Breaking Down Silos: How AP, IT, and Cybersecurity Must Work Together to Stop Fraud

Presented by: Paul E. Zikmund

IOFM

Do you need NASBA CPE credits?

- Navigate to website: **iofm.cnf.io**
  or scan the QR code →
- Check-in and check-out of your sessions to track your attendance for NASBA CPEs
- Certified with IOFM? No need to check-in and out of sessions. Self-report CEUs on IOFM.com instead after the event!

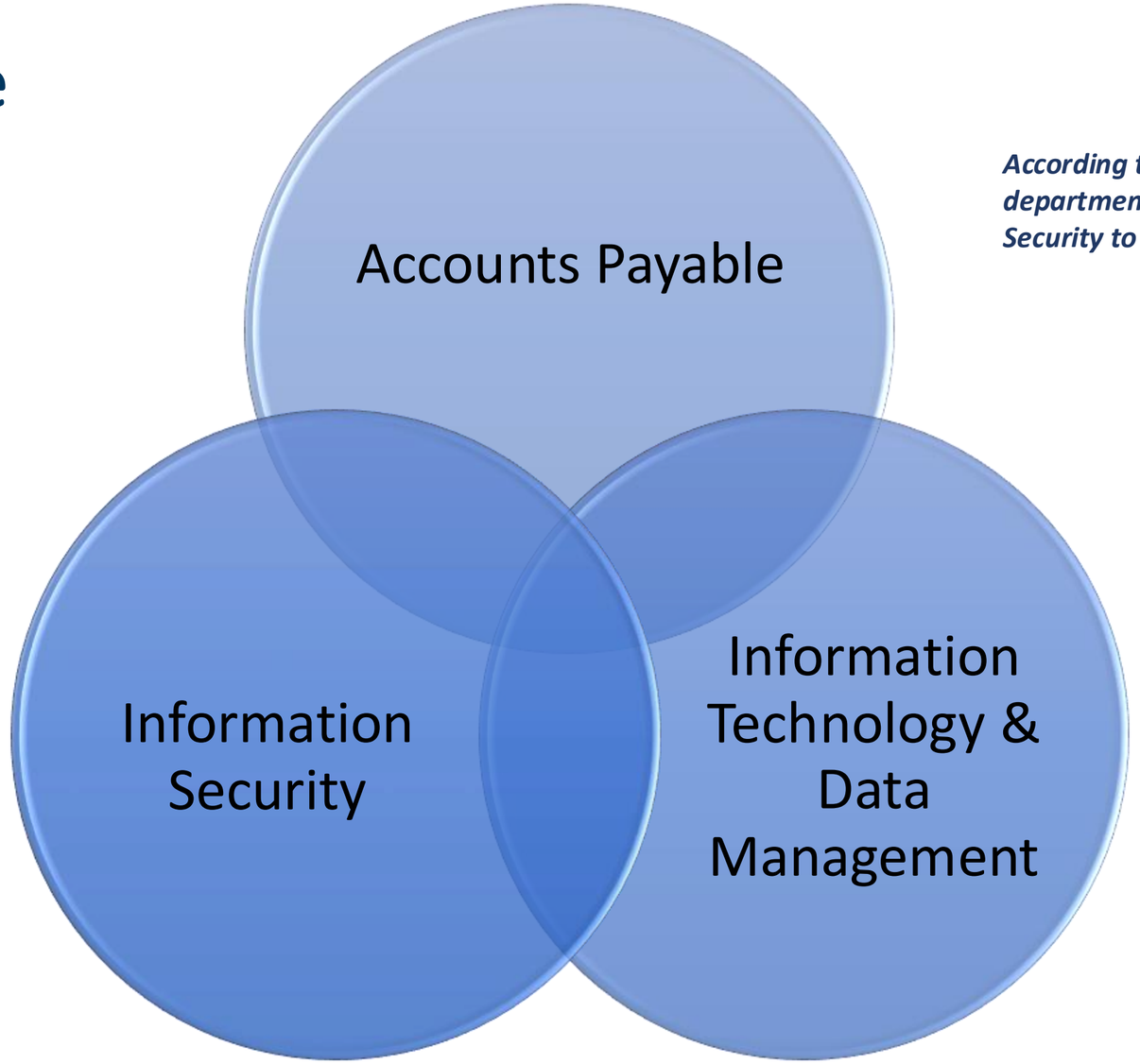
IOFM Spring
CONFERENCE & EXPO

Accounts Payable = Prime Target

High Volume and Complexity	• Large organizations process thousands of invoices monthly. Fraudsters rely on the "needle in a haystack" principle.
The "Authorized" Nature of the Transaction	• AP fraud involves tricking the system into willingly sending money. Because the payment is processed through official channels (ERP systems, bank portals), it carries a veneer of legitimacy that makes it harder for automated security systems to flag.
Vulnerability to Social Engineering	• AP professionals are in constant communication with external vendors. Fraudsters exploit this helpfulness through Social Engineering & 0Business Email Compromise (BEC).
Fragmented Data and "Siloed" Systems	• 80% of organizations struggle with data and technology issues. When the system that stores vendor bank details (the Master Data File) is not tightly synced with the system that monitors network security, a "gap" is created.
Transition to Real-Time Payments (RTP)	• The rise of instant payment rails has shortened the "window of recovery." In the past, a fraudulent check or ACH could potentially be stopped within 24–48 hours. Today, with 43% of merchants using Real-Time Payments, funds are often moved out of the country within seconds.
Insider Access	• AP is one of the few departments where a single employee might have the knowledge and access to create a vendor, approve an invoice, and initiate a payment.
Exploiting Automation Weaknesses	• While AI and OCR (Optical Character Recognition) have made AP faster, they have also created new vulnerabilities.

IOFM

Triad of Defense



According to the 2026 APF Survey, only 34% of AP departments are partnering with IT and Information Security to strengthen controls to reduce the risk of fraud.

According to the 2026 Global eCommerce Payments & Fraud Report, 80% of organizations struggle with at least one major data or technology-related issue in fraud management. This suggests that the "silo" problem is primarily a failure to integrate technical oversight with financial workflows

IOFM

Unity of Effort

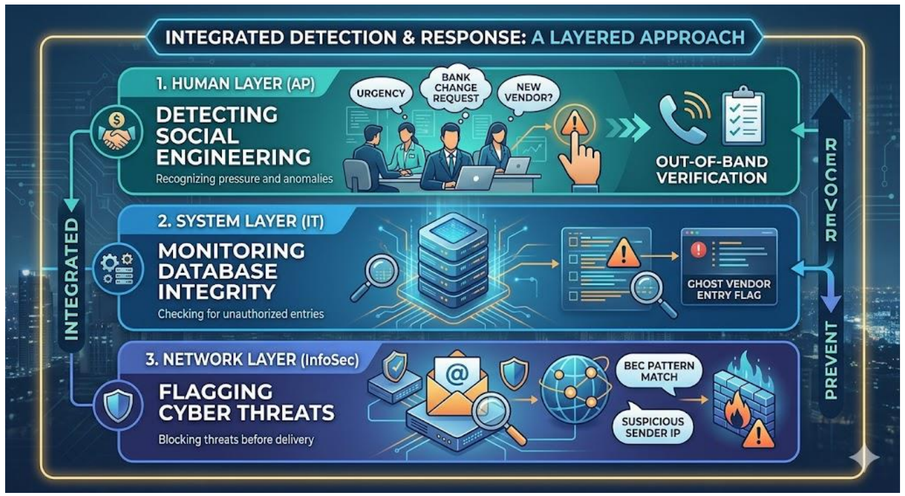
Fraud is Multimodal: Modern fraudsters don’t just "hack" a computer; they "hack" your business processes, your people, and your software simultaneously.

The Master Vendor File is a Shared Asset: AP owns the accuracy of the data, but IT owns the database it lives in, and InfoSec owns the identities allowed to edit it.

Speed is the Only Defense: In the age of instant wire transfers, the time between a "red flag" and a "payment freeze" must be measured in minutes, not days.

Technology Cannot Replace Verification: No firewall can stop a legitimate-looking (but fraudulent) invoice; only a cross-functional "out-of-band" verification process can.

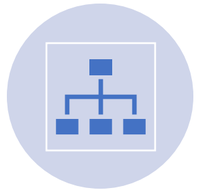
Security is a Profit Center: Preventing a single $500k Business Email Compromise (BEC) provides more value than a year's worth of standard IT optimizations.



Accounts Payable – Business Process Owners

Verification of Standing Data: Perform mandatory "out-of-band" phone authentication for any request to change vendor bank details or contact information.

Three-Way Matching: Enforce a strict match between the Purchase Order (PO), Receiving Report, and Invoice before any payment is authorized.



Segregation of Duties: Ensure that the individual who creates or edits a vendor in the Master Vendor File (MVF) is never the same individual who approves or releases payments.

Anomaly Detection: Screen for behavioral "red flags" such as high-pressure language in emails, unusual invoice formatting, or invoices just below approval thresholds.

Payment Freezing: Act as the primary "kill switch" to halt all pending transactions immediately upon the discovery of a suspicious indicator.

MVF Hygiene: Conduct quarterly audits of the Master Vendor File to identify duplicate entries, inactive vendors, or employees sharing addresses/bank accounts with vendors.

Post-Incident Reconciliation: Lead the financial recovery process by reconciling accounts and initiating "stop-payment" orders with banking partners.

IOFM

Information Technology – Infrastructure Custodians

Log Management & Retention: Maintain comprehensive, tamper-proof logs of ERP system access, database changes, and administrative actions for at least 90 days.

Access Control Management: Manage the "Least Privilege" model, ensuring users only have access to the specific ERP modules required for their job function.

System Patching: Ensure the ERP software and underlying databases are patched against known vulnerabilities that could be exploited to manipulate financial data.

Database Integrity Monitoring: Alert on unauthorized or direct "back-end" changes to the database tables that bypass the ERP's standard user interface.

Secure Backups: Maintain encrypted, offline backups of financial data to allow for system restoration in the event of a ransomware or data-wiper attack.

Account Provisioning/De-provisioning: Ensure immediate revocation of system access for terminated employees or those moving to roles outside of the AP function.

Disaster Recovery Execution: Lead the technical restoration of systems from clean backups during the recovery phase of a significant incident.

IOFM

Information Security – Threat Defenders

Identity & Access Defense: Enforce Multi-Factor Authentication (MFA) and Conditional Access policies (e.g., blocking logins from non-standard geographic locations) for all AP staff.

Email Security Governance: Implement and monitor SPF, DKIM, and DMARC protocols to prevent domain spoofing and block sophisticated phishing attempts.

Threat Hunting: Proactively scan the environment for "Indicators of Compromise" (IoCs), such as malicious inbox rules that auto-forward emails to external addresses.

Digital Forensics: Lead the technical investigation into "how" a breach occurred, analyzing email headers, IP addresses, and malware artifacts.

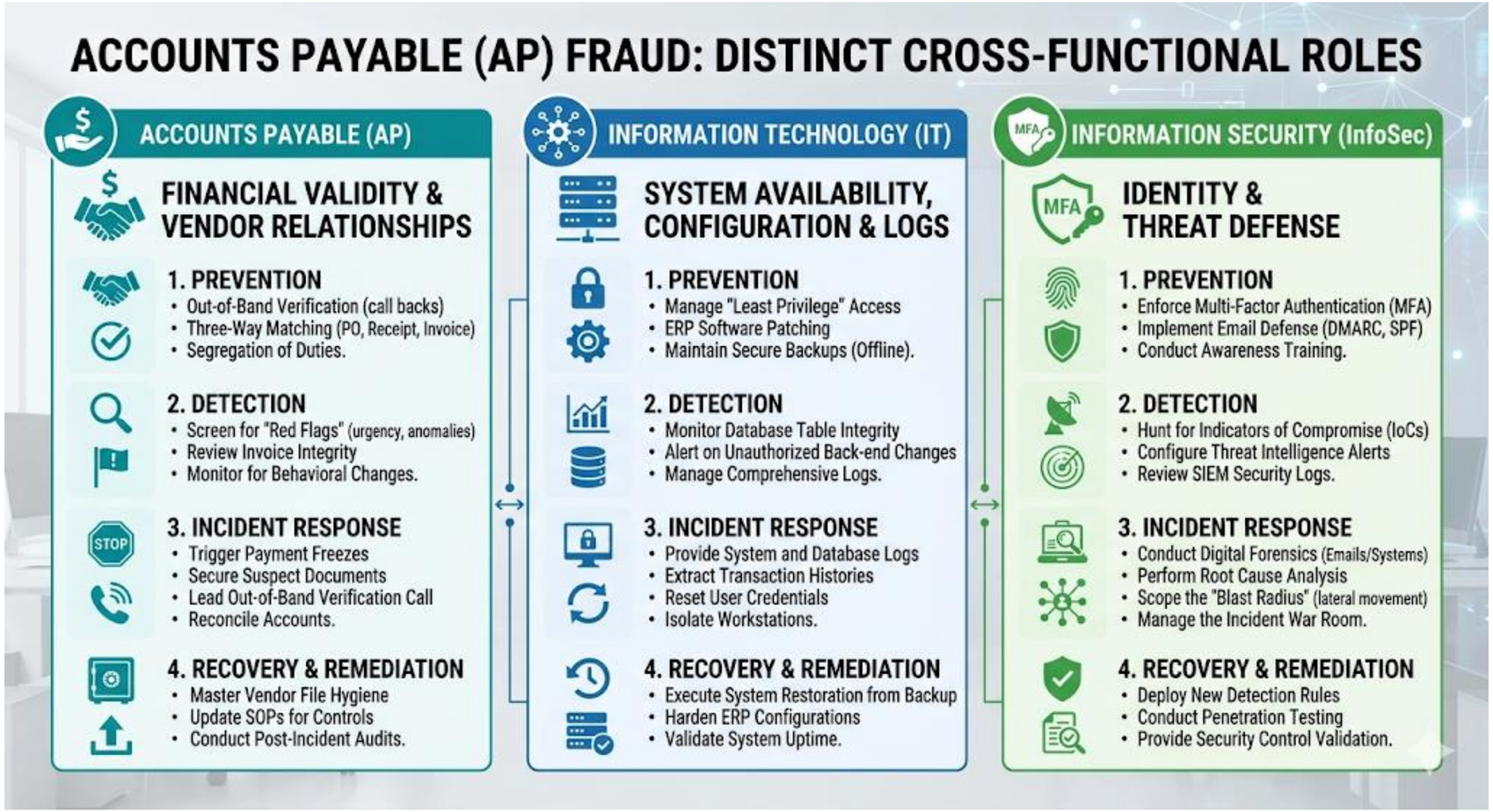
Incident Response Orchestration: Coordinate the cross-functional communication and "War Room" activities when a high-severity fraud event is detected.

Security Awareness Training: Provide specialized, role-based training for AP staff on the latest social engineering tactics, such as deepfake audio and Vishing.

Control Validation: Conduct regular penetration testing and "tabletop" exercises to simulate fraud scenarios and test the effectiveness of existing controls.

IOFM

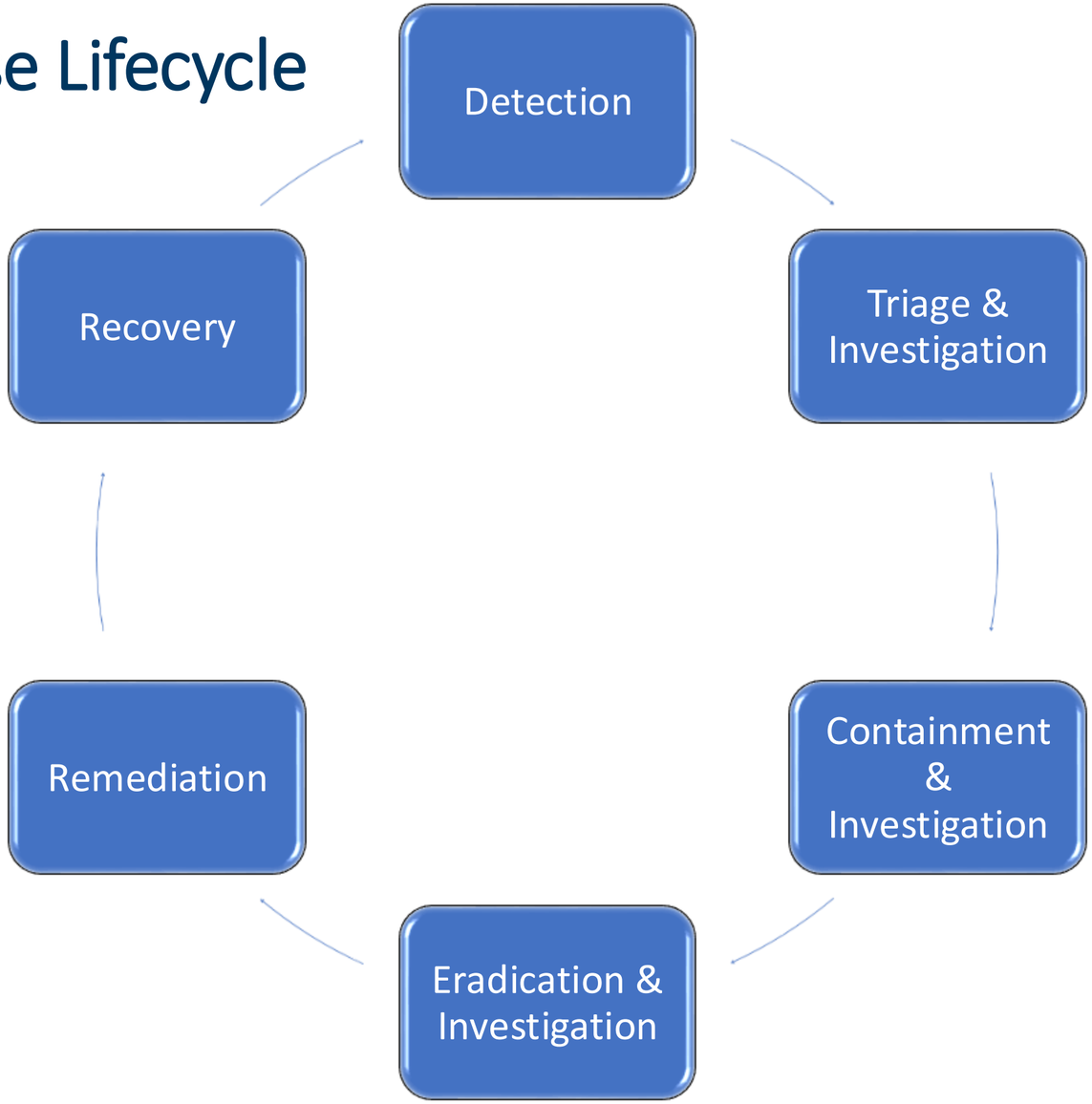
Roles & Responsibilities



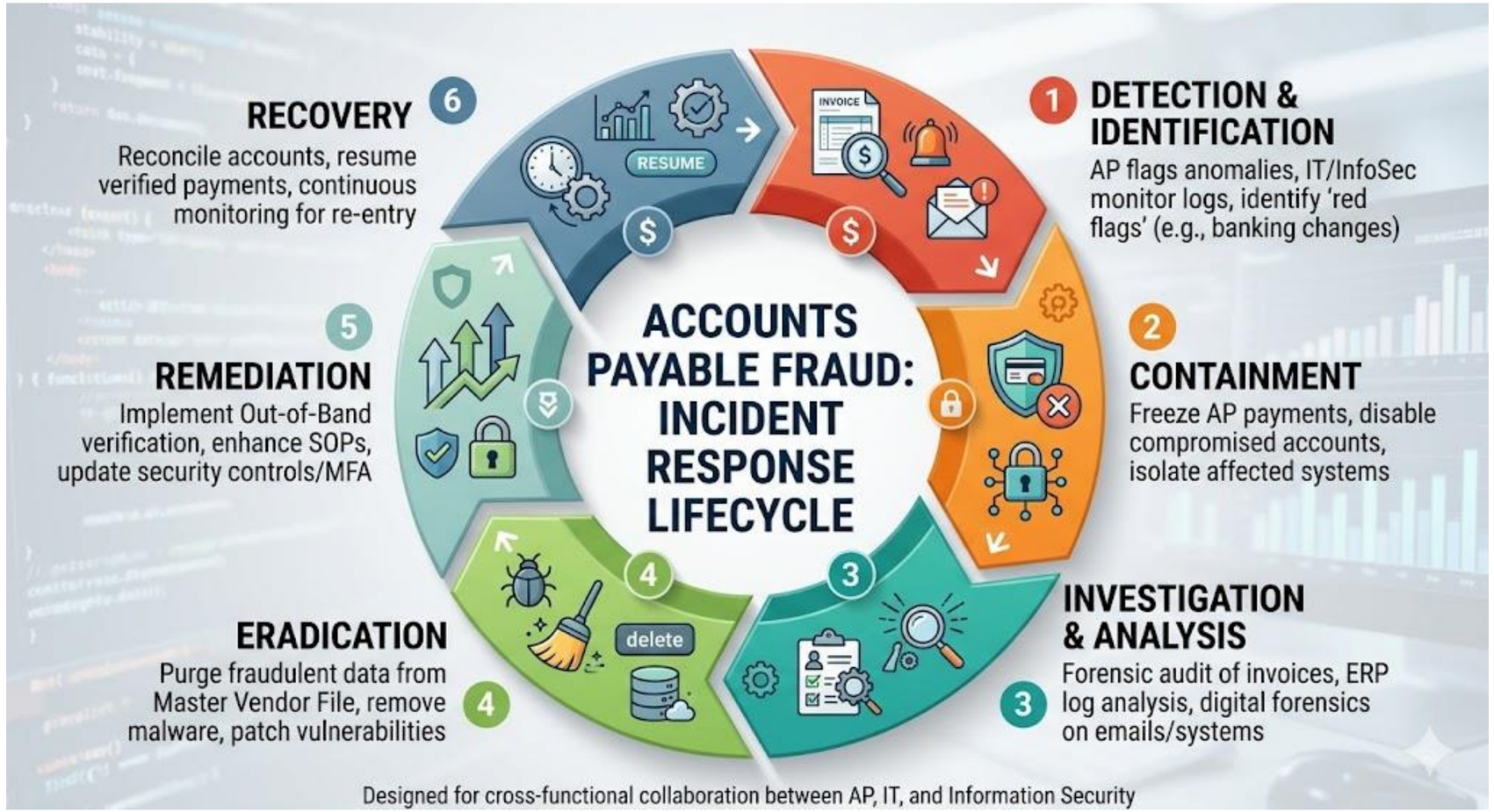
RACI Charts

Responsibility	Accounts Payable (AP)	IT Security	Cybersecurity
Vendor Identity	Verifying business legitimacy and bank changes.	Securing the portal/interface.	Monitoring for domain spoofing.
Transaction Monitoring	Spotting anomalies in invoice volume/amounts.	Ensuring data integrity between ERP and Bank.	Detecting behavioral anomalies (AI-driven).
Incident Response	Immediate "Kill Switch" for payments.	Forensic investigation of the system breach.	Threat hunting and patch management.

Incident Response Lifecycle



AP Fraud Incident Response Lifecycle



Incident Response Lifecycle

DETECTION	INVESTIGATION	CONTAINMENT	ERADICATION	REMEDIATION	RECOVERY
• AP: Flags invoice anomalies or bank change requests. • IT: Monitors ERP logs for unauthorized database access. • InfoSec: Hunts for BEC/Phishing indicators or geo-mismatches.	• AP: Performs 3-way match and forensic audit of invoices. • IT: Extracts system logs and database change history. • InfoSec: Conducts digital forensics and email header analysis.	• AP: Freezes vendor account and halts payment batches. • IT: Disables compromised user accounts in Active Directory. • InfoSec: Isolates affected network segments and revokes tokens.	• AP: Scrubs the Master Vendor File of fraudulent data. • IT: Restores systems from clean backups and patches ERP. • InfoSec: Removes malware and closes firewall/MFA gaps.	• AP: Updates SOPs for out-of-band vendor verification. • IT: Hardens infrastructure and optimizes log retention. • InfoSec: Deploys new detection rules and security policies.	• AP: Reconciles accounts and resumes verified payments. • IT: Validates system stability and performance uptime. • InfoSec: Monitors environment for signs of threat re-entry.

IOFM

Accounts Payable Fraud Threat Vectors

Employee Fraud

- Billing Schemes: Employees create "shell companies" (fake entities) and submit invoices for services never rendered.
- Check Tampering: Forging signatures, altering payee information on physical checks, or intercepting checks intended for legitimate vendors.
- Kickbacks: An employee colludes with an external vendor to approve inflated invoices in exchange for a portion of the additional profit.
- Duplicate Payments: Intentionally processing an invoice twice and rerouting the second payment to a personal account.

Third-party Fraud

- Price Fixing & Overcharging: Legitimate vendors inflating prices beyond contract agreements or charging for premium goods while delivering "substitute" lower-quality items.
- Phony Invoices: Sending invoices for unsolicited goods or services in hopes they are paid without verification.
- False Billing or Non-delivery: Where third parties bill for services not provided.

Cyber Criminal Fraud

- Business Email Compromise (BEC): A criminal hacks or spoofs the email of a high-level executive or a known vendor to request an urgent "secret" wire transfer or a change in banking details.
- Vendor Email Compromise (VEC): A specialized form of BEC where the attacker sits silently in a vendor's email thread, learns the invoicing cycle, and then sends a "corrected" invoice with their own bank details.
- Phishing & Malware: Using deceptive emails to install keyloggers or ransomware, allowing attackers to steal credentials for the ERP or banking portals.
- Deepfake Impersonation: Using AI-generated audio or video to impersonate a trusted authority figure during a phone or video call to authorize a fraudulent transaction.

IOFM

Employee Fraud

The Risk: An employee creates a "ghost vendor" in the ERP or an external bad actor hacks a legitimate vendor’s email to send "updated" bank details.

AP Role: Execute "Out-of-Band" verification (calling a known contact on a trusted number) for every bank change.

IT Role: Restrict Master Vendor File (MVF) access to a limited group and implement automated logs that alert InfoSec when bank details are modified.

InfoSec Role: Scan incoming vendor emails for "look-alike" domains (e.g., vendor-payments.co instead of .com)

Cyber Criminal Fraud

The Risk: A criminal uses a phishing link to steal an AP clerk’s login, then enters the system at 2:00 AM to approve pending payments.

AP Role: Report any "glitches" or unexpected MFA (Multi-Factor Authentication) prompts to IT immediately.

IT Role: Enforce Geofencing (blocking logins from outside specific regions) and Time-of-Day restrictions.

InfoSec Role: Monitor for "impossible travel" (a user logging in from New York and London within an hour) and session hijacking.

Whaling

The Risk: A high-pressure email, seemingly from the CFO, demands an immediate wire transfer for a "confidential acquisition.

AP Role: Adhere to a "No-Email Approval" policy—no payment is sent without a secondary verbal or portal-based confirmation.

IT Role: Implement external email banners and "Whaling" protection software that flags emails from external sources that use the names of internal executives.

InfoSec Role: Conduct regular "Phishing Simulations" tailored to AP workflows to build employee muscle memory.

IOFM

Challenges

The "Urgency" Weapon: Fraudsters rely on manufactured crises. AP teams are often pressured by vendors or internal executives to "pay now," leading them to bypass the very controls IT and Security put in place.

Data Silos: If the ERP system (IT-managed) doesn't communicate with the email security gateway (Cyber-managed), a flagged malicious email might not automatically trigger a "stop payment" alert on a corresponding invoice.

Legacy Systems: Older accounting software may lack the API capabilities to support multi-factor authentication (MFA) or automated log monitoring.

Misaligned "North Star" Metrics - Each department is often incentivized by different, and sometimes conflicting, goals:

AP Goal: Efficiency and "Days Payable Outstanding" (DPO). They want to pay bills fast to avoid late fees or capture discounts.	IT Goal: System Uptime and Stability. They are hesitant to implement complex security patches or "friction-heavy" integrations that might crash the legacy ERP system.	Cybersecurity Goal: Risk Mitigation and Zero Trust. They want to slow everything down, add three layers of MFA, and verify every packet of data.

Challenges

Lack of a Common Language - Cybersecurity talks in terms of "attack vectors," "latencies," and "payloads." AP talks in terms of "vendors," "accruals," and "reconciliations.“

The "Emergency" Loophole - Organizations often have a "Fast Track" process for emergency payments (e.g., a critical server part or a last-minute legal settlement).

Lack of training & awareness

No Human-in-the-loop

Recommendations for Success

Establish

Establish a "Fraud Response Task Force“ - Instead of meeting only when a crisis occurs, create a standing cross-functional committee that meets monthly.

- Action: Formalize a group with representatives from all three departments to review "near misses," discuss emerging threat intelligence (like new deepfake tactics), and audit current workflow bottlenecks.
- Outcome: Builds personal rapport and ensures that communication channels are "warm" before an actual incident occurs.

Conduct

Conduct Joint "Tabletop" Simulations - Security is often abstract until it's tested. Use realistic fraud scenarios to walk through the response process.

- Action: Run a 2-hour workshop where a "mock" Business Email Compromise (BEC) is reported. Watch how AP flags it, how InfoSec analyzes the headers, and how IT pulls the logs.
- Outcome: Identifies gaps in the Incident Response Lifecycle and clarifies exactly who is responsible for which "kill switch.“

Implement

Implement a "Shared Language" Risk Registry - AP speaks in terms of "invoices" and "vendors," while IT/InfoSec speaks in "logs" and "vectors.“

- Action: Develop a shared document that maps financial risks to technical vulnerabilities. For example, link the "Ghost Vendor" risk (AP) directly to "Privileged Access Management" (IT) and "Internal Threat Hunting" (InfoSec).
- Outcome: Ensures all three teams understand the business impact of technical gaps.

Rotate

Rotate Knowledge "Mini-Sessions“ - Cross-training reduces the friction that occurs when one department doesn't understand the constraints of another.

- Action: Have an AP manager explain the "3-Way Match" process to the IT team, and have an InfoSec analyst show the AP team how a credential harvesting site looks on the backend.
- Outcome: Increases empathy and helps AP staff understand why certain security hurdles (like MFA) are necessary, rather than seeing them as a nuisance.

IOFM

Recommendations for Success

Co-Author Standard Operating Procedures(SOPs) - Controls are more effective when they are designed by both the people using them and the people securing them.	• Action: When updating the procedure for changing vendor banking details, involve InfoSec to ensure "out-of-band" verification is technically sound and IT to ensure the ERP's audit trail is properly capturing the change. • Outcome: Eliminates "shadow processes" where employees bypass security because it's too cumbersome for their daily workflow.
Shared Success Metrics (KPIs) - Move away from department-specific goals that may conflict with one another.	• Action: Create a "Fraud Resilience Scorecard" that tracks metrics like: Time from initial red-flag detection to payment freeze, Percentage of Master Vendor File changes verified via two channels, ERP log availability and integrity. • Outcome: Aligns incentives so that IT and InfoSec feel a sense of ownership over financial losses, and AP feels a sense of ownership over digital hygiene.
Integrated Tooling & Alerting - Ensure that the technical tools used by IT/InfoSec can "speak" to the financial tools used by AP.	• Action: Configure the Security Information and Event Management (SIEM) tool to alert InfoSec when an AP user logs in from a new device, and simultaneously notify the AP manager to verify the activity. • Outcome: Replaces manual "checking-in" with automated, real-time collaboration.

IOFM

Metrics for Success

Attempt Detection Rate: The number of fraudulent invoices or BEC attempts identified before payment, categorized by the detection source (e.g., "Flagged by AP" vs. "Blocked by Cyber").

Mean Time to Detect (MTTD): How long a fraudulent vendor or bank change exists in the system before it is discovered.

Change Verification Compliance: The percentage of vendor banking changes that have a documented out-of-band verification attached.

False Positive Ratio: The rate of legitimate payments flagged as fraud, ensuring that controls aren't unnecessarily stifling business velocity.

Training and collaborative meetings: success stories, outcomes, follow through

Alert-to-Action Bridge: The percentage of cybersecurity alerts (like a compromised email account) that successfully triggered an automated or manual "Payment Hold" in the ERP system.

Prevented Loss Ratio: (Total Value of Prevented Fraud ÷ Total Fraud Attempts). This demonstrates the effectiveness of the triad's "shield.“

Fraud Prevention ROI: (Savings from Prevented Fraud ÷ Total Cost of Fraud Prevention Tools & Personnel).

Recovery Success Rate: For fraud that does slip through, the percentage of funds successfully clawed back via the IT-monitored "Kill Chain" (rapid alert to the bank).

Case Study:

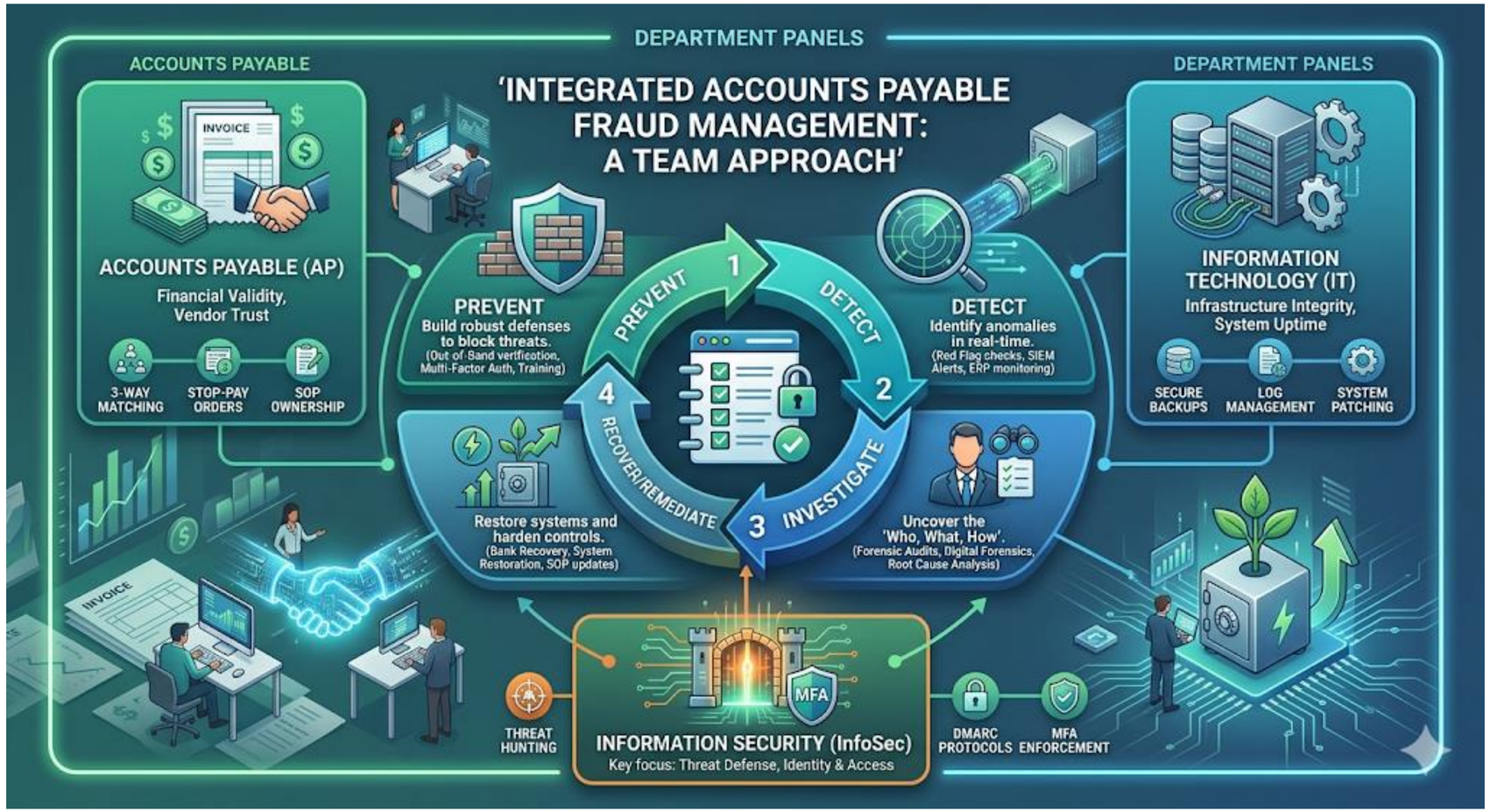
The Scenario: A long-term construction vendor’s email was compromised. The attacker sat silently in the thread, waited for an invoice to be sent, and then followed up from the actual vendor’s email account stating, "We’ve updated our banking for this project; please use the attached details.

The Triad Response:

- Cybersecurity: Their "impossible travel" alerts flagged that the vendor’s email was being accessed from an unusual IP address. They sent a silent alert to the AP manager.
- Accounts Payable: Seeing the alert, the AP clerk paused the pending $250,000 payment and initiated a "Live Voice" verification with a known contact at the vendor.
- IT: IT immediately pulled the email logs to see if any other internal departments had received similar "updated banking" instructions, identifying two other departments about to submit fraudulent invoices.

Result: The fraud was stopped before the wire was initiated. The company updated its policy to require a new testing procedures for all new bank accounts.

Team Approach to Mitigating Fraud Risks



QUESTIONS?

{Last Slide - Speaker contact details]

REMINDER!

If you checked in for NASBA CPE credit, check out at **iofm.cnf.io**

IOFM

Please tell us what you think!

- Please scan this QR code using your mobile to access a short feedback survey →
- Also accessible via the mobile app