Internal Audit Department
NeighborWorks® America

Audit Review of

Cyber-Attack Identification and Response

Project Number: NW.ITS.CA-IR.2024

Audit Review of Cyber-Attack Identification and Response

Table of Contents

Function Responsibility and Internal Control Assessment
Audit Review of Cyber-attack Identification and Response

Business Function Responsibility	Report Date	Period Covered
Information & Technology Services	August 13, 2024	From January 1, 2023, to January 31, 2024
Assessment of Internal Control Structure		
Effectiveness and Efficiency of Operations		(b) (5)
Reliability of Financial Reporting		**Not Applicable**
Compliance with Applicable Laws and Regulations		**Not Applicable**

This report was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing.*

[1] **Legend for Assessment of Internal Control Structure: 1. Generally Effective:** The level and quality of the process is satisfactory. Some areas still need improvement. **2. Inadequate:** Level and quality of the process is insufficient for the processes or functions examined and require improvement in several areas. **3. Significant Weakness:** Level and quality of internal controls for the processes and functions reviewed are very low. Significant internal control improvements need to be made.

Executive Summary of Observations, Recommendations and Management Responses

Summarized Observation Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response
Observation 1 Outdated Data Security Incident Response Plan (DSIRP) Internal audit observed that the current DSIRP was last updated September 20, 2019, and was without sufficient detail to apply suitable process management controls accordingly. A review of the Corporations IT Helpdesk ticketing system and the Security Operations Center ticketing system managed by outsourced, third party service providers showed a disconnect in the information presented by both systems. Refer to the **Observations and Recommendations** section below for full details. **Risk Rating**: (b) (5)		**Recommendation 1 Develop and establish an updated Incident Response Plan as well as a Communication Plan integrated into the IRP with annual revisions to the Plan to ensure its relevancy.** Internal Audit strongly recommends the development and establishment of an updated Incident Response Plan and Communication Plan integrated into the IRP with annual revisions to the Plan to ensure its relevancy. Refer to the **Observations and**	Yes	IT&S agrees that the DSIRP needs to be updated. IT&S is working on a Cyber Incident Response document to update and support DSIRP.	12/13/2024	IA accepts management response.

Summarized Observation Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response
		Recommendations section below for full details.				
Observation 2 Disconnect Between Helpdesk Incident Ticketing System and the Security Operations Center (SOC) Ticketing System Managed by Contracted Service Providers A review of the Corporations IT Helpdesk ticketing system and the Security Operations Center ticketing system managed by third party outsourced service providers showed a disconnect in the information presented by both systems. Examples are included.		**Recommendation 2** Internal Audit recommends IT&S integrate SOC practices in all IT support tiers for cybersecurity by adopting a proactive SOC approach to boost their security stance. All IT support teams, from first line to beyond, should consider emulating the SOC team[2]. Refer to the **Observations and Recommendations**	**Yes**	As part of the Security Team Transition Plan IT&S has been conducting weekly security alignment meetings. IT Operations, Enterprise Architecture and the NW IT security team are the attendees. Meeting series started 04/23/2024. The NW IT security team is currently writing a SOP to address cyber incident handling between the Managed Security Service SOC and NW ITSM system.	09/30/2024	IA accepts management response.

[2] *Enhancing Cybersecurity with SOC Practices in IT Support Line May 26 2024* https://www.dunetrails.com/the-cruciality-of-security-operations-center-soc-practices-for-all-it-support-lines/#:~:text=If%20all%20IT%20support%20teams,by%20all%20IT%20support%20teams.

Summarized Observation Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response
Refer to **Observations and Recommendations** section below for full details. **Risk Rating**: (b) (5)		section below for full details.				
Observation 3 Absence of a Properly Defined Service Level Agreement (SLA) Between Corporation and Third-Party Vendor Internal Audit found lack of evidence for vendor deliverables submitted as identified on page 4 in Section D Packaging and Marking in the current contract with the current third-party service provider (b) (5) . Refer to the **Observations and Recommendations** section below for full details. **Risk Rating**: (b) (5)		**Recommendation 3** Internal Audit strongly recommends that IT third-party service level agreements (SLA's) meet the general criteria elements as outlined in the **Observations and Recommendations** section below.	**Yes**	The SLA for incident escalation between the vendor ((b) (5)) and NW IT Security is in the contract.	Completion Date: 07/31/2024	IA accepts management response. IA will review contract for general criteria elements outlined.

Summarized Observation Risk Rating	Management Agreement with Observation (Yes/ No)	Internal Audit Recommendation Summary	Accept IA Recommendation (Yes/ No)	Management's Response to IA Recommendation	Estimated Date of Implementation (Month/Year)	Internal Audit Comments on Management Response
Observation 4 (b) (6) **IT&S Cybersecurity and Information Risk Management team** During the conduct of this review the entire IT&S Cybersecurity and Information Risk Management staff (b) (6) (b) (6) . However critical IT security functions that would mitigate the risk of cybersecurity attacks; managed by outsourced third party vendors remained in place. Internal Audit requested IT&S to provide a transition plan. **Risk Rating**: (b) (5)		**Recommendation 4** Internal Audit recommends that IT&S provide a Quarterly Status Report for the IT&S Cybersecurity and Information Risk Management upon completion of the Transition Plan. Internal Audit also recommends undertaking an assessment of the Transition Plan for its adequacy in continuity of the Corporations IT security.	**Yes**	IT&S will begin providing Cybersecurity status updates quarterly starting in Q4 FY24. Transition plan was provided to Internal Audit in April 2024. Also, (b) (6) as our IT Security Managed vendor.	09/30/2024	IA accepts management response. IA plans to conduct an evaluation of the Transition Plan as a follow up to this review.

Risk Rating Legend

Risk Rating: High
A serious weakness which significantly impacts on the Corporation from achieving its corporate objectives, financial results, statutory obligations, or that may otherwise impair the Corporation's reputation.

Risk Rating: Moderate
A control weakness which could potentially undermine the effectiveness of the existing system of internal controls and/or operational efficiency, integrity of reporting and should therefore be addressed.

Risk Rating: Low
A weakness identified which does not seriously detract from the system of internal control and or operational effectiveness/efficiency, integrity of reporting but which should nonetheless be addressed by management.

Management Responses to The Audit Review of: Cyber-attack Identification and Response		
# Of Responses	**Response**	**Recommendation #**
4	Agreement with the recommendation(s)	4
0	Disagreement with the recommendation(s)	0

Background

Cyber Security risks continue to be a top area of concern for many organizations and the recent reporting of high-profile cyber security incidents have only heightened the need for secure and resilient systems in the event of such an attack or incident. The most common incidents are phishing, ransomware, and social engineering which can put data and systems at risk. Considering the importance of Cyber Security risks for Corporations and the heightened attention, Internal Audit scheduled a review of the Corporation's readiness, as it relates to a Cyber security related risk event. This audit report is focused on the review of the Corporation's cyber incident detection and response protocols and capacity *before, during,* and *after* a confirmed or suspected cybersecurity incident during a one-year period between 01/01/2023 and 01/31/2024.

Objective

The objective of this review was to obtain reasonable assurance on the effectiveness of the corporation's cybersecurity incident management focusing on the policies, protocols, processes, and procedures surrounding cyber threats detection and response capabilities including compliance with company polices and applicable industry regulations.

Scope Limitations:

The introductory meeting for this project was commenced on 03/01/2024 and during the course of the review the (b) IT&S Cybersecurity and Information Risk Management team (b) (6) on April 10, 2024. Internal Audit (IA) was formally informed of this event on April 15, 2024, and causing a disruption of the review, whereupon IA requested that IT&S provide a transition plan. The IT Security Team Transition Plan was subsequently made available on April 19, 2024.

As a result, this audit was limited to reviewing the Corporation's Data Security Incident Response Plan (DSIRP) in place at the time, Penetration Test results performed and provided between 01/01/2023 and 12/31/2024 by a third-party security service provider, and service desk ticketing systems of both the Corporation and third-party security service provider. It did not include an examination of IT controls, operational processes, or interviews of the IT Cyber Security team (critical to the assessment) (b) (6) staff referenced above. As a result, the observations and subsequent recommendations below are based on the procedures performed within this limited scope. This audit scope limitation may impact the report's completeness or accuracy.

The list of observations below was compiled prior to the disbanding of the IT&S Cybersecurity and Information Risk Management team and receipt of the IT Security Team Transition Plan.

Methodology

This review was an operational/compliance review conducted in accordance with the following risk management framework, models, and principles to perform our verification and validation procedures:

- The IIA IPPF Standards *2201 Planning and Coordinatio*n and *2050 Coordination and Reliance*,
- APO12.06 Respond to Risk of COBIT 2019 Framework
- ISO/IEC 27001 standard
- CIS Controls
- NIST Cybersecurity Framework 2.0[3]
- Guidelines published by America's Cyber Defense Agency *Cybersecurity and Infrastructure Security Agency (CISA)*[4]
- Internal Audit pre-audit survey questionnaire.

Our audit review was performed focusing on the following documents provided by the cybersecurity team in response to Internal Audit's pre-audit survey questionnaire before the entire team was disbanded:

- Aligned objectives:
    - Security elements in the security incident response plan DSIRP are aligned with the enterprise's strategic objectives.
    - In the event of a security incident, the proposed actions in DSIRP support achievement of the enterprise's strategic objectives.
- Applicable Legal & Regulatory Compliance Requirements: current requirements in place include, but are not limited to:
    - General Data Protection Regulation (GDPR)
    - Payment Card Industry Data Security Standard (PCI DSS)
    - US Federal Information Security Management Act (FISMA)
- Incident Security Framework: the corporation uses a formal framework from CIS Controls as the foundation of its security incident management program to ensure program effectiveness.
- Risk Analysis/Assessment: IT&S has contracted a third-party vendor service to implement a formal methodology for assessing security incident risk and associated consequences.
- Prior Incidents: Incident identification, notification and response processes are in effect and adhere to the enterprise's cybersecurity plan DSIRP.
- Verification and validation of security information data captured during audit period in the organization's ticketing system Remedyforce managed by the IT&S Service Desk.

[3] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
[4] https://www.cisa.gov/topics/cybersecurity-best-practices

Below are the observations and recommendations that resulted from the limited procedures performed.

Observations and Recommendations

Observation 1 Outdated Security Plan DSIRP (Data Security Incident Response Plan)

Internal audit observed a lack of a current and formal Security Incident Response Plan Management in place to provide a roadmap for implementing the security incident response capability as defined by the Corporation's mission, size, structure, functions, strategies, and goals that would minimize disruptions through quick resolution of user queries and incidents (COBIT® 2019, DSS02 *Managed Service Request and Incidents*).

The plan currently in place was last updated on September 20, 2019, which was the last modification date recorded in the Revision History section in the plan. The processes and procedures defined therein were high level without sufficient details to apply suitable process management controls accordingly.

In addition, the following baseline elements are currently not included in the plan:

- A lack of prescribed change management protocols to assess and communicate how change will impact the corporation, employee expectations, and training needs; there is also a lack of a clear transition to the new protocol.
- No evidence that a postmortem review has been regularly performed to report lessons learned (Page 12, Section 1.9 F Post Incident Activity (Lessons Learned) in DSIRP).
- COBIT requires a sufficiently integrated tools and technologies portfolio to mitigate business risks and decrease costs (COBIT 2019, DSS05.07[5]) Currently, there is (b) (5) [redacted].
- Lack of a risk analysis component inclusive of asset valuation and prioritization as security processes.
- A security incident can be costly, and the absence of an updated Incident Response Plan can escalate both direct costs (expenditures associated with containment, eradication, forensic analysis, and fines) and indirect costs (potential damage to the organization's reputation and opportunities lost from not pursuing business relationships) of the Corporation.

[5] COBIT 2019 DSS05.07: Manage vulnerabilities and monitor the infrastructure for security-related event.

Recommendation 1

Internal Audit strongly recommends the development and establishment of an updated Incident Response Plan and **Communication Plan** integrated into the IRP with annual revisions to the Plan to ensure its relevancy. The IRP should have incorporated in part a definition of the incident types to enable staff discern an actual security incident; the composition of the incident response team including their roles and responsibilities. It should also include a cybersecurity list of key people who may be needed during a crisis. The communication plan should provide the protocol for communicating issues related to the cyber incident event; inclusive of the crisis team as first responders, internal communications, reporting requirements to external entities (law enforcement or regulatory agencies); external and customer communications (by General Counsel and Public Relations).

Internal Audit recommends IT&S follow best practice guidance for establishing IRP basics[6].

Observation 2 Disconnect Between IT Helpdesk Ticketing System and Security Operations Center (SOC) Ticketing System Managed by Third Party Security Service Providers

A review of the Corporations IT Helpdesk ticketing system and the Security Operations Center ticketing system managed by third party outsourced service providers showed a disconnect in the information presented by both and in addition the following discrepancies were observed:

- Incident Types are not aligned/in compliance with the most current cybersecurity attack vectors available[7]. Not keeping the attack vectors up to date with the industry potentially places the organization in a vulnerable security position.
- According to Appendix F in the current DSIRP, when a potential incident is reported, a service ticket will be created for review. Between 1/1/2023 and 1/31/2024, forty percent (40%) of the closed security-related incident tickets in Remedyforce[8] (IT&S Helpdesk Ticketing System) were missing root cause and resolution (closure) information (107 out of 272 tickets). This contradicts the protocol defined in the current DISRP resulting in incomplete information data in the system or records of Remedyforce.
- After performing data comparison between the monthly penetration test reports and Remedyforce during the audit period, Internal Audit also noticed that security-related incidents captured in the SOC ticketing system are without equivalent, corresponding tickets created in the Remedyforce System in accordance with the DSIRP protocol.
- There is a lack of evidence that incident details, sensitive information of the incident (root cause analysis), and a trail of its access are logged on the management tool.

---

[6] NIST guidance: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final; CISA guidance: https://www.cisa.gov/uscert/ncas/current-activity/2021/11/16/new-federal-government-cybersecurity-incident-and-vulnerability

[7] *Potential Threat Vectors to 5G Infrastructure* published by CISA.GOV at https://media.defense.gov/2021/May/10/2002637751/-1/-1/0/POTENTIAL%20THREAT%20VECTORS%20TO%205G%20INFRASTRUCTURE.PDF

[8] Remedyforce is the IT helpdesk ticketing system employed by IT&S to handle IT Service Management, such as Incident and Problem Management, IT Asset Management, Change Management and Service Catalog. The system is a product built on the Salesforce platform called 'Force', and marketing utilized the name Remedy, another IT Service management tool offered by the same vendor, to try to give it market share, hence the name Remedyforce.

- Lack of evidence for any known response/actions taken from previous test results, inclusive of the strategic/remediation recommendations made by the service providers;
- Lack of evidence for incident reporting and escalation documents. Copies of these documents are not available for verification and validation.
- Lack of evidence of a formal process regarding incident details, sensitive information of the incident (root cause analysis), and a trail of history records showing how many times the system or website was accessed as detected by the vulnerability assessment management tool.

Recommendation 2

Internal Audit recommends IT&S integrate SOC practices in all IT support tiers for cybersecurity by adopting a proactive SOC approach to boost their security stance and in alignment with the incident information entered into the two different ticketing systems. The question of how the Corporation manages IT Response Team is crucial, therefore, all IT security support teams, from the first line of defense and beyond, should consider emulating some of the relevant SOC best practices outlined as follows:

- **Treating cybersecurity as a shared responsibility in IT support** by fostering a security-first culture to narrow the skills gap,
- **Continuous monitoring**: All security teams, regardless of their IT support line, should establish a system for continuous network activity monitoring to identify anomalies or potential threats.
- **Intelligence Response Plan**: Teams should have a clear, well-practiced plan in place to respond to security incidents, from identifying the problem to recovering from it and preventing future occurrences.
- **Regular training and updates**: Regularly cybersecurity training sessions will keep teams abreast of the latest threats and response strategies.
- **Threat Intelligence**: Proactive gathering, analysis and application of threat intelligence can help teams understand new vulnerabilities and protect against potential threats[9].
- **Communication and Collaboration**: Encouraging open communication and collaboration can ensure everyone's active participation in maintaining security and swift identification and neutralization of threats.

Observation 3 Absence of a Properly Defined Service Level Agreement (SLA) Between Corporation and Third-Party Security Service Provider.

Internal Audit found lack of evidence for produced vendor deliverables as identified on page 4 in Section D Packaging and Marking in the current contract with the third-party service provider (b) (5) [redacted]. For instance, Internal Audit was unable to obtain evidential deliverables specified in the contractual agreement with the third-party security service provider. Some of the missing deliverables are identified below:

[9] https://www.dunetrails.com/the-cruciality-of-security-operations-center-soc-practices-for-all-it-support-lines/

- Threat hunt activity and discovery reports
- Weekly threat intelligence report and advisories
- Vulnerability scan program roadmap
- Security Health Assessment
- Playbook development
- Monthly firewall rule review
- Configuration assessment.

As result, Internal Audit was unable to perform the verification and validation testing as part of this review.

Recommendation 3

Internal Audit strongly recommends that IT third-party service level agreements (SLA's) meet the following criteria elements in general:

- Define clear service scope of work – Specify services to be provided with the Corporations expectations
- Service availability and Uptime – Define the required times of availability including uptimes and consequences for non-compliance
- Response and Resolution times – Specify response times for incident reporting, requests, and their corresponding resolution times
- Performance Metrics – Define metrics to measure performance such as mean time to resolve (MTTR) and mean time between failures (MTBF)
- Security and Data Privacy – provide expectations around data security and privacy
- Communication and Reporting – Define communication channels, the frequency and report content including incident reports and performance reports
- During the course of the review, the entire IT&S Cybersecurity and Information Risk Management team (b) (6) on April 10, 2024. Internal Audit (IA) was formally informed of this event on April 15, 2024, and causing a disruption of the review, whereupon IA requested that IT&S provide a transition plan. The IT Security Team Transition Plan was subsequently made available on April 19, 2024.
- and disputes ensuring alignment with the Corporations Incident Response Pan
- Regular reviews and revisions to the SLA to ensure continued relevancy and effectiveness
- Termination and exit clause – Define conditions for termination of agreement and Dispute Resolution

Observation 4 [redacted] IT&S Cybersecurity and Information Risk Management team

During the conduct of this review the entire IT&S Cybersecurity and Information Risk Management staff was disbanded [redacted] on April 10, 2024 and formally informed of this event on April 15, 2024. However critical IT security functions that would mitigate the risk of cybersecurity attacks; currently outsourced to two third party vendors remained in place. Internal Audit requested IT&S to provide a transition plan which was subsequently made available on April 19, 2024.

Recommendation 4

Internal Audit recommends that IT&S provide a Quarterly Status Report for the IT&S Cybersecurity and Information Risk Management upon completion of the Transition Plan.

Internal Audit also recommends undertaking an assessment of the Transition Plan for its adequacy in continuity of the Corporations IT security.

Conclusion

"Cyber threats are expected to still be a major risk into 2030. With global cybercrime expected to jump 15% per year and its annual impact predicted to hit $10.5 trillion by 2025 …'[10] In spite of the limited procedures undertaken there is still the need for an updated Incident Response Plan in combination with a communication plan to ensure the Corporations readiness in the event of a Cyber security incident. Internal audit also plans to monitor and conduct an evaluation of the Transition plan to further supplement the above referenced recommendations.

We would like to take the opportunity to thank members of the IT&S Division for their cooperation on this review.

[10] The Institute of Internal Auditors (IIA) 2024: Cybersecurity Is More Than an IT Issue — Does Your Board Know How to Manage the Dangers? (theiia.org)