March 2026

OREGON STATE TREASURY

Inside the Vault

Local Government Edition

Security Spotlight: Data Breaches

More than a decade ago, a data breach forced many organizations to realize the consequences of exposing protected data to unauthorized access and manipulation. Laws were established in response to this first "major" breach, and sensitivity to cyberattacks heightened. Fast forward to today, and that early breach seems practically insignificant compared to more recent data breaches that have exposed the personal data of countless people.

Bringing awareness to how data breaches can occur and the damage they can cause to the clients we serve is part of our turnkey approach to client service. Below, we discuss the current trend of data breaches and how you can be more prepared should a data breach happen to you.

What is a Data Breach?

Unlike cyberattacks such as ransomware, a data breach is the result of a social engineering attack that provides unauthorized access to steal confidential personal or financial data.

Current trends show that cybercriminals steal data for its monetary value, that many companies are not properly prepared for breaches, and that the number of breaches continues to increase each year. What is causing this upward trend?

- **Employee Errors:** The leading cause of data breaches around the world is employee error. These errors come in the form of compromised credentials or lost or stolen devices like company cell phones and laptops. Employee error can be caused by a lack of general awareness for how to handle, retain, and dispose of sensitive data. And a general lack of training can leave employees vulnerable to cybercriminals.
- **Phishing Attacks:** Hackers use social engineering tactics to capitalize on relationships and social behavior to manipulate people into providing access, supplying information, or performing an action. Hackers use emails, texts, or phones calls

(Continued on page 2)

Interest Rates

Average Annualized Yield

February	4.0393%

Interest Rates

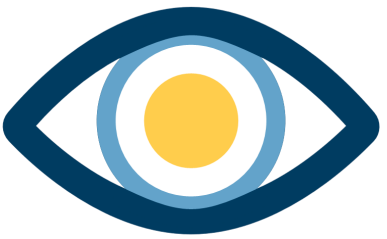
February 1–11	4.10%
February 12–28	4.00%

(Continued from page 1)

disguised as legitimate requests to trick employees into unknowingly providing protected information or unauthorized access.

- **Weak or Stolen Credentials:** Phishing attacks are often designed to obtain a user's credentials. In a study of 905 phishing attacks, 91% were found to be targeting usernames and passwords. Password guessing software is also used to search for weak credentials — passwords that are repeatedly used or that contain personal or easily-guessed information.
- **Ransomware:** This is a type of malicious software that infects, locks, or takes control of a system or encrypts important data then demands a ransom to undo it. Ransomware typically falls into two categories:
    1. Locker Ransomware - locks a user out of a system but typically leaves the underlying system and files untouched.
    2. Crypto Ransomware - encrypts files stored on a user's computer or mobile device rendering them unreadable until the victim pays for the decryption key.

  Ransomware is typically installed through a malicious email attachment, an infected software download, or a visit to a malicious website. Payment requests are made in hard-to-trace bitcoins, wire services, or gift cards. Paying the ransom does not guarantee the encrypted files will be released. Ransomware has been used against local governments and often prevent the delivery of critical services.
- **Third-Party Vendors:** As trusted partners for your organization, vendors can sometimes become unsuspecting accomplices to cyberattacks leading to data breaches. A survey by eSentire that interviewed 600 IT professionals determined that nearly half of the respondents experienced a data breach caused by a vendor, that 26% of the breaches were caused by employee errors and stolen passwords, and that the remaining breaches were the result of some form of malware such as spyware.
- **Spyware:** This type of attack often occurs when an employee unknowingly downloads spyware thinking they are performing a routine update or running a seemingly nonthreatening computer program. Instead, the malware infects a computer or network and steals personal information or other data.



- **Outdated Software:** Software companies routinely alert users to available updates that provide important software patches to fix identified vulnerabilities. When these updates are overlooked or delayed by employees, it leaves them open to hackers. For example, Microsoft sends monthly notices of available updates. These notifications are sent to software users but are often monitored by hackers too. Hackers will use this information to seek out users who have not yet applied the updates, which provides a window to exploit software vulnerabilities.

Data Breach Consequences: Beyond the Headlines

When a breach is discovered, the first course of action is typically to stop operations until the source is identified and the issue is resolved. Yet for public agencies that provide

(Continued on page 3)

(Continued from page 2)

essential services, shutting down operations may not be an option. If it is, the consequences could be detrimental to the communities served.

According to one study, the average cost of a data breach—at $3.86 million—far exceeds the cost to properly train staff and implement the internal controls necessary to help protect an organization. And a data breach often includes the following non-budgetary "costs:"

- **Damage to Your Reputation:** Building and maintaining a reputation is something that takes a lot of work, and a data breach can quickly tarnish a good reputation that has taken years to build. Forty-six percent of organizations say they suffered damage to their reputations because of data breaches.
- **Lost Trust:** Governments are responsible for all types of sensitive information. When a data breach occurs, both the public and policymakers may question the trust they had placed in that particular organization. Loss of trust can also come from how an organization responds to a breach.

What Can You Do to Avoid a Data Breach?

Unfortunately there is no way to prevent hackers from targeting your organization; however, you can establish "data hygiene" protocols to help mitigate the risk of a breach happening to you.

- **Employee Awareness, Training, and Testing:** Not understanding security risks or best practices is the root of vulnerability for organizations. Teaching employees how to recognize signs of possible fraud and how to respond appropriately is the first step toward preventing cyberattacks that may lead to a data breach. Employees should understand appropriate data retention and disposal methods, use strong passwords and multi-factor authentication, understand the process for processing and responding to requests for information, and know their roles as part of their organization's incident response plan.
    - Many data breaches are caused by improper disposal of records and equipment. Proper disposal can come in the form of employing a shredding service or properly "cleaning" machines before returning or disposing of them.
    - Requiring passwords to meet specific criteria and implementing multi-factor authentication for online account access can also help prevent a data breach. Best practice is for passwords to be as long as permissible; contain a mix of upper and lowercase letters, numbers and special characters; and never include personal information like birthdays, street names, or pets' names. Multi-factor authentication should also always be used when available. Though not fool-proof, multi-factor authentication greatly decreases the chance of accounts being compromised and helps to ensure that only authorized individuals are accessing protected systems and information.

    - An incident response plan is an organized approach to addressing the aftermath of a security breach or cyberattack. Plans should address a situation in a manner that limits damage and

(Continued on page 4)

(Continued from page 3)

reduces recovery time and costs. Without a plan in place, an organization may not be able to detect an attack or follow the proper protocol to contain the incident and recover from it.

- **Apply Technical Controls and Protection Software:** Organizations should have a routine process for distributing and installing critical security patches. They should also have trained security professionals who understand the vulnerabilities of their systems and can take proactive steps to mitigate risks. Utilizing intrusion detection systems (IDS) and intrusion prevention systems (IPS) can help to detect unusual activity behind the scenes to alert IT staff to potential cyberattacks. When alerted to a potential threat, IPS can deploy prevention tactics to fight against the attack and keep protected information secure. It is also best practice to run regular upgrades to outdated or unsupported software. Routine software upgrades apply new security patches to existing software to protect against newly discovered vulnerabilities. It is important to be aware of and to manage system vulnerabilities to ensure necessary upgrades are occurring. Vulnerability management helps to ensure software patches are in place.
- **Penetration Tests:** Employing security companies to "test" the security of your organization's network is another way to help prevent data breaches. Penetration testing, also known as ethical hacking, is the practice of testing a computer system or network to detect security vulnerabilities. These tests are performed to see if an organization's network is hackable. If an area of exploit exists, it can be quickly identified and resolved as a result of this type of testing.

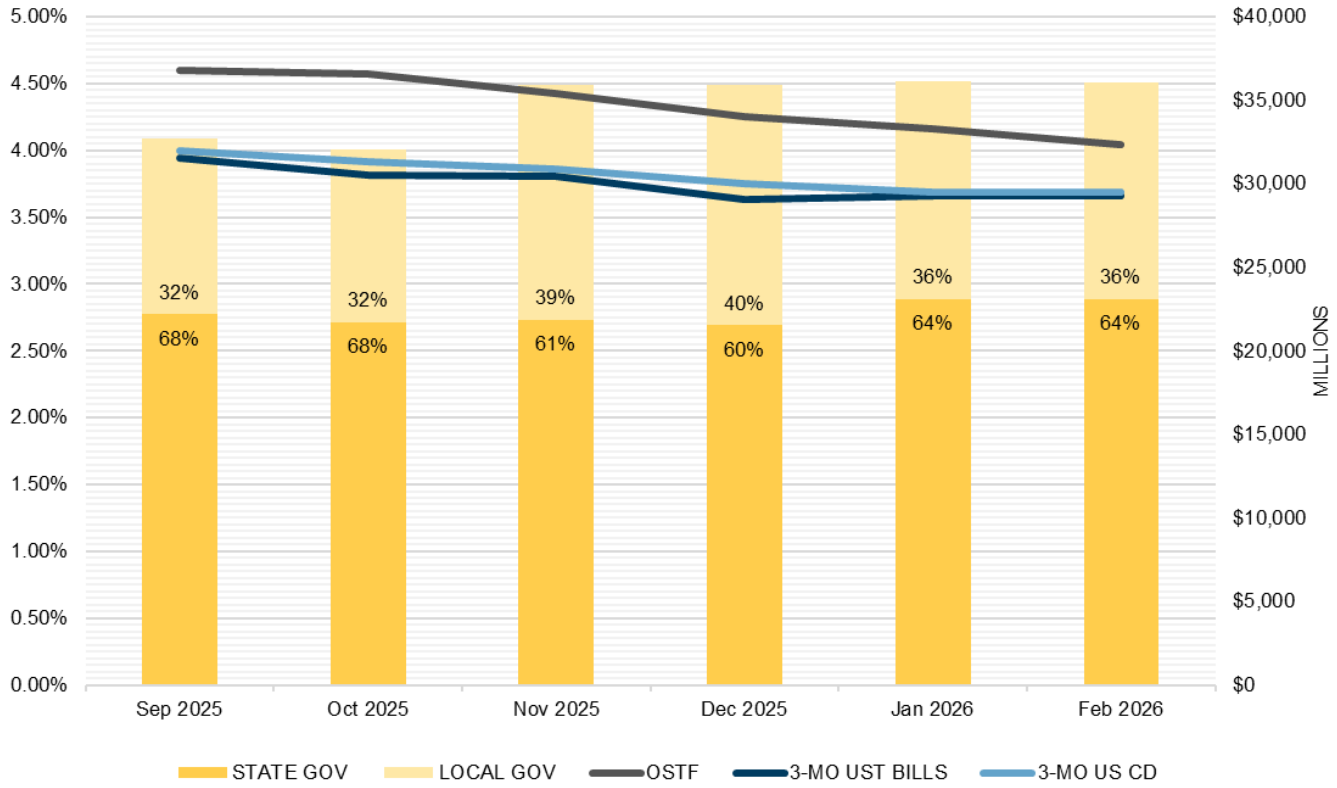
Operating in a digital environment challenges us daily to stay one step ahead of cybercriminals who want to exploit our protected information. Attacks continue to become more sophisticated and have required organizations to develop prevention measures that are equally sophisticated. Understanding how and why data breaches occur is the first line of defense. With the right mix of training, technical controls, and prevention software, organizations can fight back to protect their information and reduce their chance of becoming the next major security breach headline in the news.

LGIP and Contract Retainage

ORS 279C.570 was amended in 2024 to remove the requirement that amounts deducted as cash retainage for public improvement contracts exceeding $500,000 be deposited in an interest-bearing *escrow* account unless a contractor requests an alternate approach. Accordingly, amounts deducted as cash retainage pursuant to ORS 279C.560(2)(a) may be held in the Local Government Investment Pool.

If a contractor elects an alternate approach pursuant to ORS 279C.560(2)(b), cash retainage must be deposited in an interest-bearing account in a *bank or other financial institution* (see ORS 279C.560(5)). Because Treasury is not considered a bank or other financial institution for purposes of this statute, *the pool is not acceptable as an alternate approach*. Treasury is not responsible for determining whether the pool is an appropriate repository for any funds placed in the pool by a participant. Local government finance staff should work with their procurement/contracting peers and legal counsel to discuss what forms of retainage their organization plans to use and ensure appropriate solutions are in place.

Oregon Short Term Fund Analysis



	Sep 2025	Oct 2025	Nov 2025	Dec 2025	Jan 2026	Feb 2026
TOTAL OSTF AVG DOLLARS INVESTED (MM)	32,701	32,077	35,893	35,929	36,128	36,062
STATE GOV PORTION (MM)	22,182	21,715	21,876	21,532	23,110	23,092
LOCAL GOV PORTION (MM)	10,519	10,362	14,017	14,397	13,018	12,970
OSTF ANNUAL YIELD (ACT/ACT)	4.60	4.57	4.43	4.25	4.16	4.04
3-MO UST BILLS (BOND EQ YLD)	3.939	3.816	3.803	3.633	3.660	3.661
3-MO US CD (ACT/360)*	4.00	3.92	3.86	3.75	3.69	3.69

NOTE: The OSTF ANNUAL YIELD represents the average annualized yield paid to participants during the month. Since interest accrues to accounts on a daily basis and the rate paid changes during the month, this average rate is not the exact rate earned by each account.

3-MO UST BILLS yield is the yield for the Treasury Bill Issue maturing closest to 3 months from month end. 3-MO US CD rates are obtained from Bloomberg and represent a composite of broker dealer quotes on highly rated (A1+/P1/F1+ from Standard & Poor's Ratings Services, Moody's Investors Service and Fitch Ratings respectively) bank certificates of deposit and are quoted on a CD equivalent yield basis.

Market Data Table

	2/28/2026	1 Month	3 Months	12 Months		2/28/2026	1 Month	3 Months	12 Months
7-Day Agency Discount Note**	3.49	3.49	3.76	4.10	Bloomberg Barclays 1-3 Year Corporate YTW*	3.89	3.96	4.00	4.51
30-Day Agy Nt Disc**	3.54	3.51	3.75	4.20	Bloomberg Barclays 1-3 Year Corporate OAS*	0.51	0.45	0.51	0.52
90-Day Agy Nt Disc**	3.55	3.56	3.66	4.19	Bloomberg Barclays 1-3 Year Corporate Modified Duration*	1.80	1.79	1.81	1.82
180-Day Agy Nt Disc**	3.49	3.51	3.58	4.10					
360-Day Agy Nt Disc**	3.29	3.35	3.44	3.89	7-Day Muni VRDN Yield**	1.88	2.28	2.79	1.86
					O/N GGC Repo Yield**	3.71	3.72	4.13	4.41
30-Day Treasury Bill**	3.62	3.60	3.83	4.22					
60-Day Treasury Bill**	3.62	3.61	3.78	4.24	Secured Overnight Funding Rate (SOFR)**	3.68	3.68	4.12	4.39
90-Day Treasury Bill**	3.60	3.60	3.74	4.24					
6-Month Treasury Yield**	3.62	3.63	3.77	4.28	US 10 Year Inflation Break-Even**	2.26	2.34	2.23	2.37
1-Year Treasury Yield**	3.48	3.47	3.60	4.09					
2-Year Treasury Yield**	3.38	3.52	3.49	3.99	1-Day CP (A1/P1)**	3.64	3.62	3.89	4.28
3-Year Treasury Yield**	3.38	3.59	3.49	3.97	7-Day CP (A1/P1)**	3.64	3.62	3.89	4.29
					30-Day CP (A1/P1)**	3.67	3.63	3.87	4.33
1-Month SOFR**	3.67	3.67	3.86	4.32					
3-Month SOFR**	3.67	3.66	3.79	4.32	30-Day CD (A1/P1)**	3.66	3.67	3.90	4.34
6-Month SOFR**	3.62	3.62	3.70	4.26	90-Day CD (A1/P1)**	3.75	3.75	3.95	4.40
12-Month SOFR**	3.47	3.49	3.51	4.13	6-Month CD (A1/P1)**	3.76	3.76	3.92	4.41
Sources: *Bloomberg Index Services, **Bloomberg					1-Year CD (A1/P1)**	3.72	3.79	3.84	4.35

Director of Finance
Cora Parker
503.378.4633

Deputy Director of Finance
Bryan Cruz González
503.378.3496

Newsletter Questions
Kari McCaw
503.378.4633

Local-Gov-News Mailing List
omls.oregon.gov/mailman/listinfo/local-gov-news

Local Government Investment Pool
oregon.gov/lgip

PFMAM Client Services
855.OST.LGIP
csgmww@pfmam.com

- Connect Access
- Transactions
- Reporting
- Account/User Maintenance
- Eligibility

Treasury
800.452.0345
lgip@ost.state.or.us

- Investment Management
- Statutory Requirements
- Service Provider Issues
- General Program Inquiries

Oregon Short Term Fund Staff
503.431.7900

Public Funds Collateralization Program
oregon.gov/pfcp
503.378.3400
public.funds@ost.state.or.us

OREGON STATE TREASURY
867 Hawthorne Ave SE ⏩ Salem, OR 97301-5241
oregon.gov/treasury