

# Preventing Internal Data Breaches: Security and Controls to Protect your Data

**Amanda Barker | Aidan Parisian**

August 10, 2022



The Association of  
Accountants and  
Financial Professionals  
in Business

**ORACLE®**  
**NETSUITE**

# Webinar Features and CPE Credit

Q&A

Asking Questions



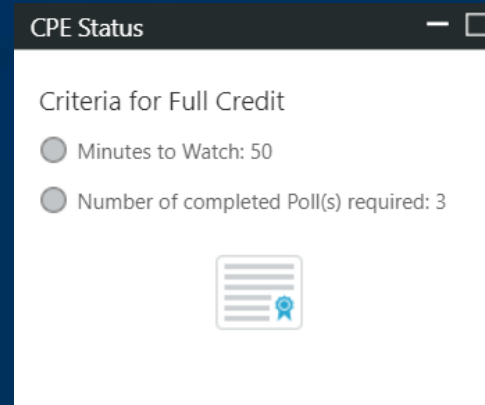
Closed Captioning



Help



CPE Credit



The Association of  
Accountants and  
Financial Professionals  
in Business

ORACLE®  
NETSUITE

# Moderator

**Steve Shannon**

**Director of Partnership Marketing,  
Business Development**

**IMA**



The Association of  
Accountants and  
Financial Professionals  
in Business

# Featured Presenters



**Amanda Barker**

**Director, Financial Operations**  
Connor Group



**Aidan Parisian**

**Senior Vice President of  
Product and Strategy**  
Fastpath

# Amanda Barker's Biography

- Amanda Barker is a Director in Connor Group's Financial Operations practice. She is an experienced risk and controls professional with a deep understanding of the challenges clients face when implementing new financial applications or optimizing processes and controls. She has helped numerous clients, from pre-IPO startups to established Fortune 100 companies, design, develop and implement leading security and controls practices.
- Prior to joining Connor Group, Amanda spent 10 years with PwC. She began her career as an IT Auditor and as a result understands the technical requirements and challenges public companies must manage. Amanda spent the last 5 years developing deep technical knowledge of ERP systems, such as Oracle and NetSuite, and has helped companies going through ERP transformation programs develop security and controls programs that support an optimal future state.

# Aidan Parisian's Biography

- As the Senior Vice President of Product and Strategy, Aidan Parisian has responsibilities including strategic planning, roadmap definition, partner management and cultivation, and thought leadership creation & education. Prior to Fastpath, Aidan spent a decade as an auditor, in both industry as well as public accounting as the Senior Manager of Internal Audit at Pure Storage, and Director of Internal Audit at PricewaterhouseCoopers.
- During his tenure at PwC, he led efforts related to privacy at a large social media company, system implementation project management at a utility provider, and was a specialist with regard to SAP and Oracle. Aidan co-founded the NetSuite Center of Excellence at PwC in San Jose.
- He is a Certified IS Auditor with degrees in Business Administration & Economics from the University of Oregon.

# Learning Objectives

1. Describe the increased threat of internal data breaches and barriers to successful security.
2. Discuss the responsibility placed on data security from regulations including - GDPR, CCPA, and Sarbanes-Oxley.
3. Explain how to quantify risk to get executive support to address security vulnerabilities.
4. Identify available risk assessment and mitigation tools.

## Poll Question 1:

Has your company had a loss of private or critical data?

- a. Yes, we have
- b. No, we have not
- c. Not that I am aware of



# Poll Question 1 Results: (Placeholder)

# The Threats

**Rapidly changing landscape of how business is done means the threats to security are ever evolving**

- Remote work – how employees' access to company networks may be less secure than pre-pandemic
- Reliance on cloud based and hosted applications and databases
- Macroeconomic environment creates pressure/rationalization for fraud
- More sophisticated external threats, changing tactics of cyber criminals

# Effect of the Pandemic on Risks

- The pandemic permanently altered how we work – remote working has become common place increasing security gaps from
  - Use of unsecured Wifi Networks
  - Increased File Sharing
  - Connecting Personal Devices to corporate network
- Unpredictable markets some are struggling with potential layoffs and uncertain income.
- These changes cause employees to succumb to the temptation to take money from their companies.



**71%**  
**expected in  
fraud over the  
next year**

# Trends in Data Breaches

- Cyberattacks are a near constant threat to modern business with attacks occurring every 10 seconds. During the month of January 2021 alone, 878.17 million data records were compromised – more than the total number of records stolen throughout all of 2017\*.
- Cyber criminals are changing their tactics – using phishing and social engineering to obtain login credentials to existing accounts accounting for 33% of all cyberattacks in 2021.
  - Other sources of data breach included: malware, ransomware and third party/supply chain vulnerabilities
- ~7% of data compromises are the result of internal actors vs 93% by external parties\*.
- 10% of data breaches in 2021 were the result of human error or improper system configuration\*.

# What's at Stake

- Financial misstatement
- Reputational risk
- Regulatory non-compliance (SOX/GDPR)
- Fraud/misappropriation of assets
- Vendor/Customer agreement compliance

# Regulations

- Regulations regarding data privacy and security (such as GDPR, CCPA, and state regulations) mean that companies are responsible for securing personal data from customers and users.
- Sarbanes-Oxley (SOX) – requires public companies to proactively employ strict controls on internal user access to business-critical systems to preserve the integrity of their financial statements.

## Poll Question 2:

Has your company performed a risk assessment to identify security risks?

- a. Yes
- b. No
- c. I don't know

## Poll Question 2 Results: (Placeholder)



# Where to start?

**There is no single solution to protect data and ensure regulatory compliance.**

**BUT...**

**There are steps a company can take today to help secure their data.**

# Step 1: Risk Assessment

- IDENTIFY where your company is most vulnerable and your biggest security threats
- A risk assessment will help with this task by assessing:
  - Where your data is stored
  - Where the company does business
  - How secure are the vendors involved in your supply chain
  - How your employees access your systems, with special emphasis on remote workers
  - Employment agreements around collection of data
  - How are roles designed in high risk systems to enforce segregation of duties

# Good Foundations: Access Management Controls

- Using your Risk Assessment and PLAN out actionable steps to address your most significant risks.
- Controls around internally managed systems are a good place to start to address risk:
  - Separate duties analysis and evaluation of role design
    - Preventive provisioning
  - Authentication/Passwords
  - Join, Move, Leave processes around users and access
  - Limiting the use of superuser accounts - monitor when you have no choice
  - Comprehensive access review and certification
  - Cyber/Vulnerability assessments

# Quantifying the Risk

- Determine “what could go wrong”
- Quantify risk of data breach
  - How many customer records, what kind of sensitive data could be available
    - Example: 2021 CVS Health data breach resulted in 1.1B compromised records as a result of lack of password protection
      - Competitors can use this meta-data
      - Decrease in consumer and investor confidence
- Quantify risk of Fraud
  - Users have access to create and pay vendors – potential exposure could be all of payables
  - Possible to see if the user actually used the access to process transactions

## Poll Question 3:

How mature do you feel your organization's access management controls are?

- a. Very mature
- b. Somewhat mature but room for improvement
- c. Lots of potential gaps we need to address
- d. What are access controls?

## Poll Question 3 Results: (Placeholder)

# Barriers to Successful Execution

Barrier	Solution
Companies focus on protecting from <b>External</b> threats, but executives are often behind the curve on <b>internal protection</b> – thinking it “can’t happen here”	Get Executive & Board of Director Buy-In from the start: <ul style="list-style-type: none"><li>• Help them understand that the risks are real and <b>quantifiable</b>.</li><li>• Lack of action now <b>does not</b> save the company money instead it perpetuates existing risks.</li></ul>
Companies see system and data security as <b>impossible</b> or <b>constraining</b> to employee productivity.	Focus on elevating security exposure and fix high-risk exposer areas first
Impossible to eliminate all separation of duties completely	Understand where the high risks exist and build compensation controls to manage
Highly manually and time-consuming efforts to go through user access requests and find and separate duty risks.	Many tools that automate these business process are available to reduce error and increase efficiency.

## Poll Question 4:

Does your organization currently have automated tools in place for security measures?

- a. Yes, we do have tools in place
- b. No, currently we do not
- c. I don't know



## Poll Question 4 Results: (Placeholder)

# Automated Tools

- You need to know who has access, what they are allowed to do with that access, and what they have done with that access
- Leverage a software solution to get your hands around identity and access
- Tools like Fastpath help companies:
  - Automatically assess risk across multiple applications in the same business process, including Separation of Duties (SOD)
  - Preventatively manage join, move, and leave leveraging risk rules
  - Monitor critical configuration and standing data changes that impact risk

# Protection for the Future

Companies **MUST** protect their business and intellectual property from external **and** internal risks.

Start with a risk based approach to address the most critical threats to your organization

Quantifying the risks of internal fraud will **motivate executive leadership to address the company's security vulnerabilities** proactively.

# Questions and Answers



**Amanda Barker**  
Director, Financial Operations  
Connor Group



**Aidan Parisian**  
Senior Vice President of  
Product and Strategy  
Fastpath



**Steve Shannon**  
Director, Partnership Marketing,  
Business Development  
IMA

# Thank You to Our Presenters!



**Amanda Barker**  
Director, Financial Operations  
Connor Group



**Aidan Parisian**  
Senior Vice President of  
Product and Strategy  
Fastpath

# Final Reminders

- ▶ **Complete the Evaluation poll** – 2 options
  - On your screen
  - Evaluation Survey icon at the bottom of your console
- ▶ **Access to your CPE Certificate** – 2 options
  - Click the “CPE” icon at the bottom of your console
  - or
  - Click the link in your post-event e-mail
- ▶ Please print a copy of the CPE certificate for your records.
- ▶ Your CPE credit will be automatically recorded in your transcript.

# Share Your Knowledge and Expertise

Submit Your  
Speaker Proposal

**ima23** Accounting  
& Finance  
Conference

June 11-14, 2023 • Hyatt Regency Minneapolis



# Thank you!

Oracle NetSuite

[www.Oracle NetSuite.com](http://www.Oracle NetSuite.com)



The Association of  
Accountants and  
Financial Professionals  
in Business

**ORACLE®**  
**NETSUITE**