CYBERSECURITY BEST PRACTICES

FOR EMPLOYEE BENEFIT PLANS

Turning DOL guidance into governance, protection, and protection, and readiness

Cameron Hodson and Diane Nesbit

Larson
CERTIFIED PUBLIC ACCOUNTANTS

CYBERSECURITY NOW HAS A PLAN FILE

Cameron

EBSA is asking how employee benefit plans protect data, systems, assets, and participants.

Plan data

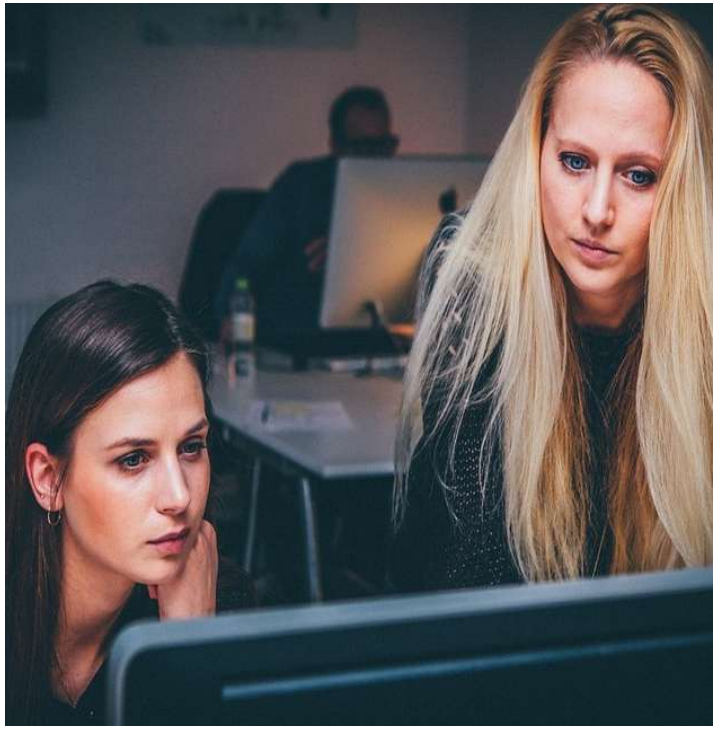
PII, PHI, payroll, eligibility, eligibility, balances, claims, claims, loans, and distributions.

Plan money

Fraud can move through through account access, access, payment changes, changes, distributions, and and reimbursements.

Plan proof

Policies only help when the organization can show they operate.



> “Compliance is not the finish line. Protecting participants is the work.”

Sources: DOL EBSA Cybersecurity Program Best Practices and FY 2026 enforcement release.

Larson CERTIFIED PUBLIC ACCOUNTANTS

THE SESSION MOVES FROM GOVERNANCE TO PROOF

Cameron

A 75-minute working session, plus a break and Q&A.

01
GOVERN

Program, roles, risk assessment, and fiduciary oversight

02
PROTECT

Access, authentication, data protection, monitoring, and secure systems

03
RECOVER

Resilience, incident response, response, vendors, and SOC report review

04
PROVE

Training, insurance, evidence files, audits, and DOL inquiry readiness

10 MIN BREAK

5 MIN Q&A

Larson CERTIFIED PUBLIC ACCOUNTANTS

POLL 1: Where does employee benefit plan cybersecurity primarily live in your organization?

SELECT THE CLOSEST ANSWER

THE DOL LIST IS THE MAP, NOT THE DECK

Cameron

The six working themes roll up into Govern, Protect, Recover, and Prove.

GOVERN

1, 2, 4

Governance

Formal program
Annual risk assessment
Defined roles

PROTECT

5, 10

Access + data

Least privilege
MFA
Encryption

8, 11

Secure systems

SDLC
Vulnerability scans
Technical controls

RECOVER

9, 12

Resilience + IR

BCP, DR, IR
After-action learning
Incident response

6

Vendor oversight

Cloud reviews
Provider assessments
Contract terms

PROVE

3, 7

Training + proof

Annual training
Third-party audits
Remediation evidence

Source: DOL EBSA Cybersecurity Program Best Practices.

Larson CERTIFIED PUBLIC ACCOUNTANTS

SPONSORS AND TPAS CARRY DIFFERENT WORK

Cameron

The same guidance creates different practical questions depending on where you sit.

PLAN SPONSOR LENS

- What controls do we operate?
- What has been outsourced?
- How do we monitor providers?
- What proof do we retain?

TPA / PROVIDER LENS

- What controls do we perform for clients?
- What evidence can we provide?
- How do we communicate limits?
- How fast can we support an inquiry?

> “The key is not doing everything yourself. The key is knowing who does what, and keeping the proof.”

01

START WITH THE DATA FLOW

Governance and fiduciary foundations

Larson
CERTIFIED PUBLIC ACCOUNTANTS

START WITH THE DATA FLOW

Cameron

You cannot defend or evidence what you have not mapped.

Participants

Accounts, claims, elections, identity

→

Sponsor systems

HRIS, payroll, email, file shares

→

Plan providers

TPA, recordkeeper, carrier, PBM

→

Downstream parties

Subservice orgs, custodians, support vendors

Retirement plan examples

- Payroll files
- Contribution elections
- Balances, loans, distributions

Health and welfare examples

- Eligibility and enrollment
- Claims and dependent data
- PHI and reimbursement records

Larson CERTIFIED PUBLIC ACCOUNTANTS

GOVERNANCE LEAVES EVIDENCE

Cameron

A defensible program shows who owns the work and how decisions are made.

Formal program

Written policies. Senior management approval. Annual review. Framework alignment. Clear expectations for employees and providers.

Defined responsibility

Plan-specific owners. Information security roles. Escalation paths. Fiduciary oversight and committee documentation.

Evidence trail

Risk assessments. Vendor reviews. Access Access reviews. Training completion. Remediation tracking. Meeting minutes.

> “Policies matter. The record of operating them matters more during an inquiry.”

Larson CERTIFIED PUBLIC ACCOUNTANTS

RISK ASSESSMENT DIRECTS THE SPEND

Cameron

Good risk assessment makes cybersecurity manageable, not perfect.

1 → Identify assets, data, systems, and providers

2 → Evaluate threats, vulnerabilities, likelihood, likelihood, and impact

3 → Map existing controls and and remaining gaps

4 → Mitigate, transfer, avoid, avoid, or accept the risk risk

5 Assign owners, due dates, and reporting

Larson commentary

A sponsor can use the broader corporate program. The missing piece is often the benefit-plan overlay: plan data, overlay: plan data, providers, internal owners, and evidence.

Larson CERTIFIED PUBLIC ACCOUNTANTS

02

ACCESS IS A LIFECYCLE

Access management, authentication, and data protection

Larson
CERTIFIED PUBLIC ACCOUNTANTS

ACCESS IS A LIFECYCLE, NOT A LOGIN

Cameron

The right access, for the right reason, for only as long as needed.

01 JOINER

Approve and provision based on on job duties

02 MOVER

Reassess when duties or departments change

03 LEAVER

Remove access promptly when the the relationship ends

Controls that should show up in the file

Role-based permissions, least privilege, unique accounts, quarterly access reviews, help desk tickets, termination checklists, and privileged-account monitoring.

POLL 2: How often does your organization formally review access?

PROTECT THE DATA WHEREVER IT LIVES

Cameron

Controls need to follow the file, the account, and the transaction.

Authentication

Strong passphrases, SSO where practical, MFA for sensitive and Internet-facing access.

Transmission

Secure portals, encrypted transfer, limited email attachments, approved storage locations.

Retention

Data classification, minimum necessary copies, retention schedules, secure schedules, secure disposal.

DATA THAT DESERVES EXTRA CARE

- PII and PHI
- Payroll and eligibility files
- Distribution and reimbursement instructions
- Participant contact and banking changes
- Administrative and privileged accounts

Sources: DOL EBSA Best Practices and Larson access-management blog draft.

Larson CERTIFIED PUBLIC ACCOUNTANTS

FRAUD OFTEN STARTS WITH A SMALL CHANGE

Cameron

A bank change, address change, or email change should not move money by itself.

SCENARIO

A participant changes an email address and bank account. Two days later, a full-balance distribution request appears.

Poll 3: What would happen in your org?

What should happen before the transaction is released?

1

Slow down

Trigger elevated review

2

Verify identity

Use independent method method

3

Separate duties

Approve outside the request path path

4

Document

Retain what was checked checked

> "The right control adds friction at exactly the right right moment."

Larson CERTIFIED PUBLIC ACCOUNTANTS

03

SECURE SYSTEMS ARE BUILT, TESTED, AND MONITORED

System security, resilience, and operational continuity

Larson
CERTIFIED PUBLIC ACCOUNTANTS

SECURE SYSTEMS ARE BUILT, TESTED, AND MONITORED

Cameron

The control story changes depending on whether you build or buy.

Build

Management-approved changes
Code review
QA and security testing
Production approval
Post-release monitoring

Buy

Review provider SDLC
Confirm relevant systems are in scope
Understand change management
Track bridge letters and updates

Test

Vulnerability scans
Penetration testing
Patch tracking
Logs and alerts
Remediation evidence

A vulnerability scan finds known weaknesses. A penetration test asks how far an attacker could get.

Larson
CERTIFIED PUBLIC ACCOUNTANTS

POLL 4: When did your organization last test recovery?

RESILIENCE TURNS DISRUPTION INTO PROCESS

Cameron

Business continuity, disaster recovery, and incident response answer different questions.

BCP

How do critical operations continue?

People, processes, facilities, communications, vendors

DR

How do systems and data come back?

Backups, applications, infrastructure, restore steps

IR

How do we respond while it is happening?

Detection, containment, evidence, notification, recovery

RTO

How long can the process be down?

RPO

How much data can the plan afford to lose?

Larson CERTIFIED PUBLIC ACCOUNTANTS

04

THE FIRST HOUR DECIDES THE TONE

Incident response, vendor risk, and SOC reports

Larson
CERTIFIED PUBLIC ACCOUNTANTS

THE FIRST HOUR DECIDES THE TONE

Cameron

Decisions move faster when authority, evidence, and communication are already defined.

- **Detect** — Report and triage
- **Contain** — Limit further damage
- **Investigate** — Preserve evidence and assess impact
- **Communicate** — Coordinate legal, insurer, provider, and participant communications
- **Recover** — Restore systems and operations
- **Improve** — After-action review and remediation

> “Do not wait for the breach to decide who can call counsel, the insurer, or insurer, or the provider.”

Larson CERTIFIED PUBLIC ACCOUNTANTS

POLL 5: Who would lead your organization's response to a benefit plan cybersecurity issue?

VENDOR OVERSIGHT RUNS THROUGH THE FULL RELATIONSHIP

Cameron

Due diligence is not a one-time document request.

01

Inventory

Services, data, criticality, owner, owner, review date, open issues issues

→

02

Diligence

Policies, SOC reports, prior incidents, continuity, subcontractors

→

03

Contract

Security requirements, notifications, audit rights, insurance, data terms

→

04

Monitor

Current reports, exceptions, incidents, remediation, organizational changes

A resilient plan depends on resilient service providers.

Larson CERTIFIED PUBLIC ACCOUNTANTS

SOC REPORTS NEED A REAL REVIEW

Diane

A SOC report is evidence. It is not a certificate.

1 **Right report?**

SOC 1 or SOC 2, Type 1 or Type 2, relevant service

2 **Current period?**

Report date, coverage period, bridge letter if letter if needed

3 **Scope?**

Product, platform, location, process, subservice subservice organizations

4 **Opinion + exceptions?**

Modified opinion, test exceptions, management response

5 **User controls?**

Complementary user entity controls and sponsor responsibilities

6 **Conclusion?**

Reviewer, follow-up, residual risk, and evidence evidence retained

Larson CERTIFIED PUBLIC ACCOUNTANTS

POLL 6: What typically happens when your organization receives a SOC report?

10-MINUTE BREAK

When we return, Diane will focus on training, monitoring, documentation, documentation, insurance, and DOL inquiry readiness.

Think about this: Which area would be hardest for your organization to evidence today?

Larson
CERTIFIED PUBLIC ACCOUNTANTS

05

TRAINING TURNS POLICY INTO BEHAVIOR

Monitoring and continuous improvement

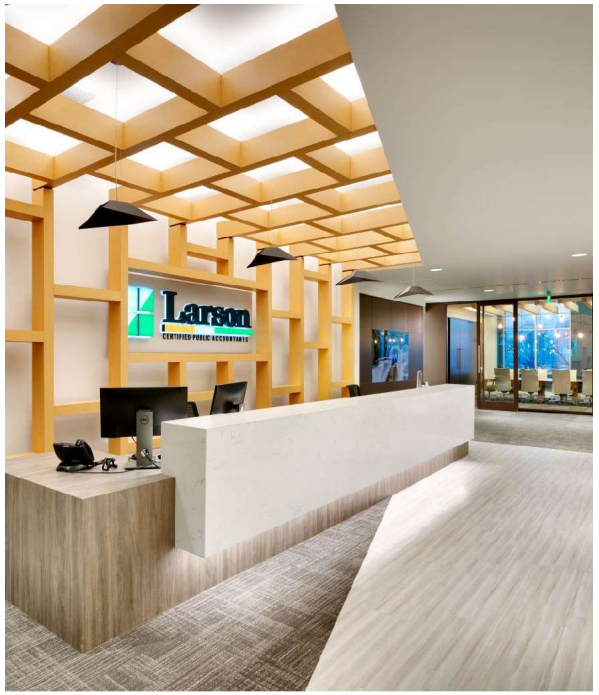
Larson
CERTIFIED PUBLIC ACCOUNTANTS

TRAINING TURNS POLICY INTO BEHAVIOR

Diane

Annual training should reflect the risks the plan actually faces.

Everyone	Phishing, smishing, passwords, MFA, device hygiene, incident reporting
Benefits + HR	Participant verification, secure file transfer, sensitive data handling handling
Payroll + finance	Banking changes, distribution requests, contribution and eligibility files eligibility files
IT + help desk	Password resets, MFA changes, privileged accounts, impersonation
Fiduciaries	Oversight, escalation, vendor evidence, incident authority



Participant education should reinforce basic online security: MFA, unique passwords, account alerts, account alerts, device updates, and reporting suspicious activity.

Sources: DOL EBSA Best Practices and Online Security Tips.

Larson
CERTIFIED PUBLIC ACCOUNTANTS

MONITORING GIVES MANAGEMENT A PULSE

Diane

A useful dashboard shows what is overdue, deteriorating, or unverified.

Training completion

Target: 100%

MFA coverage

Sensitive systems

Access reviews

Quarterly status

Vendor reviews

SOC reports and gaps

Critical vulnerabilities

Open and aged

Backups and restore tests

Last successful test

Incidents and near misses

Trend and response

Corrective actions

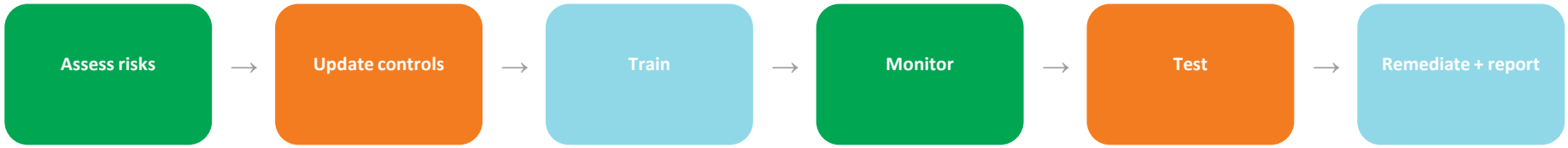
Owners and due dates

> “The best dashboard is the one that helps someone make a decision.”

CONTINUOUS IMPROVEMENT CLOSES THE LOOP

Diane

Training, testing, findings, incidents, and near misses should change the program.



What feeds the loop?

- Audit findings
- Provider exceptions
- Tabletop exercises
- Actual incidents
- Employee reports and near misses

What proves the loop?

- Assigned owners
- Target dates
- Retest evidence
- Management reporting
- Updated policies or training

06

BUILD THE EVIDENCE FILE BEFORE THE LETTER ARRIVES

Insurance, documentation, independent review, and DOL inquiry readiness

Larson
CERTIFIED PUBLIC ACCOUNTANTS

INSURANCE HAS BOUNDARIES

Diane

Know which policy is designed to respond, and what conditions apply.

ERISA fidelity bond

Fraud or dishonesty involving plan funds or property. Not the same as fiduciary liability insurance.

Fiduciary liability

Claims alleging fiduciary breach, subject to policy terms, exclusions, exclusions, and insured parties.

Cyber liability

Incident response and certain privacy, privacy, security, interruption, notification, or regulatory costs.

Ask: Is the plan covered? Are service-provider incidents covered? What notice and consent rules apply?

Sources: DOL ERISA fidelity bond publication and ERISA Advisory Council cybersecurity report.

Larson CERTIFIED PUBLIC ACCOUNTANTS

BUILD THE EVIDENCE FILE BEFORE THE LETTER ARIVES

Diane

One indexed repository turns a scramble into a response process.

Governance

Program, roles, policies, minutes

Risk + access

Risk assessment, reviews, MFA, data controls

Technical + resilience

Scans, tests, backups, BCP, DR, IR

Vendor oversight

Inventory, SOC reports, contracts, exceptions

Training + monitoring

Completion, phishing, dashboard, corrective actions

Insurance + incidents

Policies, notices, tabletop, after-action reports

> “Audit-ready does not mean perfect. It means the organization can explain what it did and show the evidence.”
> show the evidence.”

Larson CERTIFIED PUBLIC ACCOUNTANTS

INDEPENDENT REVIEW GIVES THE FILE CREDIBILITY

Diane

A third-party review is useful only when findings are tracked and corrected.

1

Define scope

Plan-related systems, data, providers, and controls

2

Pick the right work

Audit, SOC report, assessment, scan, or penetration penetration test

3

Track findings

Risk rating, owner, due date, status, and evidence evidence

4

Retest

Confirm material corrections and update management

Source: DOL EBSA Cybersecurity Program Best Practices, annual third-party audit expectations.

Larson CERTIFIED PUBLIC ACCOUNTANTS

COULD YOU RESPOND IN 10 BUSINESS DAYS?

Reported practitioner experience says some DOL cybersecurity cybersecurity information requests may move fast and may ask may ask for proof across internal teams and service providers. providers.

- **Written cybersecurity program**
- Testing and third-party audit reports
- Vendor policies, contracts, and SOC reviews
- Training records and participant communications
- Cyber insurance and incident-response evidence evidence

Source: Colonial Surety article citing EisnerAmper professionals and DOL inquiry examples.

Larson
CERTIFIED PUBLIC ACCOUNTANTS

POLL 7: How confident are you that your organization could assemble its employee benefit plan cybersecurity documentation within 10 business days?

RATE THE FILE, NOT THE FEELING

Diane

A quick readiness drill exposes the gaps before someone else does.

AREA	GREEN	YELLOW	RED
Written program	○	○	○
Risk assessment	○	○	○
Data and vendor inventory	○	○	○
Access reviews	○	○	○
Training records	○	○	○
SOC report review	○	○	○
Incident response tabletop	○	○	○
Insurance documentation	○	○	○

Do this as a tabletop: pick a request date, assign a coordinator, gather evidence, check consistency, and create a remediation list.

THE NEXT 90 DAYS SHOULD BE SPECIFIC

Joint

Small, documented steps beat a perfect plan that never starts.

DAYS 1-30

Inventory and assign

Plans, data, providers, internal owners, sponsor and provider responsibilities

DAYS 31-60

Assess and prioritize

Gap assessment, top three risks, remediation owners, due dates

DAYS 61-90

Test and document

Evidence repository, SOC review, tabletop exercise, management reporting

> “The goal is prudent oversight, appropriate controls, provider accountability, and evidence.” evidence.”

Larson CERTIFIED PUBLIC ACCOUNTANTS


QUESTIONS?
Cameron Hodson and Diane Nesbit
Larson
CERTIFIED PUBLIC ACCOUNTANTS