FUNDAMENTALS

IMRF

INACTIVE MEMBER EDITION

VOLUME 17 | NUMBER 2
FALL 2018

How IMRF keeps your information safe

Anyone who watches the news knows that cybersecurity is an ongoing challenge for any organization that stores customer data. IMRF is no exception, facing more than 900 million attempts to breach its firewall each year.

In order to keep your information safe, “cybersecurity has been elevated to the highest levels of attention that IMRF can give,” said Kathy Goerdt, IMRF Performance Excellence Manager.

IMRF’s security approach is three-pronged, according to Glenn Engstrom, IMRF’s Chief Information Security Officer.

“Security is sort of like a triangle,” Engstrom said. “You have people, you have technology, and you have processes. All of these elements play a role in securing members’ information.”

> “Our most important way to protect data is to educate the person sitting behind each computer.”
>
> *Glenn Engstrom, IMRF’s Chief Information Security Officer*

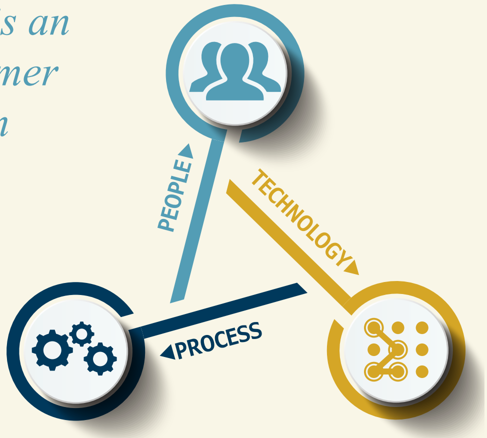
People

“Our most important way to protect data is to educate the person sitting behind each computer,” Engstrom said.

Any number of high-profile security breaches at other organizations have occurred because of an action taken by someone inside the organization—for example, clicking on a dangerous link in an unsolicited email.

To protect against this kind of attack, IMRF provides ongoing phishing training for its employees. Phishing is fraudulent email that appears to be from a reputable source, but is actually designed to trick the recipient into revealing sensitive information or taking an action that could give a hacker access to their computer.

“Our training is really focused on helping our staff identify when they’re getting email that is dangerous, or could be dangerous,” Engstrom said.



The Three Elements of Cybersecurity

In addition to phishing training, IMRF staff is trained in other security protocols, such as physical security and proper handling of sensitive information. An outside security firm then tests IMRF’s security protocols to ensure that the lessons have been well-learned, reporting back to IMRF about any weaknesses so they can be corrected.

Technology

To support the people on the front lines, IMRF harnesses technology, periodically upgrading its various systems to address changing security concerns.

- **Firewall:** In early 2017, IMRF upgraded its firewall using the latest security technology in order to better guard against attacks.

continued on page 2

continued from page 1

- **Email filtering:** IMRF filters its email so that many phishing emails and other malicious messages are never even seen by staff.
- **Detection systems:** "We have strong detection systems, which constantly analyze activity that's going on in our systems and on our network," Engstrom says. IMRF staff uses the information provided by the detection systems to evaluate potential threats.

"It's an ever-moving target," Goerdt said. "The smarter we get, the smarter the hackers get, so we have to be constantly looking at not just what's happening now, but what could occur in the future."

Process

Using the cybersecurity framework provided by the National Institute of Standards in Technology (NIST), IMRF is constantly improving its security processes in light of known best practices and developing threats.

"One of the advantages of utilizing NIST is that the federal government has much broader resources, and they have intelligence as to what the threats are—not just at the local level like we have, but state, federal, global," Goerdt explained. "They have all of this knowledge which we could not afford to garner on our own, that they are taking and compiling and boiling down into a framework that we can utilize."

The NIST framework, which stretches across industries, provides an approach for identifying critical systems and improving security practices. It also offers methods for achieving consistency in documenting processes and analyzing how well they've been put into practice.

Engstrom said that, while NIST's approach touches on many different aspects of what any good business must do to protect itself, it can be summed up in five steps:

1. Identifying what the organization needs to protect.
2. Figuring out how to protect it.
3. Being able to detect unusual activity.
4. Addressing the unusual activity—putting a stop to it if it's harmful, or noting it for reference if it's an employee who's just doing something out of the ordinary.
5. Having a recovery plan in place in the event of a security breach.

"No matter how our technology or our business or anything changes, these five steps will always help us maintain a secure environment," Engstrom said. "It's timeless." ■

How you can protect your personal data

Thieves don't need to hack into IMRF directly to gain access to your account. You may be able to save yourself time and trouble by taking steps to protect your personal information.

In October 2017, 103 members of the Iowa Public Employees' Retirement System (IPERS) discovered their member accounts had been compromised when they did not receive their scheduled pension payment.

The Des Moines Register reported that IPERS's computer system was not hacked. Instead, cybercriminals had obtained stolen Social Security Numbers and other personal information from another source, then used that personal data to register for IPERS online access accounts in those members' names and change their direct deposit information. (This is one reason that, as a cautionary measure, IMRF doesn't provide immediate Member Access account access; instead, we send a registration key through the mail to your address on file in order to thwart this type of attack.)

Your account contains personal information like your beneficiaries, service credit, and Member ID Number, so it is to your advantage to keep this information private. **(IMRF has purchased cyber-liability insurance to make sure its members are protected in the event of a breach.)**

The following tips for protecting your private data, at IMRF and elsewhere, are not a comprehensive list of what to do to keep your information secure, cautions Glenn Engstrom, IMRF's Chief Information Security Officer. However, taking these steps today will make you safer than you were before.

- **Keep your private data private.** "Keep your login and password private," Engstrom said. "Don't share it with your spouse; don't share it with your kids. And of course, don't write it down next to your computer and say 'this is my password.' Keep it private, and make it something that you'll remember." If you have difficulty remembering your passwords, there are security products that essentially function as a password vault for which you only have to maintain a single password.
- **Change your password periodically.** "You don't have to do it every month, but change it a couple times a year," Engstrom said. If you are hacked or your security is otherwise compromised, change your passwords immediately. "You can even create a whole new Member Access account," he said.
- **Install antivirus software on your computer.** "If you don't have an antivirus, there are plenty of free ones," Engstrom said. "A lot of Internet service providers have an antivirus that you can download and use."
- **Keep your operating system and your software up to date.** "The software companies and especially your operating systems are continually sending updates to ensure your security," said IMRF Performance Excellence Manager Kathy Goerdt. "If you're five updates behind, you have a whole bunch of holes that have not been patched."
- **Back up your files and essential information.** If you back up your files regularly, not even a malicious hacker will be able to part you from the files you rely on. ■

2017 Annual Financial Report

Investment portfolio returns 15.73%

IMRF's fiduciary net position up $4.9 billion last year, $8.1 billion over five years

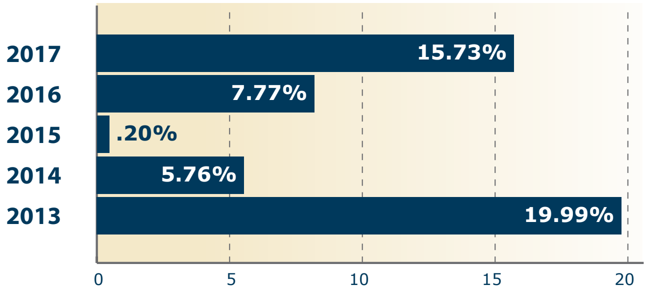
INVESTMENTS

The IMRF investment portfolio returned 15.73%, after investment-management fees, during 2017.

IMRF's international and U.S. equity performed particularly well during 2017, driving much of the overall return. IMRF's allocation to international equity returned 27.53% after fees, and IMRF's U.S. equities returned 19.6% after fees.

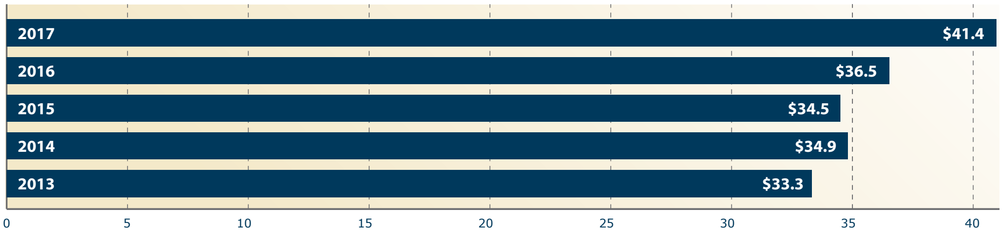
IMRF's long-term goal is to earn an annualized total fund return of 7.5%, after investment-management fees. With a return of 15.73% in 2017, IMRF achieved its goal. IMRF has also achieved its investment return goal over longer time horizons. For example, over the last five years, IMRF has earned 9.7% after paying investment-management fees.

TOTAL FUND RETURNS FOR THE PAST 5 YEARS



FIDUCIARY NET POSITION

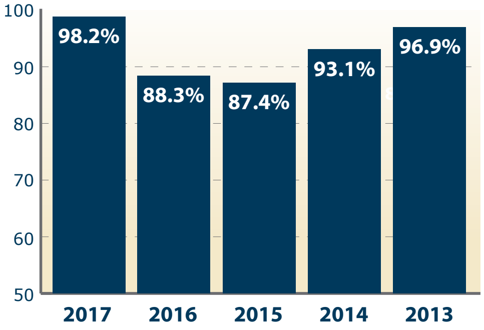
IMRF's fiduciary net position—total assets minus liabilities—was $41.4 billion as of December 31, 2017. That was an increase of $4.9 billion, or about 13.4%, from 2016. The increase is attributable to strong 2017 investment returns. Over the last five years, IMRF's fiduciary net position has increased by $8.1 billion.



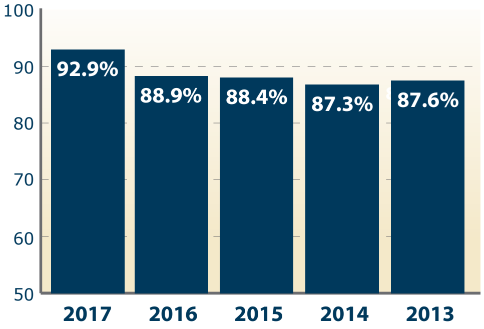
FUNDING STATUS

IMRF's funding status is a key indicator of its financial health. It reflects the percentage of benefit promises that IMRF has assets to pay. IMRF strives toward full funding because it guarantees that the system can meet its obligations. Full funding is also most cost-effective for taxpayers.

MARKET FUNDING STATUS: PAST 5 YEARS



ACTUARIAL FUNDING STATUS: PAST 5 YEARS



There are two measures of funding status. Market funding status describes the percentage of assets IMRF has to pay all current and projected benefits, as of a specific date. As of December 31, 2017, IMRF was 98.2% funded on a market basis. IMRF's market funding status increased from 2016 to 2017 due to strong investment returns.

The other measure is actuarial funding status. For this measure, independent actuaries determine the actuarial value of IMRF assets using a "smoothing" technique that recognizes investment gains and losses over a five-year period. The actuarial funding status is less volatile than the market funding status, which is why it is used to set IMRF contribution rates for participating units of government. As of December 31, 2017, IMRF was 92.9% funded on an actuarial basis.

Excerpted from IMRF's *2017 Popular Annual Financial Report for Members*. Read the full report at **www.imrf.org/annual-financial-report**.

IMRF
Suite 500
2211 York Road
Oak Brook, IL 60523-2337

Locally funded, financially sound.

FUNDAMENTALS

is published twice a year for inactive members of IMRF.

Erin Cochran, editor, ecochran@imrf.org
1-800-ASK-IMRF (275-4673) • www.imrf.org

Don't leave money on the table!

IMRF urges you to apply for your pension now if you are an inactive Tier 1 member who is:

- Vested
- At least age 55
- Not working for a reciprocal system

You might think it is better to wait until age 60 or 62 to start your IMRF pension, but in most cases you will end up losing money by waiting:

The earlier you start payments the more total payments you receive over time.

If you are between 55-60

Although your pension will be reduced since you are under age 60, the earlier you start payments the more total payments you will receive.

Over time you will get more money, even with the reduced amount. The longer you wait, the more payments you will miss out on.

If you are at least 60

You have reached full IMRF retirement age. IMRF pensions do not follow the same rules as Social Security.

Waiting until age 62 or later for your IMRF pension will most likely not increase your pension, and you will be missing out on years of monthly payments.

Visit **www.imrf.org** or call 1-800-ASK-IMRF (275-4673) if you have any questions. ■