



We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Welcome

2025 Minnesota Nonprofit Finance Conference

May 19, 2025



The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

Agenda

9:15 – 10:05 a.m. — Scenario Planning in an Uncertain Funding Environment

10:05 – 10:55 a.m. — Modernizing Data Management

10:55 – 11:10 a.m. — Break

11:10 a.m. – 12 p.m. — HR & Tax Hot Topics

12 – 1 p.m. — Lunch

1 – 1:50 p.m. — This Is Why We Can't Have Nice Things

1:50 – 2:40 p.m. — Risk Management & Cybersecurity Trends

2:40 – 3 p.m. — Closing

3 – 4 p.m. — Social Hour



OUR PURPOSE

CLA exists to create opportunities
for our clients, our people,
and our communities.





We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Scenario Planning in an Uncertain Funding Environment

Agenda

- Introductions and Neighbor Meet and Greet
- Federal Funding Current State and Recent Trends
- Scenario Planning Approaches and Discussion
- Compliance Considerations
- Approaching Funder Conversations
- Q&A



Learning Objectives

At the end of this session, you will be able to:

Recognize the current state of federal funding sources most impactful to nonprofits

Identify ways your organization can build scenario plans and budget models

Identify how you might create structure around what decisions you will make- and when- as the new reality emerges





Federal Funding Updates



Administration Activity

Every new administration does a review of its program spending and alignment with administration priorities

We have seen over 170 Executive Orders, directives, and policy shifts issued by the current administration



Executive Orders

Signed 143 executive orders

Of those orders, nearly :

- 40% focused on government reform, accountability and deregulation,
- 20% pertained to foreign policy and national security

Faced more than 120 lawsuits challenging the legality and implementation of these executive orders, with nine actions currently fully blocked by the courts.



Executive Order Impacts on Nonprofits

Federal
government
relations

Diversity, equity,
and inclusion
programs

Immigration
services

LGBTQ+
community
services

Environmental

House of worship
/ faith-based
groups

Foreign aid

Arts, humanities
and museum and
library services



What We Are Seeing

Delayed or uncertain payments

Slowed or stopped correspondence with grants officers

Program pause / cuts / award terminations



Program Cuts

USAID

Department of Education

Minority Business Development Agency

National Endowment for the Arts

Department of Health and Human Services



Administration's FY2026 Budget Cuts

- On May 2, The President released a “skinny” budget (<https://www.whitehouse.gov/wp-content/uploads/2025/05/Fiscal-Year-2026-Discretionary-Budget-Request.pdf>), outlining his spending priorities for Fiscal Year (FY) 2026.
- Cuts are subject to Congressional vote and are not yet in effect.



Administration's FY2026 Budget Cuts

- The president proposes to eliminate or deeply cut:
 - Resources enacted by Congress under the Infrastructure Investment and Jobs Act (cut by \$15.2 billion) and other energy-efficiency programs (cut by \$2.6 billion).
 - FEMA preparedness grants and state-level programs (cut by \$646 million).
 - Substance use disorder programs administered by the Substance Abuse and Mental Health Services Administration (SAMHSA) (cut by \$1.06 billion).
 - Funding at the EPA to support clean and drinking water (cut by \$2.46 billion).
 - Assistance for refugees (cut by \$650 million).
 - Fair housing enforcement (cut by \$60 million).
 - Heating assistance for low-income households (cut by \$4 billion).
 - Community services block grants (cut by \$770 million).
 - Rental assistance (cut by \$26 billion) and resources to build affordable housing (cut by \$1.2 billion) and revitalize communities (cut by \$3.3 billion).
 - AmeriCorps and other workforce programs.





Significant Proposed Budget Impacts

Increased funding

- Defense Department: +13% [\$113.3B]
- Homeland Security: +65% [\$42.3B]

Reduced funding

- State Department: -84% [\$49.1B]
- Housing and Urban Development: -44% [\$33.5B]
- Health and Human Services: -26% [\$33.2B]
- Education: -15% [\$12B]

Termination Letters

“Pursuant to the applicable version of 2 C.F.R Section 200.3401 – Termination, “The Federal award may be terminated in whole or in part ... [b]y the Federal awarding agency or pass-through entity, to the greatest extent authorized by law, if an award no longer effectuates the program goals or agency priorities.”

As part of efforts to streamline and reduce the cost and size of the Federal Government, the Department is reprioritizing funding and staff to support only those activities directly related to its current programmatic goals and mission priorities. After careful review of this award, the Department has determined that this project’s activities neither effectuate these undertakings nor advance the Administration’s objectives.”



Termination Letters

To this end, and as provided above, your award was terminated on DATE; therefore, should you decide to continue project activities beyond DATE, you do so at your own risk and will not be reimbursed for any project costs incurred after that date.

You will be notified in writing concerning close-out instructions for this award.”

Note that within § 2 CFR 200.472 there are certain termination costs that are allowable due to early termination, including loss of useful value, unavoidable costs, and settlement costs and per § 200.343 costs during suspension or after termination are allowable if the costs result from financial obligations which were properly incurred by the recipient or subrecipient before the effective date of suspension or termination, and not in anticipation of it



Tips to Navigating the Uncertainty

Be prepared to adapt or make modifications as needed.

Assemble an internal team that can help with rapid decisions that need to be made.

Review your grant agreement to identify and understand the terms, especially clauses related to funding availability and reimbursement.

Closely monitor budget obligations to avoid overspending while awaiting anticipated future funding.



Tips to Navigating the Uncertainty


Stay in contact with your program or grant officer to confirm that there are no changes affecting your award.

Monitor policy updates and keep an eye on announcements from your funding agencies for any updates on funding availability or compliance updates.

Review information received from granting agency as it becomes available.



Tips to Navigating the Uncertainty



Stay well-informed and proactively engage with policy changes and leverage your organizational strengths.

Stay on top of the current state of the situation can help your organization develop strategies for addressing these funding changes effectively.



Flow Down of Federal Impacts

1 Changes in state and local government funding

2 Changes in philanthropic funding

3 Changes in economic landscape

4 Changes in community and participant needs



Discussion

Has your organization
been impacted recently
with funding changes?

Are there any anticipated
upcoming impacts?

How has your organization
responded?

What concerns are you
hearing from individuals or
communities you serve?

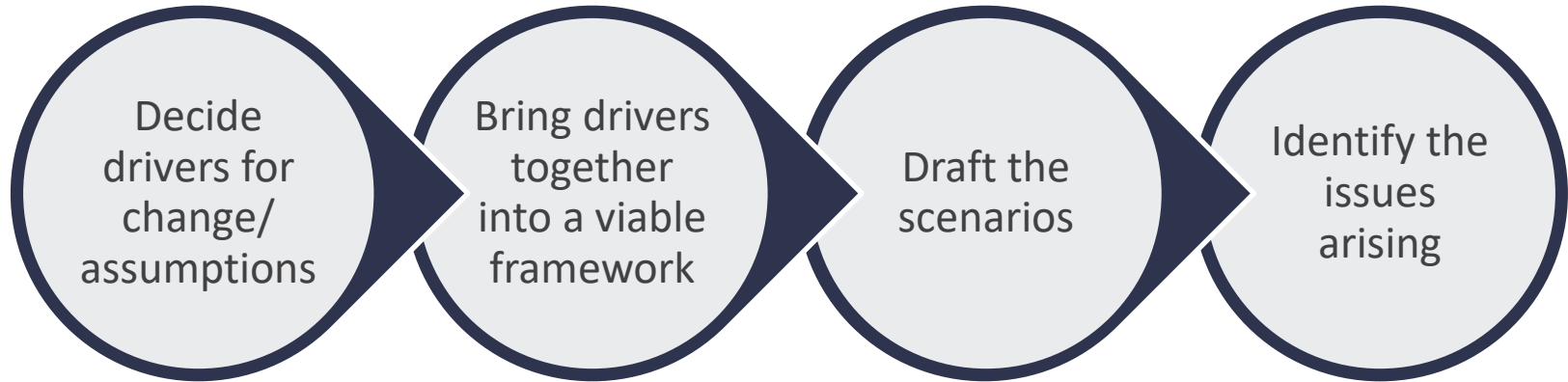




Scenario Planning



Risk Planning Scenario



1. Funding Source Risk Analysis – Example

Funding Source	Source	CY Budget	Risk/Notes
Grant 1	Federal (direct)	\$250k	Moderate
Grant 2	Federal (via state alliance)	\$250k	Moderate
Grant 3	State	\$500k	Low
Grant 4	Philanthropic	\$250k	Low
Grant 5	Philanthropic	\$250k	Moderate
Other Funding	Various	\$1M	No anticipated impact
Total Revenue		\$2.5M	CY Budget
		\$750k	30% Moderate Risk
		\$750k	30% Low Risk



2. What We Know Today Re: At Risk Sources

Grant 1: Pays for ABC

Funder advised to plan for reduction; TBD what/how much

Grant 2: Pays for XYZ

Funder is non-responsive; grant is DEI-related; likely at-risk

Grant 3: Pays for 123

including 20% indirect. State funding not yet impact but state budget is 40% federal; expect potential trickle-down impacts.

Grant 4: Unrestricted; Funder has indicated no changes in CY but focus may shift in future years. Could be +/- for Club.

Grant 5: Pays for 456; Funder primarily funds refugee resettlement and has messaged it plans to redirect some funding that direction; may be at risk for Club



3. Current State Financial Analysis



Cash flow projection before cuts



YTD Statement of Activities vs. YTD and Annual Budget



Accounts Receivable Aging by Grantor



Government Funding Risks and Strategies

Risks

- Delayed reimbursements
\$250K outstanding 3/15/25
- Denied reimbursements
\$50K as of 3/15/25
- Existing grants are frozen, reduced, or not renewed

Strategies

- Submit reimbursements timely and frequently
- In-depth documentation for approved expenses only
- Proactively identify reductions
- Pursue alternative revenue sources



Scenario #1: Extended Delays in Reimbursements

Assumptions

- All reimbursements will be received but time to receive cash will be elongated
- Current grant operations will continue as agreed to in existing grants

FY2025 Impact

- Utilization of line of credit to cover cash shortfalls
- Renegotiate terms with vendors to extend due dates
- Potential erosion of investment balance
- Elimination of non-essential expenses



Scenario #2: 50% Reduction in At Risk Government Funding

Assumptions

- All reimbursements outstanding will be paid
- Grant related personnel impacted; some reductions

FY2025 Impact

- Revenue reduction = \$250K
- \$200K in salaries and 4-5 people would be eliminated
 - Could reduce hours/salaries
- \$50K in other expenses would need to be identified





Scenario #3: All At Risk Government Funding Stopped 3/31

Assumptions

- All reimbursements outstanding will be paid
- All grant related personnel would be reduced

FY2025 Impact

- Revenue reduction = \$500K
- \$400K in salaries and 9 FTE would be eliminated
- \$100K in other expenses would need to be identified

Action Portfolio – Changes We Can Make

Potential Change	Est. \$\$ Impact	When to Activate
Downsize Program A	\$250k	Funder alert of reduced programming OR non-payment of outstanding AR by 6/30
Eliminate Program A	\$500k	Funder alert of cancelled program OR non-payment of AR by 9/30
Hiring Pause	\$100-300k	Pause backfilling any open positions; currently 4
Other ideas?		



Discussion

What other ways are your organizations approaching scenario planning and/or budgeting in the current time?





Accounting Considerations



Accounting Considerations



Subsequent events

Going Concern

Aging A/R balances



Conversations with Funders



Framing Productive Funder Conversations

Preparing for the conversation

- Gather relative evidence and data to support your case
- Understand your funder's perspective
- Clarify your objectives for the conversation
- Set the right tone and environment



Framing Productive Funder Conversations

Tips for during and after the conversation

- Communicate clearly and effectively
- Manage emotions and reactions
- Find common ground and solutions
- Follow-up promptly and continued communication



Type of Conversations with Funders



Grant funding
advances



Budget
modifications



Grant renewal
likelihood



New funding
opportunities

Q&A



CLAAconnect.com



CPAs | CONSULTANTS | WEALTH ADVISORS

©2025 CliftonLarsonAllen LLP. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See [CLAGlobal.com/disclaimer](https://claglobal.com/disclaimer).
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.



We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS



Modernizing Data Management

At Midwestern Higher Education Compact

Learning Objectives

At the end of this session, you will be able to:

- Describe the importance of data to mission and components that make for a sound data strategy
- Recognize how adopting a digital strategy can further advance your nonprofit's mission and goals
- Recall real life challenges, mistakes, and learnings from an organization on its own data journey



Speakers



Ben Aase
Principal
CLA



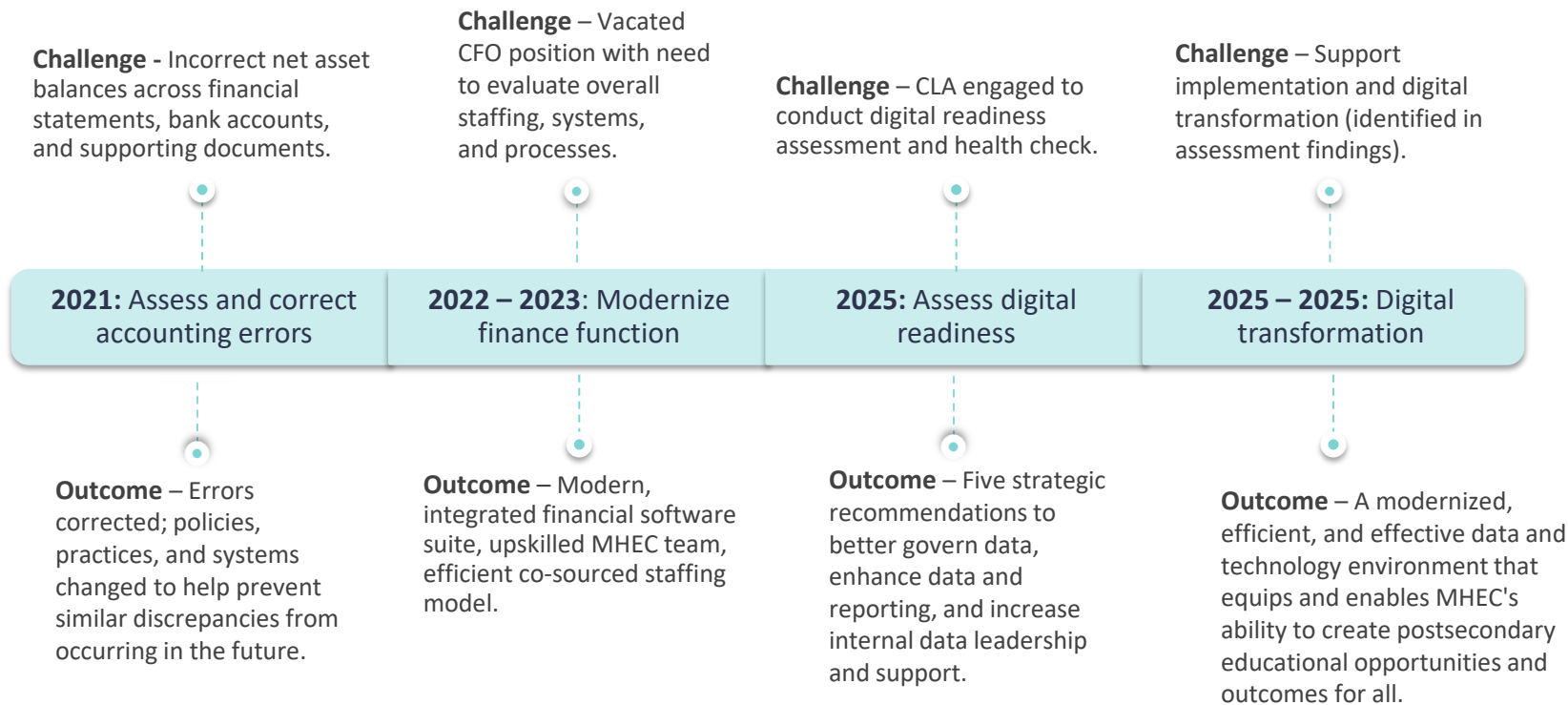
Patrick Connally
Manager
CLA



Susan Heegaard
President & CEO
MHEC



MHEC + CLA Journey



Digital Readiness Assessment: Key Themes

Challenged sources of truth

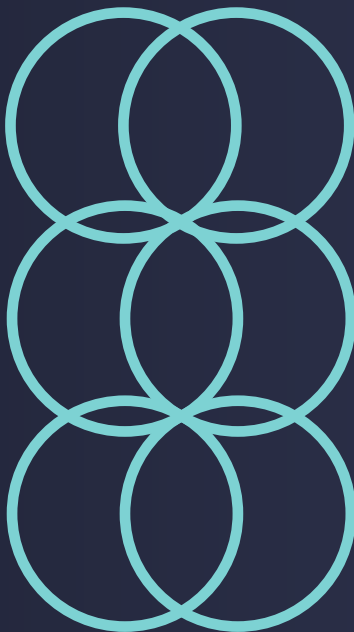
- Data silos and duplication, in small scale, exist.
- These challenge confidence in the data, systems, and reporting in various departments, resulting in separate, manual reporting.

Reporting and adoption varies by team

- Power BI reports not fully meeting needs and outcomes.
- Variation across MHEC exists re: technology maturity, accuracy, and fit; this impacts adoption and can impact data efficiency.

Complex data and reporting needs

- Current Tableau and Power BI dashboards have complex data collection for the critical reporting needs.



Manually intensive processes

- Critical, departmental functions and activities are manually orchestrated (e.g., cost savings, state insights).
- This impacts ability for those roles to focus on more valuable knowledge work.

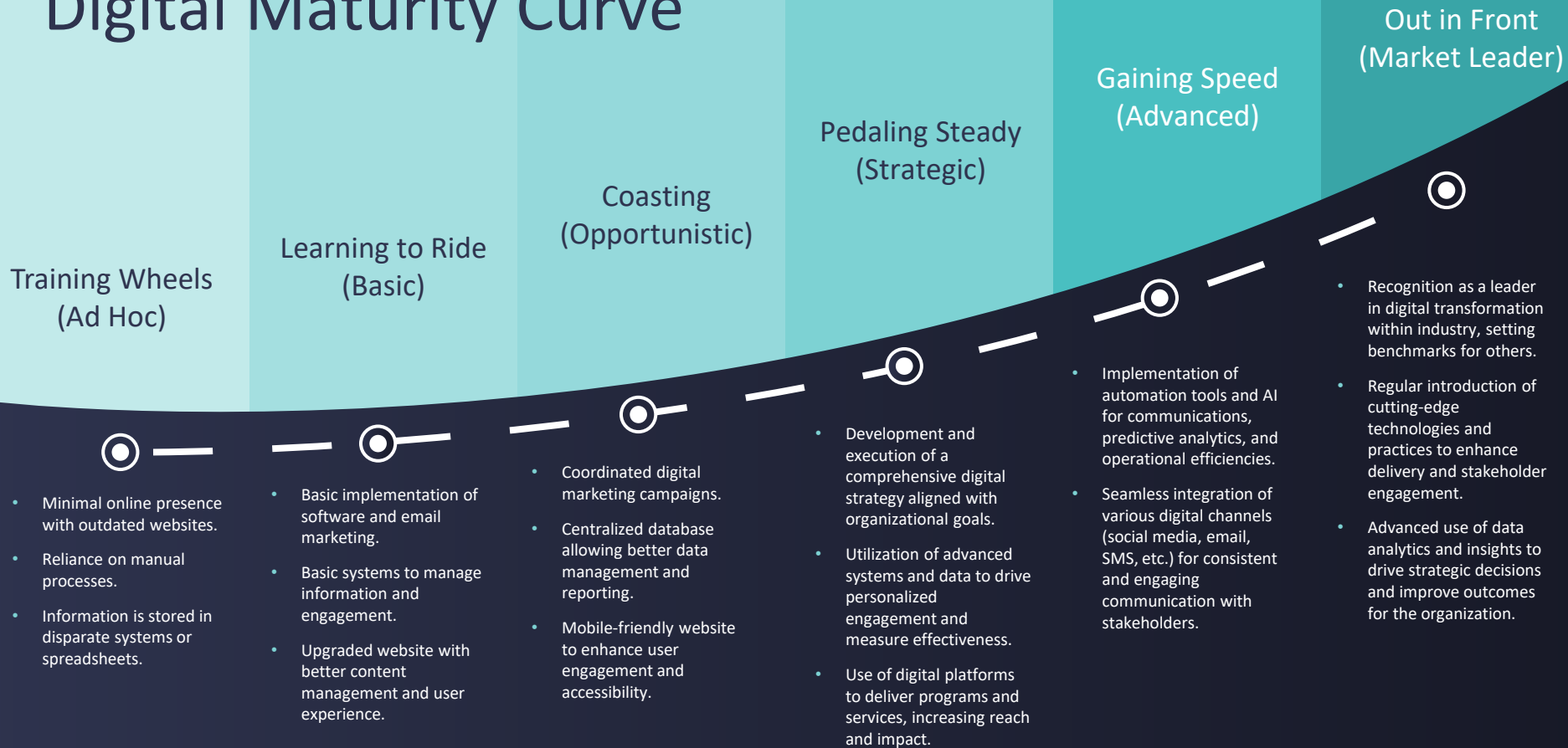
Challenged CRM

- Limited use, varied adoption, application configuration, and data retention (e.g., retaining historical info) challenges.

Lack of data governance

- No clearly defined or mandated technology governance, standards, or use (e.g., one Macbook in use, others using PCs; variation in tool/platform use — Tableau vs. Smartsheet vs. Power BI).

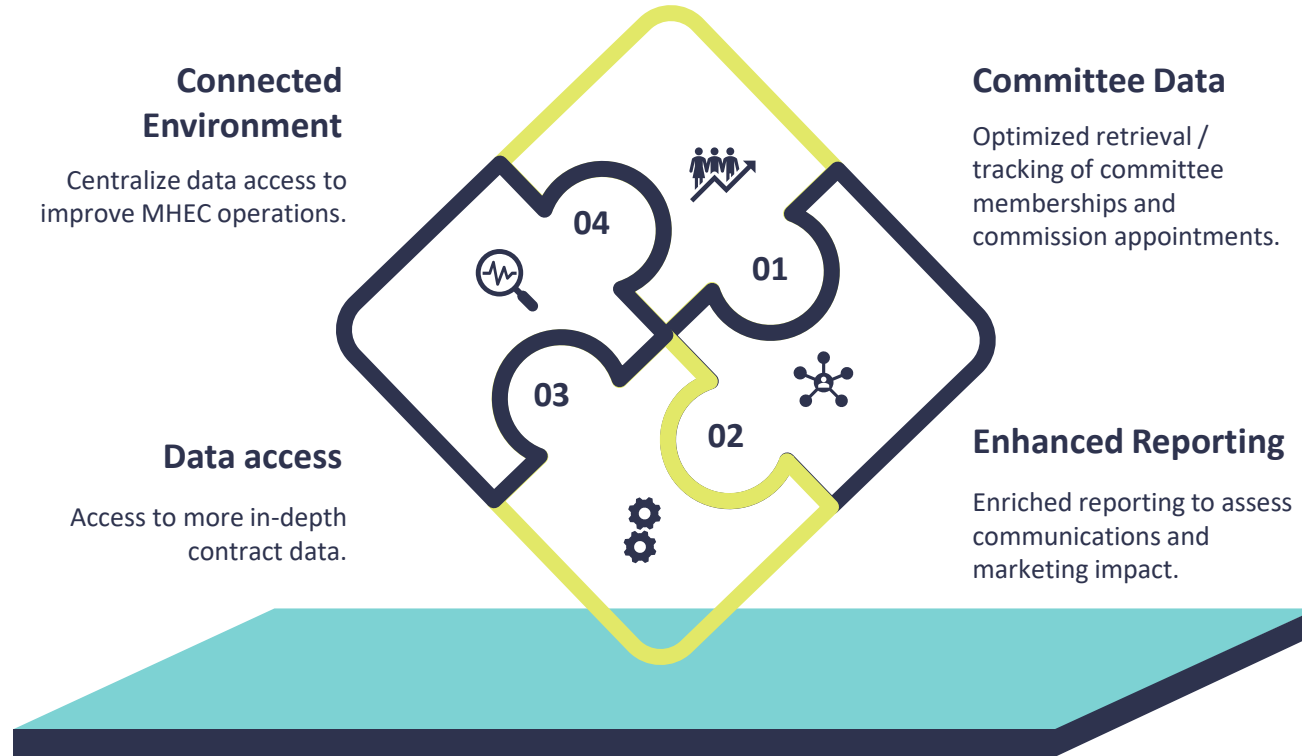
Digital Maturity Curve



Digital Maturity Curve Nonprofits



The Big Opportunity: MHEC Strategic Outcomes



The Journey Ahead



Data
governance



Data
warehouse



Reporting



CRM



Data
leadership

Alignment to MHEC Priorities



Connected environment

Recommendations: Data warehouse, reporting



Data access

Recommendations: Data warehouse, reporting and data governance, increased data leadership



Committee data

Recommendations: Data governance, CRM



Reporting

Recommendations: Data governance, data warehouse, reporting



Common Questions and Challenges

- | | |
|---------------------------|---------------------------|
| 1 Advocacy for investment | 2 Lack of technical staff |
| 3 Change management | 4 User adoption |
| 5 Proving ROI | 6 Knowing where to start |



Looking Ahead

What *questions* do you
have?



Insights

Read more about MHEC's
digital journey, stay informed,
and prepare for what's next.





15 Minute Break

10:55 - 11:10 a.m.





We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Minnesota HR Compliance Update:

Pay Transparency, Family Leave, and Sick and Safe Time

Knowledge *Check*



Learning Objectives

1

Explain recent changes to Minnesota statutes regarding paid family leave, pay transparency, and Minnesota earned sick and safe time

2

Identify the implications of these changes on HR practices and payroll tax topics

3

Identify strategies for compliance with the new regulations and effectively manage HR processes



Agenda

- Introduction
- What is pay transparency?
- Why is it important?
- What are paid leave laws?
- MN paid leave 2026
- MN Sick and Safe Time (ESST)
- Q and A



Meet Your CLA Speakers



Michelle Kohls
HR Systems and
Payroll Director



Courtney Scott
HR Director,
Consulting and
Outsourcing,
Talent Solutions



What Is Pay Transparency?



Definition

Pay transparency involves openly sharing information about compensation for employees within an organization.

- This can range from general salary ranges to specific pay details.

May be used to refer both to internal (only within the organization) and external (shared with the public).

As of January 1, 2025, 14 states have pay transparency laws, including MN!





Types of Pay Transparency

Full transparency

Detailed pay information is shared across the organization and/or publicly.

Partial transparency

Salary ranges are disclosed but individual salaries are kept confidential.

Relative transparency

Pay structure and criteria for determining compensation are shared, but specific salaries are kept confidential.





Why Is Pay Transparency Important?



Lack of Transparency Leads to Mistrust

- Due to how often employers are found guilty of discrimination (which can be intentional or accidental), lack of transparency can lead to mistrust, which can lead to **lack of engagement**, and then eventually **turnover**.





Steps for Employer Compliance



MN Pay Transparency: Covered Employers

One or more sites within the state of Minnesota



Any “individual, corporation, partnership, association, nonprofit organization, group of persons, state, county, town, city, school district, or other governmental subdivision”



Employs 30 or more employees



MN Pay Transparency Requirement

An employer must disclose in each posting for each job opening with the employer the starting salary range, and a general description of all of the benefits and other compensation, including but not limited to any health or retirement benefits, to be offered to a hired job applicant.



Additional Considerations for MN Employers



Definition: For purposes of the law, a job “posting” is defined as any solicitation intended to recruit job applicants for a specific available position made electronically or via printed hard copy that includes qualifications for desired applicants.

Recruiters/third party agencies that post job opportunities on the employer’s behalf are required to comply.

MN Pay Transparency: Implementation

- Review all public and internal-facing job postings and advertisements to include the required wage and benefit information.
 - The legislation defines “salary range” as the “good faith estimate” of the minimum and maximum annual salary or hourly wage range for the position.
 - If there is no salary range for a position, the employer must list the fixed pay rate for that role.
 - A salary range cannot be open-ended (i.e., \$50,000 and up is not acceptable).



Recommended Steps for All Employers

- Evaluate current practices
 - Review existing pay structures and compensation data to identify any disparities and understand current practices.
 - Update job descriptions to accurately reflect roles and responsibilities, and that they align with compensation.
- Update policies and procedures
 - Revise compensation policies and align with pay transparency requirements.
 - This might include how pay ranges are determined and communicated.
 - Create or update a policy that outlines how pay information will be shared within the company and with job candidates.



Recommended Steps for All Employers (cont.)

- Communicate
 - Internally, to let employees and teams know how the new transparency measures will affect pay practices.
 - Externally, by updating job postings, company websites, and recruitment materials, to include the pay and benefit information required.
- Train
 - Educate managers and HR teams about the new laws, the importance of pay transparency, and how to handle employee questions about pay.





Paid Leave Laws





Medical

Employees can take time off for their own medical conditions or disabilities.

Parental

Time off for the birth, adoption, or foster care placement of a child.

Family

To care for a family member with a serious health condition or bonding with a new child

Bereavement

Time off to attend a funeral and meet family obligations for a loved one.

Types of Paid Leave

Paid leave laws can differ widely depending on the state or locality.





MN Paid Leave Law 2026



Minnesota's new paid leave law, effective **January 2026**, requires both employers and employees to contribute equally to the program, providing up to 12 weeks of paid medical leave per benefit year

Provides paid time off in the event of serious health condition, to care for a family member or a new child, for certain military-related events or for certain personal safety issues.



MN Paid Leave Law

- **Contribution split:** Both employers and employees will contribute to the program. Employers must pay at least 50 % of the total premium and can deduct the remainder from employee pay. Employers can also choose to pay more than 50%, which would be a greater benefit than required under the new state law.
- **Benefit details:** Eligible employees can access up to 12 weeks of paid medical leave per benefit year, and in specific circumstances, up to 20 weeks, to be used for various purposes, including personal medical conditions, family care, and other qualifying reasons.
- **S-Corp shareholders:** In Minnesota, S-Corp shareholders are considered employees and are generally required to pay into the state's medical leave program; they will contribute to the premiums for their own potential medical leave benefit.





Steps for Employer Compliance



Paid leave covers most Minnesota employers with one or more employees, with exceptions for employees of tribal nations or the federal government and self-employed individuals who choose to provide their own coverage for themselves.

Small businesses with 30 or fewer employees will be eligible for reduced premiums and may be eligible for small business assistance funding to hire temporary workers or to increase an existing worker's wages.



MN Employers: Things to Remember

- **Employee communication:** Employers are responsible for verifying that employees are aware of their rights and the procedures for applying for paid leave.
- **Equivalent plan option:** Employers can offer an equivalent plan option, under Minnesota Paid Leave, by providing employees with an equivalent plan that meets or exceeds the coverage offered by the state. There are two options through an insurance carrier or under a self-insured plan Note-some equivalent plans may require state approval.
- **Reporting requirements:**
 - December 2025 – deadline for employers to notify employees about paid leave benefits.
 - January 2026 – individuals and families can begin taking paid leave. Payroll deductions begin for employers and employees January 2026.
 - April 2026 – first quarterly premiums are due from employers.



Recommended Steps for Employers

- Update policies and display workplace posters by the fall of 2025 to reflect the new law, effective 2026
- First premium is due April 30, 2026 *(note that the premium rate for the program's first year, 2026, has not yet been set)*
- When Paid Leave begins for Minnesotans in 2026, the premium rate will be 0.88 percent. After the first year in 2026, the premium rate will be set annually. Learn more about the premium rate, including the reduced rate for small employers, and [estimate your premium payments](#)."

Minnesota Paid Leave | <https://mn.gov/deed/paidleave/employers/premiums/>





Minnesota Sick and Safe Time



What Is the MN ESST?

- Effective January 1, 2024, all organizations with employees who work a minimum of 80 hours in Minnesota are required to provide earned sick and safe time (ESST). The new ESST requirements include:
 - Providing the required paid time off
 - Notifying employees of the change
 - Including earned and used ESST balances on paystubs
- At a minimum: employers must provide each employee in Minnesota with one hour of ESST for every 30 hours worked, with the ability to accumulate at least 48 hours of ESST each year.
 - Employees must be able to roll over up to 80 hours
- A paid time off plan or other type of paid leave (including sick or vacation time) can satisfy the ESST law if the plan meets Minnesota's ESST requirements.



What Can ESST Be Used For?

1. The employee's mental or physical illness, treatment or preventive care;
2. A family member's mental or physical illness, treatment or preventive care;
3. Absence due to domestic abuse, sexual assault or stalking of the employee or a family member;
4. To make funeral arrangements, attend a funeral service or memorial or address financial or legal matters that arise after the death of a family member;
5. Closure of the employee's workplace due to weather or public emergency or closure of a family member's school or care facility due to weather or public emergency; and
6. When determined by a health authority or health care professional that the employee or a family member is at risk of infecting others with a communicable disease.



Options for Offering ESST

Option 1. Accrual and carryover

- ESST accrues at a rate of at least one hour for every 30 hours worked;
- Employees accrue a minimum of 48 hours of ESST in a year (more if the employer agrees to a higher amount); and
- Employees can carry over unused ESST into the next year. However, at no time can an employee's accrued ESST exceed 80 hours (unless the employer agrees to a higher amount).

Option 2. Front loading with pay out and no carryover

- A minimum of 48 hours of ESST is provided to an employee and made available for immediate use at the start of each year; and
- Unused ESST hours are paid out at the end of the accrual year at the employee's base rate.

Option 3. Front loading with no pay out and no carryover

- A minimum of 80 hours of ESST is provided to an employee and made available for immediate use at the start of each year; and
- ESST hours the employee did not use are not paid out at the end of the accrual year.

Option 4. Company PTO plan compliant with one of the above; employee may use PTO for any sick and safe reasons



Recommended Steps for MN Employers

- In addition to ESST compliance with one of the four options, employers are required to:
 - Provide employees with the total number of earned sick and safe time hours available for use, as well as the total number of earned sick and safe time hours used at the end of each pay period;
 - Provide employees with a notice by Jan. 1, 2024 — or at the start of employment, whichever is later — in English and in an employee's primary language if that is not English, informing them about ESST; and
 - Include a sick and safe time notice in the employee handbook, if the employer has an employee handbook.





The Talent Solutions Team Can Help



Become Pay Transparency and Paid Leave Ready!

Advise on
compliant job
posting with new
laws

Assess current HR
/ Recruiting /
Compensation
practices

Develop new
policies and
procedures

Develop
communication
plan(s)

Train HR teams,
managers, and
employees

Market price jobs
and build a pay
structure

Develop salary
ranges that meet
pay transparency
requirements

Evaluate current
employees against
pay ranges

Support with state
reporting
requirements

Assess current PTO
practices against
the MN ESST

Advise on a
compliant ESST
policies



Talent Solutions at CLA

Overcome workforce challenges and grow your organization by growing the people within it.



Total recruitment

Overcome recruiting challenges like high turnover and candidate experience – while saving time and money in the hiring process



Total HR

Creating and implementing people strategy, policies, HR systems, and managing daily employee needs.



Total payroll

Full suite of human capital management, reliable payroll, and reporting system



Connect With Us Today!

Michelle Kohls

HR Systems and Payroll Director
michelle.kohls@CLAconnect.com
262-641-2283



Courtney Scott

HR Director,
Consulting and Outsourcing
Talent Solutions
courtney.scott@CLAconnect.com
317-569-6215



Questions





Lunch Break

12 - 1 p.m. – Recharge Room





We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

This Is Why We Can't Have Nice Things – The Ramifications of Nonprofit Leaders Behaving Badly

Emmett Robertson & Marcus Pope

Learning Objective

At the end of this session, you will be able to:

Recognize the ethical implications and lessons learned from recent high-profile cases to promote integrity and accountability in nonprofit leadership





We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Risk Management and Cybersecurity Trends

Safeguarding Your Organization and the Digital Frontier

Presenters



David Anderson

Principal, Minneapolis, MN

David is a principal and cybersecurity consultant with more than 13 years of experience in the Cybersecurity field. He performs, and provides project management for network penetration testing, internal vulnerability assessments, and social engineering engagements.



Jake Taylor

Principal, Minneapolis, MN

Jake is a principal in CLA's Value and Risk practice. Jake has more than 15 years of professional experience in providing internal audit (business process and IT) and risk assessment services.



Learning Objectives

- Review common approaches used to identify risk in your organization
- Understand the latest trends in cybersecurity risk
- Explore ways to mitigate risk – both across your business processes and your IT environment





Identifying Risk



Identifying Risk

Businesses today face
ever-increasing and
changing risks

How do we compete in a world of artificial intelligence?

How do we attract, hire and retain top performers?

How do we keep our finger on the pulse of changing laws, regulations, and compliance matters that impact our organization?



Identifying Risk

Identifying risks will help your organization:

- Think about which risks are most critical to your success
- Align your resources (people, time, money) to focus on areas of greatest risk
- Drive a common understanding across your leadership and governance teams regarding your critical risks
- Provide a starting point on risk tolerance... what risks are we willing to take vs. what risks do we want to try and avoid
- Look for opportunities in those risks



Identifying Risk

- Identification can be driven from multiple sources
 - Enterprise risk management
 - Audit results
 - Internal team discussions
 - Networking / industry associations
 - Risk publications
- Your approach will vary – what makes sense for one organization may not make sense for you



Identifying Risk – ERM

Enterprise risk management

- Ties to your strategy (top-down risk assessment)
- Uses a risk framework
- Involves gathering feedback on risk from key leaders
 - Help significantly with buy-in
- Ranks the risks gathered above
 - Impact
 - Likelihood



Identifying Risk – ERM

- Enterprise risk management
 - Drives to risk rankings that help you easily prioritize the highest risks
 - Leads to formal mitigation plans as a means to reduce the identified risks
- Overall
 - A very formal process
 - May be the most expensive method
 - But a widely-accepted process used by many organizations

Identifying Risk – Informal Approaches

- Audit results
 - What did your external audit team find?
 - Risk: focused more on financials... might miss important operational or strategic risks
- Internal team discussions
 - What do your teams think about risk? What do they experience daily that may be an indication of risk?
 - Risk: could lead to transactions or process risks... may not be critical to achieving your strategy



Identifying Risk – Informal Approaches

- Networking / industry associations
 - What are your peers struggling with?
 - What topics are being discussed at conferences you attend, local industry association meetings, etc.?
 - Risk: are all risks relatable (your size, location, clientele may be different)
- Risk publications
 - What's out there in the public realm?
 - Risk: are all risks relatable (your size, location, clientele may be different)



Identifying Risk

- If you go through the effort to identify your risks... *do something about it*
- Identification alone won't help
 - How will you respond to the risks?
 - How will you monitor the risks?
 - Who is tasked to champion the effort?
 - How often will you revisit?





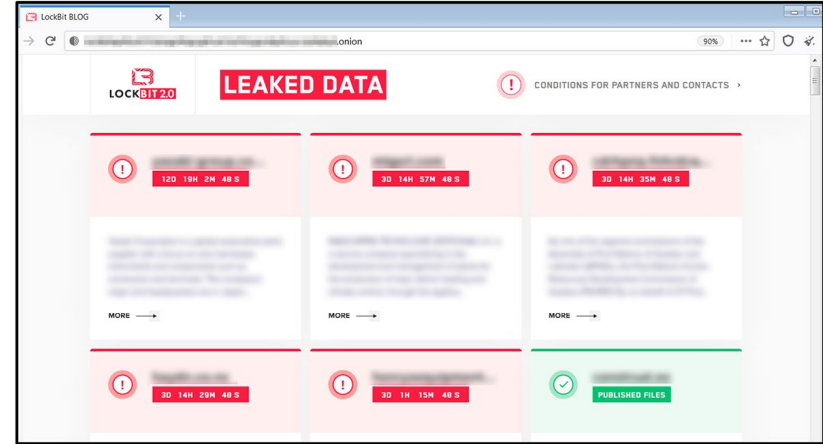
Trends in Cybersecurity Risk



Cybercrime and Black-Market Economies

- Black-market economy to support cyber fraud
 - Business models and specialization
 - Underground marketplace (The Dark Web)
 - Ransomware-as-a-Service
- Most common cyber fraud scenarios we see affecting our clients
 - Diverting payments
 - Ransomware and interference with operations

To the Hackers, we all look the same.



They will hit you with any or all of the following:

1. Email Spear Phishing Attacks
2. Password Guessing and Business Email Account Takeovers
3. Payment and Funds Disbursement Transfer Fraud
4. Ransomware
5. Extortion to avoid breach disclosure

Microsoft Digital Defense Report

Credentialed phishing schemes on the rise – indiscriminately target all inboxes



The volume of phishing attacks in orders of magnitude *greater than all other threats*



Over 700 million phishing emails blocked per week



Business Email Compromise (BEC)



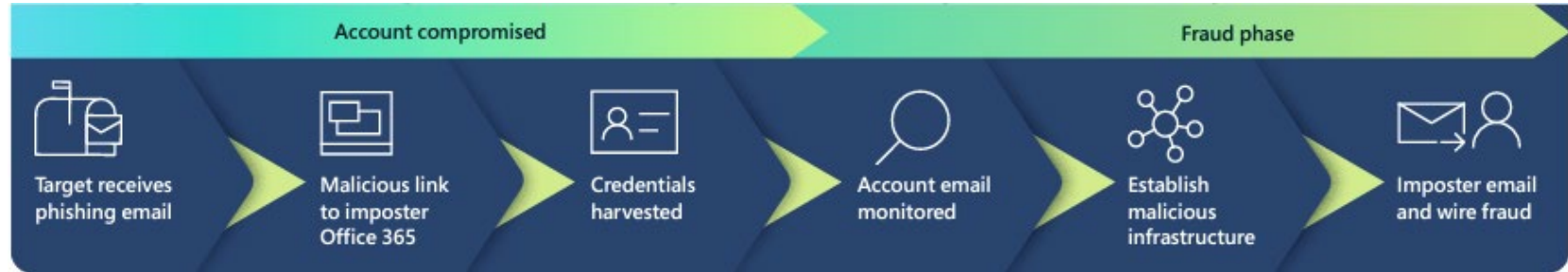
THE \$55 BILLION SCAM

Fraudsters impersonate employees, service providers, or vendors via email in an attempt to change:

- Change vendor payments, change direct deposit, purchase gift cards, etc.

*Attackers focusing on
Microsoft 365*

BEC Timeline



1. Vendor was phished via a fake M365 website and provided password to attacker
2. Hacker monitored vendor's email for months and noticed a monthly payment
3. Hacker created new, similar email address and attacked AP department to update bank account information

<https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022>



Homoglyph in Action

- A homoglyph domain that looks identical to a mail domain the victim recognizes is registered on a mail provider with a username that is identical
- Hijacked email is then sent from the hijacked domain with new payment instructions

Technique	% of domains showing homoglyph technique
sub l for I	25%
sub i for l	12%
sub q for g	7%
sub rn for m	6%
sub .cam for .com	6%
sub 0 for o	5%
sub ll for l	3%
sub ii for i	2%
sub vv for w	2%
sub l for ll	2%
sub e for a	2%
sub nn for m	1%
sub ll for l, sub l for i	1%
sub o for u	1%

Analysis of over 1,700 homoglyph domains between January–July 2022. While 170 homoglyph techniques were used, 75% of domains used just 14 techniques.

<https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022>



Fw: Payment

DP ○ Dwayne Pearse <dwayne@vend0r.com> Friday, November 22, 2024 at 1:25 PM

To: ○ Andrew Johnson

Payment.pdf
1.2 MB

Download • Preview

⚠ This message is high priority.

We have an update in receiving payments, Via ACH. Kindly advice how we effect this change immediately.

Dwayne Pearse
dwayne@vendor.com
549-555-2232

From: Dwayne Pearse <dwayne@vendor.com>
Sent: Thursday, November 21, 2024 2:15 PM
To: Natalie Berger <william@vendor.com>; Barb Rogers <barbara@vendor.com>
Subject: FW: Payment

From: Andrew Johnson <bjohnson@company.com>
Date: Thursday, November 21, 2024 at 2:14 PM
To: Dwayne <dwayne@vendor.com>, Natalie Berger <william@vendor.com>
Subject: Payment

Good afternoon,

Attached is the backup for invoices paid from the company.

Andrew Johnson
Accounts Payable Supervisor

○ Dwayne Pearse <dwayne@vend0r.com>

Hacker purchased
look-alike domain

Hacker inserted themselves into
legitimate email thread



Ransomware

- Attack on the *availability* of data
- Encrypt / lock up critical systems, applications, and data
- Ransom demands (**PLURAL**)
 - To unlock systems/decrypt data
 - To *NOT* disclose sensitive data that was stolen
- Payments are often in cryptocurrency (Bitcoin)



Top Causes of Ransomware

Exploited vulnerability



Compromised credentials



Malicious email





Mitigating Risk



Mitigating Risk – General

- Will risk be reduced to zero?
- Can all risk be mitigated?
- Numerous methods exist that may help your organization mitigate risk
 - Insurance, contracting, vendor management
 - Financial statement, operational audits, IT audits / assessments
 - Policies, procedures, internal controls
 - Code of ethics, ethics hotline



Mitigating Risk – General

- Insurance, contracting, vendor management
 - Can you insure for the risk... cyber insurance?
 - Can you structure contracts to reduce risk?
 - How do you assess vendors to reduce the risk they present to your organization?
- Financial statement, operational audits, IT audits / assessments
 - Beyond the external financial statement audit... how frequently are you reviewing your other key processes?



Mitigating Risk – General

- Policies, procedures, internal controls
 - Are policies and procedures documented to guide employee's actions when processing transactions?
 - Do you have controls implemented?
 - Are your controls effective?
- Code of ethics, ethics hotline
 - What guides employee's overall behavior?
 - What are employees held accountable to?
 - Is there a reporting mechanism in place?



Mitigating Risk – General

Risk Event #	Inherent Score	Residual Score	Risk Tolerance	Risk Trend
2.1	25	15	12	N/A
2.2	20	14	12	N/A

Cyber Security and Data Privacy Protection Dashboard

Last Review Date	Category	Definition	Executive Owner
N/A	Compliance	Sample Company's ability to maintain adequate cybersecurity measures/controls to protect against malicious attacks and/or intrusions impacting the confidentiality, integrity, and availability of critical data/systems. This, also, includes ability to protect sensitive information and comply with requirements of privacy and security regulations.	CFO

Risk Headline Event *(inherent risk score)*

2.1 Sensitive data hosted outside of CFP is impacted by a data breach stolen/exposed causing the company reputational damage. (25)

2.2 Key systems and data hosted outside of CFP are not available or corrupted due to a key vendor experiencing ransomware, denial-of-service attack (DoS), etc. causing resulting in loss of revenue and reputational damage. (20)

Potential Root Causes

- Increasing external threats - volume and severity
- Weak Third-Party Risk Management Practices
- Excess or unauthorized access to sensitive Data
- Credentials obtained through Phishing
- Data provided/ used by third party without proper authorization
- Internal malfeasance

Key Mitigation Strategies

Third-Party Risk Mgmt.

Access & Provisioning

Data Governance

Phishing Training/ Testing

Employee Background Checks

Incident & Crisis Mgmt.

Insurance

Risk Rating and Scores

Risk Rating	Risk Score
Inconsequential	1-5
Minor	6-9
Moderate	10-15
Major	16-20
Catastrophic	> 20

Risk Trend Indicator

Increasing	↑
Stable	↔
Decreasing	↓

Mitigation Status

Assessing
Strengthening
Enhancing
Monitoring



Mitigating Risk

Business Email Compromise

- Block email from newly-created domains
- Develop formalized processes for updated payment details
 - Do **NOT** rely upon email
 - Call back known, good number
 - Approval process
 - Train accounting / finance staff on processes



Mitigating Risk

Business Email Compromise

- Configure strong password requirements
- Require multi-factor authentication for all users
- Configure email headers / banners that warn users of external emails



Mitigating Risk

Ransomware

- Strong patch management
- Logging and monitoring
- Cybersecurity insurance
- Strong passwords / authentication
- Antivirus / endpoint controls
- Secure (isolating) backups





Data Backups

Attackers are getting smarter and deleting or encrypting online backups; so, organizations should certify that they have **IMMUTABLE** or **OFFLINE** copies of backup and restore files available.

Perform an in-depth review of file permissions for network file shares and pay special attention to locations storing electronic backup and restore files.

Practice a full system and data restore to verify your confidence in full system and data restore capabilities.



CLA Digital Services Overview

Experience our data
driven difference

Rethink business and **turn challenges into opportunities** with modernized systems and processes adapted to your business.

Artificial Intelligence

Leveraging the power of AI and Machine Learning to improve operations and achieve strategic outcomes.

Data Analytics & Insights

Developing customized dashboards and data warehouse solutions to highlight key metrics, benchmarking, and performance indicators.

Cybersecurity

Combining technical expertise and risk-based methodologies to help protect an organization's systems and data with a strong cybersecurity plan.

Automation & Integration

Improving organizational efficiency through automated workflow management solutions and enhanced communication platforms.

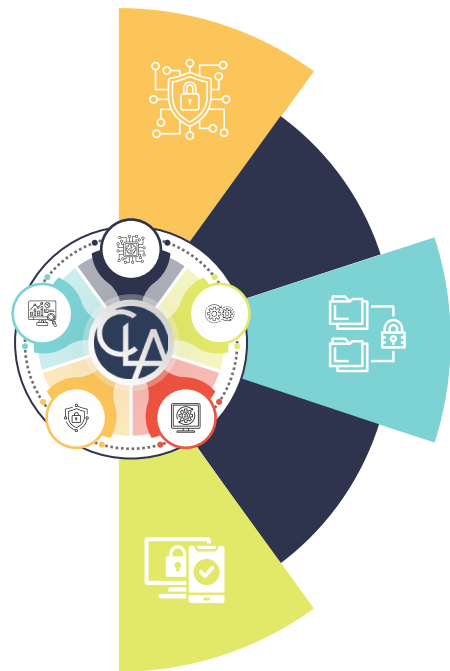
Software Reseller

Software solutions to help you automate and streamline your processes.



Nonprofit Cybersecurity Services

CLA's Nonprofit Cybersecurity practice has several packages available to take the guess work out of security assessments. Each package has been tailored for the organization's size and complexity, while still being focused on identifying key risks within the environment.



Size and Estimated Fees

Key Services

Risk Identification and Strategic Value

Large Size and/or
Complex
Environment

\$18,000+

- External and Internal Penetration Test
- Cloud Tenant Security Review
- Cyber Readiness Assessment and Strategy Workshop

- More robust assessment of the current technologies and controls in place to protect the environment against external and internal attacks.
- In addition to the technical assessment, the team will conduct a governance and operational review to produce a strategic roadmap for future enhancements.

Medium
Size and
Complexity

\$7,500 - \$18,000

- External Vulnerability Assessment
- Cloud Tenant Security Review
- Rapid Internal Penetration Test

- Detailed review of the technologies and controls in place to protect the organization against external threats.
- Health assessment of the current configuration of the Cloud tenant and internal network architecture.

Small Size and/or
Basic Environment

\$4,500 - \$7,500

- External Vulnerability Assessment
- Self-Assessment Cyber Questionnaire and CLA Review Session

- Initial introduction to cyber risk assessments, focusing on the organization's externally facing assets.
- Meeting with one of CLA's cyber professionals to review the results of the external and self-assessment risk profile.



Questions and Answers



Thank You!

David Anderson, OSCP
Principal, Cybersecurity

612-376-4699

david.anderson@CLAconnect.com

Jake Taylor, CPA

Principal, Business Risk Services

952-463-7811

jacob.taylor@CLAconnect.com



CLAconnect.com



CPAs | CONSULTANTS | WEALTH ADVISORS

©2025 CliftonLarsonAllen LLP. CLA (CliftonLarsonAllen LLP) is an independent network member of CLA Global. See [CLAglobal.com/disclaimer](https://claglobal.com/disclaimer).
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.



Thank you for joining us today!

It takes balance.TM

It's our job to engage in conversations, listen to what you really want, and apply our talents and experience to make extraordinary impact on your organization and life.





Social Hour

Until 4 p.m. on the Terrace

