CFO ROUNDTABLE

CFOS ON TACKLING CYBERSECURITY THREATS AND DEFENSES

BY NINA LINCOFF ○ NLINCOFF@BIZJOURNALS.COM ○ @SFBJMONEY ○ 786-533-8214

PHOTOS BY JOCK FISTICK

Nine top CFOs discussed how they fit into the fight against cyberattacks during the Feb. 10 CFO Roundtable at the Business Journal's Miami offices.

In the analog world, a CFO's concern was largely the balance sheet and helping to guide a company away from risk and toward reward. But in today's digital world, a major risk facing businesses is cybersecurity attacks.

Organizations both small and large are constantly under siege from hackers and malicious software. In fiscal year 2015 alone, the U.S. government was hit by more than 77,000 cyber incidents – including data thefts or other security beaches, according to the White House. Along with Uncle Sam, Main Street businesses and Fortune 500 companies are also targets.

The *Business Journal* hosted a CFO Roundtable on Feb. 10 at its Miami office to discuss evolving cybersecurity vulnerabilities and the different ways CFOs fit into the fight against cyberattacks. The discussion was moderated by Editor-in-Chief Mel Meléndez, and sponsored by Randstad Professionals and MBAF.

These were some of the takeaways from the nine CFOs with major South Florida companies who took part in the discussion on cybersecurity concerns for contemporary business. It is part of the *Business Journal*'s ongoing Roundtable Series, where leading CFOs, CEOs and HR executives discuss a salient topic of interest to our readers.

When establishing a cyber strategy, it's all about people and procedures

While specific cybersecurity strategies may vary from industry to industry and company to company, what doesn't necessarily change is the culture. A strong people-and-practices strategy for protecting data can be mirrored across many different sectors and businesses.

An array of cybersecurity products is available, and choosing the right one can be very difficult. But more important than what products are purchased and how data is structured in an organization are the people and procedures that interface with sensitive data on a day-to-day basis. As CFOs, ensuring that employees and other executives are onboard with cybersecurity processes is key to successful defense.

> *"At the end of the day, there is a human interacting with [the system], and it should be the right person with the right mindset."*
>
> **JUSTIN IRIZARRY,** co-founder and CFO, OrthoNOW

"It doesn't matter the systems you have, the weakest point is always going to be your users," said Justin Irizarry, co-founder and CFO of Doral-based orthopedic urgent care center network OrthoNOW. "At the end of the day, there is a human interacting with [the system], and it should be the right person with the right mindset."

A significant percentage of cybersecurity breaches happen because of human error. About 95 percent of all security incidents involve human error, according to a report from IBM. Many successful security breaches occur because an external attacker identifies and lures insiders

CONTINUED ON PAGE 24

CFO ROUNDTABLE

MEET THE PANEL

STEWART L. APPELROUTH
Co-founder, Appelrouth Farah & Co.
999 Ponce de Leon Blvd., Suite 625, Coral Gables 33134
305-444-0999, ext. 228
stewart@appelrouth.com

SANDRA BRIDGEMAN
CFO, Miami-Dade Aviation Department
2100 N.W. 42nd Ave., Miami 33126
305-876-7731
sbridgeman@miami-airport.com

EVELYN D'AN
CFO, Enterprise Risk Management
800 S. Douglas Road, North Tower, No. 940, Coral Gables 33134
305-447-6750
evedan@emrisk.com

EDICSA FELIZ
CFO, Zarco Einhorn Salkowski & Brito
100 S.E. Second St., 27th floor, Miami 33131
305-374-5418
efeliz@zarcolaw.com

CHRISTINE S. GUZMAN
CFO, Inktel Holdings
8200 N.W. 33rd St., Suite 100, Doral 33122
305-523-1145
christine.guzman@inktel.com

JUSTIN IRIZARRY
Co-founder and CFO, OrthoNOW
3650 N.W. 82nd Ave., Suite 201, Doral 33166
305-735-1415
justin@orthonowcare.com

BRIAN MARK
Principal, Avison Young
500 W. Cypress Creek Road, Suite 350, Fort Lauderdale 33309
954-375-2068
brian.mark@avisonyoung.com

STAN RUBIN
Executive VP, CFO and chief risk officer, Ocean Bank
780 N.W. 42nd Ave., Suite 600, Miami 33126
305-569-5122
srubin@oceanbank.com

DAVID L. TUYO II
Senior executive VP, COO and CFO, Power Financial Credit Union
2020 N.W. 150th Ave., Pembroke Pines 33028
954-538-6228
dtuyo@powerfl.org

CFO ROUNDTABLE

CONTINUED FROM PAGE 22

within an organization or business to unintentionally provide the attacker with sensitive information or access.

"That comes down to culture, that comes down to behavior training and education," Irizarry said.

At Doral-based Inktel, an outsourcer of business and direct marketing services, the behavior of employees is monitored to ensure that people are not developing habits or doing things that could open up risks for the company.

"For example, we have our frontline people. We have call center operations," CFO Christine Guzman said. "What are they doing? Where are they creating the vulnerability for us? We monitor that, and we also have a security officer in place. And we have an ethical hacker to be 10 steps ahead, even though the hackers may be 20 steps ahead."

Banks and other financial institutions keep and make business decisions off of loads of sensitive personal data and, because of that, they have long had to keep up with changing compliance and regulatory requirements.

"In the financial industry, we've had to comply with financial regulation since '99," said David Tuyo II, senior executive VP, COO and CFO of Power Financial Credit Union. "We've continued to add layer after layer to cybersecurity defense"

At Miami-based Ocean Bank, an ethical hacker is used to probe the system, but it always comes back to the people.

"You engage [ethical hackers] and, if it's done right, you will not know when, where, why, how they penetrate your systems," bank CFO Stan Rubin said. "Breaches can be even mundane things like leaving a thumb drive in a bathroom. Does somebody plug it in? Things like that."

Evelyn D'An of Enterprise Risk Management

> *"It's a top-down approach …. Employees fail consistently, and they will continue to fail. It is a culture change that has to take place at all levels."*
>
> **EVELYN D'AN**, CFO, Enterprise Risk Management

Depending on the industry, companies can have different vulnerabilities when it comes to cybersecurity. Regardless of what those risks are, employee willingness to follow protocol will either help to safeguard a system – or open it up to problems.

"The challenge for us is that we do a lot of commercial property management, and we have 175 different bank accounts and, let's say, 25 people in our accounting department. It's about simple things such as training employees not to share usernames and passwords," said Brian Mark, principal in the Fort Lauderdale office of brokerage and property management company Avison Young. "It sounds very basic, but it drives me crazy when someone is logging on as another person because they didn't have their own login."

Employees of many companies will be familiar with the practice of changing passwords every 30, 60 or 90 days. It can often be frustrating when a system rejects a password change because there isn't the right combination of characters, numbers or capital letters, etc. But the practice is becoming more and more commonplace as businesses look to protect company data.

"We have a mandate where we're changing passwords every 30 to 60 days," Mark said.

The good news is that cybersecurity and employee training strategy isn't the sole responsibility of a CFO; it's dependent upon a team.

"It's important to have the right team in IT that understands your needs and that understands what your risks are and where your weaknesses are," said Edicsa Feliz, CFO of Miami-based law firm Zarco Einhorn Salkowski & Brito. "Training of your employees is extremely important."

Companies and CFOs that are new to cybersecurity or looking to revamp their cyber strategy may be confounded when faced with different options for cybersecurity architecture. But a system won't work – no matter the version, brand or price point – unless executives are on board.

It comes down to culture, and the people and practices in place.

"It's a top-down approach …. Employees fail consistently, and they will continue to fail," said Evelyn D'An, CFO of Coral Gables-based cybersecurity firm Enterprise Risk Management. "It is a culture change that has to take place at all levels."

Justin Irizarry of OrthoNOW

Christine S. Guzman of Inktel Holdings

Brian Mark of Avison Young