resolved to improve business security.

CASE STUDY

Manitoulin, a small Canadian transportation company, suffered a ransomware attack followed by data exfiltration in 2020. The company claimed it did not believe the hacker had enough information concerning them and decided not to pay the ransom, which resulted in the data leak.

READ FULL STORY

Manitoulin Transport Incident

RECOMMENDED READING

Security Best Practices for Microsoft 365

microsoft.com/microsoft365

How to Implement a Strong Password Policy

at-bay.com/articles/password-policy

Security Details

These materials have been prepared by At-Bay for informational purposes only. All information is provided as is with no guarantee or warranty of any kind, express or implied, concerning the completeness, accuracy, usefulness, and timeliness of the information provided. At-Bay is not responsible for any errors or missions, or for the results obtained from the use of the information provided.

Email Security

01 EMAIL AUTHENTICATION

! Implement a recommended SEG to protect against email-based attacks

We discovered your organization does not use an SEG on all email domains. At-Bay recommends implementing a recommended SEG on all email domains to protect against phishing and other email-based attacks. Look for SEG software with these features: anti-malware, anti-spoofing, data loss protection, sandboxing, secure encryption, and threat intelligence and protection

Learn how to implement an SEG

Higher risk SEG vendor MX records:
Domain: topekametro.org, MX Record: topekametro-org.mail.protection.outlook.com.

02 EMAIL TECHNOLOGIES

Detected email technologies:
office365

◆ Strengthen Microsoft 365 security settings to avoid email compromise.

We discovered your email service provider is Microsoft 365. At-Bay recommends implementing best practices and regular checks to ensure all security controls are properly configured and always up-to-date. In addition, make sure to turn on auditing.

Learn how to turn on auditing for Microsoft 365.

Domains with Microsoft Office 365:
Domain: topekametro.org

03 EMAIL SECURITY

No issues detected.

HOW SERIOUS IS THE ISSUE?

⊖ **Critical**
Critical issues must be resolved to bind your policy.

! **Important**
Important issues may impact your premium or coverage.

◆ **Moderate**
Moderate issues should be resolved to improve business security.

RECOMMENDED READING

Security Best Practices for Microsoft 365
microsoft.com/microsoft365

Remote Access

01 PORTS

No issues detected.

02 VPN

No issues detected.

HOW SERIOUS IS THE ISSUE?

⛔ **Critical**
Critical issues must be resolved to bind your policy.

❗ **Important**
Important issues may impact your premium or coverage.

⁝ **Moderate**
Moderate issues should be resolved to improve business security.

Network Security

01 **DATABASE PORTS**

No issues detected.

02 **OTHER VULNERABILITIES**

No issues detected.

HOW SERIOUS IS THE ISSUE?

⛔ **Critical**
Critical issues must be resolved to bind your policy.

❗ **Important**
Important issues may impact your premium or coverage.

🟡 **Moderate**
Moderate issues should be resolved to improve business security.

Access Controls

01 DATA ENCRYPTION

No issues detected.

02 DATA BACKUPS

No issues detected.

03 PASSWORD MANAGEMENT

🟡 **Implement a strong password policy to avoid email compromise.**
At-Bay recommends implementing a password policy that follows cyber security best practices, such as prompting employees to use special characters and prohibiting dictionary words. We also recommend forcing employees to change their passwords every 3-6 months to minimize the impact of a potential cyber attack, as well as blocking users after multiple failed password attempts to protect against brute force attacks.

Learn how to implement a strong password policy.

HOW SERIOUS IS THE ISSUE?

⛔ **Critical**
Critical issues must be resolved to bind your policy.

❗ **Important**
Important issues may impact your premium or coverage.

🟡 **Moderate**
Moderate issues should be resolved to improve business security.

RECOMMENDED READING

How to Implement a Strong Password Policy

🗋 at-bay.com/articles/password-policy

Website Security

01 CERTIFICATES AND SSL

No issues detected.

HOW SERIOUS IS THE ISSUE?

⛔ **Critical**
Critical issues must be resolved to bind your policy.

❗ **Important**
Important issues may impact your premium or coverage.

🟡 **Moderate**
Moderate issues should be resolved to improve business security.

FAQ

01 **What does my security score mean?**

Your security score reflects the strength of your business' cyber security. Scores range from 0 to 100. A high score means your business already has strong security controls in place, while a low score means the strength of your security can be enhanced.

02 **How was my security score calculated?**

We conduct a non-invasive security scan of your business to collect data from multiple sources. Your security score is based on the findings of our scan. The findings are divided into five categories: ports, vulnerabilities, email, access controls, and website. Each category is scored separately, though some categories are weighted more heavily than others, and the final total is your security score.

03 **What should I do with my security report?**

Please review your security report to see all of the potential issues identified by our security scan. Critical issues (labeled red) must be resolved to bind your policy with At-Bay, while Important and Moderate issues (orange and yellow) are recommended improvements from our security team. We also recommend sharing your security report with relevant team members, such as the Chief Information Security Officer (CISO), security teams, and IT vendors.

04 **What if the security scan missed an issue?**

Your security report only reflects the findings of our security scan, which means the issues are visible from an external view. Your organization may have issues that were not discovered by our scan, and we recommend that you maintain security best practices.

05 **How did you source the case study?**

The case study referenced in your security report was selected based on similarities to your industry and business size. All of our case studies are compiled using publicly available information, and none of the businesses are current At-Bay customers.

06 **What if I need help addressing a security issue?**

We encourage you to first read through our Recommended Reading section, which provides information and instructions on how to resolve the issues. You can also find more support articles in our Broker Knowledge Center. If you require more help or have additional questions, please contact our Security Team.

CONTACT OUR SECURITY TEAM

Security Team
security@at-bay.com

Appendix

01 **GIVEN DOMAINS**

topekametro.org