city of CINCINNATI
Interdepartmental Correspondence Sheet

Date: January 4, 2021

To: Paula Boggs Muething, City Manager

From: Lauren Sundararajan, CFE, Internal Audit Manager

Copies to: Internal Audit Committee
Christopher A. Bigham, Assistant City Manager
Jeff McCord, ETS Interim Director

Subject: **Remote Work Cyber Risk Audit**

Attached is the Remote Work Cyber Risk audit report. The primary objective of this performance audit was to assess whether IT governance and security controls were adequate for remote operations and the impact of increased demand during a pandemic environment. This audit was conducted in accordance with the current audit agenda.

We would like to thank the management and staff of ETS for their assistance and cooperation during this audit.

If you need any further information, please contact me.

Attachment

Remote Work Cyber Risk Audit

January 2021

Lauren Sundararajan, CFE
Internal Audit Manager

Pam King
Senior Internal Auditor

Jennifer Sherman
Senior Internal Auditor

Table of Contents

Executive Summary 1

I. Introduction 2
- Background
- Audit Selection
- Audit Objective
- Audit Scope and Methodology
- Statement of Auditing Standards
- Commendations

II. Audit Findings and Recommendations 4

III. Conclusion 14

IV. ETS Department Response 15

Executive Summary

Internal Audit (IA) conducted a performance audit of Enterprise Technology Solution's (ETS) Remote Work Cyber Risk. The primary objective of this performance audit was to assess whether Information Technology (IT) governance and security controls were adequate for remote operations and the impact of increased demand during a pandemic environment.

The mission of the ETS department is to ensure the availability of citywide technology applications and infrastructures and enable the procurement and implementation of innovative, secure, and cost effective technology and business solutions through collaborative partnerships with all City of Cincinnati (City) departments, inclusive governance, and effective security policy administration. Due to the Covid-19 pandemic in the spring of 2020, there was an accelerated shift in City employees working remotely. As more employees shifted from the office to remote work, this raised concerns regarding the risks of cyber-attacks as end users pose the greatest risk to securing City IT assets and data.

IA identified several issues in the documentation of remote access security policies. The current Internet Security Policy (ISP) does not explicitly address remote access processes while working from home and security controls that should be in place. There is also a lack of documented and established succession planning for key personnel roles. As a result, sudden personnel changes could significantly compromise internal control systems that oversee cyber security risks.

I. Introduction

Background

The mission of the ETS department is to ensure the availability of citywide technology applications and infrastructures and enable the procurement and implementation of innovative, secure, and cost effective technology and business solutions through collaborative partnerships with all City departments, inclusive governance, and effective security policy administration. ETS manages and maintains the city's metropolitan area fiber optic and wireless business network (MAN), central data center, cybersecurity, Human Resources (HR) and financial systems, law enforcement data systems, geographic information systems, and a central IT help desk. ETS also leads citywide IT governance, procurement, and annual IT capital project request activities and partners with IT resources in other city departments to facilitate and coordinate IT service delivery citywide.

Due to the Covid-19 pandemic in the spring of 2020, there was an accelerated shift in City employees working remotely. As more employees shifted from the office to remote work, this raised concerns regarding the risks of cyber-attacks as end users pose the greatest risk to securing City IT assets and data.[1] According to a cybersecurity reported issued by McKinsey and Company, "the digital response to the COVID19 crisis has also created new security vulnerabilities. Attackers seek to exploit the gaps opened when telecommuting employees use insecure devices and networks."[2] The Department of Defense has also warned of cyber risks. "Organizations spend enormous effort creating a secure IT environment to protect their network and data. The moment employees relocated from the office to their homes for work, much of the secure environment is bypassed and a host of new exposure points opened."[3]

With the increased telework capability and increased cyber threats, ETS personnel must not only maintain heightened awareness, but also need the tools to effectively monitor and respond to any cyber security threats. According to ETS, their incident response logging platforms are currently decentralized. There is advanced technology available that would allow ETS to consolidate these platforms allowing for a more efficient response in the event of a cyber security attack, however budgetary constraints have not allowed them to step into a stronger cybersecurity posture.

[1] Ninety percent of cyber data breaches were caused by user error last year, according to analysis of data from the UK's Information Commissioner's Office (ICO) by the cyber security awareness and data analytics company, CybSafe.
[2] "A dual cybersecurity mindset for the next normal." Mckinsey and Company. July 2020.
[3] "Evolving Cyber Risks in a Covid-19 World." Toby DeRoche, Institute of Internal Auditors. 2020.

Audit Selection
IA conducted this audit in accordance with the Audit Work Plan.

Audit Objective
The primary objective of this performance audit was to assess whether IT governance and security controls were adequate for remote operations and the impact of increased demand during a pandemic environment.

Audit Scope and Methodology
In order to achieve the objective, IA reviewed current IT security practices surrounding remote access to the City's networks and assets. The time frame of the audit was determined by the sample size required to provide reasonable assurance of statistical accuracy of the impending analysis. IA compared the City's remote work security practices to relevant City policies and industry standards, sought verification of procedures through documented reports, interviewed staff, calculated statistics of relevant data and reviewed authorization documentation for multiple systems.

Statement of Auditing Standards
As required by the Cincinnati Administrative Code Article II §15, this audit was conducted in accordance with the Generally Accepted Government Auditing Standards (GAGAS), except for standard 5.90 pertaining to external peer review requirements. This exception did not have a material effect on the audit.

IA continues to conduct internal quality reviews to assure the conformance with applicable GAGAS. IA performed the fieldwork between July of 2020 and October of 2020.

Commendations
IA commends the staff of the ETS department for their cooperation throughout the audit.

II. Audit Findings and Recommendations

A remote access work from home policy has not been established and documented.

Comprehensive IT security policies and procedures assist management with providing direction to staff and are a key component of internal controls. In Version 3.0.1 of ETS' ISP there is a section devoted to remote access, however, it does not explicitly address remote access processes while working from home and security controls that should be in place.

The lack of comprehensive policies increases the likelihood of lapses in security controls when remote users are not fully educated of best practices. According to the National Institute of Standards and Technology's (NIST) *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*, "major security concerns include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, and the availability of internal resources to external hosts."[4]

Recommendation 1: ETS should work with the HR department to develop a comprehensive policy that defines remote access requirements and addresses how to configure devices and home networks to mitigate risks associated with cyber-attacks.

Department Response: Agree. ETS, IT Governance, HR, and CMO should collaborate on a policy that addresses the technology, security, and workforce risk factors for a comprehensive remote/home policy.

Lack of documented and established succession planning for key personnel roles.

Succession planning is the process of identifying internal personnel with the ability to fulfill key roles within an organization and fostering the development of these individuals. As personnel turn over, a succession plan facilitates business continuity. Succession planning is also particularly significant in our current pandemic climate as the City has offered early retirement in order to navigate a significant budget deficit. As a result, more than 20 ETS employees are eligible with many representing key personnel roles. These roles include a significant amount of institutional knowledge and multiple decades of work experience at ETS. IA was informed that although ETS does have some informal succession planning drafts that are primarily in a memo format, there is no formal plan in place. Consequently, sudden personnel changes could significantly compromise internal control systems that oversee cyber security.

Recommendation 2: Management should develop and document a detailed succession plan for key personnel roles.

Department Response: Agree. ETS and CMO are working on a TO plan and identifying key resources to help address succession planning.

[4] "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security." NIST Special Publication 800-46 Revision 2. July, 2016.

Interdepartmental coordination efforts need improving.

As established by Administrative Regulation 74, the Executive IT Leadership Committee provides IT governance in order to ensure that oversight and approval processes of all City IT functions were equitably distributed among City departments.[5] Through interviews, IA sought to review the effectiveness of the committee and interdepartmental coordination efforts. IA found that although some departments expressed that this does remediate communication issues that arise from a decentralized model of IT functions, other departments believe that it still does not adequately represent City departments. IA was also informed that communication with ETS was lacking. This included efforts from departments to offer input in coordinating resolutions to challenges and arising issues. Some departments also felt as though their concerns are never considered.

In an effort to increase coordination efforts, ETS has been trying to establish monthly meetings with department directors to discuss IT needs and concerns. Additionally, IA was notified at the pre-fieldwork stage of this audit that ETS has been trying to establish a policy framework that would include conducting department assessments and how their cyber risks can be incorporated into this framework. However, IA was informed that monthly meetings have still not occurred and a policy framework along with department assessments has not been established or documented. With a large portion of the City's workforce currently conducting business remotely, the lack of coordination across City departments could allow for significant variation among cybersecurity priorities and lead to duplication in processes as well as weaknesses in security controls.

Recommendation 3: Implement monthly meetings with department directors to ensure that IT needs and concerns are adequately addressed.

Recommendation 4: Implement regular assessments of each department to determine how their cyber risks can be incorporated into a policy framework.

Department Response: Agree. Beginning November 2020 ETS has held monthly or bi-monthly meetings with all City departments leadership teams, to address funding, projects, support, and any other IT needs.

[redacted]

[5] "Administrative Regulation No. 74." City of Cincinnati. Revised December, 2016.

[redacted]

[redacted]

[redacted]

[redacted]

Oversight of the Scorecard needs improvement.

ETS utilizes an internally developed platform called the Scorecard to track various patches and updates on all City IT assets and devices. The Scorecard is configured to pull data from the City's AD and KACE to display the status of needed patch and update deployments per device per department. ETS recommends that the Scorecard should be reviewed daily. However, ETS indicated that departments and their corresponding IT liaisons are not doing this and are only reviewing the Scorecard when a problem is realized.

In response, IA interviewed multiple City departments and was informed that the Scorecard often displays inaccurate data and can include devices that have been previously decommissioned. When asked how this may occur, ETS responded that departments and their respective IT service desks are responsible for ensuring the information reported on the Scorecard is accurate as far as displaying active devices that are on the City's domain.

Regardless, the reliance on departments to accurately stay up to date and report issues with their department IT assets creates a gap in ownership of the data that is displayed. This further creates opportunities for unreliable data that could lead to lapses in security controls when needed patches and updates are not properly accounted for.

Recommendation 14: Ensure that all departments are reviewing the Scorecard daily and reporting any errors or issues in a timely manner.

Recommendation 15: Provide sufficient oversight of the Scorecard to ensure that all data is as accurate as possible. This may include increasing coordination efforts with departments and regularly conducting IT asset audits.

Department Response: Agree. ETS and City departments should review the scorecard daily and work together to verify accuracy and resolve any issues.

[redacted]

[redacted]

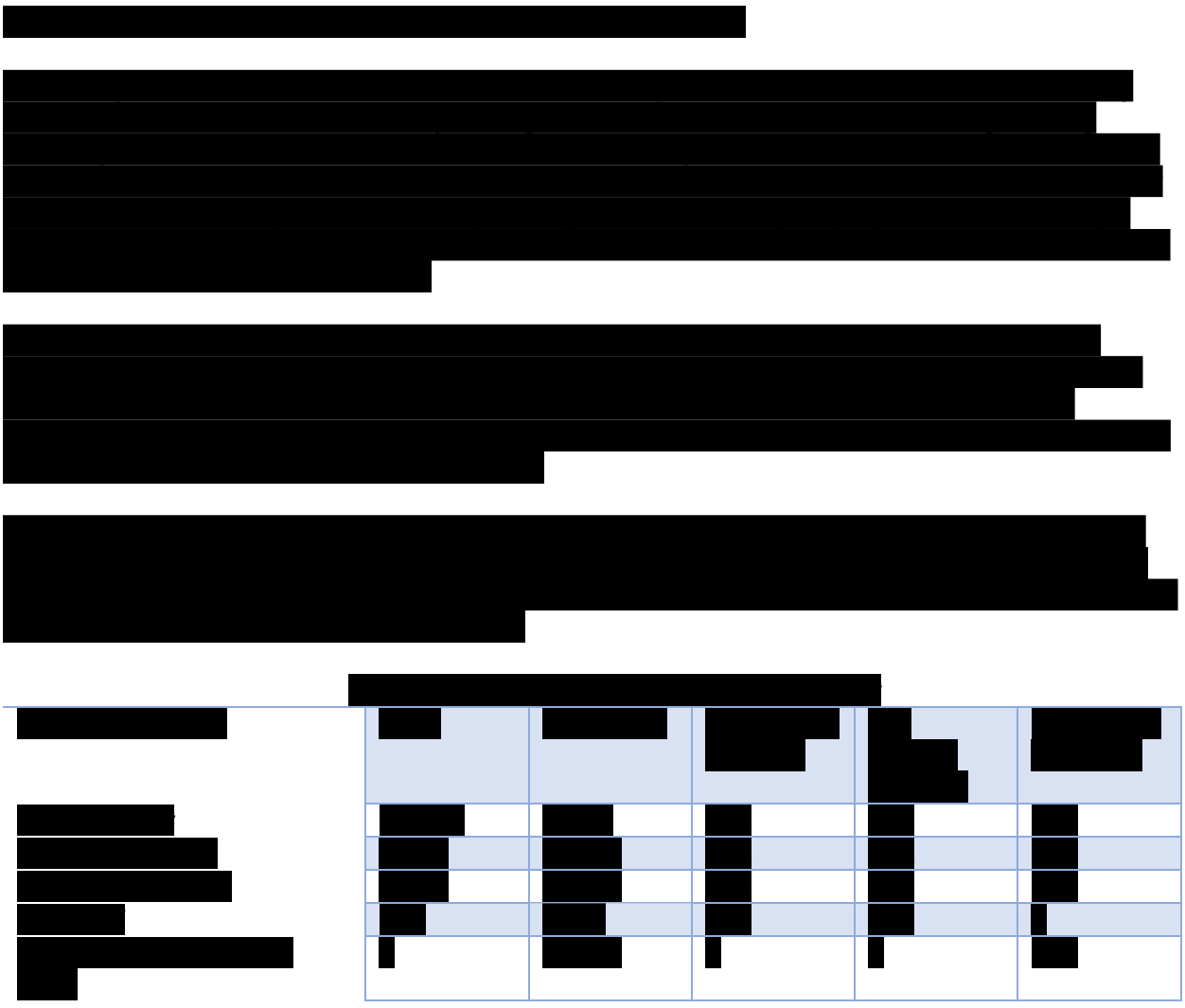
Key performance indicators have not been adequately established and documented.

In addition to limited reviews of audit logs and established guidelines for incident handling, ETS currently does not have established and documented key performance indicators (KPI) for

identifying operational trends and inefficiencies surrounding malware and phishing incidents. Instead, they rely on high level KPIs which are not documented. Regardless, using high-level or minimal KPIs does not fully capture opportunities for mitigating risks in addition to assisting personnel in identifying operational trends and efficiencies. For example, the use of data driven KPIs could provide further examination into the effectiveness of the security controls of IT systems and the impact of anti-virus incidents.

Recommendation 19: Develop measurable KPIs to expand the tracking of remote access risks and cyber security attacks that would assist staff in examining operational trends.

Department Response: Agree. ETS is updating the ISP, filling vacant positions, and have requested additional CIP funds to help Cybersecurity projects and controls for 2021.

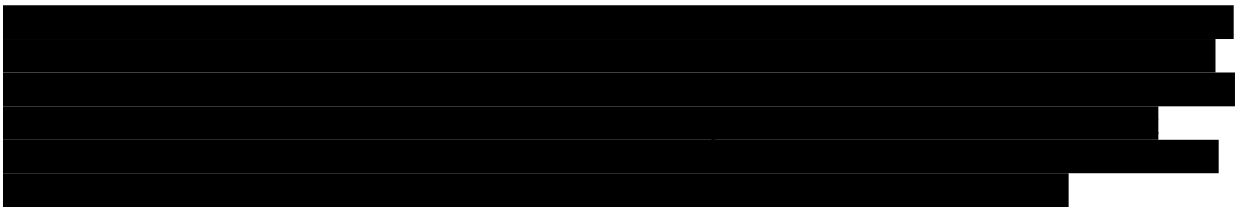


[redacted]

[redacted]

III. Conclusion

Internal Audit conducted a performance audit of Enterprise Technology Solution's Remote Work Cyber Risk. The primary objective of this performance audit was to assess whether IT governance and security controls were adequate for remote operations and the impact of increased demand during a pandemic environment. The audit revealed several opportunities for improvement in ETS' security controls.



IV. ETS Department Response

Recommendation 1: ETS should work with the HR department to develop a comprehensive policy that defines remote access requirements and addresses how to configure devices and home networks to mitigate risks associated with cyber-attacks.

Department Response: Agree. ETS, IT Governance, HR, and CMO should collaborate on a policy that addresses the technology, security, and workforce risk factors for a comprehensive remote/home policy.

Recommendation 2: Management should develop and document a detailed succession plan for key personnel roles.

Department Response: Agree. ETS and CMO are working on a TO plan and identifying key resources to help address succession planning.

Recommendation 3: Implement monthly meetings with department directors to ensure that IT needs and concerns are adequately addressed.

Recommendation 4: Implement regular assessments of each department to determine how their cyber risks can be incorporated into a policy framework.

Department Response: Agree. Beginning November 2020 ETS has held monthly or bi-monthly meetings with all City departments leadership teams, to address funding, projects, support, and any other IT needs.

[redacted]

[redacted]

Recommendation 14: Ensure that all departments are reviewing the Scorecard daily and reporting any errors or issues in a timely manner.

Recommendation 15: Provide sufficient oversight of the Scorecard to ensure that all data is as accurate as possible. This may include increasing coordination efforts with departments and regularly conducting IT asset audits.

Department Response: Agree. ETS and City departments should review the scorecard daily and work together to verify accuracy and resolve any issues.

[redacted]

Recommendation 19: Develop measurable KPIs to expand the tracking of remote access risks and cyber security attacks that would assist staff in examining operational trends.

Department Response: Agree. ETS is updating the ISP, filling vacant positions, and have requested additional CIP funds to help Cybersecurity projects and controls for 2021.

[redacted]

[redacted]

[redacted]

[redacted]