PERAC

M E M O R A N D U M

TO: All Retirement Boards

FROM: Bill Keefe, Executive Director

RE: Cyber Attack

DATE: June 26, 2025

Please be aware that a retirement board's IT network was accessed by an unauthorized third party. The unauthorized third party then placed ransomware to encrypt and to prevent access to network files. It is not clear yet when the unauthorized third party accessed the network before launching the attack nor how access was made, though similar attacks have used phishing and malicious links.

Fortunately, as of this writing, no funds are missing and there are no reports of misuse of any personal or sensitive data. The investigation is ongoing.

Also fortunately, the board had taken a number of steps to prepare for this scenario and then took immediate action when it happened.

- The board had backups of its data and files offsite in the cloud.
- The board has a disaster recovery plan and put it into action. There is no threat to the monthly payroll being generated.
- The board has a cyber insurance policy and immediately contacted the carrier.
- The board immediately contacted its IT provider and attorney, and together with the cyber insurance carrier, they have developed an action plan and are executing it.
- The board also immediately contacted law enforcement, investment professionals, financial institutions, its pension software vendor and the state's Executive Office of Technology Services and Security (EOTSS).
- The board immediately contacted PERAC so that we can assist where possible and disseminate information to put other boards on alert.

TO: All Retirement Boards
FROM: Bill Keefe, Executive Director
RE: Cyber Attack
DATE: June 26, 2025

Boards should work to ensure that their data and files are backed up. Review disaster recovery and business continuity plans and if those plans aren't in place, strongly consider developing them. Make sure important contact information is readily accessible. The slides PERAC distributed on March 25 from the cybersecurity webinar have a list of who to contact in a cyber emergency in the EOTSS attachment. Additionally, the full package of those slides contains other resources and valuable information. Assess the board's cyber insurance status. Boards with insurance should review their policy and ensure it is current and sufficient. Boards without insurance should discuss coverage with their municipality or IT provider and board counsel. PERAC is working on holding a cyber insurance webinar in late summer.

IT professionals often say it's not a matter of if an organization will get hacked, but when. The best we can do is to take proactive steps to prevent attacks as well as to take preparations to act in the event of an attack and to mitigate its effects.

Should you have IT-related concerns or questions, please contact PERAC IT Director Dan Boyle at daniel.m.boyle2@mass.gov or 617-591-8902.