MOODY'S
INVESTORS SERVICE

SPECIAL SERIES Global Cyber Risk Issuer Surveys

SECTOR IN-DEPTH
24 April 2024

Send Your Feedback

TABLE OF CONTENTS

Contacts

Dmitriy Plit +1.646.947.9944
AVP-Analyst
dmitriy.plit@moodys.com

Yoni Katz +1.212.553.3492
Ratings Associate
yoni.katz@moodys.com

Rachael Royal McDonald +1.212.553.4456
Associate Managing Director
rachael.mcdonald@moodys.com

Susan Fitzgerald +1.212.553.6832
Managing Director
susan.fitzgerald@moodys.com

Steven Libretti +1.212.553.1826
AVP-Cyber Credit Risk
steven.libretti@moodys.com

Lesley Ritter +1.212.553.1607
SVP-Cyber Credit Risk
lesley.ritter@moodys.com

State Housing Finance Agencies – US

HFAs lead in cyber governance, match public finance peers in other measures

Summary

Housing Finance Agencies' (HFA) strengths and weaknesses in cybersecurity mostly mirror those of the public finance sector as a whole, according to our 2023 cyber survey. HFAs' small staff size relative to other public enterprises allows them to have more agile cybersecurity operations than other sectors, but leads to less robust long-term planning. While HFAs are less likely to have multiyear road maps for managing cyber risk, they have a regular cadence of cyber briefings to chief executives, engage their employees in cybersecurity education, and conduct extensive vendor exposure reviews. Looking ahead, HFAs plan to increase their funding for cybersecurity, and maintain or enhance their cyber insurance policies.

» **HFA cybersecurity personnel reports directly to senior executives.** Given their smaller size relative to other enterprises in the public finance sector, HFAs typically have fewer dedicated cybersecurity personnel. But this leaner structure has a benefit: it allows their cybersecurity experts to report directly to chief executives.

» **Cybersecurity occupies a larger share of HFA technology budgets than in 2019.** HFAs continue to invest in cybersecurity and will maintain the same cyber insurance coverage level in the near future. Furthermore, they allocate more of their technology budget to cybersecurity than they did four years ago.

» **Basic cyber hygiene practices are now standard.** While HFAs, along with their public finance peers, have high adoption of basic cyber hygiene practices, more advanced protection measures, such as penetration testing or tabletop simulations, are less frequent.

» **Most surveyed HFAs always conduct third-party vendor reviews to assess cybersecurity risks.** While HFAs are less likely to have multiyear road maps or strategies for managing cyber risk than other entities in the public sector, they are also more likely to review new and existing vendors' products for cybersecurity risks.

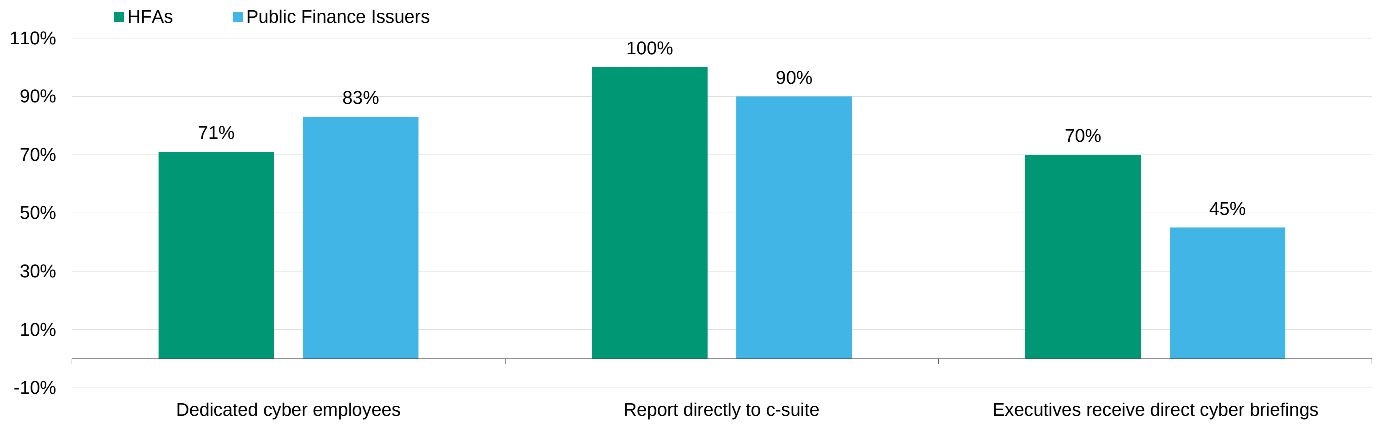
We conducted a survey of HFAs to assess their cybersecurity in the context of their governance, organizational structure, operations and risk transfer policies, and we received responses from 18 agencies. These HFAs vary in size from $50 million to nearly $4 billion in terms of outstanding debt. Their median debt outstanding was slightly below $1.5 billion, indicating that the responding agencies are generally smaller than other larger public finance enterprise issuers.

HFA cybersecurity personnel reports directly to senior executives

HFAs' small size compared with public enterprises often means they have fewer dedicated cybersecurity staff. Approximately 71% of surveyed HFAs have employees whose primary responsibility is cybersecurity, compared with 83% of public finance issuers. Despite having fewer dedicated cybersecurity employees, HFAs' leaner structure allows those employees more direct and more frequent access to agency executives to brief them on cybersecurity developments (see Exhibit 1).

Exhibit 1

Most HFAs have dedicated cyber employees who report directly to senior executives at least monthly



Source: Moody's Ratings

This direct line of communication can lead to more efficient decision-making. When cybersecurity managers report directly to the CEO or other executives, their insights and recommendations can be addressed promptly, and any necessary changes can be implemented more swiftly. This flexibility can allow HFAs to tailor their cybersecurity strategies to match their specific needs, resources and risk profiles and to enhance their overall cybersecurity posture.

However, despite tight reporting lines between HFA cybersecurity staff and executives, only a small number of CEOs have their financial compensation tied to their agency's cybersecurity performance. Inclusion of cyber performance metrics in CEO compensation can serve as an incentive for prioritizing cyber preparedness across an organization. Only 13% of HFA CEOs have cyber performance as part of their compensation package, lower than the 17% average for all reporting public finance issuers.

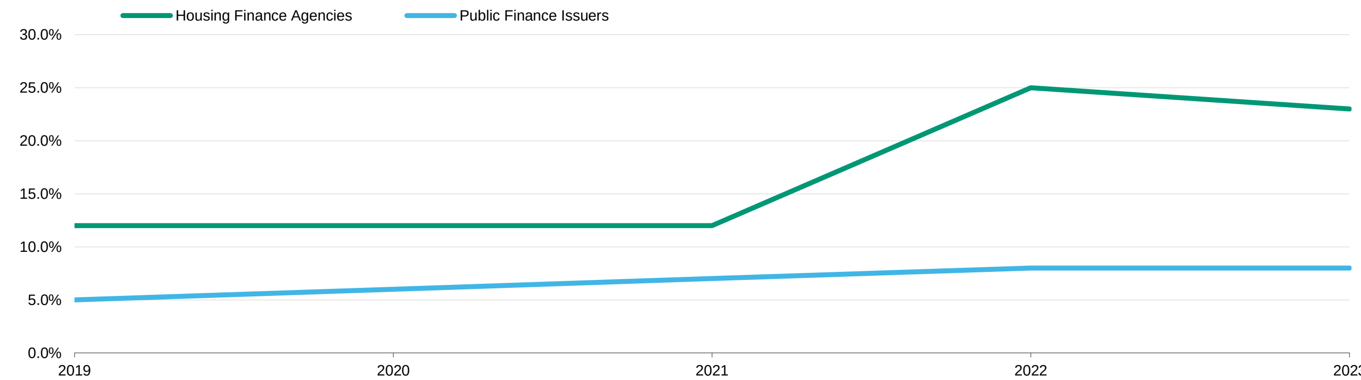
Cybersecurity occupies a larger share of HFA technology budgets than in 2019

Housing Finance Agencies are now allocating a larger share of their technology budget to cybersecurity than four years ago – 23% in 2023 compared with 12% in 2019 – outpacing their counterparts in the public finance sector. In public finance overall, cyber budget as a percentage of IT was 8% in 2023 (see Exhibit 2). However, in terms of total spending, HFAs significantly increased their cybersecurity spending by 39% from 2019 to 2023, but they are trailing their public finance peers, which posted a 60% increase in cyber spending over the same period.

Exhibit 2

HFAs have ramped up cybersecurity investment as a percentage of IT spending since 2021, outpacing other public finance issuers

Cyber investment as a percentage of IT

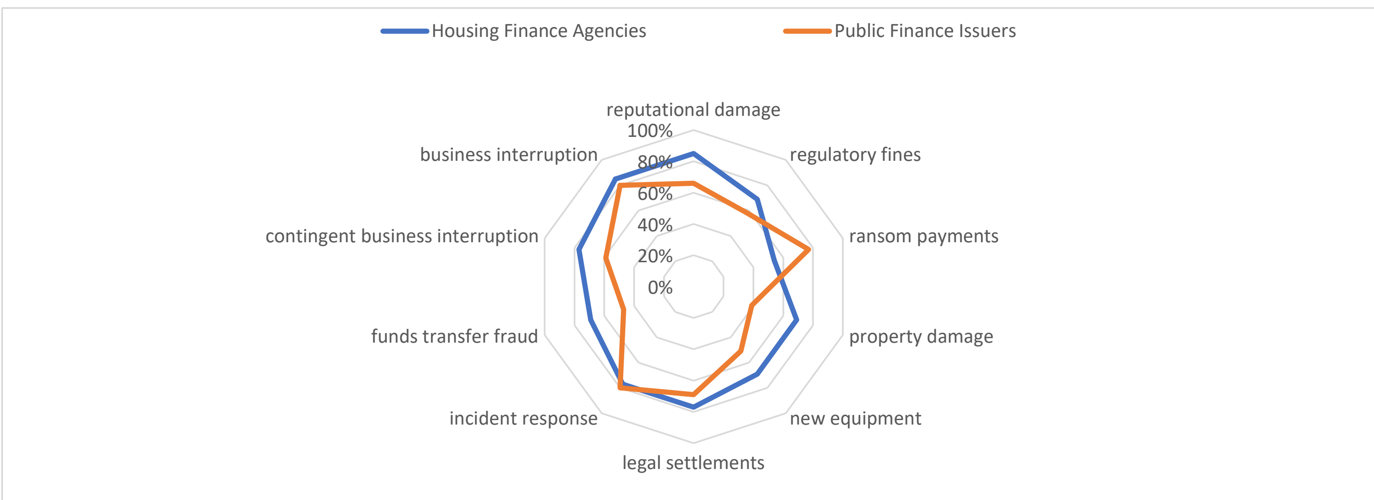


Source: Moody's Ratings

Another way HFAs mitigate cyber risk is through cyber insurance. Over 75% of HFAs that participated in the survey have standalone cyber insurance, which provides coverage for both expenses and liabilities related to a covered cyber incident. This can include protection against lawsuits filed as a result of security breaches and allegations of failure to protect sensitive information. Most cyber insurance policies taken out by HFAs cover and mitigate business interruption, property damage and equipment risks, and generally provide broader cyber coverage than those of peer public finance issuers (see Exhibit 3).

Exhibit 3

HFAs report broader cyber insurance coverage than peer public finance issuers



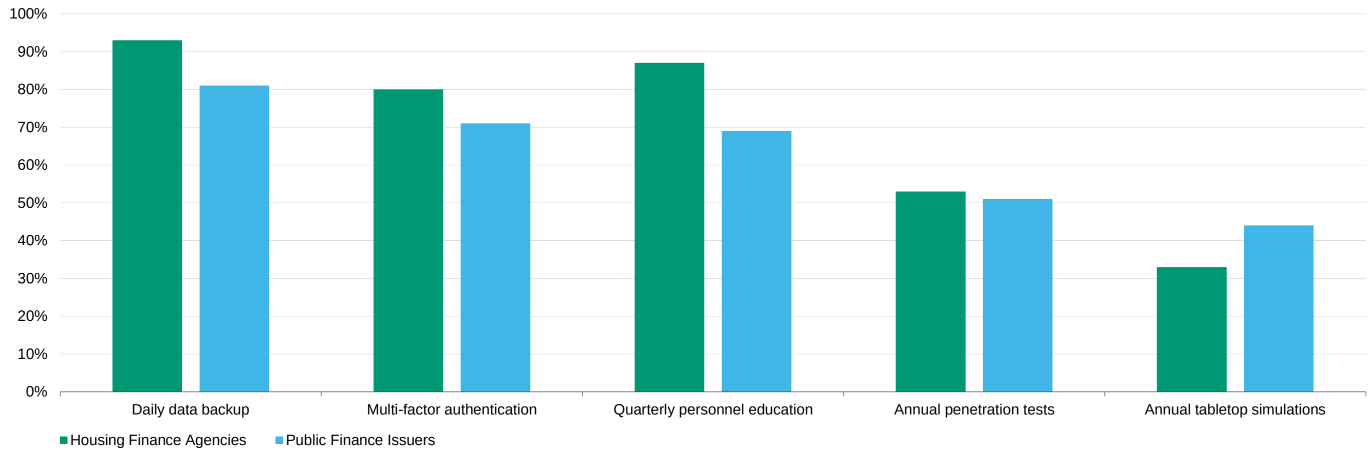
Source: Moody's Ratings

Looking ahead, 83% of HFAs indicated their intention to maintain their insurance policies, while 17% expect to increase cyber risk coverage, a positive factor when it comes to mitigating potential losses.

Basic cyber hygiene practices, including employee education, are now standard for HFAs

Most HFAs have adopted basic proactive measures against potential cyber threats, such as multifactor authentication and daily cadence of data backups, which are performed by 93% of responding HFAs (see Exhibit 4). More expensive and resource-intensive proactive measures, such as cyberattack simulations and penetration tests, are performed much less frequently, typically once a year or less.

Exhibit 4
Most HFAs use daily backups and MFA as standard proactive measures



Source: Moody's Ratings

HFAs are stronger than their public finance peers on basic protection measures. Some 80% of HFAs always use MFA to manage remote access to internal resources, compared with 71% of public finance entities. Similarly, 93% of HFAs back up their data daily, against 81% of the broader sector. Most HFAs also educate personnel on cybersecurity issues at least quarterly, consistent with most public finance organizations. These efforts indicate that HFAs are committed to modernizing their workforces and ensuring staff are well equipped to handle the evolving threat of cyber risk.

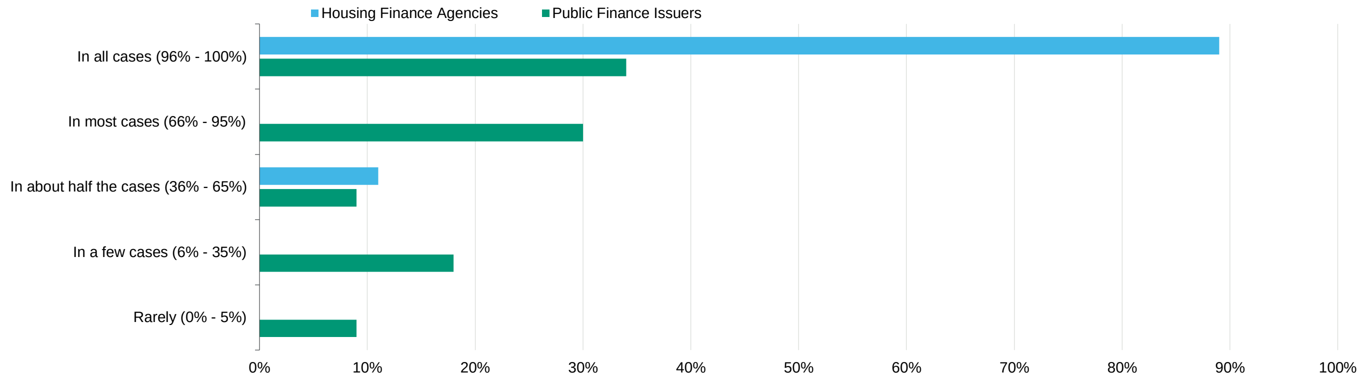
While HFAs, along with their public finance peers, have high adoption of basic cyber hygiene practices, more advance protection measures are less frequent. Tabletop attack simulations and issuer penetration tests are typically conducted by HFAs once a year with 33% and 53% annual cadence, respectively. Similarly, peer public finance issuers typically conduct tabletop simulations and penetration tests on a yearly basis. Tabletop exercises are used to test an organization's incident response plans, including its tools, procedures and proficiency in responding to different cyberattack scenarios. Penetration testing (or pen testing) is a simulated cyberattack to assess an organization's internet-accessible applications and networks.

Most surveyed HFAs always conduct third-party vendor reviews to assess cybersecurity risks

While fewer HFAs report having multiyear strategies for managing cyber risk than larger public finance enterprises (57% and 83%, respectively), they are more likely to review new and existing vendors' products for cyber vulnerabilities (see Exhibit 5). Ongoing periodic vendor reviews help agencies minimize the risk of cyberattacks from third-party vendors whose personnel or products have access to an issuer's computer systems. In fact, 89% of HFAs report that they always conduct periodic reviews of their current vendors, compared with 34% of all public finance issuers, which reduces HFAs' third-party risk. As part of the review, HFAs verify that third-party vendors comply with agencies' security policies and requirements. This mitigates potential entry points for cyberattacks, making the review process a crucial part of their defense strategy.

Exhibit 5

Most surveyed HFAs' cybersecurity personnel conduct periodic reviews of current vendors



Source: Moody's Ratings

REPORT NUMBER 1398599

CLIENT SERVICES

Americas	1-212-553-1653
Asia Pacific	852-3551-3077
Japan	81-3-5408-4100
EMEA	44-20-7772-5454