AVIONTÉ CONNECT

CONNECT

CONNECT DAY 3

Cybersecurity and Data Protection

How Avionté and Your Team Work Better Together.

- *This presentation is for informational purposes only.*

Introductions

Welcome to CONNECT! Thank you for joining our session.

Montasir Azad

PRINCIPAL SECURITY ARCHITECT

SECURITY ARCHITECTURE

Tommy Teague

SENIOR CYBERSECURITY ANALYST

SECURITY OPERATIONS

Our Platinum, Gold & Silver Sponsors

PLATINUM

- Benefits in a Card
- Experian Employer Services
- LLH Healthcare
- rapid! by Green Dot
- Timerack

GOLD

- ADP
- Asurint
- Choice Screening
- Equifax
- Hooray Health
- Marsh McLennan Agency
- Ringover
- Sense
- Sunset Cove Solutions

SILVER

- Advance Partners
- ConverzAI
- daXtra
- Greenshades
- Haley Marketing
- HRlogics
- Joveo
- Momenta Benefits
- Selerix ACA
- Scale Funding
- Staffing Referrals
- Talroo
- Yardstik

Trusted Avionté+ Certified Partners powering CONNECT 2026

Our Certified Integration Sponsors

CallMantra	ClearEdge	Compagno	Curately.AI	FactoryFix
GLYDE	HeyMilo	Insight Worldwide	Lochness Medical	PitchMe
TaTiO	Tenzo	The Safety Standard	Veritable Screening	Whippy

Glossary of Terms & Abbreviations

Programs, Roles & Compliance

MFA (Multi-Factor Authentication): An extra step beyond your password, like a code sent to your phone.

PII (Personally Identifiable Information): Data that can identify a person — SSNs, addresses, bank info.

PCI DSS (Payment Card Industry Data Security Standard): Security rules for businesses that accept card payments.

HCM (Human Capital Management): Avionté's platform for payroll, onboarding, and the talent portal.

SSN (Social Security Number): A unique nine-digit US identifier, often targeted in identity theft.

I-9: The federal form verifying a new hire's identity and work eligibility.

SOC 2: An independent audit of a company's security controls.

Threats & Technology

Phishing: Fake messages that trick people into sharing credentials.

Ransomware: Malware that locks systems until a ransom is paid.

Credential Stuffing: Using stolen logins from other breaches to break in.

SIM-Swap Attack: Hijacking a phone number to intercept text codes.

TLS (Transport Layer Security): Encryption that protects data moving between systems.

Deepfake: AI-generated audio or video that impersonates a real person.

DBIR (Data Breach Investigations Report): Verizon's annual report on real-world breaches.

Goal for today's session

1. The Threat Landscape
2. MFA: Your First Line of Defense
3. Protecting PII
4. PCI and Payment Data Security
5. Artificial Intelligence (AI) in Cybersecurity
6. Shared Responsibility

Disclaimer

- The information in this session is being presented by Avionté as a general informational and educational service to its clients and prospective clients.
- This information should not be construed as, and does not constitute, legal advice nor accounting, tax, or other professional advice or services on any specific matter.
- Participants should consult with their legal counsel or other professional advisor before acting on any information contained in this session.
- Avionté expressly disclaims all liability in respect to actions taken or not taken based on the contents of this session.

The Security Landscape

Why Staffing Firms Are High-Value Targets

Your business runs on sensitive data — and attackers know it.

What you hold:

- SSNs, bank accounts, I-9 documents, and tax forms for every worker
- Login credentials across self-service portals used on personal devices
- Payment data flowing through payroll, direct deposit, and client billing

How attackers exploit it:

- Phishing and credential stuffing exploit high turnover and reused passwords
- Ransomware locks operations and threatens to leak PII
- Third-party integrations and vendor connections widen the attack surface

The Real Cost of a Data Breach – IBM 2025 Report

$4.44M

Global average breach cost in 2025

$10.22M

US average breach cost. (record high, up 9% YoY)

241

Days to identify & contain a breach

53%

Of breaches expose customer PII

Source: *IBM Cost of a Data Breach Report 2025. Global costs declined 9% due to AI-driven faster detection; US costs hit a record high driven by regulatory fines. Staffing firms handling dense PII face above-average exposure.*

How Attackers Get In – Verizon DBIR 2025

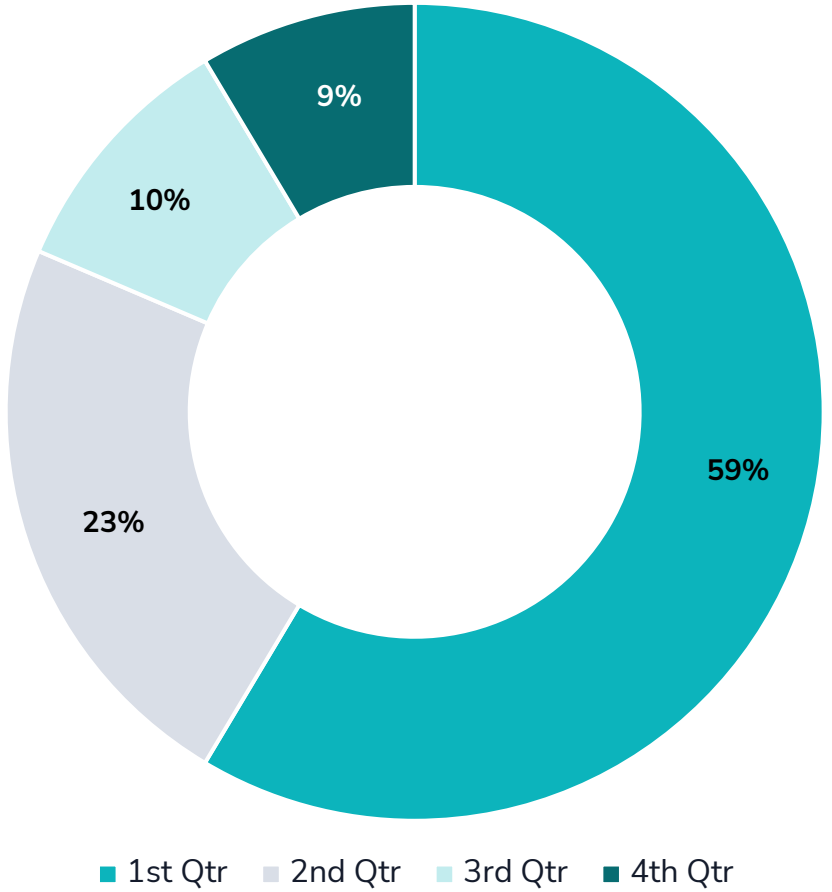
Key Finding: Stolen credentials are the #1 attack vector — used in 22% of all breaches.

Initial access vectors (Verizon DBIR 2025):

- ❑ Human error is present in 60% of all breaches
- ❑ Stolen credentials — 22% of breaches
- ❑ Vulnerability exploitation — 20% (↑34% YoY)
- ❑ Phishing — 16% of breaches
- ❑ Ransomware — present in 44% of all breaches
- ❑ AI-powered attacks — in 1 in 6 breaches

88% of web app attacks use stolen credentials.

30% of breaches involve a third-party vendor — doubled from last year.



Source: Verizon Data Breach Investigations Report 2025

MFA: Your First Line of Defense

Why Passwords Fail and How MFA Fixes It

What MFA Can (and Can’t) Prevent

Case 1: No MFA Enabled

A staffing client discovered payroll fraud after direct deposit details were changed through the portal, redirecting pay for at least four talent users to fraudulent accounts.

Every affected account had already seen brute-force login attempts paired with stolen credentials — and none had MFA enabled.

⚠ MFA would have stopped every one of these logins.

Case 2: MFA Enabled, Password Reused

A staffing client flagged suspicious direct deposit changes for a talent user.

The talent user reused his Gmail password as his portal password. Attackers logged in, reset his email-based MFA, and used the code to redirect his direct deposit.

⚠ MFA only protects you if attackers can’t reset it themselves.

Enable MFA everywhere — and never reuse your passwords.

⍰ Quick Poll – Let's See Where We Stand

Question: What does MFA adoption look like across all Avionté client agencies today?

A. MFA is fully enabled and enforced

B. MFA is set up but optional — not enforced

C. MFA is partially enforced

D. MFA is not enabled at all

E. Not sure what our current setting is

Answer:

C. MFA is partially enforced

Current MFA adoption across BOLD platform

Category	% MFA Enabled
HCM Users (BOLD FO)	**71.4%**
Manager Users (BOLD Managers)	**10.9%**
Talent Users (BOLD FO)	**8.1%**

Why Passwords Alone Won't Protect You

If a password is all that stands between an attacker and your workers' data, it's only a matter of time.

The reality (Verizon DBIR 2025):

- Stolen passwords are the #1 way attackers get in — behind 22% of all breaches
- The average person reuses passwords across half their accounts
- Phishing captures passwords in real time — no amount of complexity helps

What this means for your agency:

- One compromised login can expose every candidate's SSN, bank info, and I-9

Attackers don't hack in — they just log in with a stolen password

Avionté MFA Options

Text Message (SMS)

A one-time code is sent to your phone as a text message. Enter it to confirm it's really you.

✓Simple and familiar — no app required.

⚠ Exposure arises when a number gets ported or intercepted, though pulling that off means deceiving the mobile carrier through social engineering.

Email

A one-time code is sent to your registered email address each time you log in.

✓No phone needed — works anywhere you can check email.

⚠ Only as secure as your email account itself.

Text is the preferred method: it's tied to a device you physically hold. Email is just another account — if that account is compromised, so is your MFA.

Risk of Not Enabling MFA

Most clients have not enabled MFA for talent and employee portal users. This is Avionté's most urgent shared security risk.

What a talent or employee account can access:

- Social Security Numbers (SSNs)
- I-9 employment documents
- Direct deposit bank account details
- Home address and contact information
- Pay stubs and full earnings history
- Government-issued ID scans

Without MFA, a single stolen password grants full access to all items listed.

Consequences of a compromised account:

- **Worker identity theft** — PII sold or exploited
- **Paycheck redirection** — wages stolen before payday
- **Follow-on fraud** — stolen SSNs and IDs resold or reused elsewhere
- **Client liability** — if MFA was available but not enforced, your firm is responsible

Two Ways to Enable MFA for Talent

Turning on MFA isn't self-service — it's configured for your account by your Avionté team.

Enforce MFA for All Talent

MFA is required for every talent user, with no exceptions.

The most straightforward and most secure option for a staffing agency.

✓Recommended for most agencies.

Opt-In MFA for All Talent

Talent can choose not to enable MFA on a per-user basis.

Without it, they're limited to onboarding and timesheets. Full portal access — including PII — requires opting in.

⚠ Sensitive data stays protected only for those who opt in.

Both are Super-Admin settings: talk to your Avionté account team to get either one turned on.

Protecting PII

What's At Risk and Best Practices

The PII You Handle Every Day

Every staffing agency is a data warehouse. Here's what's sitting in your systems right now — and what's at stake if any of it leaks.

Personal & Identity Data:

- Social Security Numbers and dates of birth
- Bank account and routing numbers for direct deposit
- I-9 employment authorization documents
- Driver's licenses and government-issued IDs
- Home addresses and emergency contacts

Financial & Employment Data:

- Tax forms: W-2, W-4, 1099
- Payroll history and earnings records
- Background check results
- Health or disability disclosures (where applicable)

Pro Tip: ***Every record is a liability. If you don't need it, don't keep it.***

Practical Steps to Protect PII – Best Practices

A layered approach to protecting personally identifiable information across your staffing operations.

01. **Least-Privilege Access**

Only grant access by role.

Review quarterly.

- Remove departing staff access the same day they leave.
- Over-privileged accounts are a top internal breach cause.

02. **Protect Data on the Move**

Avionté encrypts your data. Make sure your vendors do too.

- Include exports and backups — not just live systems.
- A stolen export is just as damaging as a live breach.

03. **Data Retention Policies**

Don't keep records longer than you need to.

- Deletion is manual, by request — handled by Technical Services.
- *Data you no longer need is data you no longer have to defend.*

04. **Train Your People**

Your recruiters are your biggest security asset — and risk.

- Run phishing simulations quarterly, not just once a year.
- *Human error is present in 60% of all breaches — Verizon DBIR 2025.*

PCI and Payment Data Security

Protecting Cardholder Data In Your Payment Flows

Payment Data Security – It Applies to You Too

If your business touches card payments anywhere — client invoicing, pay cards, online portals — PCI DSS compliance applies to you, not just to retailers.

Where card data shows up in your operations:

- Client invoices and subscription payments processed by credit card
- Pay cards or prepaid debit cards issued to workers
- Client-facing portals or pages that accept card payments
- Payment processors and gateways connected to your platform

Non-compliance means fines, audits, and potentially losing payment processing.

The Cost of PCI Non-Compliance

$33.41B

Global card fraud losses in 2024

42%

Share of global fraud losses borne by the US

$100K

Max fine per month for non-compliance

51

New rules now mandatory

Source: *The Nilson Report (2024 global card fraud data); PCI Security Standards Council. All future-dated v4.0.1 requirements became mandatory March 31, 2025; fines escalate the longer a gap stays open.*

Artificial Intelligence (AI) in Cybersecurity

Threats, Opportunities, and Responsible Use

Smarter Attacks, Smarter Defense

- **Attackers now have AI on their side.**
- **Common tactics:**
  - Phishing emails written with a natural tone — no typos, no red flags
  - Deepfake voice calls impersonating executives to approve payments
  - Automated tools testing stolen passwords against your portals, nonstop
- **Phishing remains staffing's top AI-driven risk.**

- **AI gives your security team the same kind of edge.**
- **How AI helps defend you:**
  - Flags unusual logins — new locations, odd hours, rapid attempts
  - Watches for threats around the clock — no manual monitoring required
  - Adjusts access controls in real time as risk changes
- **AI is a defense tool, not just a shortcut.**

How AI Is Supercharging Phishing

- Phishing used to be easy to catch.
- **The old telltale signs:**
  - Awkward grammar and obvious typos
  - Generic messages blasted to everyone
  - The same script, every single time
- Basic training was usually enough.

- AI has erased those old warning signs.
- **What AI changes:**
  - Natural tone and zero typos — the red flags are gone
  - Personalized using scraped LinkedIn and company details
  - Thousands of tailored variations generated in seconds
- Watching for typos doesn’t cut it anymore.

How to Spot Phishing – and Where to Practice

Red Flags to Watch For

⚠ A sender domain that mimics a trusted brand (e.g., a lookalike domain instead of the real one)

⚠ Urgent or shocking content designed to make you click before you think

⚠ A push to click a link or open an attachment right away

⚠ Links that don't go where they claim — hover before you click to check

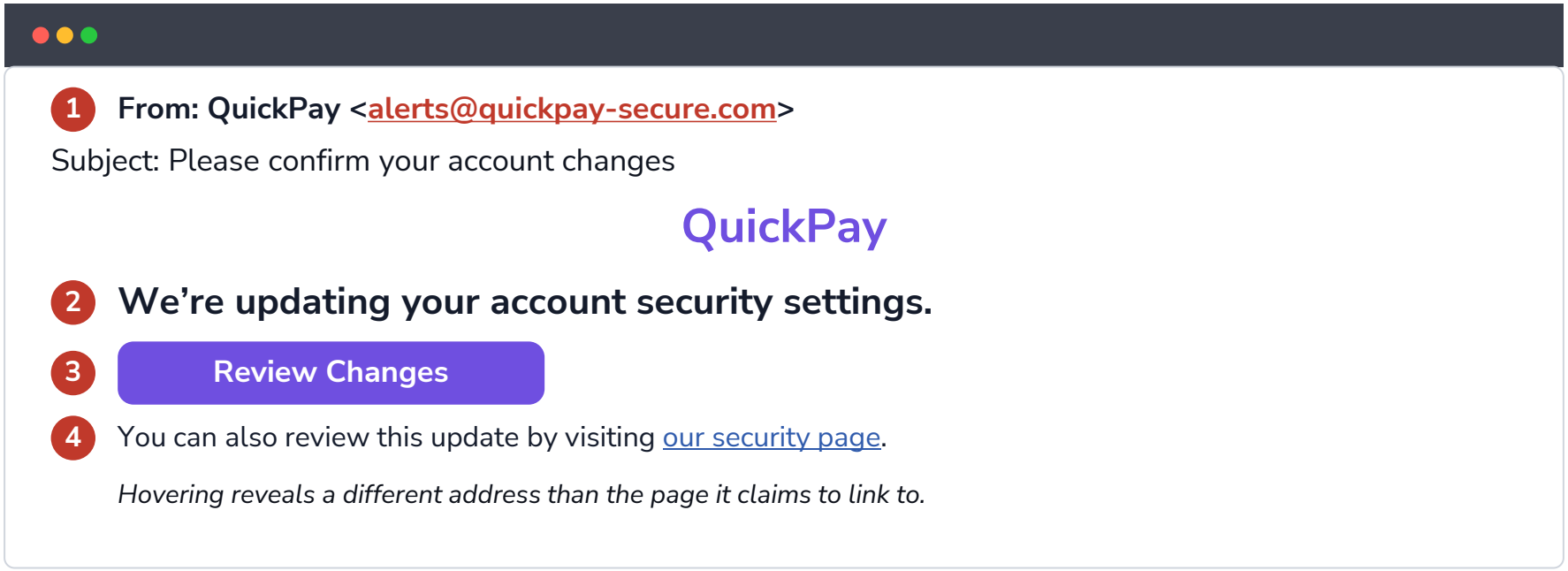
Practice & Training Resources

✓ **Recommended:** KnowBe4 — our platform for ongoing simulated phishing tests and security awareness training.

Free self-study: The Lab at justforphishing.com — free, open-source phishing quizzes and simulators for extra practice.

An independent, open-source project — a good supplement, not a replacement for KnowBe4.

Anatomy of a Phishing Email



1 **Lookalike sender domain**

2 **Urgent, alarming heading**

3 **Pressure to click immediately**

4 **Link goes somewhere else**

Recreated for training purposes — the brand, name, and domain shown are fictional.

Responsible AI Use: Best Practices for Your Team

AI is already part of how your team works — responsible use starts with a few simple habits.

Build these into your workflow:

- Keep candidate and client sensitive data out of public AI tools — assume anything you paste can be retained
- Stick to approved AI tools with data protection agreements in place
- Put your AI policy in writing: approved tools, allowed data, consequences for misuse
- Review every AI-generated output before it goes out — AI can hallucinate or leak context
- Vet every AI vendor: what do they retain, for how long, and who can access it?

Good AI hygiene is just good security hygiene.

Shared Responsibility

What's Ours, What's Yours, and What's Next

Security Is a Partnership

What Avionté Owns

- We secure the platform your business runs on — always, without exception.
- We handle:
  - Platform security and SOC 2 compliance
  - Data encryption at rest and in transit
  - 24/7 infrastructure monitoring and patching
  - Incident response and breach notification
  - Regular penetration testing and audits

What You Own

- Your team's daily actions are the last line of defense.
- Your responsibilities:
  - Enforce MFA for all users — note every exception
  - Review and restrict user access quarterly
  - Train staff on phishing and social engineering
  - Make sure all systems are security updated
  - Report anything suspicious immediately

Your Action Plan

Enable MFA

- Contact your account manager to enable MFA today
- Start with admin accounts, then roll out to all talent users
- Use an authentication method that Avionté supports.
- Set a 7 to 14 days grace period for worker enrollment

Lock Down Your Data

- Audit every user — remove departed staff and excess admins immediately
- Enforce least-privilege: recruiters only see what their role requires
- Set a data retention schedule — purge what you no longer need
- Check your PCI DSS v4.0.1 status — all requirements mandatory as of March 2025

Build Your Security Culture

- Write an AI usage policy before your team's next project
- Brief your IT team and leadership on what you learned today
- Assign a security point person in your agency
- Schedule quarterly phishing simulations for your recruiters

CONNECT

Thank You

Help shape future content by rating this session.

1. Open the Bizzabo app and select Agenda
2. Locate session: ***Cybersecurity and Data Protection: How Avionté and Your Team Work Better Together***
3. Rate and leave feedback