Cybersecurity Readiness Assessment

Governance & Audit Report No. 2022-4

Issued on July 7, 2022

EXECUTIVE SUMMARY

Background

The FY 2022 Internal Audit Work Plan approved by the Governance and Audit Committee included a review of cybersecurity readiness.

Cybersecurity risk has increased as transit agencies become more automated and data-intensive, with farecard acceptance, passenger counts, centrally aided dispatch, automated vehicle location, signal management and other technologies. Visible threats have included ransomware attacks, phishing attempts, data breaches and network compromises.

Our assessments are performed in accordance with the professional practice standards of the Institute of Internal Auditors. This report was prepared for use by IndyGo's Board of Directors, Governance and Audit Committee, and management.

Objective and Scope

- Obtain an understanding of IndyGo's processes and controls and framework related to managing cybersecurity risk
- Review key processes related to:
  - Threat and vulnerability assessment
  - Phishing and spoofing prevention, including training for employee awareness
  - Data management and protection Project roles and responsibilities
  - External vendor support and reporting
  - Cybersecurity program staffing and associated resources
  - Recently issued TSA Cybersecurity Information Guide
  - Consideration of NIST Cyber Security framework
- Assess the effectiveness of the design and operation of internal controls
- Identify potential opportunities for process and control improvements or revenue enhancement.

We did not perform a deep technical assessment, network scanning or penetration testing as part of this readiness assessment.

Overall Report Rating & Observations
(See Appendix A for definitions)

	Report Rating	Number of Observations by Rating		
		High	Medium	Low
Cybersecurity Readiness	**High**	**1**	**2**	**0**

Overall Summary and Review Highlights

IndyGo has not experienced a significant cyber intrusion resulting in data or monetary loss. Management is aware of industry trends and the Transportation Security Administration's (TSA) recommended cybersecurity measures, and has recently hired an individual to manage IT security and cybersecurity. The IT Department's strategy of moving key applications to the cloud, vs on-premise, has also shifted but not eliminated the risk profile for these applications.

Our following report includes three recommendations. We have rated the overall risk associated with Cybersecurity Readiness as "High." See Appendix A for the report and observation rating definitions.

This rating is based on our observations and the inherent risk and pervasive nature of cybersecurity threats. Our report observations relate to:

- Cybersecurity Plan, and compliance with TSA's recommended cybersecurity measures
- Cybersecurity Monitoring and Detection Tools
- Cybersecurity Policy

We would like to thank IndyGo staff and all those involved in assisting us in connection with the review.

Questions should be addressed to the IndyGo Department of Governance and Audit at: batkinson@indygo.net.

1. Cybersecurity Plan

Observation:	**Recommendation:**	
IndyGo has not adopted TSA's recommended cybersecurity measures, including developing a cybersecurity incident response plan.	Develop a plan and timetable to adopt the TSA's recommended cybersecurity measures, including an incident response plan, and circulate a summary to all employees.	
Observation Rating: High		

The Transportation Security Administration (TSA) issued an Information Circular, effective December 31, 2021, recommending various measures to strengthen cybersecurity across the transportation sector.
 	
The guidance recommends that over-the-road bus operators:
 	
1. Designate a cybersecurity coordinator. IndyGo has recently hired an individual to manage IT security and cybersecurity, but has not reported his name to TSA.
 	
2. Report cybersecurity incidents to TSA within 24 hours. IndyGo has not experienced any cyber events that would require reporting, but has not implemented a process for reporting to TSA.
 	
3. Develop and implement a cybersecurity incident response plan to reduce the risk of an operational disruption. IndyGo has not developed or tested an incident response plan.
 	
4. Complete a cybersecurity vulnerability assessment to identify potential gaps or vulnerabilities in their systems. IndyGo has hired external vendors to annually assess IT security risks, but has not competed the recommended vulnerability assessment using the TSA forms.
	The IT Department is aware of the TSA Circular and recommended cybersecurity practices. IT has also recently hired an individual to manage IT security and cybersecurity.
	
	IT should develop a plan and timetable to fully adopt the TSA's recommended cybersecurity measures.
	
	The TSA recommends that the Cybersecurity Incident Response Plan include measures to:
	• Reduce the risk of operational disruption, through the:
	  ○ Prompt identification and segregation of infected systems, networks and devices
	  ○ Security and integrity of backed up data
	  ○ Established capability and governance
	• Identify individual responsibilities
	• Conduct annual situational exercises
		Management Action Plans:
		
		Now that we have hired our Cybersecurity Coordinator (IT Control Analyst), we have a dedicated resource for constructing and implementing the IndyGo Cybersecurity Plan.
		
		We will develop an agency-wide Cybersecurity Plan incorporating TSA's recommended cybersecurity practices.
		
		Once developed, the plan will be included with our existing Incident Management Plan.
		
		Responsible Parties:
		
		Marcus Burnside, Chief Information Officer, and
		Justin Janik, IT Controls Analyst
		
		Due Dates:
		September 30, 2022

2. Cybersecurity Monitoring and Detection Tools

Observation:	**Recommendation:**	
IndyGo handles their IT and cybersecurity internally, using various commercial tools for network and data protection.	IndyGo could increase its cyber resilience through the use of outside monitoring forms or more robust technology tools	
Observation Rating: Medium		

IndyGo primarily handles their IT and cybersecurity internally. IndyGo has engaged two external firms to perform annual internal and external vulnerability scans and risk assessments. IndyGo has not engaged a firm to provide real-time network monitoring and threat detection.
 	
The IT Department also utilizes various tools for:
 	
• Email and data cybersecurity assessment and quarantining.
• Network vulnerability assessment and threat detection. Our review of the use of one primary tool and its output reports indicated that it:
  ○ Requires manual action to run, rather than automated ongoing detection routines
  ○ Has only been run once recently. If prior IT personnel ran any reports, they were not archived.
  ○ Has additional capabilities which could be deployed. The current testing configuration assessed traditional areas such as password length and reuse, unsupported applications and operating systems, and outdated virus or spyware detection.
  ○ Generated internal vulnerability scan reports which IndyGo followed up on. However, remediation actions and resolutions were not documented. External vulnerability scans were not run. No overall dashboard or incident summary reports are produced.
	IndyGo has not experienced any known cybersecurity incidents resulting in data or monetary loss. However, given the increasing level of threats and attempted intrusions, IndyGo should assess whether the use of an outside vendor and/or a more robust automated threat detection tool is warranted to increase it cyber resilience.
	
	There are multiple tools and providers in the marketplace. IndyGo could consider whether increased protection is warranted.
	
	For example, Security Information and Event Management (SIEM) technology providers support:
	• Security incident management
	• Automated threat detection
	• Compliance reviews
	• Real time logging correlation and analysis
	• Dashboard reporting
		Management Action Plans:
		
		The IT Department utilizes several existing tools, including real-time internal and edge devices monitoring that have dashboards for snapshot views and ad-hoc reports.
		
		We will explore additional monitoring tools to enhance our existing assessment tools.
		
		If this recommendation requires additional funding outside the proposed FY2022 and FY2023 budget, there will be unbudgeted requests submitted to Finance.
		
		Responsible Parties:
		
		Marcus Burnside, Chief Information Officer, and
		Justin Janik, IT Controls Analyst
		
		Due Dates:
		
		Ongoing through March 31, 2023.

3. Cybersecurity Policy

Observation:	**Recommendation:**	
IndyGo has several draft IT polices, but not a specific cybersecurity policy.	Develop a cybersecurity policy. Add a cybersecurity section to add to the overall IndyGo Business Continuity Plan.	
Observation Rating: Medium		
IndyGo has created several policies to guide IT and user behavior and protect IndyGo resources and assets. These include: ○ Acceptable Encryption ○ Equipment Use Agreement ○ Information Resources Use Agreement ○ Password ○ Virtual Private Network ○ Wireless communication ○ Workstation Security The polices are comprehensive and clear. However, most are still in draft form, and have not been fully distributed throughout the IndyGo organization. However, there is not a separate cybersecurity policy. Also, the IndyGo Business Continuity Plan (BCP) does not contain any refences to recovery plans for ransomware, denial of services or other cybersecurity risks.	The IT Department should finalize and issue the draft policies. IT should also create a formal separate cybersecurity policy. This policy could incorporate elements of the "Framework for Improving Critical Infrastructure Cybersecurity" issued by the National Institute of Standards and Technology (NIST), and other resources. The NIST Cybersecurity Framework's core structure is organized around functions, which organize basic cybersecurity activities at their highest level, including: • Identify • Protect • Detect • Respond • Recover The IT Department should also add a cybersecurity section to the overall IndyGo Business Continuity Plan. This section could include guidelines for recovering from potential attacks, such as ransomware or Denial of Service (DOS). Topics could include: • Performance of a periodic Business Impact Analysis • Maintaining of an ongoing third-party risk assessment • Incident response plan • Crisis communication plan, including key contact information to a short list of specialized cybersecurity response vendors	**Management Action Plans:** The IT draft policies have been developed using National Institute of Standards and Technology (NIST) templates and have been under departmental review since Q1 2022. Our IT Controls Analyst will perform the final evaluation of the draft plans before they are submitted to our Chief Policy Officer for enforcement. Although the draft policies contain some language pertaining to cybersecurity, a separate Cybersecurity Policy is warranted. We will develop a separate Cybersecurity Policy in conjunction with the Cybersecurity Plan. **Responsible Parties:** Marcus Burnside, Chief Information Officer, and Justin Janik, IT Controls Analyst **Due Dates:** September 30, 2022.

APPENDIX A – RATINGS DEFINITIONS

Observation Rating Definitions	
Rating	**Definition**
Low	Process improvements exist but are not an immediate priority for IndyGo. Taking advantage of these opportunities would be considered best practice for IndyGo.
Medium	Process improvement opportunities exist to help IndyGo meet or improve its goals, meet or improve its internal control structure, and further protect its brand or public perception. This opportunity should be considered in the near term.
High	Significant process improvement opportunities exist to help IndyGo meet or improve its goals, meet or improve its internal control structure, and further protect its brand or public perception presents. This opportunity should be addressed immediately.
Not Rated	Observation identified is not considered a control or process improvement opportunity but should be considered by management or the board, as appropriate.

Report Rating Definitions	
Rating	**Explanation**
Low	Adequate internal controls are in place and operating effectively. Few, if any, improvements in the internal control structure are required. Observation should be limited to only low risk observations identified or moderate observations which are not pervasive in nature.
Medium	Certain internal controls are either: • Not in place or are not operating effectively, which in the aggregate, represent a significant lack of control in one or more of the areas within the scope of the review. • Several moderate control weaknesses in one process, or a combination of high and moderate weaknesses which collectively are not pervasive.
High	Fundamental internal controls are not in place or operating effectively for substantial areas within the scope of the review. Systemic business risks exist which have the potential to create situations that could significantly impact the control environment. • Significant/several control weaknesses (breakdown) in the overall control environment in part of the business or the process being reviewed. • Significant non-compliance with laws and regulations. • Observations which are pervasive in nature.
Not Rated	Adequate internal controls are in place and operating effectively. No reportable observations were identified during the review.