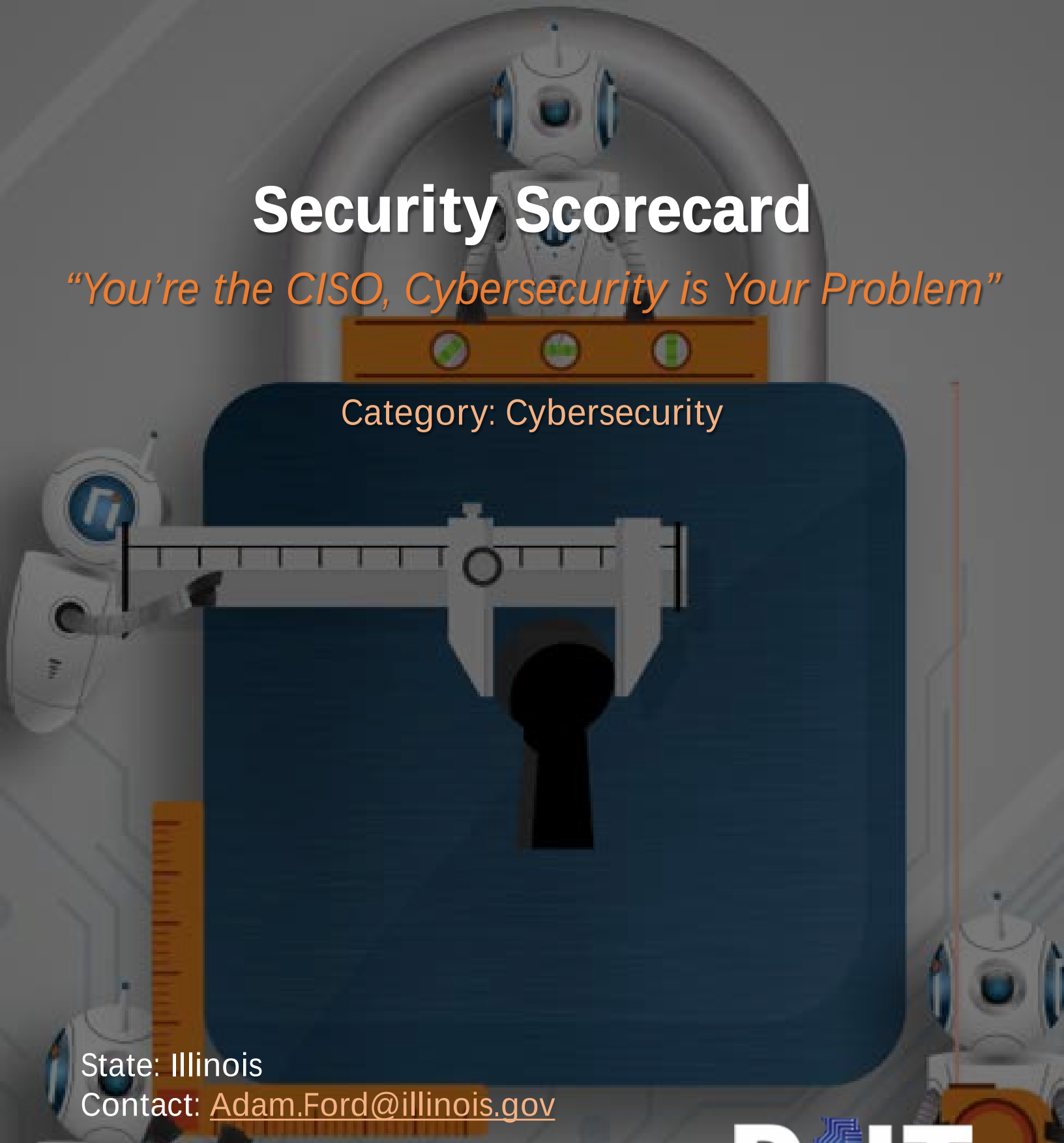
Security Scorecard

"You're the CISO, Cybersecurity is Your Problem"

Category: Cybersecurity



State: Illinois

Contact: Adam.Ford@illinois.gov

Initiation Date: 2020 October

End Date: Project Continues

DoIT

Illinois Department of Innovation & Technology

EXECUTIVE SUMMARY

Robert Frost tells us that "[g]ood fences make good neighbors" in his poem "Mending Wall." The parties on seemingly opposite sides of the structure have different perspectives and responsibilities, but both hold a common interest to come together to maintain the wall. Akin to the wall in the poem, operation of a successful state government information security program requires the active participation of both the Chief Information Security Officer (CISO) and state agency directors to ensure that IT systems are operated securely and are available to meet agency needs. In a consolidated IT state, the division of responsibility between the CISO and agency director can seem blurred. Treating cybersecurity solely as an IT problem and ignoring the agency responsibilities as system owners is a recipe for failure.

To be effective, the relationship between the CISO and agency directors needs to include objective, business-friendly metrics that are commonly understood and used to make business decisions. It is imperative to demystify cybersecurity risk by avoiding jargon and having a shared perspective on the shared risks. The Security Scorecard was developed as a quarterly report for each agency director that provides clear actionable information related to that agency's specific security posture. The Security Scorecard is used as a baseline for further conversations between the CISO and agency directors.

IDEA

The State of Illinois consolidated agency IT functions in 2018 and created a Statewide CISO within the Department of Innovation & Technology (DoIT) to oversee information security. DoIT operates thousands of IT systems in support of state agency programs that serve the residents of Illinois. Consolidation allows the State to reap the rewards of standardization, specialized expertise, and facilitation of a unified approach to the operation of information security technology.

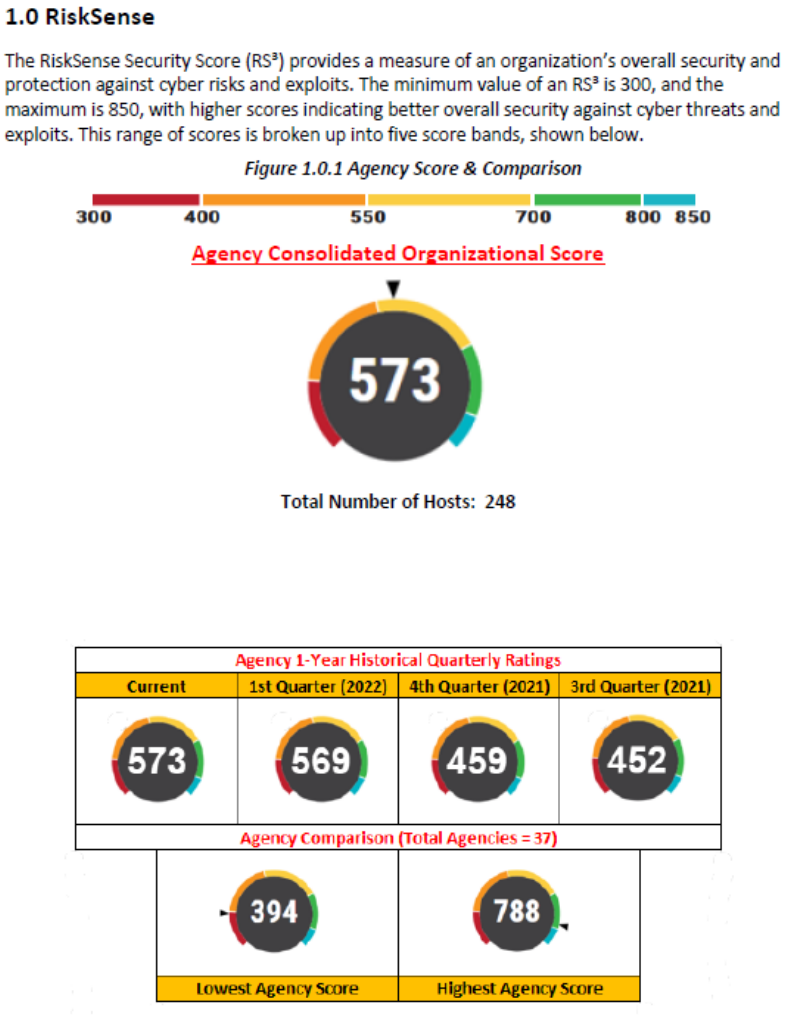
Cybersecurity does not exist in a vacuum. Successful programs require executive sponsorship and cooperation from state agency directors. Although the CISO is responsible for the operation of the security tools that protect agency applications, it is agency directors who have responsibility for their programs, and, by extension, what applications and systems must be operated to enable these programs. Protecting these systems requires collaboration between the CISO and the agency directors. For this relationship to be productive, the CISO must be positioned to effectively communicate the key risks to each agency's systems, the business and financial obstacles faced to mitigate these risks, and agency user behavior that might be increasing these risks, in an objective, business-friendly manner.

DoIT developed the Security Scorecard idea to provide a quarterly report to state agency directors of the key risks and security challenges at their agency. While not comprehensive, the Scorecard provides objective, actionable information to the agency director from the CISO and serves as a basis for conversations between the CISO and agency director.

IMPLEMENTATION

The Security Scorecard is a clear, though incomplete, snapshot of each agency's security posture. Updated Security Scorecards are provided quarterly so progress or regression can be made visible. The items included in the Scorecard are selected because they are both objective and actionable by an agency director. Some of the actions a director might need to take include things such as making a budget request to replace an outdated system, reminding employees of their responsibility to report phishing emails, and ensuring that HR is providing offboard notices in a timely fashion so that user accounts are disabled at separation.

The Scorecard is laid out in five sections, each covering a critical and measurable aspect of the agency's cybersecurity posture. The first section consists of a RiskSense score, similar to a FICO score, that represents the health of the agency's servers. The CIO serving each state agency provides summaries of the efforts underway or roadblocks related to applications that are responsible for the five lowest scoring servers.



(NOTE: This graphic is for demonstration purposes only and does not contain actual Illinois data.)

The second section discusses resiliency and disaster recovery plans for applications identified as critical to agency business functions through the Business Impact Analysis process. Ideally, resiliency plans should be completed for each critical application.

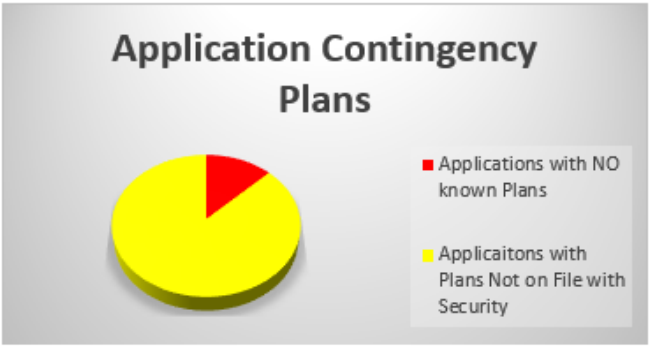
2.0 Critical Applications Contingency Planning

Below outlines the critical applications supporting critical business functions surrounding the first 8 hours of an business impact event.

Table 2.0.1 Critical Applications

Application Name & Description	Critical Business Functions App Supports	Plan on File in Security
Critical Client Systems System utilized by Central Office and Caseworkers to determine new application eligibility	General Counsel, Home Services, Placement Clearance/Leads, Business Analytics and Information Systems, Business Services, Management, Research and Analysis	NO
Medical Dispensary System Supports the distribution of all medications	Business Analytics and Information Systems, Clinical, Admin and Program Support, Hospital Operations, State Operated Developmental Centers, Business Analytics and Information Systems	NO
Medical Data Information System Provides on-line access to specific clinical information	Clinical, Admin and Program Support, Hospital Operations,	NO
Rations Control System Tracks the inventory used.	Admin Support, Clinical	NO KNOWN PLAN EXISTS
Accounting System Accounts Payable and has a general non-recipient Accounts Receivable	Clinical, Admin and Program Support,	NO

Figure 2.0.2 Agency Applications Contingency Plans



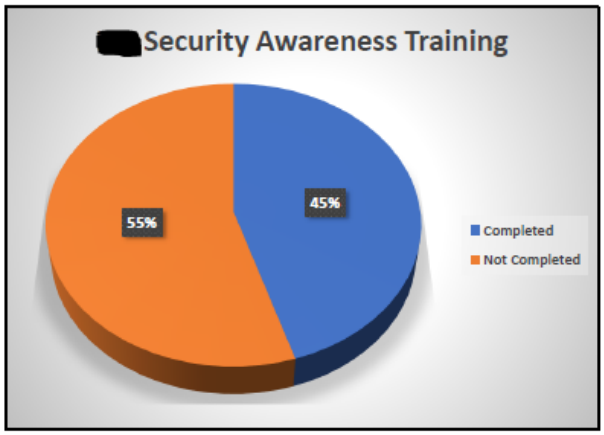
CIO Comments:
We have just completed the BIA process and are working to update existing DR plans and build new plans where they are missing.

The third section is related to security awareness training compliance and agency user performance on proactive phishing campaigns conducted during the quarter.

3.0 End User Risk

3.1 Security Awareness Training

Figure 3.1.1 2021 Security Awareness Compliance as of March 30, 2022

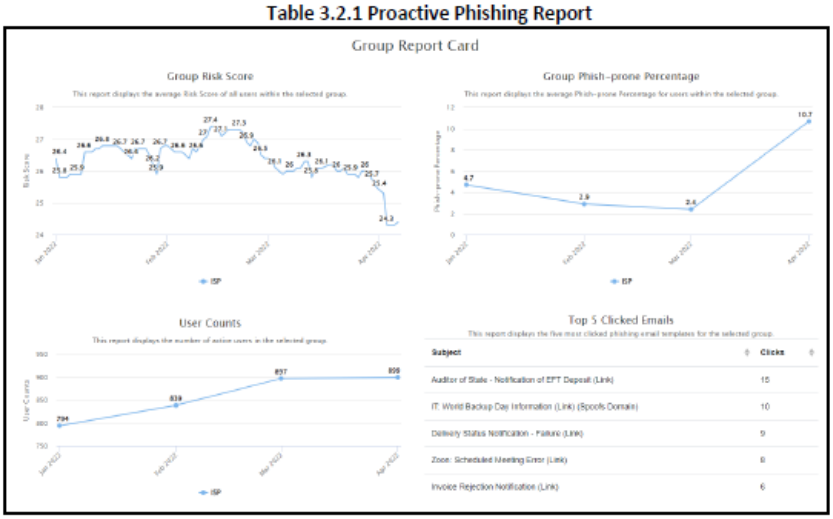


Important note about the figure above. This figure does not take into consideration if the agency has started their training period, which is determined by the agency. Training periods are decided at the agency level to help guide compliance. Overall compliance is determined at the end of the calendar year when security awareness training is legally due.

3.2 Proactive Phishing Reports

Proactive phishing is an anonymous and nonpunitive indicator of opportunities for training, education, and culture building for all State of Illinois employees. This is designed to help users detect threats at work AND at home (where they don't have a team dedicated to helping them detect and overcome the threat landscape.) Through this report card we can track the effectiveness of proactive phishing campaigns over time.

Table 3.2.1 Proactive Phishing Report



The figure above demonstrates the change in user behavior over the course of the current year. Fluctuations up and down are completely normal, while a downward trend is preferable, an upward trend indicates that Security Awareness may want to increase targeted training for specific scenarios to build knowledge, trust, and foster a culture of security.

Section four describes the CISO's view of the completeness of agency-specific policies, procedures, and roles that the agency needs to implement to address the agency responsibilities being audited by the Office of Auditor General during compliance audits.

4.0 Agency Specific Cyber Security

Table 4.0.1 Agency Specific Cyber Security

	Completed	Date
Security Roles and Responsibilities has been performed and documented	Yes	04/01/2021
Formal Risk Assessment has been performed	Yes	01/25/2019
Formal Business Impact Analysis has been performed	Yes	12/13/2021

Section five contains the responsiveness and results from the monthly Human Resources account validation process. In this monthly process, employee user accounts that have been unused for 60 days are flagged and HR is asked to validate the current employment status of the users. This process is a necessary check for accounts that have not been properly offboarded at the time of employee separation.

5.0 Off-boarding of Users and Logins

Monthly a report is compiled of user accounts which have not be used within the past 60 days. To reconcile and remove accounts no longer in use, we notify agency HR teams to advise if these users have separated and can be removed.

Table 5.0.1 Agency Response & Count of Users Off-boarded to Remove

2021	Responded	Offboarded
April	Yes	22
May	Yes	42
June	Yes	73
July	Yes	60
August	Yes	16
September	Yes	21
October	Yes	11
November	No	13
December	No	9
2022		
January	Yes	63
February	Yes	8
March	Yes	20

IMPACT

The Security Scorecard has been wildly successful. There has been significant improvement by state agencies in the areas measured and reported on in the Security Scorecard. The number of unsupported systems has greatly decreased, employee performance at agencies on proactive phishing campaigns has improved, and compliance audit findings at agencies have been reduced.

The overall impact to the State's security culture has been far greater than just improvements to the categories in the report. The Security Scorecard serves as a conversation topic between agency directors, the CISO, and the DoIT Secretary using a common language that easily translates into actionable tasks that will directly improve the agency and the State's security posture. Some state agency directors meet with the CISO team monthly or quarterly to discuss the performance of their agency and to seek guidance on how to improve. The Scorecard demystifies cybersecurity, provides a framework for agency directors to openly communicate risks at their agency, and helps them understand how the decisions they make about their programs impact the State's cybersecurity posture.

State agency directors utilize the information provided in the Scorecard to make budget requests for system upgrades and more frequently engage the CISO early in the acquisition process. Security Scorecards are also frequently referenced by agency directors when discussing their agency's cybersecurity posture when testifying in legislative committees. Usage of the Scorecards has not only enabled data-driven decision making related to cybersecurity risk, but has also converted agency directors from passive customers into vocal advocates for modernization and increased security efforts statewide.