STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2023-074
December 2022

RANSOMWARE CONTROLS

At Four Selected School Districts

Sherrill F. Norman, CPA
Auditor General

Superintendents

The table below shows the four school districts included in the scope of this information technology operational audit and the respective superintendents who served during the period April 2021 through March 2022.

District	Superintendent
Desoto	Dr. Bobby Bennett
Escambia	Dr. Timothy A. Smith
Indian River	Dr. David K. Moore
Pasco	Kurt S. Browning

The team leader was Joseph Garcia, CISA, and the audit was supervised by Heidi Burns, CPA, CISA.

Please address inquiries regarding this report to Heidi Burns, CPA, CISA, Audit Manager, by e-mail at heidiburns@aud.state.fl.us or by telephone at (850) 412-2926.

This report and other reports prepared by the Auditor General are available at:

FLAuditor.gov

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 · 111 West Madison Street · Tallahassee, FL 32399-1450 · (850) 412-2722

RANSOMWARE CONTROLS

At Four Selected School Districts

SUMMARY

This operational audit focused on evaluating selected information technology (IT) controls applicable to the prevention and mitigation of ransomware for the data and critical infrastructure at four selected school districts.[1] Our operational audit disclosed the following:

Finding 1: Security awareness training programs for the Desoto and Pasco County School Districts need improvement to reduce the risk for district data to be compromised.

Finding 2: Certain district IT security controls related to authentication, account management, data recovery, configuration management, vulnerability management, and data protection need improvement to ensure the confidentiality, integrity, and availability of district data and IT resources.

BACKGROUND

Ransomware is a type of malicious software, or malware, that prevents access to computer files, systems, or networks. Using ransomware, an attacker encrypts an organization's data and demands payment as a condition of restoring access to that data. A ransomware attack may also be used to steal an organization's confidential and sensitive data and demand payment as a condition of not disclosing the data to the public. Although the methods ransomware uses to gain access to an organization's information and systems are broadly common to other cyberattacks, ransomware attacks differ from other cybersecurity events by threatening an immediate impact on business operations and attempting to force a ransom payment. The option to not pay rests with management's ability to successfully restore operations following an attack.

According to the *2022 Verizon Data Breach Investigations Report*,[2] ransomware breaches increased 13 percent during the 2022 calendar year, which is greater than the combined increases over the past 5 years. Key trends that continue in the distribution of ransomware include phishing e-mails, unpatched systems, supply chain attacks, double extortion, and ransomware as a service.

In addition, Sophos' *The State of Ransomware 2022* [3] reported that 66 percent of the responding 5,600 cross-sector organizations were victims of ransomware in 2021, marking an increase of 37 percent. Of the respondents representing lower education, 56 percent reported a ransomware attack and, of the respondents representing higher education, 64 percent reported a ransomware attack. Consequently, as a combined sector, 60 percent of education respondents reported ransomware attacks.[4] Previously,

[1] From the 67 school districts in the State, we judgmentally selected the Desoto, Escambia, Indian River, and Pasco County School Districts to obtain an understanding of school district ransomware controls.

[2] The Verizon *Data Breach Investigations Report* is an annual publication providing analysis of information security incidents reported from organizations world-wide with a focus on data breaches.

[3] The Sophos security software company (Sophos) annually commissions a study of real-world ransomware experiences of IT professionals across multiple industries and representing multiple countries.

[4] The 60 percent with ransomware attacks comprised 56 percent of 320 lower education organizations and 64 percent of 410 higher education organizations.

according to *The State of Ransomware 2021* report, education was a top target for ransomware at a 44 percent attack rate. Although, according to *The State of Ransomware 2022* report, ransom payment typically enabled some data return, only 4 percent of organizations received all data back and, on average, only 61 percent of the data was restored.

Cyber insurance may be used as a means for recoverability, but as *The State of Ransomware 2022* report notes, it has also been a driver for increased cyber defense. A tightening cyber insurance market has resulted in challenges to securing coverage, including increasing standards for qualification, costs, and policy complexity. In response to the market changes, 97 percent of organizations that have cyber insurance have made changes to their cyber defense to improve their cyber insurance position. Our survey of 38 Florida county school districts disclosed that 22 districts purchased cyber insurance during the 2021-22 fiscal year at an average cost of $47,284. Twelve of the 38 districts purchased ransomware insurance at an average cost of $17,751 and the other 4 districts had not purchased either type of insurance coverage.[5] One district reported a claim in the amount of $637,000 for the 2021-22 fiscal year.

The *Center for Internet Security* (*CIS*) *Critical Security Controls*® (*CIS Controls*®) identifies ransomware as one of the top five most prevalent attack types and details foundation safeguards that provide a prioritized path for improving an organization's cybersecurity posture. To defend against ransomware attacks, *CIS Controls*® lists management and control of software assets, data protection, secure configuration of enterprise assets and software, account management, access control management, continuous vulnerability management, malware defenses, data recovery, and security awareness and skills training.

Because of the continued threat of ransomware and noted prevalence of education as a targeted sector, school district preparedness for preventing and responding to ransomware attacks is critical. Accordingly, we evaluated the effectiveness of ransomware controls at four selected school districts: the Desoto County School District (Desoto), Escambia County School District (Escambia), Indian River County School District (Indian River), and Pasco County School District (Pasco). The four school districts are part of the State system of public education under the general direction of the Florida Department of Education and are governed by State laws and State Board of Education rules. Geographic boundaries of each district correspond with those of the applicable county. A district school board (Board) is the governing body for each of the school districts. Each Board is composed of five elected members with the Superintendent of Schools serving as the Executive Officer of the Board. Table 1 shows, for the 2021-22 fiscal year, the number of district-operated schools and centers, charter schools, and reported unweighted full-time equivalent (FTE) students.

[5] For the 34 districts that purchased insurance during the 2021-22 fiscal year, cyber insurance premiums ranged from $4,608 to $375,000 with a median premium cost of $24,591 and ransomware insurance premiums ranged from $4,136 to $59,031 with a median premium cost of $12,149.

Table 1

Number of District Schools Operated and FTE Count by Selected District

For the 2021-22 Fiscal Year

District	Schools and Centers	Charter Schools	FTE
Desoto	11	-	5,719
Escambia	64	5	46,118
Indian River	27	5	20,355
Pasco	92	12	91,752

Source: Florida Department of Education.

FINDINGS AND RECOMMENDATIONS

Finding 1: Security Awareness Training

A comprehensive security awareness training program instructing all employees on the importance of preserving the confidentiality, integrity, and availability of data and information technology (IT) resources entrusted to them is a foundational control for security vigilance and a district's prevention and mitigation of ransomware. An effective security awareness program includes identification of the specific knowledge, skills, and abilities needed to support district security and educates all employees about how to interact with data and IT resources in a secure manner.

As part of our audit, we examined applicable Board policies, district procedures, and district records supporting employee security awareness and skills training. We found that policies had been established and procedures implemented to generally mitigate security awareness training concerns at the Escambia and Indian River School Districts. However, we also found that security awareness training programs for the Desoto and Pasco County School Districts need improvement. Specifically, we found that:

- The Desoto County School District had not conducted security awareness training since the District ended use of an online learning platform in 2020 and District procedures had not been established to require training for all employees. According to IT management at the District in February 2022, the District began evaluating new processes for security awareness training using vendor-developed content. However, as of August 2022, a comprehensive, mandatory security awareness training program had not been established.
- The Pasco County School District provided ransomware and other security-related incident training for help desk staff, online training resources for employees explaining Internet usage and e-mail security best practices, and ad-hoc training for employees targeted by phishing messages. However, as of April 2022, the District had not established a comprehensive, mandatory security awareness training program. In response to our inquiry, Pasco management indicated that District procedures had not been established to require training for all employees.

Effective security awareness training programs include authentication and data handling best practices, sessions to recognize social engineering attacks, instructions to understand causes of unintentional data exposure, guidance for recognizing and reporting security incidents, and a requirement that all employees receive security awareness training. The lack of a comprehensive, mandatory security awareness

training program increases the risk that employees may compromise the confidentiality, availability, and integrity of district data and IT resources.

Recommendation: To reduce cybersecurity risks, Management at Desoto and Pasco County School Districts should establish a comprehensive, mandatory security awareness training program to ensure that employees are aware of their responsibilities and the importance of securing District data and IT resources.

Finding 2: Security Controls – Authentication, Account Management, Data Recovery, Configuration Management, Vulnerability Management, and Data Protection

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. In conducting this audit, we evaluated security controls identified by *CIS Controls*® to defend against ransomware attacks, including security controls related to access control management (authentication); account management; data recovery; management and control of software assets, secure configuration of enterprise assets and software, and malware defenses (configuration management); continuous vulnerability management (vulnerability management); and data protection. Our audit procedures disclosed that certain security controls related to authentication, account management, data recovery, configuration management, vulnerability management, and data protection need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the confidentiality of district data and related IT resources. However, we have notified appropriate management at each of the four school districts of the findings in the areas needing improvement identified in Table 2.

Table 2

Areas Needing Improvement by District

(One Finding Noted for Each Area)

District	Areas for Improvement
Desoto	- Authentication - Account Management - Data Recovery - Configuration Management - Vulnerability Management - Data Protection
Escambia	- Authentication - Account Management - Configuration Management
Indian River	- Authentication - Account Management - Data Recovery - Configuration Management - Vulnerability Management - Data Protection
Pasco	- Authentication - Account Management - Configuration Management - Data Protection

Without appropriate security controls related to authentication, account management, data recovery, configuration management, vulnerability management, and data protection, there is an increased risk that a ransomware attack will compromise the confidentiality, integrity, and availability of District data and related IT resources.

Recommendation: Management at each of the four school districts should improve applicable IT security controls to ensure the confidentiality, integrity, and availability of district data and IT resources.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this information technology (IT) operational audit from December 2021 through September 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected significant Desoto County School District (Desoto), Escambia County School District (Escambia), Indian River County School District (Indian River), and Pasco County School District (Pasco) IT controls applicable to prevention and mitigation of ransomware for District data and critical infrastructure during the period April 2021 through March 2022, and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives were:

- To determine the effectiveness of selected significant IT controls in achieving management's objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the IT systems included within the scope of the audit, deficiencies in management's internal controls that were significant to our audit objectives; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT systems included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding

of and evaluating the IT systems and related significant controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, waste, abuse, or inefficiency.

In conducting this audit, we:

- Reviewed applicable laws, rules, district procedures, and other guidelines; interviewed district personnel; and examined district records to obtain an understanding of district operations related to ransomware protection and mitigation and to determine whether district operations were designed properly and operating effectively.
- Evaluated the sufficiency of district controls, observed, documented, and tested key processes, procedures, and controls related to district IT processes for ransomware prevention and mitigation, including inventory and control of software assets, data protection, system configuration, authentication and account management, vulnerability management, data backup and recovery, and security awareness training.
- Evaluated district procedures and examined selected records to determine the adequacy of district procedures for maintaining a software asset inventory and ensuring only authorized software is installed on the network.
- Evaluated the effectiveness of district data protection controls, including data identification and classification and procedures for data handling, storage, and transmission.
- Evaluated the effectiveness of district configuration management controls, including establishing and maintaining secure configurations; disabling insecure protocols, implementing firewalls or port filtering to protect network resources, and timely applying software updates and managing device end-of-life.
- Examined selected security settings related to district network infrastructure, externally facing applications, remote access systems, and other critical servers and databases to determine whether authentication controls were configured and enforced in accordance with IT best practices, including the use of multi-factor authentication.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges within the four default network administrator system groups for district root domains. Specifically, we examined and evaluated applicable account access privileges as of:
    - February 10, 2022, for Desoto.
    - December 17, 2021, for Escambia.
    - February 10, 2022, for Indian River.
    - December 9, 2021, for Pasco.

- Evaluated district procedures for reviewing dormant accounts.
- Evaluated policies and procedures for scanning, analysis, and remediation of identified vulnerabilities and examined selected scan reports to determine the effectiveness of district vulnerability management controls.
- Evaluated district procedures and examined selected reports to determine the adequacy of district malware defense.
- Examined and evaluated select district patch management controls for operating systems and network devices to ensure secure configurations are maintained. Specifically, we examined and evaluated for:
    - Desoto, the 16 server and computer operating systems and 2 selected critical network devices.
    - Escambia, the 15 server and computer operating systems and 2 selected critical network devices.
    - Indian River, the 12 server and computer operating systems and 2 selected critical network devices.
    - Pasco, the 7 server and computer operating systems and 2 selected critical network devices.
- Evaluated district procedures and examined select backup testing reports to determine the adequacy of the district data recovery procedures to restore district IT assets to a pre-incident trusted state.
- Evaluated the effectiveness of district security awareness training programs.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE

The School District of DeSoto
Dr. Bobby Bennett
Superintendent

December 16, 2022

Ms. Sherrill F. Norman, CPA
Auditor General, State of Florida
Claude Denson Pepper Building, Suite G74
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman,

The School District of Desoto County is happy to respond to the preliminary and tentative audit findings for the information technology operational audit of the Desoto County District School Board, Ransomware Controls. Our response to the findings are listed below:

Finding 1: Security Awareness Training
Recommendation: To reduce cybersecurity risks, Management at Desoto and Pasco County School Districts should establish a comprehensive, mandatory security awareness training program to ensure that employees are aware of their responsibilities and the importance of securing District data and IT resources.

Response: The School District of Desoto County management agrees with this recommendation and is in process of evaluating resources to implement a mandatory training program for all staff.

Finding 2: Security Controls
Recommendation: Management at each of the four school districts should improve applicable IT security controls to ensure the confidentiality, integrity, and availability of district data and IT resources

Response: The School District of Desoto County management agrees with this recommendation and has taken corrective action to continue to improve security controls in the mentioned Areas for Improvement.. Additionally, The School District of Desoto County will continue to evaluate the ever-changing technology, systems, and softwares to ensure the continued security, confidentiality, and integrity of the data housed by The School District of Desoto County.

Sincerely,

Bobby Bennett

Post Office Box 2000 Arcadia, Florida 34265
Telephone: 863.494.4222 x1000
bobby.bennett@desotoschools.com

THE SCHOOL DISTRICT OF ESCAMBIA COUNTY
75 NORTH PACE BOULEVARD
PENSACOLA, FL 32505
PH (850)432-6121 FX (850)469-6379
http://escambiaschools.org
TIMOTHY A. SMITH, Ed.D., SUPERINTENDENT

December 16, 2022

Ms. Sherrill F. Norman, CPA
Auditor General
111 West Madison Street
Tallahassee, FL 32399-1450

Subj: Preliminary and Tentative Audit Findings and Recommendations for the Information Technology Operational Audit of the Escambia County District School Board--Dated November 21, 2022

Dear Ms. Norman:

The District is committed to protecting our students' and staffs' privacy through maintaining strong privacy and security protections. The privacy and security of this information is a significant responsibility, and we value the trust of our students, parents, and staff. The District is committed to protecting data and will continue to improve security controls to do so.

Below is the District's response to the preliminary and tentative audit findings for the Information Technology Operational Audit dated November 21, 2022.

Finding 1: Security Awareness Training

N/A

Finding 2: Security Controls

The District will continue to improve the identified IT security controls to ensure the confidentiality, integrity, and availability of district data and IT resources.

Sincerely,

Timothy A. Smith

TAS/TI/dh

School District of Indian River County

6500 57th Street • Vero Beach, Florida, 32967 • Telephone: 772-564-3000 • Fax: 772-564-3054

David K. Moore, Ed.D. - Superintendent

December 13, 2022

Sherrill F. Norman
Auditor General
111 West Madison Street
Claude Pepper Building, Suite G74
Tallahassee, FL 32399-1450

Dear Ms. Norman,

We are pleased to respond to the preliminary and tentative audit findings and recommendations concerning Ransomware Controls for Indian River County District School Board. In accordance with your request, our response to findings is listed below:

Finding 2: Security Controls

Recommendation: Management at each of the four school districts should improve applicable IT security controls to ensure the confidentiality, integrity, and availability of district data and IT resources.

Management's Response: School District in Indian River management agrees for the need for improvement in the following areas: Authentication, Account Management, Data Recovery, Configuration Management, Vulnerability Management, and Data Protection. Indian River School District has begun implementing security controls and drafting policy to address recommendations.

If you have any questions regarding this information, please feel free to contact us at (772) 564-3180.

Sincerely,

David K. Moore, Ed.D.
Superintendent of Schools
Indian River County School Board

Pasco County Schools
Kurt S. Browning, Superintendent of Schools
7227 Land O' Lakes Boulevard • Land O' Lakes, Florida 34638

December 9, 2022

Ms. Sherrill F. Norman, CPA
Auditor General
Claude Denson Pepper Building, Suite G74
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Ms. Norman,

The purpose of this letter is to respond to the preliminary and tentative findings resulting from your information technology operational audit of the Pasco County District School Board, Ransomware Controls.

The District concurs with the two (2) preliminary and tentative findings received. Below is a response/corrective action plan for each finding, which is provided by finding number.

Finding 1:
The Pasco County School District will modify and update the existing security awareness training course to include authentication and data handling best practices, examples on how to recognize social engineering attacks, instructions to understand causes of unintentional data exposure, and guidance for recognizing and reporting security incidents where those aspects are not currently covered in the existing course. Additionally, the Pasco County School District will setup a mechanism to require and track that all employees receive this security awareness training.

Finding 2:
The Pasco County School District has addressed the confidential findings in the areas found to be in need of improvement.

We appreciate the opportunity to respond to these findings.

Sincerely,

Kurt S. Browning
Superintendent of Schools

xc: Kevin Shibley, Assistant Superintendent for Administration
Nicholas Funaro, Director of Technology and Information Services
Christopher L. Jackson, Senior Manager of Technology and Information Services
Carolyn McGriff, Director, Internal Audit

(813) 794-2000 • (352) 524-2000 • (727) 774-2000 • www.pascoschools.org