# CLOSING THE GAPS

## UNDERSTANDING & MITIGATING YOUR AP, COMPLIANCE, DATA AND CYBER RISKS

MARCH 31, 2020

CACUBO

FISCAL TECHNOLOGIES®
Protecting Organizational Spend

IMA HIGHER EDUCATION

paymerang

THE COALITION FOR COLLEGE COST SAVINGS

# TODAY'S PRESENTERS

***Eric Hayes – Vice President of Services, Fiscal Technologies***

Eric Hayes has two decades' experience in financial operations and recovery audit services. He has personally managed the recovery audit and payment error prevention initiatives of dozens of organizations from Higher Ed, Retail, Manufacturing, Health Care, and Oil and Gas industries. Eric has a passion for providing AP, P2P, and Internal Audit teams with overpayment and fraud prevention technologies, best practices and strategies. Eric leads FISCAL Technologies' partnership with The Coalition for College Cost Savings.

***Brian Cook – Senior Vice President of Higher Education, Paymerang***

Brian Cook has 19 years of experience working with various educational procurement and consortia programs designed to lower the cost of delivering high quality education, provide efficiency gain, and protect institutions against the proliferation of fraud. He leads the partnerships with several associations and coalition procurement programs for Paymerang and will identify as well as sharing best practices on reducing exposure to common compliance and fraud problems that plague institutions today.

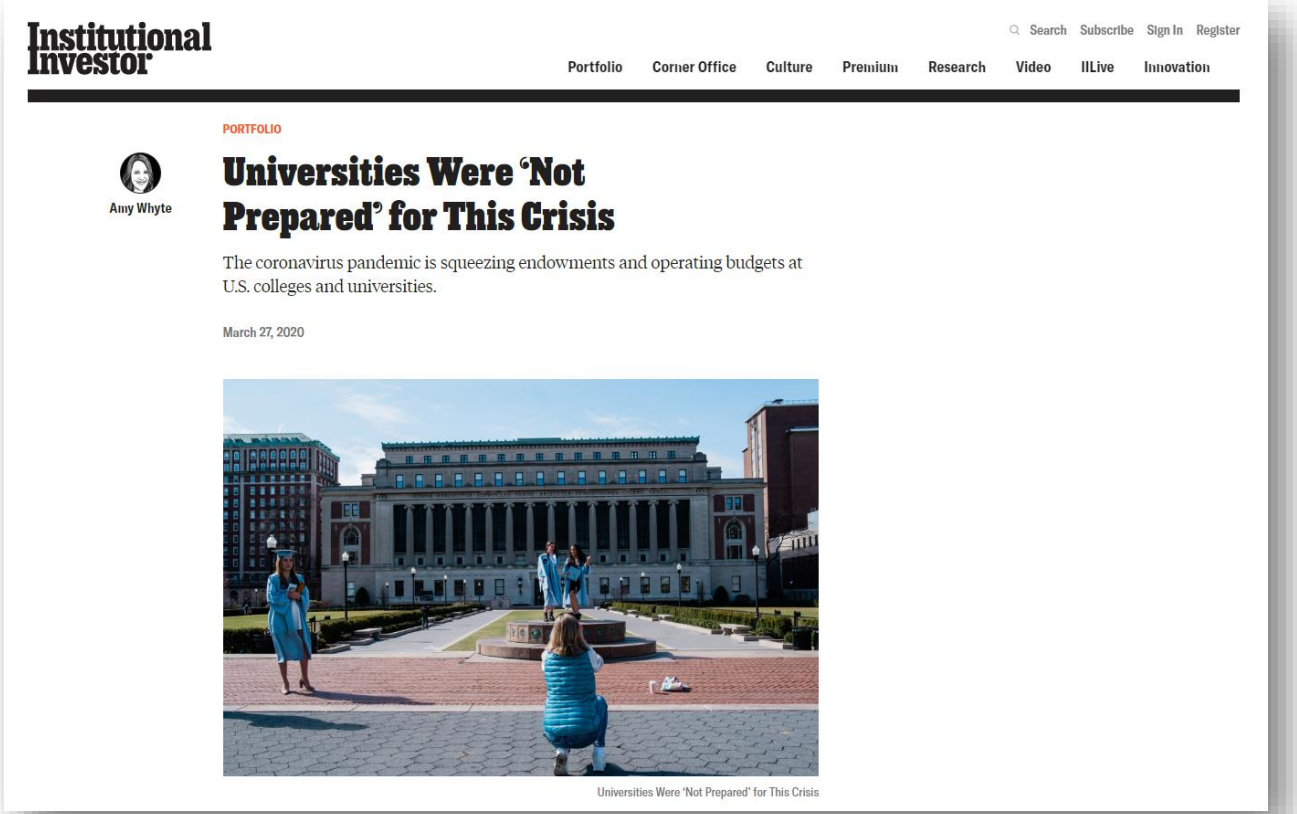
***Blake Wells – Vice President, IMA Higher Education Program***

Blake joined IMA in 1996 and led the development of the IMA Private College Insurance and Risk Management Practice. He works with many colleges and universities to assist in the design of cost effective and efficient insurance and risk management programs, including employee benefits plans, and athletic and student health insurance. Blake collaborates with private college leadership at the state and national level and is involved directly, or as a sponsoring partner to associations including The Coalition for College Cost Savings, URMIA, NACUBO, CACUBO, SACUBO, NAICUSE and many state private college associations.

# AGENDA

1. An Unexpected Storm
2. AP/P2P Transactional Oversight
3. Payment Oversight
4. Cyber Risk Management & Insurance
5. Questions and Calls to Action

We are experiencing an
Unexpected Storm of Threats
in the form of noncompliance, risk, and fraud
FISCAL
TECHNOLOGIES®



Institutional Investor

Search Subscribe Sign In Register

Portfolio Corner Office Culture Premium Research Video IILive Innovation

PORTFOLIO

Amy Whyte

# Universities Were 'Not Prepared' for This Crisis

The coronavirus pandemic is squeezing endowments and operating budgets at U.S. colleges and universities.

March 27, 2020

Universities Were 'Not Prepared' for This Crisis

***"This situation was completely unexpected."***

- Liz Clark, NACUBO VP of Policy and Research

CACUBO FISCAL TECHNOLOGIES Protecting Organizational Spend IMA HIGHER EDUCATION paymerang THE COALITION ON COLLEGE COST LEADERS

# COVID-19 BUSINESS DISRUPTION

## WHAT TO EXPECT…

1. **Acute Phase**
   - Very disruptive; forced decentralization; transactional errors
   - Current phase; may extend several more weeks
   - FRAUD very prevalent

2. **Restoration Phase**
   - Restoring “normalcy”
   - 6-9 months time period is the best “guesstimate”
   - Continued heightened FRAUD risk

3. **Recovery Phase**
   - Resume pre-crisis levels
   - Rethinking processes

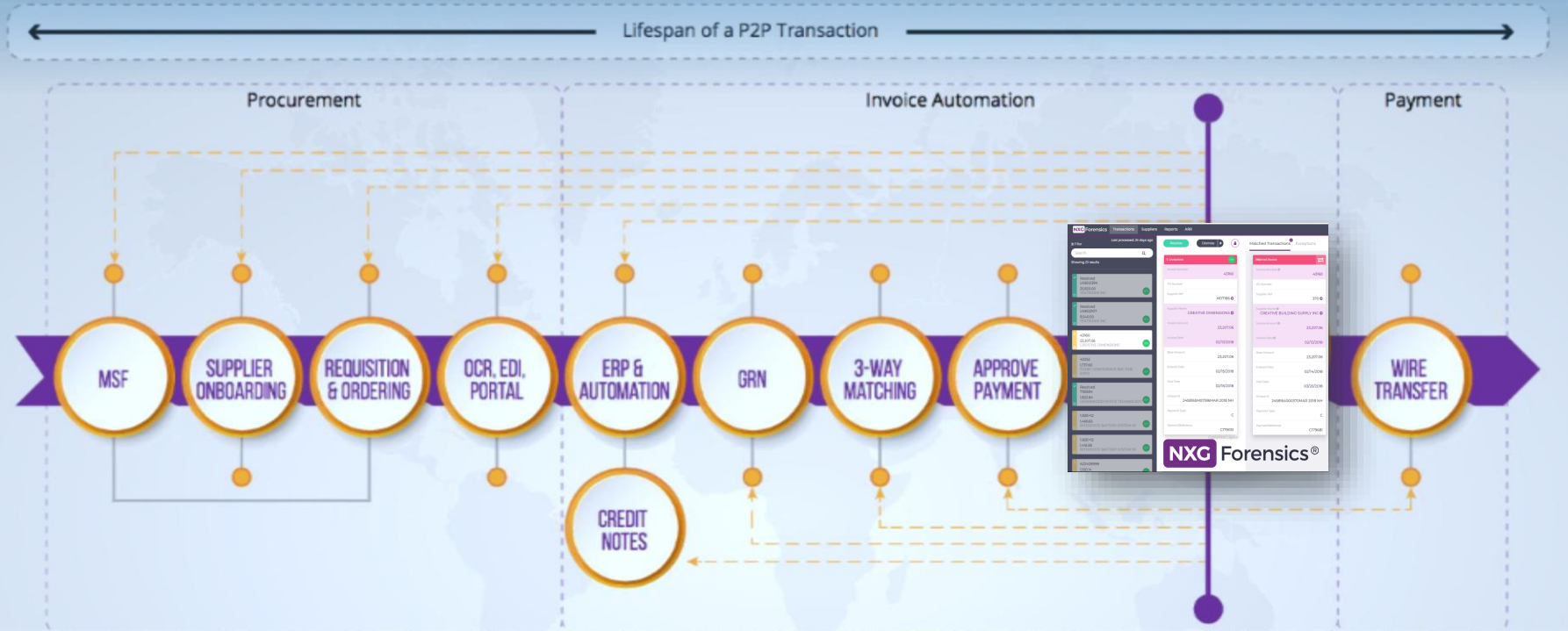
# MITIGATING AP/P2P RISKS:
# WHAT KPIs SHOULD I BE MEASURING/MONITORING?

- % Invoice Exceptions
- Source of Errors
- Type of Errors
- % Low Dollar Transactions (< $500)
- Potential Dupe Vendors
- % Low/No Activity Vendors
- % Credit Memos
- Invoices Processed Per FTE
- % Electronic Payments
- Purchase Order Rate

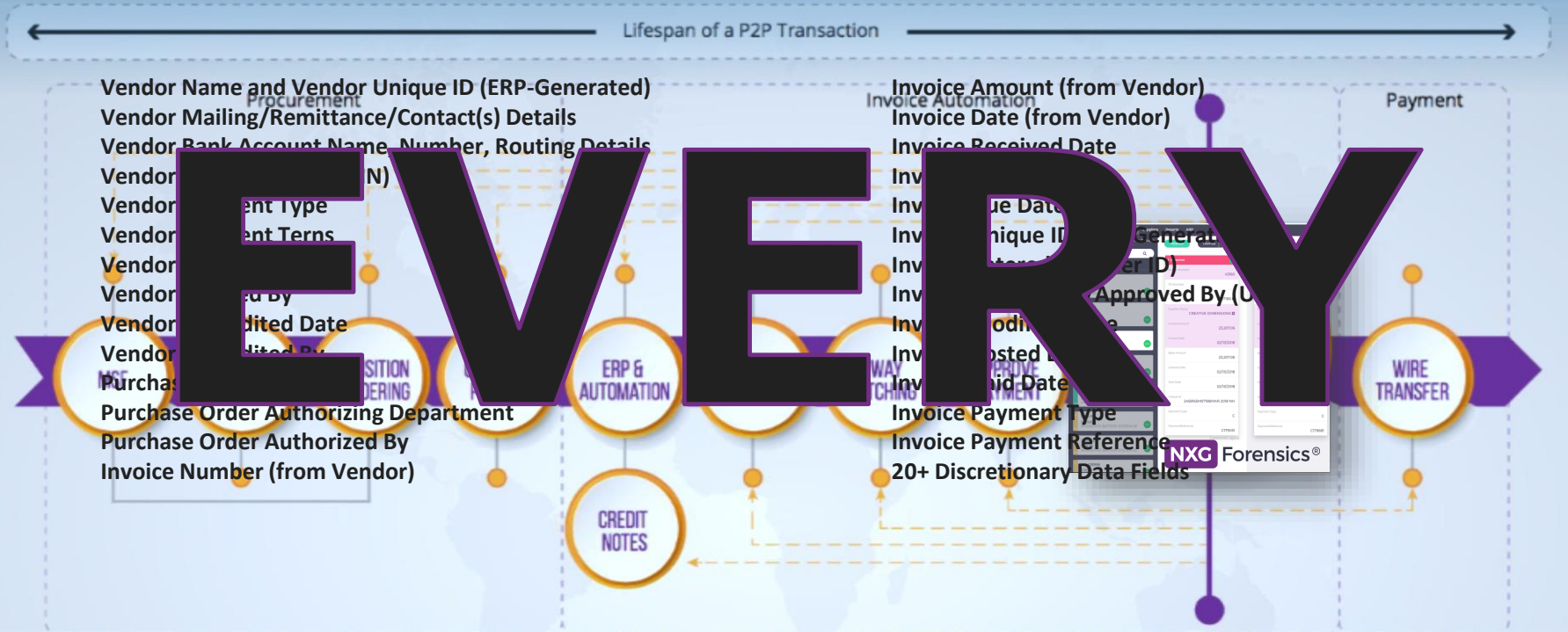
# MITIGATING FRAUD RISKS:
# WHAT TESTS SHOULD I BE MEASURING/MONITORING?

- Vendor Master – Employee Master
- Benford's Analysis
- Credit Note Frequency
- Date Entered – Date Paid
- Invoice Numbering Structure
- Even Dollar Amounts
- Transaction Spikes
- Initials in Vendor Name
- P.O. Boxes
- Vendor Addresses

# MITIGATING AP, COMPLIANCE, & PAYMENT RISKS: LEVERAGING STRUCTURED DATA ELEMENTS



# MITIGATING AP, COMPLIANCE, & PAYMENT RISKS: LEVERAGING STRUCTURED DATA ELEMENTS




EVERY

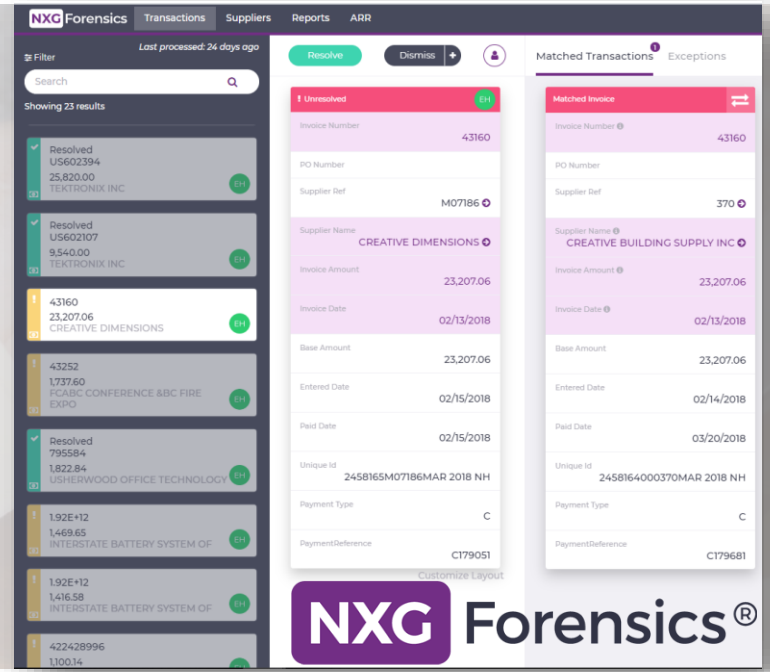
# NXG FORENSICS:
# A COMPREHENSIVE AP/P2P OVERSIGHT PLATFORM

## 100% DAILY

Identifies AP/P2P risk (noncompliance and fraud)

Prevents AP payment errors

Mitigates P2P transactional risks




## EVIDENCE

Identifies source of noncompliance

Enables oversight of staff and vendors, providing near real-time correction

Protects and empowers AP and finance

CACUBO · FISCAL TECHNOLOGIES · IMA HIGHER EDUCATION · paymerang · THE COALITION FOR COLLEGE COST LEADERS

# MITIGATING RISK AND ENSURING AP/P2P TRANSACTIONAL OVERSIGHT SINCE 2003

Incorporated

**2003**

**GLOBAL**
Higher Ed Client Base

Protected **1B** Transactions & **$7T** in Spend

Provide cloud-based **forensic tools**

Creating **Best-In-Class** Financial Operations

NXG Forensics®

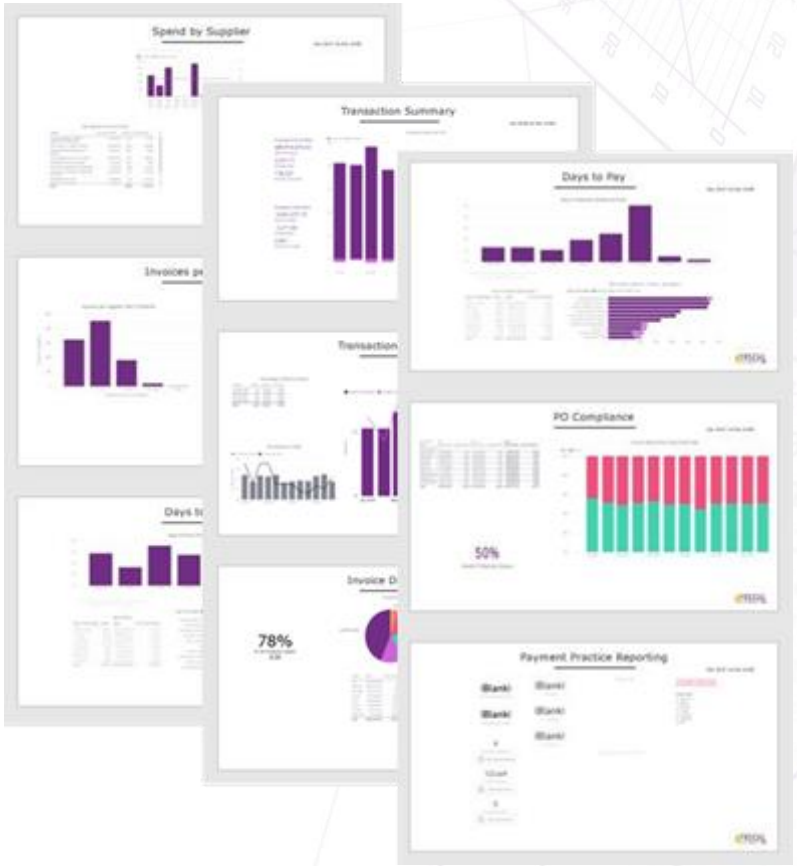
CACUBO FISCAL TECHNOLOGIES IMA HIGHER EDUCATION paymerang

# COMPLEMENTARY FORENSIC RISK REPORT

An **independent analysis** of high risk payments and vendors, vulnerabilities, and noncompliance

**Evidence** of immediately available recoveries from historical payment errors

Prioritizes process improvements leading to **cost savings**



# EASY AS ONE-TWO-THREE

**Requires ONE Simple Data Extract**

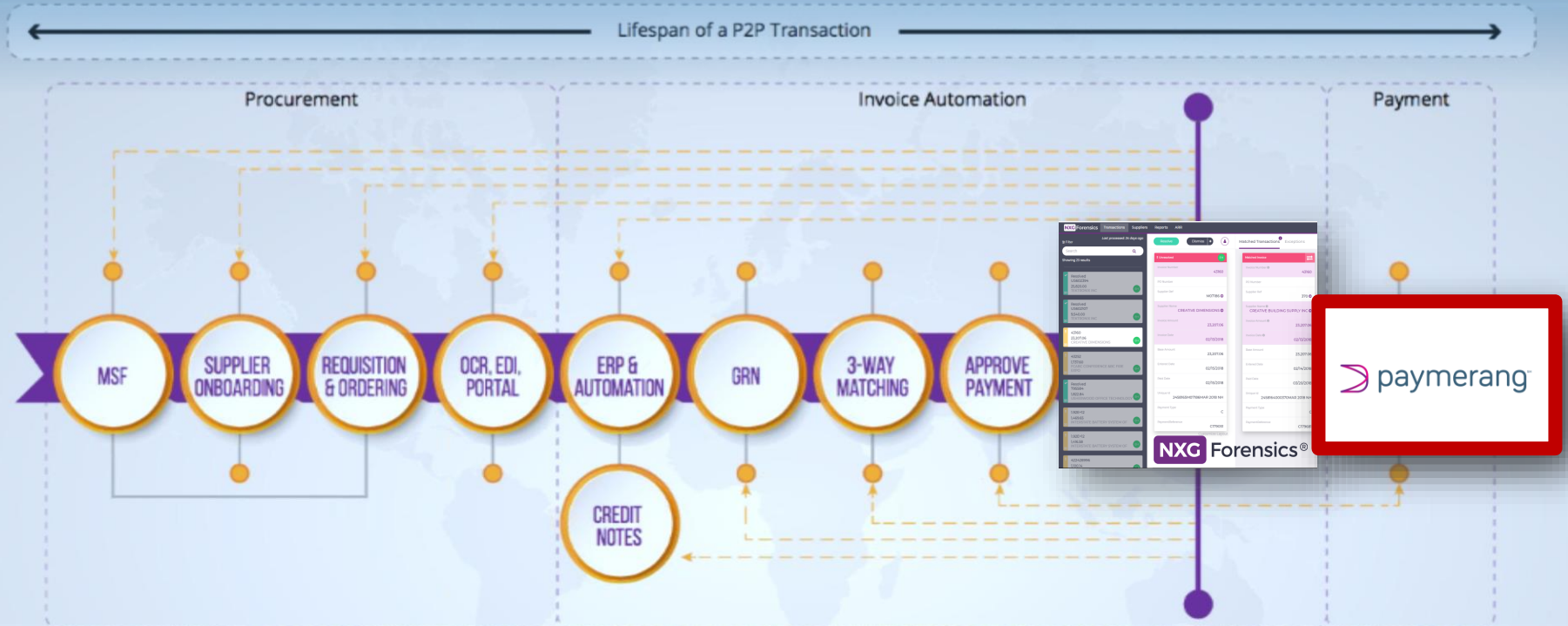
**Initial Results Within TWO Working Days**

**A Full Analysis Up To THREE Years of Your Data**

**Complete**
**data protection**
**and confidentiality**

FISCAL TECHNOLOGIES®

# MITIGATING AP, COMPLIANCE, & PAYMENT RISKS



paymerang℠

# Crush Payment Fraud Risk in 2020

1 The key threats of payment fraud

Four layers of protection available

Practical steps you can take

# THE FACTS ABOUT CHECKS

"On that check is my name, address, phone number, my bank's name and address, my bank account number, routing number, and my signature."

*Frank Abagnale (Catch Me If You Can)*

## CHECK FACTS & BENEFITS

- **#1 risk of fraud. 75% of businesses in 2017**
- Your bank cannot stop a fraud from happening
- Checks are the most time consuming and expensive way to pay vendors
- Most payment problems are check related
- Simple (always done it this way)

## KEY THREATS:

- **Duplicate a check**
- Electronically process it for a different amount
- Pay fraudulently (internal)
- Bank account data right on the document

## PRACTICAL SOLUTIONS

- **Positive Pay**
- **Stop paying vendors by check, use electronic payments**
- Engage a third party to process payments

# IS ACH THE SOLUTION?

## ACH FACTS & BENEFITS

- **More secure than checks**
- Payments process like clockwork
- Cost effective
- Control delivery

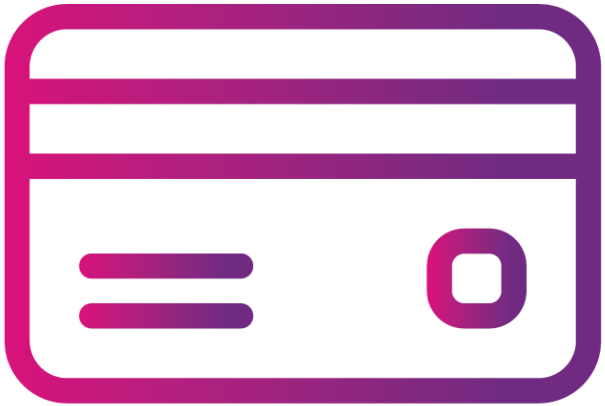
## DOWNSIDE & RISK

- Months to set up
- **Acquire, manage and secure vendor banking data**
- Remittance information to vendor
- **Compliance Violations**
- **Phishing and hacking**

## PRACTICAL SOLUTIONS

- Process ACH over check whenever you can
- **Read, understand, implement and train NACHA compliance**
- Encrypt vendor banking data
- Engage a third party to process payments

# IS CARD THE ANSWER?



## CARD BENEFITS

- **Liability is limited for unauthorized payments**
- Set controls around use of the card account
  - Establish authorization limits
  - Block Merchant Category Codes (MCCs)
- **Opt for single-use virtual card accounts vs. physical plastic**
- Commercial rails can assist with payment traceability and reconciliation

## KEY CONSIDERATIONS

- **Management of credit lines at company or account level**
- Tying payment and vendor management strategies
- Determine card issuance strategy to mitigate misuse
- Balancing prevention and employee experience

## PRACTICAL SOLUTIONS

- Use card whenever possible, which often includes rebates
- **Incorporate single use virtual cards accounts in addition to traditional plastic**
- Determine the best payment strategies to optimize working capital and mitigate risk

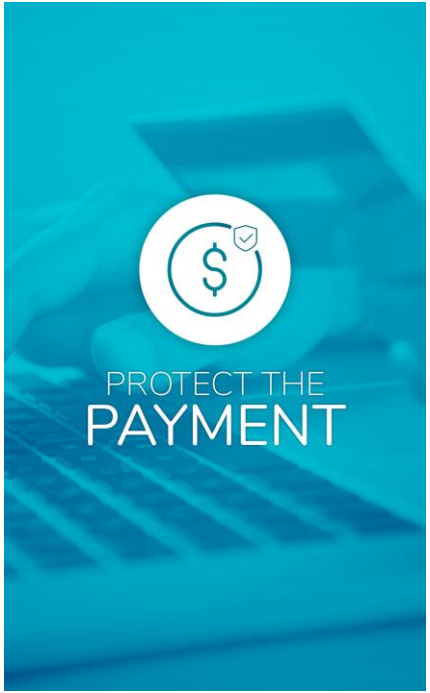
The key threats of payment fraud

2

Four layers of protection available

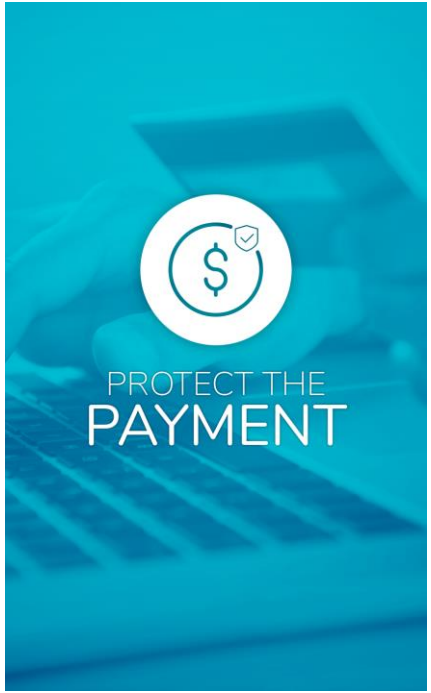
Practical steps you can take

# FOUR LAYERS OF PROTECTION AVAILABLE



CACUBO FISCAL TECHNOLOGIES IMA HIGHER EDUCATION paymerang

# PROTECT THE PAYMENT




## POSITIVE PAY

**WHY:** To ensure only the authorized party on a check is allowed to cash that check and reduce the likelihood of payment to a fraudulent entity.

**HOW:** Enroll in the Positive Pay service at the financial processor where check payments are sourced.

## VIRTUAL CARDS

**WHY:** To limit the exposure of open, higher limit credit lines that are in use for payments.

**HOW:** Transact using VISA virtual debit cards (vCards) to limit payments to a one-time use, preloaded payment amount.

## ACH PAYMENT

**WHY:** Use of electronic payments that can be trusted through an established network, where the likelihood of fraud is reduced.

**HOW:** Register to use ACH payments with the bank account where payments are sourced and take additional steps to protect the payment information (i.e. encrypt sensitive data).

## PROCEDURES

**WHY:** Procedures need to be in place to validate payment relationship information before action is taken to modify accounts or payments.

**HOW:** Before engaging with vendors or making any changes to information, the identity of the other party must be verified. Limit the information your employees can see and do not allow them to change sensitive data without approvals.

# SECURE THE OPERATIONS

## SECURE ENVIRONMENT

**WHY:** All payment data needs be protected in the operating environment where processed.

**HOW:** Use a combination of a clean desk policy, removal of all payment information from open office view, and a certified shredding service.

## TRAINING

**WHY:** The payment team members are an important line of defense for ensuring a secure operation.

**HOW:** Conduct security awareness training by qualified staff on a regular basis to ensure team is aware of threats and how to detect suspicious links or fraudulent email addresses. Provide ongoing payment threat awareness information so the team knows what is considered suspicious and are ready to respond to it.

## FRAUD DETECTION

**WHY:** To detect fraudulent payments and ensure that only legitimate payments are made.

**HOW:** Verify any anomalous changes made to vendor account information before processing payments. Assign fraud scores based on recent account changes.

## PROCEDURES

**WHY:** To ensure operational controls are present throughout the payment process.

**HOW:** Set up all payment processes with multiple approvals, single payment limits and segregation of duties. Implement job rotation and cross-training for payment team members. Appropriate access controls.

# FORTIFY THE NETWORK

## END POINT PROTECTION

**WHY:** To ensure that only safe and trusted software run on computers that process payments.

**HOW:** Provide protection with the use of anti-virus software coupled with best in class application whitelisting technology to protect against forms of malware.

## EMAIL DEFENSES

**WHY:** To reduce the amount of unsafe email into the payment process and protect sensitive information sent in payment email.

**HOW:** Deploy layers of spam/phishing defenses, including spear phishing detection, along with email encryption and rights management to protect sensitive email content.

## VULNERABILITY MANAGEMENT

**WHY:** To identify exploitable software and security weaknesses in the payment system in order to reduce exposure to possible system compromise.

**HOW:** Enable a vulnerability management program with regular security posture scanning, software patching, and expert penetration testing.

## THREAT PROTECTION

**WHY:** To determine when suspicious actions are being attempted or carried out against the payment system.

**HOW:** Enact intrusion and anomalous behavior detection capabilities with multi-factor authentication and full logging in the appropriate layers of the payment system.

# LOCK DOWN COMPLIANCE

## NACHA

**WHY:** To ensure automated payments are processed in a trusted and controlled environment.

**HOW:** Process payments using the ACH Network which maintains the highest level of safety and security for its participants through governance oversight by NACHA.

## SOC-2

**WHY:** To verify the operating effectiveness of a service provider's Availability, Integrity and Confidentiality (AIC) security controls, by an audit expert, for companies wanting to use the service.

**HOW:** If you are a service provider, then contract an audit service to conduct a SOC-2 assessment, in accordance with AICPA Trust Service Criteria.
If you are a consumer of a supplied service, then request the SOC-2 Report from the supplier and confirm any gaps in expected controls.

## PCI

**WHY:** If payment cards are processed or stored there is a security standard mandated by the Payment Card Industry (PCI) that must be attested.

**HOW:** Implement the PCI Data Security Standard (PCI-DSS) to ensure that cardholder data is maintained in a secure environment accordingly.

## OFAC LIST

**WHY:** To reduce the likelihood of payments being sent to individuals or organizations determined to be threats to US national interests.

**HOW:** Compare the US Treasury Office of Foreign Assets Control (OFAC) Sanctions List against pending payments and stored supplier data to identify possible threats.

The key threats of payment fraud

Four layers of protection available

3

Practical steps you can take

# PRACTICAL STEPS

As long as there is money and valuable data, there will be fraud attempts and threats to security.

## PAYMENT

- Positive pay
- E Pay
- Use one-time use, preloaded virtual cards
- Encrypt account information
- Verify vendors before making changes
- Limit employee access
- Require approval for changes

## OPERATIONS

- Clean desk and secure documents
- Utilize certified shredding service
- Verify anomalous changes
- Assign fraud scores
- Suspicious links and fraudulent email detection training
- Multiple approvals
- Single payment limits
- Segregation of duties
- Job rotation and cross training
- Defined access controls

## NETWORK

- Antivirus Software and whitelisting technology
- Vulnerability management program
- Security posture scanning
- Software patching
- Expert penetration testing
- Spam and phishing defenses
- Email encryption
- Multi-factor authentication

## COMPLIANCE

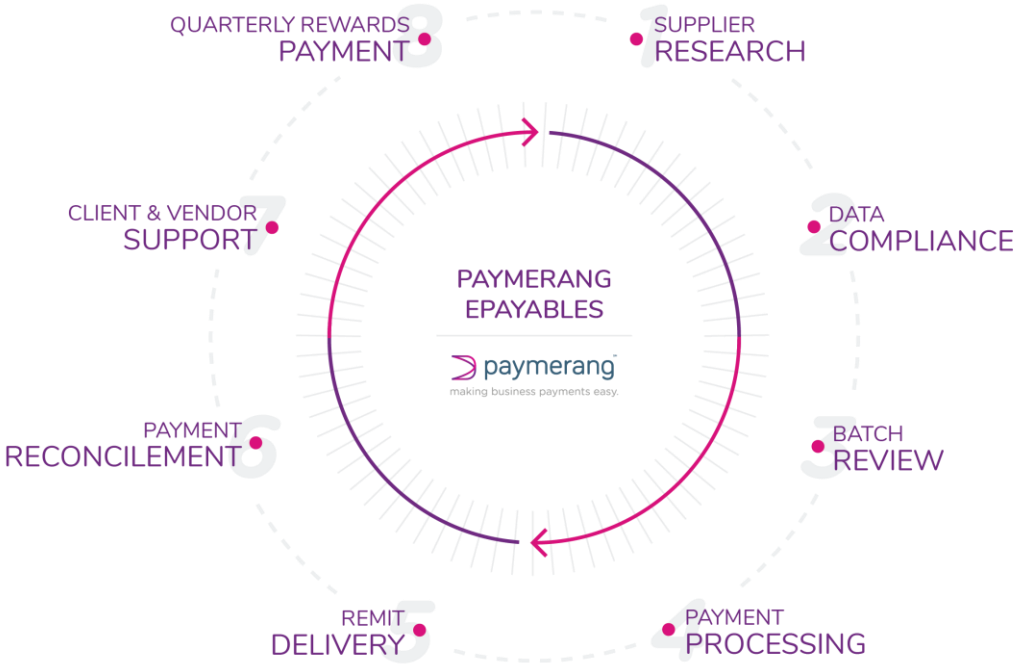
- NACHA - read it, learn it, train it
- Do not store banking data if you can avoid it
- PCI- Secure cardholder data
- SOC 2- Security controls for integrity and confidentiality
- OFAC- Know your vendor and where your money is going

# GET HELP TODAY

- **ASK FOR A FREE PAYABLE ANALYSIS A FINANCIAL BENEFIT REVIEW**

paymerang℠

Since 2010. Paymerang has helped hundreds of companies, secure and shield their payments and bank accounts from fraud and has relieved the burden of vendor payments, reconciliation, data retrieval, management, storage and compliance.



# HIGHER EDUCATION

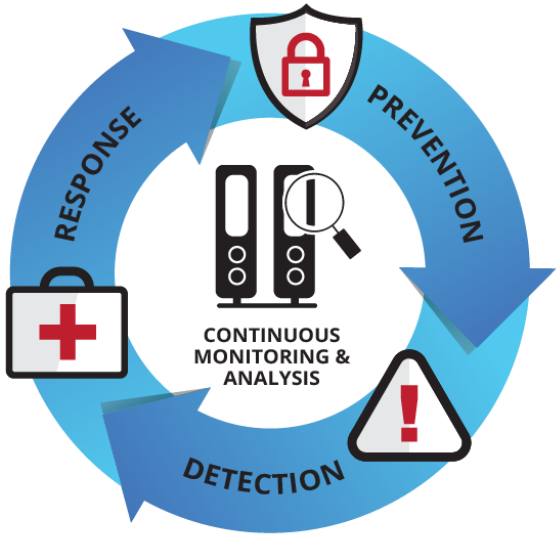
- Ranked as the 6th largest privately held insurance brokerage firm in the United States.  800+ Associates
- IMA's Higher Education practice has a 100% Success Rate in Driving Down colleges net cost of their Property & Casualty Insurance Program.
- Team & Risk Management Resources Dedicated to Higher Education
- Goal Today:  Best Practices in Cyber Risk Management & Insurance

# A BASIC CYBER RISK MITIGATION SECURITY STRATEGY

**Prevent:** set of policies, products and processes that are put into place to prevent a successful attack. The key goal of this stage is to reduce the attack surface.

**Detect:** capabilities are designed to find attacks that have evaded the prevention layer. The key goal of this stage is to reduce the "dwell time" of threats and, thus, reduce the potential damage they can cause.

**Respond:** proficiencies are required to remediate issues discovered by detective activities, provide forensic analysis and recommend new preventive measures to avoid repeat failures.




***GOAL:* 360° of security protection - visibility, prevention, detection, response and containment.**

CACUBO FISCAL TECHNOLOGIES IMA HIGHER EDUCATION paymerang

# COVID-19 AND INCREASED CYBER EXPOSURE

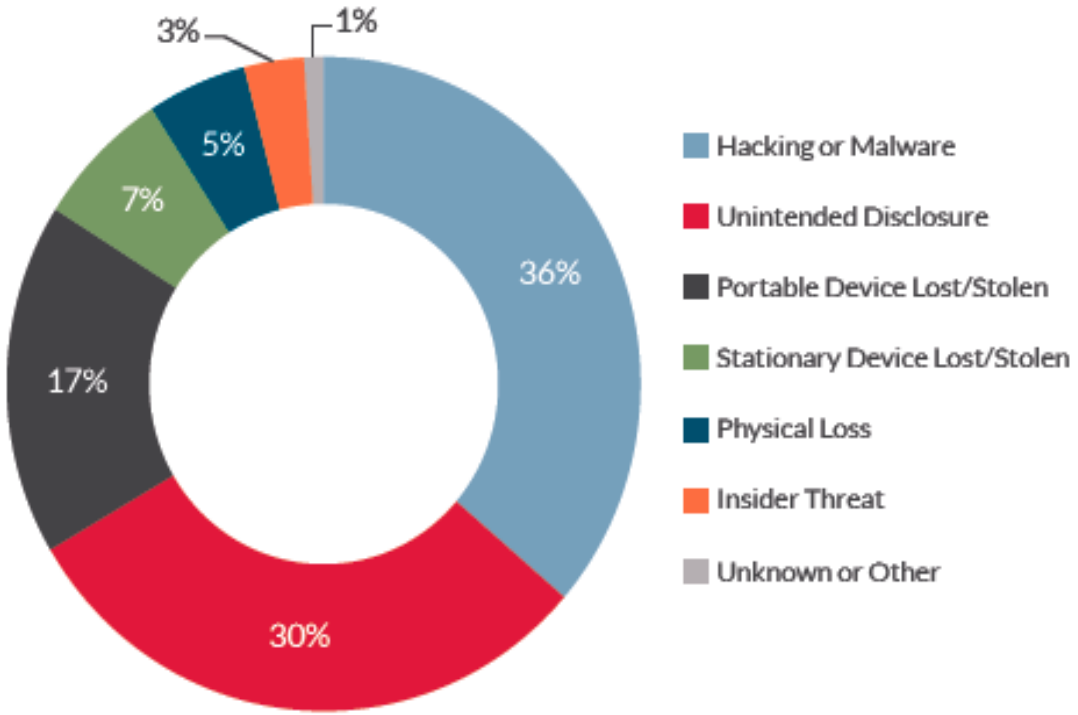
- INCREASED Phishing Attempts – Fake emails impersonating real entities to get you to click on a link
  - World Heath Organization, Medical Supplies / Masks, Airlines, Charities, Twitter Accounts
  - Since 2016, 93% of Healthcare facilities have had a cyber incident / breach
- INCREASED Remote Desktop Protocol (RDP) opens gateway to hackers
  - Many do not require /have Mutli Factor Authentication (MFA)
  - 80% of RANSOMWARE attacks are through RDP
- Recommendations
  - Test / Retest - Remote Login Security & Capabilities
  - Additional "Phishing" training for employees to spot fake / malicious attacks
  - Implement / Review Incident Response Plan (IRP)
  - Review 3rd Party Vendor Access / Shared Data assessments / requirements
    - 50% of cyber incidents since 2016 due to insiders / vendors / 3rd party partners
- Resources
  - URMIA, ACE Engage, Campus Safety
  - IMA COVID Alert Center / Cyber Risk Management Report

# UNDERSTAND HIGHER EDUCATION CYBER RISKS

- INSTITUTION / BOARD ISSUE - Top 3 concern for institutions. No longer just IT Issue
- NOT STATIC RISK - Cybercriminals are getting smarter, Not only is Technical Data being compromised, but human qualities are as well; i.e.. Voice, fingerprints, etc. and who knows what is next.
- PRIME TARGET -Educational Institutions are heavily targeted as is healthcare due to amount of Private Information available. Imagine the years of employee and student information you have access to.
- ADDITIONAL STANDARDS / COMPLIANCE / REGULATION - International Students – GDPR (European Union's Regulation of General Data Protection Regulations) Would you know what those regulations are?? Have the time and expertise to find out?

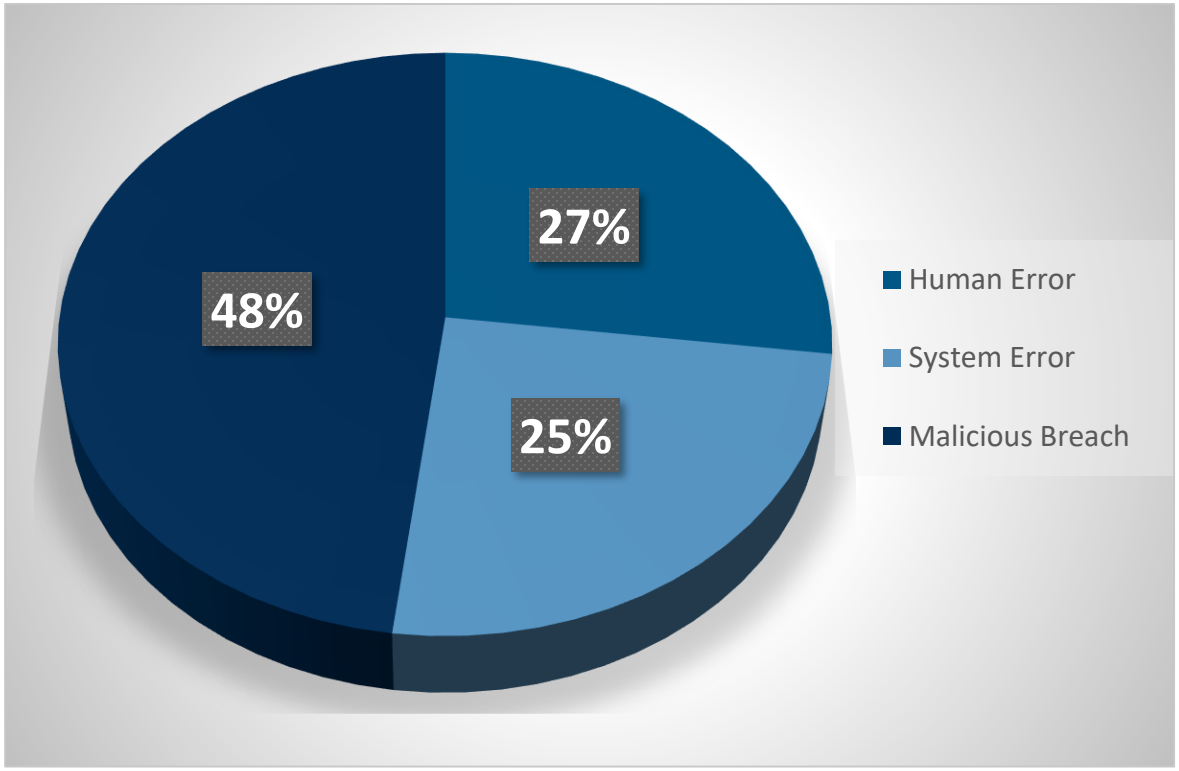
# EDUCATIONAL SYSTEMS VULNERABILITIES

- Massive BYOD environments
- People process technology
- Large wireless networks
- Lack of threat intelligence
- Cultural resistance
- Cyber security budgets
- Decentralized
- Poorly documented networks




CACUBO FISCAL TECHNOLOGIES IMA HIGHER EDUCATION paymerang

# SOURCES OF CYBER BREACH




- 52% Human or System Error
- 48% Malicious Breach

# COMMON TYPES OF CYBER ATTACK

## TYPES OF DIGITAL ATTACKS

**Phishing/Spearphishing** – Emails that target everyone or a specific person or role within an organization that include malicious links or entice users to enter their credentials or other personal information on a website designed to mimic a legitimate site.

**Social Media Deception** – Bad actors create fake profiles to befriend their victims, posing as a current or former co-worker, job recruiter, or even someone with a shared interest on social media. The goal is to trick the victim into providing sensitive information or downloading malware onto their device.

**Pre-texting** – Attackers focus on creating a false but believable fabricated story, or pre-text, prompting their target to provide certain information in order to confirm their identity.

**Water Holing** – Attackers compile information about a specific group of individuals within a certain organization or industry, including legitimate websites this group visits. Attackers then look for vulnerabilities in these sites in order to infect them with malware. Once the individuals in the targeted group visit those sites, they become infected with malware.

# CLAIMS DATA / EXAMPLES

**Campus Safety report on Oct 4, 2019 reported 500+ Educational Institutions including Universities were affected by Ransomware in 2019.** Trends reported:

- Attacks thru Managed Service Providers, Cloud Providers are on the rise. Many believe these providers will protect them if something happens.
- Ransom demands are getting bigger, partially due to cyber insurance paying
- Email attachments continue to cyber criminals #1 choice.

**April 24, 2019 – Kentucky School $3.7 Mil Cyber Phishing Scam**

- School sent electronic funds payment to who they thought was a regular vendor. Unfortunately, fraudulent routing numbers sent funds to criminals account. Classic example of a phishing scam, also known as fraudulent instruction or social engineering. Many times tracing the funds is almost impossible.

# CYBER EXPOSURE & INSURANCE

If you currently purchase this coverage or considering purchase, there are numerous coverage solutions that could apply.

**Cyber Crime:** Will reimburse for loss of funds associated with social engineering exploits.

**Network Business Interruption:** Will indemnify for loss of income due to down time (subject to a waiting period).

**Cyber Extortion/Ransomware:** Will fund investigative expenses and ransom payments.

**Incident Response:** Funds to engage first responders (legal counsel, forensic investigators and crisis management firms) in the event of an actual or suspected event.

It is also worth noting that most Cyber policies come with complimentary loss control solutions that can help provide additional resources.

# INCIDENT RESPONSE

- **Average Breach cost is $178,000.**
- Cyber Incident Response
- Legal and Regulatory Costs
- IT Security and Forensics Costs
- Crisis Communication Costs to help with media and protect reputation.
- Third Party Privacy Breach Management Costs ie. Notices, Credit monitoring
- Post Breach Remediation Costs help mitigate future breaches

# SYSTEM DAMAGE AND BUSINESS INTERRUPTION

- **Average Loss of "Profits" & System Damage is $343,000.**
- System Damage and Rectification Costs to help recover or rebuild data
- Income Loss and Extra Expense
- Dependent Business Interruption
- Consequential Reputational Harm
- Claim Preparation Costs
- Hardware  Replacement Costs

# LEGAL & LIABILITY ISSUES

- **Average Legal Fees $181,000**
- Network & Privacy Security Liability – Protection if sued due to breach.
- Management Liability – Sr. Officers named in suit protection
- Media Liability – Defamation & Intellectual Property Rights
- Regulatory Fines
- PCI Fines, Penalties and Assessments

# CYBER TRAINING & RESPONSE RESOURCES

**IMA Cyber Risk Hub / Best Practices Center**

- Incident Response Roadmap – suggested steps to take following a network or data breach, free consultation. Very helpful if you do not currently buy Cyber. If you do, your Cyber Carrier will be your primary call if an event.
- News Center – Cyber risk stories, security and compliance blogs, security news, risk management events and helpful industry links

**24/7 Global Cyber Incident Response Center with Multi-lingual call handlers**

**Cyber Risk Rating Report**

- Provide comprehensive security risk rating report by reviewing key features regarding your internet presence. Your rating is similar to a consumer credit score and allows you to benchmark yourself against your peers.

**Cyber Risk Awareness Training**

- Phishing focused eLearning tool helps protect you from social engineering attacks. It provides a tool to test your users and prepare them for inevitable phishing campaigns.

**Cyber Breach Alert**

- Breach monitoring service searches the dark web for information specific to your institution and alerts you in real-time.

**Cyber Awareness Videos**

- Up to 25 complimentary licenses for security awareness videos.

**Cyber Incident Response Plan Builder**

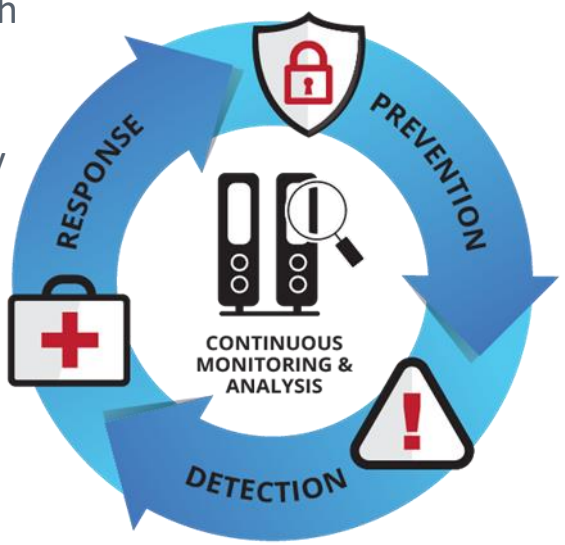
- Toolkit brings together wide range of templates to help you produce a tailored incident response plan.

# IMPORTANT QUESTIONS ABOUT CYBER INSURANCE

- What are the policy limits? Single Aggregate or Multiple Limits?
- Is there a retro-date for prior acts coverage?  Dwell time could be 2 years.
- Is there coverage for phishing scams, telephone hacking, ID theft?
- What coverage is provided for hardware costs?
- What if the government fines the school?
- What cyber services are provided?
- What are the EXCLUSIONS in the policy? No 2 policies created equal

# CYBER RISK MANAGEMENT & INSURANCE CONCLUSIONS

- New cyber regulations are coming
- The criminals are always finding new methods to make money through cyber crime
- The cyber threat is constantly  changing and evolving so you must stay ahead
- Schools are most venerable to cyber attacks due to limited resources
- A multi-layer cyber risk management strategy is key
- Insurance is a vital part of any cyber program
- Update, revise ,review, and test your cyber risk strategy annually
- Rigorous employee training  reduces your liability exposure




CACUBO FISCAL TECHNOLOGIES IMA HIGHER EDUCATION paymerang

# THANK YOU - QUESTIONS – NEXT STEPS

**BRIAN COOK**
**SVP of Higher Education**
Paymerang
804-317-9229
bcook@paymerang.com
paymerang.com

**ERIC HAYES**
**Vice President**
Fiscal Technologies
919-277-0333
ehayes@fiscaltec.com
fiscaltec.com

**BLAKE WELLS**
**Vice President**
IMA, Inc.
316-266-6213
blake.wells@imacorp.com
imacorp.com/higher-education