

# PEO INSIDE

PUBLISHED BY THE NATIONAL ASSOCIATION OF  
PROFESSIONAL EMPLOYER ORGANIZATIONS\*

THIS MONTH'S FOCUS

## CYBERSECURITY

PREPARE

TRAIN

REACT

COVER STORY

# FROM HR MANAGER TO PEO OWNER

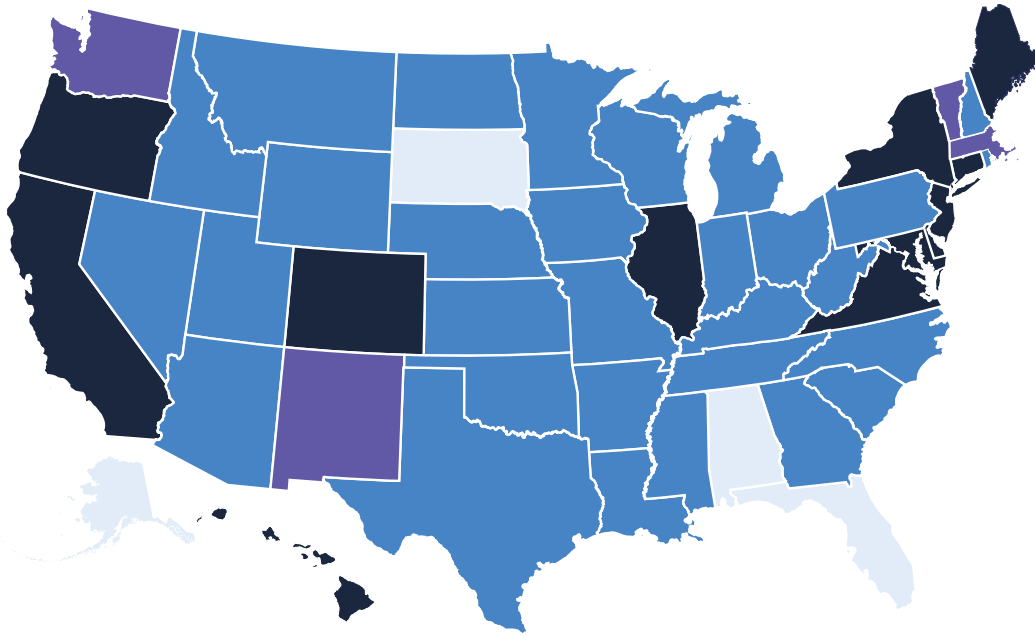
Celeste Johnson, CEO, The Applied Companies

THE SOURCE FOR PEO EDUCATION\* 707 NORTH SAINT ASAPH STREET, ALEXANDRIA, VA 22314 [WWW.NAPEO.ORG](http://WWW.NAPEO.ORG)

VOL. 27 ISSUE 2

MAR 2023

# State Mandated Retirement Plans for Small Businesses



Source: Georgetown University for Retirement Initiatives

**Is your PEO ready?**



RECORDKEEPER • TPA • INVESTMENT ADVISOR

[www.slavic401k.com](http://www.slavic401k.com)



► **Celeste Johnson, CEO, The Applied Companies**

**32**

**COVER STORY:**

From HR Manager to PEO Owner:  
Celeste Johnson and The  
Applied Companies

# Conte

**THIS MONTH'S FOCUS: CYBERSECURITY**

**12**

**PREPARE**

Why Cybersecurity Should Not Be the Sole Responsibility of the IT Department

*Jenna Marceau*

Employees are vulnerable at almost every entry point. Cybersecurity is an essential aspect of business operations, which is why it cannot be viewed as the sole responsibility of the IT department.

5 Questions to Ask a Cloud Service Provider About Cybersecurity

*Dwayne Smith*

Cloud security requires you to think about security differently than on-premise security or data center security. While many of the same concepts apply, you may require different tooling and approaches to enable the correct level of security.

**20**

**TRAIN**

Protecting the PEO: The Employee's Impact on Client and Organizational Security

*Geoff Webb*

Every business, of every size and in every industry faces a common threat - the security of critical data. Security readiness in the face of persistent and determined threats is multi-faceted.

Is Your Company Already in the Crosshairs?

*Russel James*

None of us would think about leaving our property unguarded. Why would you take the chance with your digital property? Here are some techniques to enhance your cyber security protocols.

**24**

**REACT**

Disaster Recovery for PEOs

*Hamesh Chawla*

Disasters are inevitable, and their timing is unpredictable. Preparing your company and employees before disaster strikes can make the difference between a catastrophe or an inconvenience.

Turning Risk Into Reward: The Cyber Opportunity

*Paul Hughes*

The exposure to being an employer is dynamic and untenable for a small employer. In recent years, many PEOs have commenced new insurance offerings, the hottest of all is cyber.



# ments

## TRACKS

- |  |   |
|--|---|
| <b>07</b> Letter from the NAPEO Chair      | <b>43</b> HR, Employment, & Benefits      |
| <b>08</b> Quick Hits                       | <b>49</b> PEO Growth                      |
| <b>32</b> PEO Voices                       | <b>54</b> Letter from the NAPEO President |
| <b>40</b> Legal, Legislative, & Regulatory |   |

## NAPEO THANKS ITS 2023 MEDALLION PARTNERS

### INDUSTRY CHAMPION



**isolved**Network



**SLAVIC401K**

### BLACK DIAMOND

Ameritas  
Aon  
PEO Velocity by Compass/PRM  
PRO Software, LLC  
SUNZ Insurance Company

### DIAMOND

Fisher Phillips  
Guardian Life Insurance  
Company

Poster Guard® Compliance  
Protection

Gallagher - Formerly Stonehenge  
Insurance Solutions  
McHenry Consulting  
ThinkWare Corporation  
Transamerica

### PLATINUM

AmWINS Specialty Casualty  
Solutions, LLC  
BrokerQuoter  
Key Risk (A Berkley Company)  
Libertate Insurance LLC  
MetLife  
Normandy Insurance Company  
PayPlus Software, Inc.

### GOLD

BLR  
Juice Financial  
Mercer Health & Benefits, LLC  
Payroll Funding Company LLC  
UKG Ready

### SILVER

Aetna  
Barrow Group, LLC  
U.S. Risk, LLC  
UnitedHealthcare

### BRONZE

Espyr  
Tabulera, Inc.

# PEO INSIDER®

## OFFICERS

**CHAIR**  
Kristen Appelman  
**VICE CHAIR**  
Steve Politis

**SECRETARY-TREASURER**  
David Feinberg  
**IMMEDIATE PAST CHAIR**  
Bruce Cornutt

## DIRECTORS

Joe Beers  
Erica Brune  
Alex Campos  
Tara Conger  
Ted Crawford  
Haley Crum  
Monica Denler  
Abram Finkelstein  
Celeste Johnson  
Hank Johnson

Wendy Katz  
Britt Landrum, III  
Andrea McHenry  
John Polson  
Carlos Saladrigas, Jr.  
Thad Steele  
Terry Sukalski  
Vic Tanon  
Geoffrey Vandal  
Samantha Wellington

## STAFF

**PUBLISHER**  
NAPEO

**CEO/PRESIDENT**  
Patrick J. Cleary

**EDITOR**  
Chris Chaney

**LEGAL EDITOR**  
Nicholas P. Kapiotis, Esq.

**DIRECTOR OF  
MEMBERSHIP  
DEVELOPMENT**

Nancy Benoudiz  
703/739-8169  
nbenoudiz@napeo.org

**DESIGN**  
Yes&

*PEO Insider*® (USPS 024-492)(ISSN 1520-894X) is published monthly except June/July and December/January, which are combined, by the National Association of Professional Employer Organizations, 707 North Saint Asaph Street, Alexandria, VA 22314-1911. \$150 of each member's dues goes towards his/her annual subscription to *PEO Insider*®. The annual subscription rate for non-members is \$150. Periodicals Postage paid at Alexandria, Virginia, and additional mailing offices. POSTMASTER: Send address changes to *PEO Insider*®, 707 North Saint Asaph Street, Alexandria, VA 22314-1911.

Opinions expressed in this publication are those of the individuals who have contributed articles and are not necessarily those of NAPEO, its officers, directors, or employees. No part of this publication may be reproduced or distributed without the written permission of NAPEO.

Subscribe Online

Renew or subscribe to *PEO Insider*® online! Save time and postage. Join NAPEO or renew your membership at [www.napeo.org](http://www.napeo.org).

© 2023 NAPEO. All Rights Reserved.





# Staying Ahead of Cybersecurity Threats

Securing your data is our top priority. That's why we're on the leading edge of cybersecurity through our fully integrated systems which are faster and safer than ever. You can rest easy knowing your data is protected.

For information on increasing your company's cybersecurity, read the [article on page 16](#) written by Dwayne Smith, PrismHR's chief information security officer.

Learn more about our commitment to security.  
Visit [prismhr.com](https://prismhr.com) today.



# SPRINGING INTO ACTION

BY KRISTEN J. APPLEMAN

**H**ave you ever blinked your eyes and a whole month has flown by? For me, that was February. I knew it would be action packed—but wow! I blinked, and it was gone.

NAPEO staff were seen across the country. Welcome Jason Gabhart, our new senior director of state government affairs, to the NAPEO team! In California, a strategy meeting was held to map out a game plan for needed legislation benefiting our industry in California. There was a flurry of efforts in New Mexico for the hearing of our benefits bill. Shout out to Emily Marsh for the extra efforts and her “can do” determination. In New York, NAPEO’s Advocacy Day had almost 20 members in Albany, educating state Assembly and Senate members about our industry. New York is an important state for our industry! Kudos to Leadership Council Co-Chairs Andy Lubash and Steve Politis, along with Kristin Baldwin, for their efforts to make this day happen!

On my favorite topic of ERTC, NAPEO continued to advocate for our industry in February. I am thankful for the incredible support and all the efforts being taken. Be it submitting a question for the Senate Finance



#EmbraceEquity

Committee’s nomination hearing for Daniel Werfel, to a letter sent by NAPEO to members of Congress, this is an industry-wide effort. It does not stop there. In addition to Hill meetings that occurred at the end of January in conjunction with the FGAC meeting, I will be back at the end of this month continuing to share our message.

But wait, there’s more...more ahead that is! In the land of PEO, we don’t sit still. Ever.

In March, we have the CEO Forum in Palo Alto supporting continued executive learning with Stanford professors, followed by the Q1 board of

directors meeting and retreat. I have recognized the velocity of state activity and, as such, will be focused on our Leadership Chair Councils and how we best leverage the councils to build momentum for favorable PEO practices across the country.

There are many NAPEO webinars bringing you important information this month, too. Visit [napeo.org/events](http://napeo.org/events).

Please join me in celebrating Women’s History Month. This month honors the trailblazing women who led and who lead the way for change. This year’s theme is #EmbraceEquity. Gender equity is about an inclusive world. We can drive change and challenge gender stereotypes, draw attention to bias and build inclusive practices. It is not just a call to action for women, you all are an ally. You can help fight the good fight.

Inclusivity enables all of us to learn about each other and our cultures. In March, St. Patrick’s Day is full of festivities celebrating Irish culture and heritage. In my community, I have enjoyed learning about and celebrating Holi Festival with neighbors. For those that have not experienced, it has many names such as Festival of Colors or Festival of Spring. As one of the biggest celebrations in India, this holiday signifies overcoming evil through goodness and continuing to live life through generosity, goodness and sincerity. With that in mind, I will leave you with an old Irish blessing, fitting for this month...

“May your troubles be less and your blessings be more, and nothing but happiness come through your door.”  
Cheers! ■



**KRISTEN J. APPLEMAN**

2022-2023 NAPEO Chair  
SVP, Health, Wealth, Tax,  
Compliance & Business  
Development ADP TotalSource  
Alpharetta, GA

# IN MEMORIAM:

## REX ELEY



Rex Eley passed away on Sunday, February 12, 2023. An industry pioneer, Eley co-founded and operated a regional PEO for 11 years, served as president of NAPEO in 1993-94 and has served in numerous other chapter and national leadership roles in the PEO industry over the past two decades, including chairing the national government affairs, standards, and education committees. He is also a recipient of the 2000 Michaeline A. Doyle Award, the PEO industry's highest honor.

He was also the long-time CEO of the Employer Services Assurance Corporation (ESAC) and served as CEO of the Certification Institute.

"Rex's vision of an organization dedicated to excellence in the PEO industry will forever be the benchmark of his incredible legacy. Without him,

ESAC would only be a dream," says Bill Maness, CEO of Syndeo and Chair of ESAC.

"Legend, pioneer, advocate, mentor, friend... these are just a few of the adjectives we've heard this week about our friend Rex Eley," says Kerry Brooks, CEO of ESAC.

"He and other industry leaders were ahead of their time when they realized the fledgling PEO industry of the 1990s needed a credible third party to assure PEO clients, vendors and regulatory agencies that their PEO partners were reliable. For over two decades, Rex's vision and leadership helped ESAC grow and provide this assurance to over 103,000 businesses and over 2.8M employees, with accredited PEOs paying more than \$200B of wages in 2022. Our industry is stronger today thanks to his leadership and vision," Brooks adds.

"Rex Eley introduced me to the PEO industry, then called the staff or employee leasing industry. Something he said must have resonated, because here I am 30 years later," says Kathleen Hillegas of Inspirity.

"Rex was a pioneer of the industry and a true believer. Those of us who had the pleasure to work for and with Rex can attest that there was no stopping Rex once he believed. Rex was analytical to a fault – an attribute - in what is a highly complex and complicated industry. Were some of his ideas "out there" – yes. Did they all "pan out" – no, but one very big idea did – PEO. The moniker, professional employer organization, was Rex's brainchild – and it was a very good idea indeed. Thanks Rex," Hillegas continues.

"It is impossible to overstate Rex's influence on this industry," says NAPEO President & CEO Pat Cleary. "Throughout his PEO career, he was an advocate for the industry. That was Rex."

He leaves behind a legacy of service to the industry that we are grateful for. Rest in peace, Rex.



DON'T MISS OUT

# NAPEO'S 2023 RISK MANAGEMENT WORKSHOP

NAPEO's 2023 Risk Management Workshop is headed to Charlotte, North Carolina! Mark your calendars for April 18-19 for the workshop to be held at the Omni Charlotte. The Queen City boasts a bustling culinary scene, a variety of arts and entertainment, and eclectic neighborhoods all within its walkable Uptown.

This event has evolved into the largest gathering of PEO risk management professionals, carriers, brokers, and agents, and it offers a mix of in-depth, PEO education and fun networking opportunities. You'll have the chance to learn from leading experts on risk management topics impacting your PEO.

2023 topics include the role of the PEO risk manager, ideal risk management dashboards, the EOR model, EPLI exposure, and more!

The workshop is geared for PEO industry veterans and newcomers alike. Whether you need a refresher on a topic or need to learn about it for the first time, Risk Management Workshop offers valuable programming and content.

You can register at [napeo.org/rmw](https://napeo.org/rmw).



NAPEO PAC

## NAPEO PAC HOLDS FIRST FUNDRAISER OF 2023

NAPEO's federal political action committee held its first fundraiser of 2023 for Rep. Beth Van Duyne (R-TX), a new member of the House Ways and Means Committee. Members discussed the PEO industry and its importance to her small business constituents. To learn more about NAPEO PAC and how you can get involved, visit [napeo.org/pac](https://napeo.org/pac) to sign the PAC form to learn more.

## Top Benefits PEOs Want in Retirement Plans



- Easy to administer
- Plan compliance
- Minimize fiduciary responsibility



- Cost competitive
- Actionable technology
- Established data integrations with dozens of payroll providers



Ameritas, a main street market leader in retirement plans, acquired BlueStar Retirement Services, LLC and now provides PEOs access to a full range of custom-tailored retirement plans, outsourcing services, and fiduciary management programs that seamlessly integrate with benefit administration and HRIS systems.



Scan the QR code to see the differences and similarities between PEPs vs. MEPs.

### Ready to help your clients grow?

Contact Ameritas retirement plans at 800-923-2732 or [PEO@ameritas.com](mailto:PEO@ameritas.com).



Fulfilling life® is a registered service mark of affiliate Ameritas Holding Company. © 2023 Ameritas Mutual Holding Company

AD 706 2-23

## QUICK HITS

### CONGRATULATIONS

## BBSI EARNS 2023 GREAT PLACE TO WORK CERTIFICATION

NAPEO member BBSI has again been Certified by Great Place to Work. The award is based solely on what current employees say about their experience working at BBSI. “We are thrilled to become Great Place to Work-Certified™ as we consider our people to be our greatest resource. We constantly strive to be an employer of choice and owe this achievement to our team of dedicated BBSI employees. We celebrate all their hard work supporting business owners and creating the amazing culture that helped us achieve this incredible recognition,” said BBSI President and CEO Gary Kramer in a release on the recognition.

### KUDOS

## INSPERITY HONORED AS ONE OF THE BEST PLACES TO WORK IN 2023 BY GLASSDOOR

NAPEO member Insperty recently announced that it has been honored with a Glassdoor Employees' Choice Award, recognizing the best places to work in 2023 with the ranking of number 28. The Glassdoor Employees' Choice Award is based solely on the input of employees, who voluntarily provide anonymous feedback by completing a company review about their job, work environment, and employer. “This honor is a testament to our long-standing commitment to supporting the needs and desires of our workforce so they can achieve individual and corporate success. The Glassdoor Employees' Choice Award further shows the same work we do for our clients to help them create an amazing employee experience while providing a positive and strong company culture,” said Insperty President and Chief Operating Officer Steve Arizpe in a release announcing the award.

### WELL-DESERVED

# PAYCHEX NAMED AMONG FORTUNE MAGAZINE'S MOST ADMIRABLE COMPANIES FOR 2023

NAPEO member Paychex has been named by Fortune magazine as one of the publications' most admired companies in 2023. The annual list recognizes companies globally for their outstanding financial performance, products, investment value, innovations, social responsibility programs, leadership, and more. “This recognition is a testament to the dedication of our 16,000 employees with a purpose of helping businesses succeed, and the strength of our company's values and culture. Our inclusion on this list demonstrates that our commitment to having a positive impact on our customers, our employees, and the communities we serve is being recognized by other business leaders around the world,” said John Gibson, president and CEO of Paychex, in a release announcing the award.

### NICE WORK

## EXTENSIS HR CELEBRATED FOR EXCELLENT WORKPLACE CULTURE WITH 3 COMPARABLY AWARDS

NAPEO member ExtensisHR recently announced that it has received three awards from workplace culture site Comparably. Selected out of thousands of companies across the U.S., ExtensisHR placed in the “Best Company Culture,” “Best Company for Women,” and “Best Company for Diversity” categories. “It is an incredible honor to receive such positive feedback from our team. We continue to implement new changes and provide meaningful benefits to support our diverse roster of employees. Whether it's promoting mental and physical health, prioritizing personal and professional development, ensuring pay parity, providing paid parental leave, and offering flexible work options, we're so grateful that our employees appreciate our ongoing commitment to creating an inclusive and desirable workplace for all,” said David Pearson, senior vice president of people and culture at ExtensisHR. ■



The Power to be **Different.**

SUNZ  
INSURANCE



941.306.3077 | [SUNZinsurance.com](http://SUNZinsurance.com)



# WHY CYBERSECURITY SHOULD NOT BE THE SOLE RESPONSIBILITY OF THE IT DEPARTMENT

BY JENNA MARCEAU

**I**t is often said that employees are the greatest asset to a company, but when it comes to cybersecurity, they are often the greatest weakness. So why would we assume that all things related to cybersecurity belong to the IT department? Think about your employees. The one who innocently clicks on a phishing attempt, or the one who fails to set up two-factor authentication. They could even be on their second day of employment and receive an email allegedly from the organization's president that tells them to go pickup gift cards on their behalf. Employees are vulnerable at almost every entry point, and while it may seem like a company's IT department can

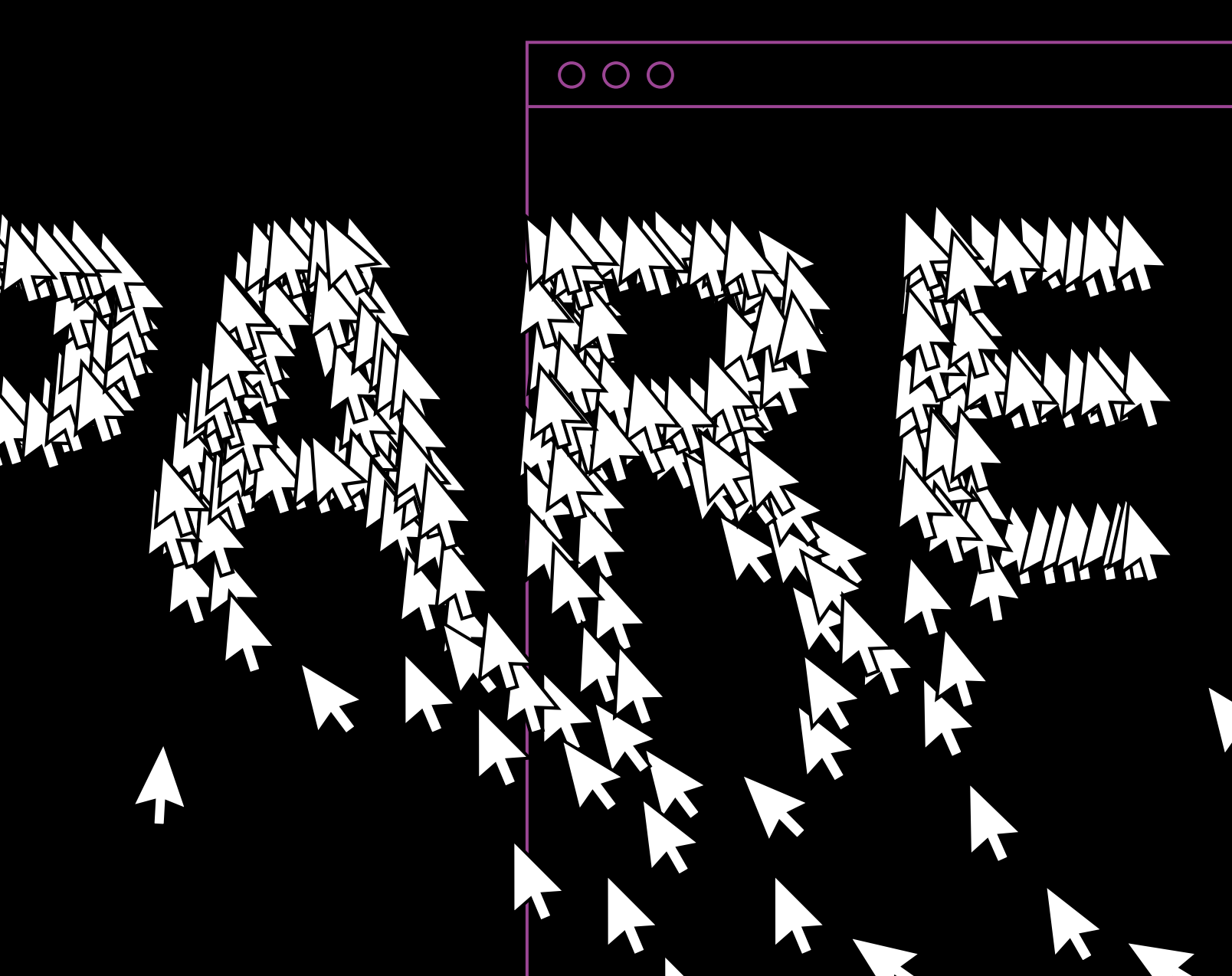
prevent an incident, IT professionals cannot cover everything.

Cybersecurity is an essential aspect of business operations, which is why it cannot be viewed as the sole responsibility of the IT department. Cybersecurity threats evolve daily and organizations can best prepare and protect themselves by taking a shared responsibility to protect the company's assets and data. When you think about it, cyber threats are not limited to technical issues. Cyber criminals use a wide range of tactics to gain access to sensitive information, including social engineering, phishing and malware. These tactics are often directed at non-technical employees, making it even more important that all

employees are aware of the risks and are trained to recognize and respond to potential threats.

When adopting a shared approach to cybersecurity, where all departments and employees split the responsibility for protecting the company's assets and data, an organization should include the following elements:

- A cybersecurity policy that outlines the organization's approach to protect sensitive information and the roles and responsibilities of all employees.
- Regular training and awareness programs for all employees to help them understand the risks and recognize potential threats.

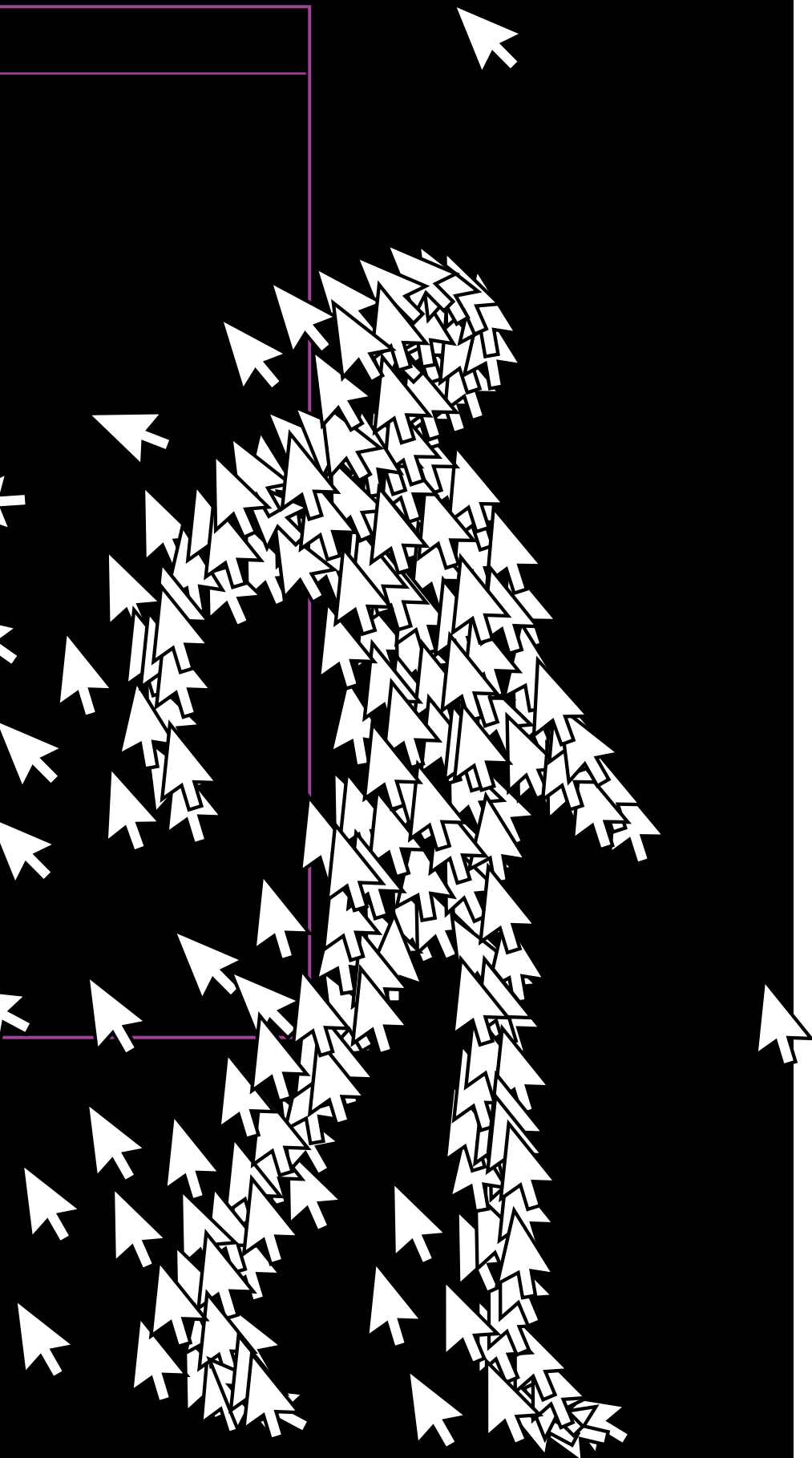


- Regular testing and monitoring of the organization's security systems and processes to identify vulnerabilities and respond to potential threats.
- Strong incident response and disaster recovery plans to minimize the impact of a security incident or outage.
- Regular communication and collaboration between IT and other departments, to ensure that all employees understand the risks and are aware of the organization's cybersecurity policies and procedures.

Allow cybersecurity to permeate through every aspect of your organization. Begin the process with onboarding new employees. Explain to them the



A cybersecurity champion acts as an advocate for their team, promoting a strong cybersecurity environment and helps others understand and strive toward maintaining it.



importance, give them examples and allow them to ask questions. Tell them to trust their gut, challenge information that appears skeptical and give them the tools and knowledge to minimize risks. We encourage our teams to prepare for the worst by planning for what could happen. Talk through situations, how they would be handled and what actions should take place. Involve everyone and allow them to feel comfortable with how they would respond. Shift the mindset from fear to awareness.

Measure, monitor and have a champion in every department. Often, employees are nervous about questioning things that are not normal. Having someone they trust to check-in with, show or explain what they have come across, can be beneficial. A cybersecurity champion acts as an advocate for their team, promoting a strong cybersecurity environment and helps others understand and strive toward maintaining it. These champions become the central team that you communicate with to help advocate and share best practices and updates to their department.

Including multiple people in backup processes and incident response plans can also provide protection to the organization.

Overall, an organization's cybersecurity policy is only as effective as its least careful employee. Cybersecurity is a complex and ever evolving field that cannot be left solely in the hands of the IT department. If you create a shared responsibility, involving all employees and all departments in the approach, an organization can better protect sensitive information and minimize the impact of cyber threats on its operations. ■



**JENNA MARCEAU**

*Chief Information Officer  
Syndeo  
Wichita, KS*





# 5 QUESTIONS TO ASK A CLOUD SERVICE PROVIDER ABOUT CYBERSECURITY

BY DWAYNE SMITH

One of the questions I'm frequently asked by PEOs is simple: Is the cloud safe?

Actually, this is a trickier question than it seems. The answer is yes, of course, but like any internet-based endeavor, there are certainly many caveats. Cloud security requires you to think about security differently than on-premise security or data center security. While many of the same concepts apply, you may require different tooling and approaches to enable the correct level of security. PEOs also need to be more cloud savvy through the use of SaaS, IaaS and PaaS (more on this in a bit).

One point I can't stress enough is that everyone has a role to play to ensure your data and systems are safe from cyberattacks. Most breaches begin when someone lets their guard down and gets tricked into revealing information (passwords and such) through phishing, which could put the entire organization at risk. A quick click on a link from a phony email or engaging with a supposed "executive" through a social engineering attack (where someone impersonates someone from the company's C-suite or another high-ranking official affiliated with the organization) could open the floodgates at any time.

Cybersecurity is never an easy job, but with the proper protocols and tools in place, companies can help ensure their systems and information is protected as well as their customers'.

Also known as Software as a Service (SaaS), cloud computing has changed the way we work by giving everyone in the organization the ability to access the tools, software and information they

need to do their job whenever and wherever they want. Whether you're in an office, a factory, at home or even taking a respite on a beach in Tahiti, as long as there's a Wi-Fi signal or cellular connection available, information will always be at your fingertips.

Unless the cloud solution has been compromised by a cyberattack, that is.

In Hiscox' latest Cyber Readiness report<sup>1</sup>, the cyber insurance company found that companies with \$100,000 to \$500,000 in revenue now face as many cyberattacks as those making \$1 million to \$9 million. In other words, cyberattackers are not just looking to go after the bigger players anymore. Everyone is a potential target in today's cyberworld!

As with any internet-related technology, hackers and cybercriminals continually mine for weaknesses in the cloud, and attacks don't always happen instantaneously.

Did you know that the average data breach takes 277 days to detect and resolve? That's because once an attacker breaches someone's system, they might want to keep a low profile to get as much information as they can before they launch a full-blown attack, or they might want to spend time inside the network just practicing and experimenting to prepare for future attacks, or searching for information about bigger companies with which you do business. Additionally, after an attack is detected, it can take some time to push the cyberattackers out after they've gotten in. Having a backup system is critical, but even that can take several hours or more to deploy.

Thankfully, cloud security has gotten stronger and stronger as cloud service

providers have evolved and matured. As well, the pandemic and the influx of hybrid- and remote-working arrangements accelerated cybersecurity efforts, but that doesn't mean there aren't lots of bad actors out there still looking to exploit new vulnerabilities.

It's been that way since the very beginning.

## HISTORY OF THE CLOUD


Believe it or not, the idea of cloud computing was floated all the way back in 1963 when the Massachusetts Institute of Technology (MIT) was awarded a \$2 million grant from the Defense Advanced Research Projects Agency (DARPA) to develop a computer that could be used simultaneously by two users as part of its Project on Mathematics and and Computation (Project MAC) endeavor.

As DARPA itself explains<sup>2</sup> on its website, "A major thrust of Project MAC was to develop general purpose time-sharing capabilities, which later influenced the design of computer systems for commercial and defense uses. Within years of its start, Project MAC would evolve into the world's first online community, complete with online bulletin boards, email, virtual friendships, an open-source software exchange—and hackers."

And hackers indeed.

## ONE SIZE DOES NOT FIT ALL

To be clear, there are different types of cloud computing software out there: from private clouds (often set up by a third-party vendor) to public clouds (think Amazon Web Services, Azure and Google Cloud) to hybrid clouds (could be one private and one public, etc.) to multiclouds



Cyber attackers are constantly looking for new ways to penetrate an organization's cyber defenses, so it's important for any cloud company to practice constant vigilance.

(a way to keep cloud data separated). Besides SaaS, there's also Platform as a Service (PaaS), think external networks, servers, operating systems or storage as well as Infrastructure as a Service (IaaS) where companies rent or lease servers for computing and storage.

There is also third-party software you undoubtedly already use that is cloud-based, such as Microsoft Teams or Google Docs.

I bring all this up here just to put cloud cybersecurity into proper context for how complex it truly can be. In the early days, we struggled to get two computers to communicate with each other. Today it is almost impossible to keep them from communicating when we don't want them to.

### CHECK THE DEFENSES

A good cloud-based software provider will audit its own cybersecurity initiatives. At PrismHR, we use the American Institute of CPAs' (AICPA's) System and Organization Controls 2 (SOC 2) criteria, which is an industry standard framework for measuring an organization's cybersecurity initiatives.

Besides asking a cloud provider about whether it follows SOC 2, another way PEOs can check a provider's cybersecurity strength is through asking about

penetration testing. This is where an organization pays an ethical hacker to see if they can break into their systems. Keep in mind that this is not something every company does because it can be cost-prohibitive and may have an impact on the service to customers, but it is something you certainly can ask a cloud provider about to help gauge its commitment to cybersecurity.

There's also so-called "attack" tooling that will give you a vulnerability score, but keep in mind that bad actors have access to the same tools, so it works both ways. You can find out how vulnerable a cloud provider or even your organization is to a potential cyberattack, but so can they. You should also work with your cloud provider before using any "attack" tooling or conducting unannounced penetration testing. Not doing so could have unpredictable consequences.

Cyber attackers are constantly looking for new ways to penetrate an organization's cyber defenses, so it's important for any cloud company to practice constant vigilance. Cloud providers and PEOs can never afford to let their guard down when it comes to cybersecurity.

So what should you be asking cloud providers about cybersecurity? Good

question. Here are a few things that come to mind.

### QUESTIONS TO ASK CLOUD COMPANIES ABOUT CYBERSECURITY

1. Has the cloud provider gone through an independent assessment about what their security controls are for where the data is stored, and do they monitor for vulnerabilities?
  - If they have been independently assessed, you should be able to review a summary of the assessment, but you should also research the assessment company as well, especially if it's not a well-known one.
  - In terms of technical controls, you need to know where the data is housed (U.S./abroad). If you do business in California, for instance, you need to know that the cloud provider's protections comply with different geographic regulations, such as the California Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR) as two examples.
2. What is their public reputation?
  - Look for independent reviews from trusted sources from an

accrediting body website, industry peers and previous customer letters of past performance.

- Does the company have customer referrals available to offer insight into how they support and respond to different things from a security or IT perspective? Always try to talk to a customer to gauge their confidence in the cloud company and how responsive they are. If a breach or outage occurs, you'll want to know that you can get in touch with the cloud company based on your business needs.

3. Does the cloud provider allow single sign on (SSO), and do they support multifactor authentication (MFA)?
  - SSO is a great way to allow your employees and customers to access all of their cloud solutions through one convenient password at login. The potential problem, of course, is that a cyberattacker could be able to access more data should there be a successful breach. That's why a state-of-the-art MFA option is important. A good cloud provider will provide MFA to ensure there is at least one other action a user must take to gain access to the software/data, whether it's through an authenticator app, text message confirmation, email, phone call, etc.
4. Can we set up role-based access?
  - Not everyone in an organization needs access to all information. Being able to limit the number of people who have access to sensitive information is essential.
  - Placing users into roles also ensures that changes to the system are controlled and can be audited.
5. Most importantly, what is the disaster recovery process?

- Any backup system will take time to launch, so you need to know what the company would be able to do within 24 hours (you might have to pay more for quicker turnaround times, but find out from the outset).

Cloud software is a critical tool in today's business world, asking the right questions can help ensure your PEO's data and systems remain safe now and in the future. ■

- 1 Hiscox. (2022, n.d.). Cyber Readiness Report. Hiscox.
- 2 DARPA. (2023). Project MAC. DARPA. [www.darpa.mil/about-us/timeline/project-mac](http://www.darpa.mil/about-us/timeline/project-mac)



**DWAYNE SMITH**

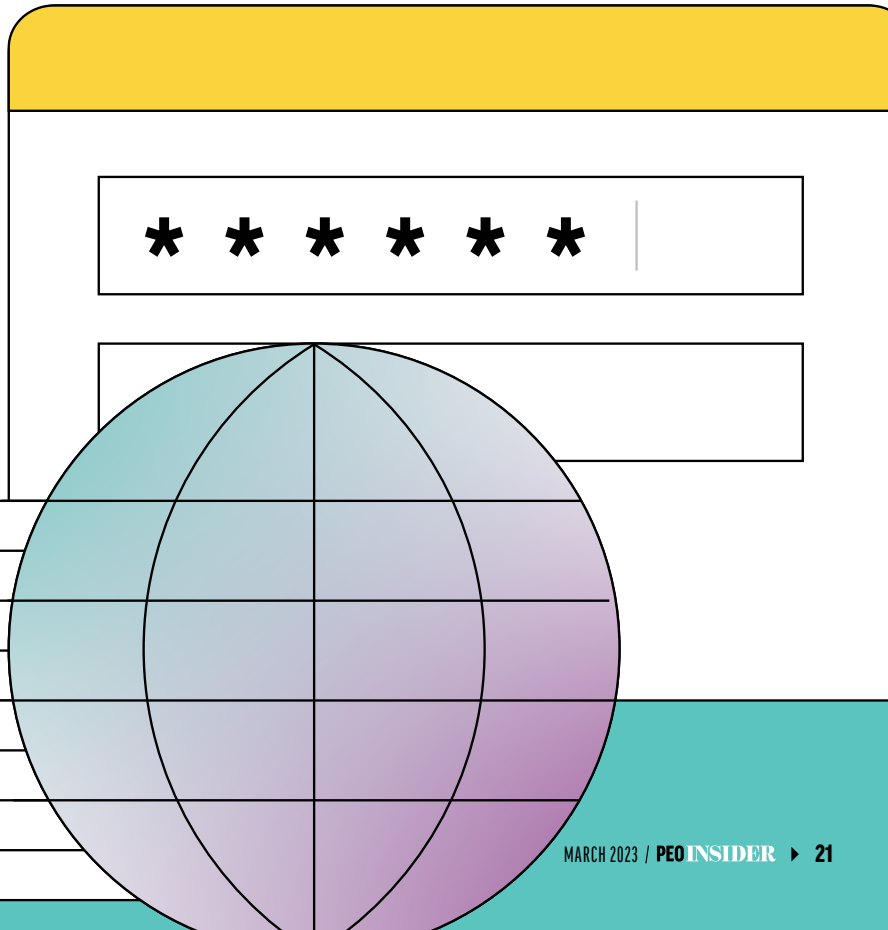
*Chief Information Security Officer  
PrismHR  
Hopkinton, MA*



# TRAIN

PROTECTING THE PEO: THE  
EMPLOYEE'S IMPACT ON CLIENT  
AND ORGANIZATIONAL SECURITY

BY GEOFF WEBB



**E**very business faces different challenges whether from competitors, market changes, supply chain disruptions, or myriad external or internal forces. Yet every business, regardless of size or industry, faces a common threat: the security of critical data. Whether it's the leak of proprietary business information or customer data, or a breach, or a malicious software attack, it can be devastating. Security incidents result in disruption, fines and a loss in customer confidence that can take years to recover.

Security readiness in the face of persistent and determined threats is multi-faceted.

First, of course, there's investment in good security technology and controls. Whether those are on-premise technologies such as firewalls that guard a network perimeter or services such as managed security services, the core security technology must be present and operational to stop basic attacks and accidental breaches. Second, of course, is the infrastructure of a network itself. For example, the systems and servers that run in a building (e.g., employees' computers, employees' personal mobile devices).

Third, there is what is known as "third-party risk." This arises when services are provided by a third party, usually through the cloud. Attackers will often seek out service providers to attack and gain access or control over services used by their customers (for example the 2013 Target breach when 41 million credit cards were stolen after hackers breached Target's system through the HVAC provider). So, it's essential that any third-party system in use is at least as well secured as the organization's own security systems, otherwise a breach there will cascade and affect them just the same.

All of this is well known and understood, although admittedly always a work in progress. What is often underappreciated, though, is the importance of the other side of that security readiness coin – the human element.

While technical controls and security tools have continued to develop rapidly, humans haven't changed much in at least several thousand years. And that means the human element remains the attack vector of choice for many hackers.

This is why attacks like "phishing" or compromising email accounts remain the most common forms of successful attack. People, even experienced employees, can often be relatively easily fooled into opening a document, clicking a link, visiting a website or simply handing out

sensitive information, all of which can lead to a devastating security breach.

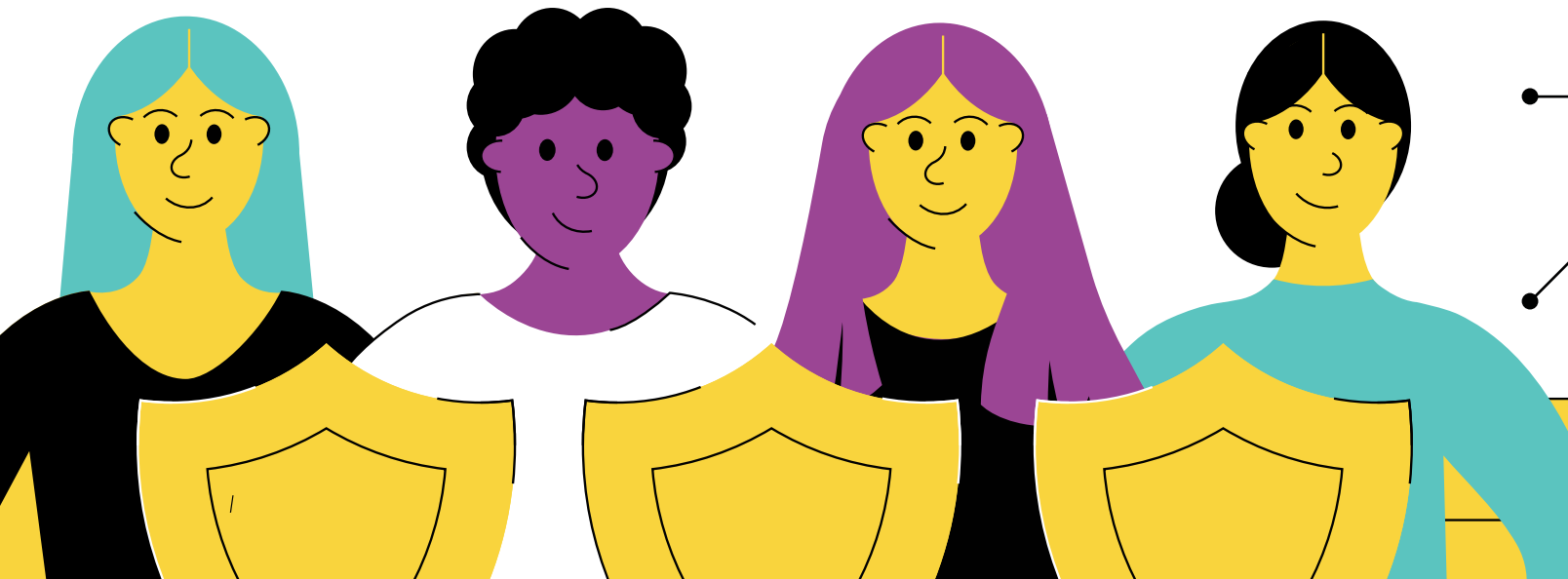
For PEOs this represents a special challenge given the amount of sensitive information they handle for customers (and their employees).

Interestingly, this is why HR teams and service providers are now very much on the front lines of defending against hackers. Simply put, the best defense against cyber attacks is a workforce that can spot an attack, or one that can at least recognize suspicious activity and respond in the right way. All of this requires a very prepared workforce.

Good hiring practices are, of course, essential to keeping data secure, and solid background checks are a critical first step in keeping potential security risks out.

But what happens after a company has hired the best employees? How do leaders make sure they are ready to face the inevitable moment when a hacker targets that business?

The answer is to invest in building what security experts refer to as the "human firewall." In other words, employees who are trained, educated and ready to stop attackers before they get a foothold. They can also spot a suspicious attack before it develops, and they know how to respond when they see a hacker trying to get in. This is where HR best practices must work hand-in-hand with IT and security teams.



But what happens after a company has hired the best employees? How do leaders make sure they are ready to face the inevitable moment when a hacker targets that business? The answer is to invest in building what security experts refer to as the “human firewall.”

There are three consistent steps that PEOs must take to keep their employees (and those of their customers) safe from attack.

Step 1 is to clearly establish support from senior stakeholders for a dedicated and focused security awareness training program. This first step is critical, because without support (and funding) from senior management, it will be impossible to establish and sustain the level of training necessary to make a difference. There's plenty of resources out there that can be used to clearly demonstrate the financial impact of a breach, including reputable reports like the annual Verizon Data Breach Report.

Step 2 is to work with IT or security teams to establish the training program. Most companies start with third-party content on security training (and there's a lot out there to choose from). Make it relevant, try to keep it enjoyable (there are some really good video training tools out there) and if possible, add a little incentive for employees to finish the

training. Regardless, if PEOs have Step 1 nailed down, the HR team can push hard to make security training mandatory, and often that's the only way companies will get everyone to follow through.

Once PEOs have a security program established as part of onboarding and regular updates, it's time to focus on Step 3—keep it. This is often the most challenging. The world of security, threats, responses and best practices is constantly changing, so staying up to date is vital for any meaningful security program. Even more importantly, regular testing and training is important to keep security muscles toned; it's easy to get busy and forget the basics or make a silly mistake. Even highly experienced security practitioners get caught from time to time, so leaders will want to make sure training and testing is repeated at least every six months.

Attackers are constantly testing businesses to spot weaknesses and vulnerabilities. They also know that busy

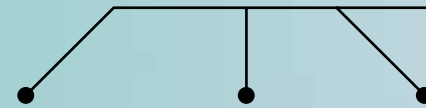
employees, trying to be helpful, can be easily fooled into leaving a virtual door open to attack. In fact, most successful business breaches occur for exactly that reason. PEOs must invest in training their employees to be ready when attacks call. It's not about trusting, or not trusting employees, it's about a serious commitment to keeping company and customer data safe. If the CIA can be breached (and they have been more than once), there's a good chance any employee can make a simple mistake that leads to millions in lost business, fines and bad publicity. Yet, studies also show that once attackers see a business has good security tools and training in place, they will often simply move on looking for easier targets.

Don't be an easy target. ■



**GEOFF WEBB**

*VP of Solution Strategy  
isolved  
Cypress, TX*



## IS YOUR COMPANY ALREADY IN THE CROSSHAIRS?

BY RUSSELL JAMES

We all have locks and alarms on our homes, businesses, and vehicles. None of us would think about leaving our property unguarded. Why would you take the chance with your digital property?

So, what can PEOs do internally to help secure the vulnerable areas of their business? As IT Manager at ESI, I have the task of guarding the gates of ESI through various techniques. Hopefully, by sharing some of these techniques, we will add some nuggets to your cybersecurity protocol.

### FIRST LINE OF DEFENSE FOR CYBERSECURITY

You need to focus on a proactive first line of defense before implementing the coverages of cyber policies and developing reactive workflows to address worst-case scenarios. The following are some minimal security profile suggestions your company can implement quickly to raise your threat awareness tremendously to help avoid cybersecurity compromises. In addition, usually, these suggestions are mandatory when applying for a cybersecurity insurance policy.

First and foremost, secure passwords for all employees throughout the company. To help assist with this protocol, we suggest a secure password management system.

With an enterprise level system, each employee has an account to save all of his or her login and sensitive information. A shared folder feature allows employees or entire departments to share standard folders/files. The employer will manage access based on the individual user or the groups we have assigned them. The employer can also see how well each employee performs with password strength on the security dashboard. There you have an overview of at-risk passwords for each user. You can also add email addresses to the dark web monitoring where companies can proactively be alerted if sites in our vaults (all registered user web access points) have been breached. Another benefit of most enterprise accounts is a free family account for each of your users. This allows each employee to have a five-user family account where they can secure their passwords and login info. Family accounts will enable them to share passwords between family members. For example, think of streaming accounts shared with the parents and kids and bank accounts shared with only the parents.

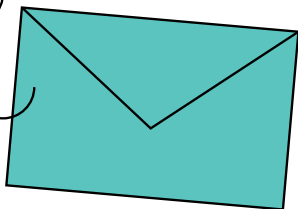
After securing the passwords, implement a two-factor or multi-factor authentication (MFA). In the new era of mobility and mostly work-from-anywhere, having a two-factor authentication needs to be a standard to protect your network and servers. Do you understand the work environment of every employee? Install your electronic front door bouncer on all remote login systems. Any system that your users access should have MFA

enabled, if possible. There are too many examples of previous cyber events that could have been prevented if MFA had been allowed. MFA can take many forms, from a simple text message or email code to an authenticator app or security key. Users should also be encouraged to add MFA to their accounts at home.

Another great tactic is an internal testing protocol for phishing scams. Some companies provide a service sending fake phishing and scam emails to your employees. The benefit is that you, as the employer, can monitor the emails and see who clicks and enters their passwords. The testing will help you identify and train these users without putting your company at risk. Most systems allow you to configure training for users who click on links. Hopefully, the extra training helps if a real phishing or scam email gets through your regular email defenses. Incoming emails need to be going through a screening process before your users see anything. On average, one out of every 101 emails is phishing or malicious, and about 85% of emails are spam.

Phishing emails come in two main categories, with and without malware.

- Emails without malware attempt to impersonate a trusted sender, your CEO, CFO, or IT department, to trick the user into giving away corporate information or assets.
- Many of these emails include links to imitation login pages allowing attackers to obtain the user's credentials. With these compromised credentials, they might be able to access your company resources, gain access to your internal systems, or start sending more phishing emails from your users.
- Emails that include malware download to the network when an





employee opens the email. Others contain a link that tries to convince you to download a program to your computer. Usually, this will seem like a helpful program, but it will contain malicious code along with the program. Some emails will download a small program on the user's computer that will then "phone home" to download more malicious software. Once the additional malware is in place, that action will allow the attacker to move sideways through your network without you knowing. This process is the most popular way ransomware attacks start.

After accumulating the testing data, review the findings at your next company round table or teams page. The more experience every employee has identifying scams, the lower your overall risk factor. Cyber thieves are training each day; make sure your teams are too.

Another central area of concern is your technology. Your computers and servers should be programmed to install security updates as soon as they are available automatically. The same goes for your software programs and network technology. When there is an option to allow automatic updates, we recommend allowing them if possible. There needs to be a severe business case not to enable security updates. The hackers are working overtime to get into your systems, and you do not have enough protection to allow doors to be left open for them to walk in.

The monitoring of your systems is imperative to be effective. It would be best if you had someone responsible for looking at the security profile and following up with your employees to help them make behavior changes. Having the systems in place is only part of the package. The hackers are working every day to get in, so you must work every day

to keep them out and keep your data safe. In addition to good security practices and training to keep your data secure, it can be worth employing the assistance of third-party software and tools for added protection.

While attacks may seemingly happen overnight, the majority take days, if not weeks or even months, to be discovered. In return, it highlights one of the biggest challenges small businesses face regarding cybersecurity: awareness and available resources to defend against the threat actors. The key is to know what you're up against. FireEye has an infographic, *Defending Against Malicious Email Attacks* | FireEye, that helps to put it all together in one place<sup>1</sup>. This graphic helps to give you a bird's eye view of the threats businesses face today.

## BOTTOM LINE

There is no singular approach to minimizing the human risks that lead to breaches. Employees must browse the web, open emails, and even answer the phone with a healthy amount of suspicion. An organization with a strong cybersecurity culture is an organization with a small social engineering attack surface. With 60% of small businesses closing within six months of a cyberattack, improving your security posture isn't just logical; it's vital to the survival of the organization<sup>2</sup>. ■

1 [www.fireeye.com/content/dam/fireeye-www/offers/pdfs/pdf/email/ig-it-only-takes-one-email.pdf](https://www.fireeye.com/content/dam/fireeye-www/offers/pdfs/pdf/email/ig-it-only-takes-one-email.pdf)

2 <https://www.sec.gov/news/statement/cybersecurity-challenges-small-midsize-businesses>

3 <https://www.forbes.com/advisor/business/common-cyber-security-threats>

4 <https://www.cisa.gov/uscert/resources/smb>



## SECURITY UPDATE

Another central area of concern is your technology. Your computers and servers should be programmed to install security updates as soon as they are available automatically.



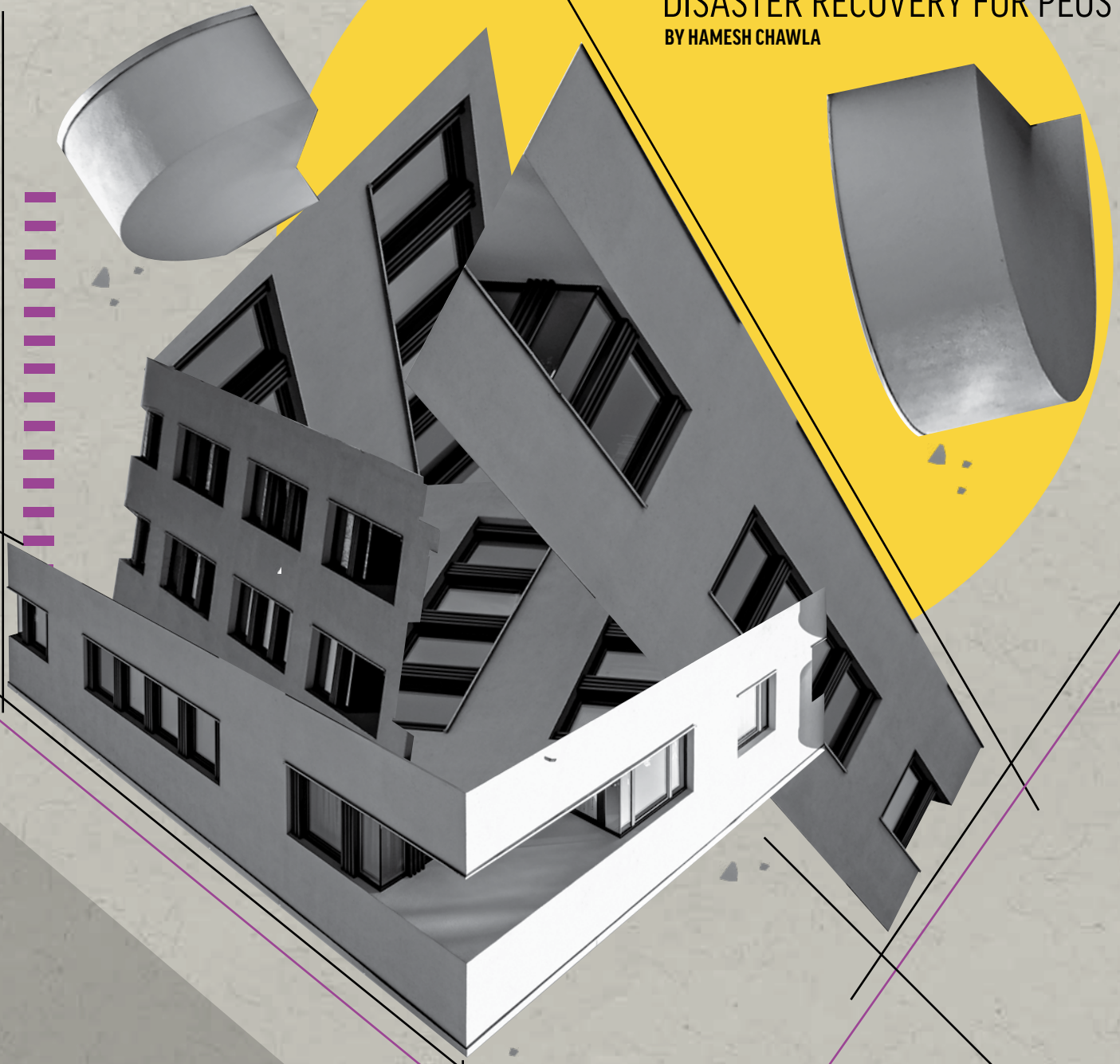
**RUSSELL JAMES**

*IT Manager  
ESI  
San Antonio, TX*

CYBERSECURITY

# REACT

DISASTER RECOVERY FOR PEOS  
BY HAMESH CHAWLA



**D**isasters are inevitable, and their timing is unpredictable. Preparing your company and employees before disaster strikes can make the difference between a catastrophe or an inconvenience. While no one wants to experience a business disruption, especially any technology-related disruption, there are many reasons that you could end up in that position. A 2018 BCI Survey Report said that the top disruptors are general IT outages, cyberattacks, and transport disruption, usually caused by natural or manufactured disasters. For PEOs, creating a Disaster Recovery Plan (“DRP”) protects your company and the livelihood of all the companies and worksite employees you serve by providing a roadmap for how to recover and return your business to normal once a disaster strikes. A documented and tested DRP will help minimize your downtime, the impact to your revenue, and the impact on your customers.

## COST OF DISRUPTION

If you need more reason to invest the time to create a DRP, look no further than the financial impact on your business. According to Gartner, IT downtime costs companies \$5,600 per minute on average across the United States.

## DISASTER RECOVERY METRICS

The two most important metrics for disaster recovery are Recovery Time Objective (“RTO”) and Recovery Point Objective (“RPO”), as these concepts help companies understand the business impact of disruptions and develop plans to address them.

### Determine your Recovery Time Objective (RTO)

This is how long a particular service can be offline without a significant business impact. For PEOs, the ability to process payroll cannot be down for more than a few minutes because payroll is a core service of their business. In contrast, accessing historical data reports could be down for a couple of hours without significant impact.

### Determine your Recovery Point Objective (RPO)

RPO refers to your target for the maximum amount of data that the business can tolerate losing measured in time (i.e., starting from when the failure occurs and going back to your last

working backup). We usually discuss security changes or data backup when addressing vulnerabilities during disasters. The best way to prevent data loss would be to back up critical information in tiered servers or in the cloud. The RPO determines how frequently this needs to be done for each asset or function. This metric tells you how outdated your data can afford to be when an unplanned incident occurs.

For example, you can lose marketing metrics that were generated over the last 24 hours without causing real damage to your core business services, but losing more than the last 5 minutes of banking transactions would result in a large impact. In this example, you would set a longer RPO for the system that stores your marketing metrics and a relatively short RPO for the system that stores your banking transactions.

## BUSINESS IMPACT ANALYSIS

To ensure that you protect the most financially impactful items in your environment, you should perform a Business Impact Analysis (“BIA”) for your critical business processes. The goals of the BIA are to identify the business impact when key processes are not functional and to identify the technology or planning necessary to restore functionality. If you have in-house IT personnel, they should help lead this project. If not, it is best to work

with your Managed Service Provider or a trusted consultant.

For most PEOs, the items that you should spend the most time analyzing are:

- **Internet connectivity** – With most of your platforms being cloud-based and not hosted on-premise, internet connectivity is one of the essential items.
- **Payroll platform** – If your payroll platform is hosted, you need to have a conversation with your software vendor to ensure that they have a written DRP with documented RTO and RPO for each critical system.
- **Financial platforms** – All financial platforms, including what you use to transmit ACH files to banks for money movement.

After you complete the BIAs for your critical processes, you should start working on Risk Assessments for those same processes to identify the conditions or situations that may lead to an outage.

## CREATE REDUNDANCY

Creating a world-class infrastructure is a good first step. However, an excellent second step is to create redundancy. Identify all possible reasons for failure; electrical, air conditioning, network, and computer systems, and ask yourself what would happen if a computer system were to go down unexpectedly. Would your business stop, or do you have a backup plan? Creating redundancy will reduce the time it takes for your business to come back up after a disaster. Common types of redundant sites are as below.

### Cold site

Cold sites are infrastructural backups — office spaces with power, cooling, and communication systems. They do not house any hardware or have a network configured. In the case of primary



## FOR PEOs, CREATING A DISASTER RECOVERY PLAN ("DRP") PROTECTS YOUR COMPANY AND THE LIVELIHOOD OF ALL THE COMPANIES AND WORKSITE EMPLOYEES YOU SERVE BY PROVIDING A ROADMAP FOR HOW TO RECOVER AND RETURN YOUR BUSINESS TO NORMAL ONCE A DISASTER STRIKES.

system failure, the operational teams will need to migrate servers and set everything up from scratch. It is the least expensive option. However, it requires extra labor after the fact and may not meet the organization's RTO requirements if there is a problem with executing the transfer.

### Hot site

A hot site is the exact copy of the primary data center setup. It has all the necessary hardware, software, and network configured. Data is backed up based on RPO goals. In case of outages, the operations connect to the hot site without delay and continue with minimal downtime. Since this requires a constantly functioning setup, this is the most expensive option. It is also the most effective.

### Warm site

A warm site houses the necessary hardware with some pre-installed software and network configuration. Only mission-critical assets are backed up at less frequent intervals. This is a good option for organizations with less critical data and higher RPOs. A cost-benefit analysis may be required to decide between hot and warm sites.

### Cloud and SaaS

Cloud disaster recovery is like traditional disaster recovery, but with some special considerations that will largely depend on your infrastructure. For

example, if you are already using a Cloud Service Provider (e.g., Amazon AWS, Google Cloud Platform, Microsoft Azure, Oracle Cloud, etc.) for critical business functions, then you will need to account for the complexities of migrating data and services from those providers in the event of an extended outage.

With SaaS, the provider is supplying both the application and the infrastructure beneath the application as part of the service you are buying. Since the provider is responsible for maintaining the availability of the software, your disaster recovery focus will be on the business function being performed by the SaaS solution and the required data. For example, suppose you use a SaaS solution to execute ACH payments. In that case, your DRP should document the process for manually obtaining the correct data for ACH payments, your bank's back-up payment process, and the steps you need to follow to switch over in an outage.

Another key consideration with SaaS providers is whether they have put in place the appropriate safeguards that will enable them to maintain the availability of the software you are buying. You should ask for applicable certifications which show a vendor's compliance with recognized information security and data protection industry standards, such as ISO 27001 and SOC 2 Type 2. Ideally, you should request certifications and have these conversations before you begin a relation-

ship with a vendor, but, if not, you should do it as part of this process

### TESTING AND UPDATES

Document your disaster recovery plan, simulate a real-world disaster, and test it several times a year to remove any kinks in your plan. If you take backups, restore them to understand how quickly your systems can be online. If you run your infrastructure in the cloud, work with your vendors to understand their Service Level Agreements ("SLAs") and document customer communication plans during downtime.

Things are stressful during a disaster. All team members must play their part during such times to prevent extended business downtime. Assign individuals roles and responsibilities so everybody knows their responsibilities when disaster strikes.

A well-documented, frequently tested, and up-to-date DRP will go a long way to minimize downtime and revenue impact.

For more information, please visit NAPEO's cyber resources at [napeo.org/cyber](http://napeo.org/cyber). ■

▼ This article is designed to give general and timely information about the subjects covered. It is not intended as legal advice or assistance with individual problems. Readers should consult competent counsel of their own choosing about how the matters relate to their own affairs.



**HAMESH CHAWLA**

CEO  
Mulberri  
Sunnyvale, CA

# Want software that can:

- Help your company make more money?
- Increase efficiency?
- Reduce errors?

If you answered "Yes" to any of these questions, call PRO today!

"With our previous software, our Payroll department was the busiest in the office. By switching to PRO, they now have a 50% increased capacity. I can't fathom why the leadership of a PEO would not want to be a PRO client."

— Stephen Cilley, owner of Ataraxis PEO, the largest PEO in Idaho.

Marketing@prosoftware.com  
prosoftware.com

**PRO**  
SOFTWARE

  
**PEO DEFENDER**

BLACK



DIAMOND



small employers in a PEO model versus traditional to buy EPLI or not is at least three-fold if not more within the PEO community. Deals are won and lost maybe not solely on this offering, but certainly the weighting of it has become heavier as the importance of coverage without an excessive retention is paramount.

Just in January of 2023, news-worthy hacks of companies such as T-Mobile, Mail Chimp, Pay Pal, Chick-fil-A, Twitter, and the FAA have been made public. Events like these have made employers aware that cyber espionage is all around us, and the need for protection in this area is real.

In a recent survey by the global insurer Allianz, liabilities from activities in the cyber realm topped the chart in terms of top threats in 2023 for employers. According to the Allianz Risk Barometer, cyber incidents (34%) and business interruption (34%) are the top concerns of businesses in 2023.<sup>2</sup>

Additionally, business interruption and political risks are indirectly associated with cyber exposure as well.

As a result, the move by employers to purchase cyber insurance has been swift. “During 2021, insurers writing stand-alone cyber coverage reported approximately \$3.2 billion in direct written premiums on the Cyber Supplement. The stand-alone cyber insurance direct written premiums for 2021 increased by 94.7% from the prior year, and the total number of stand-alone policies reported in 2021 increased by 31.8% from the number written in 2020,” reports NAIC.<sup>3</sup>

This vulnerability to our clients creates a specific need that a PEO’s internal and external insurance team can address. It

## TURNING RISK INTO REWARD: THE CYBER OPPORTUNITY

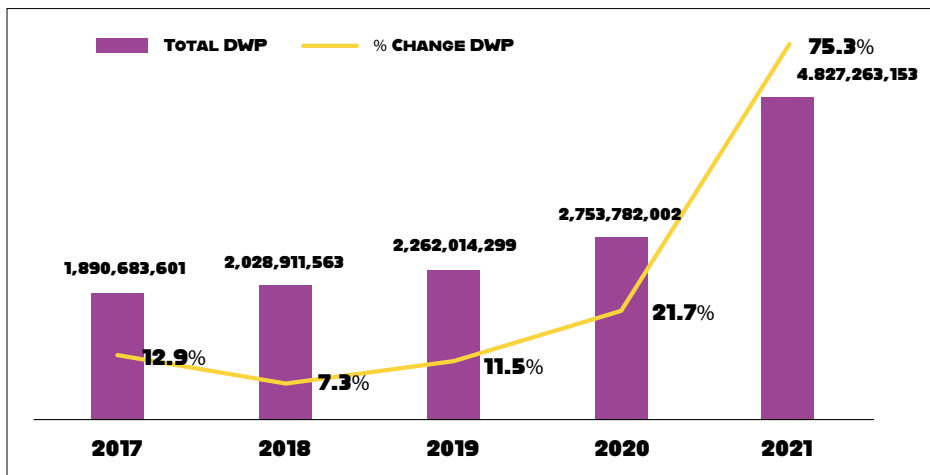
BY PAUL HUGHES

**T**he number of devices connected to the internet, currently at 15 billion, is expected to double over the next eight year.<sup>1</sup>

The exposure to being an employer is dynamic and untenable for a small employer which is why PEOs are so crucial to businesses. While core PEO responsibilities such as payroll, procurement of workers’ compensation, and human resources are foundational, value propositions to assist employers in addition to these areas are what makes one PEO more attractive than another in the selection process. The biggest problem to solve for your client company? Maybe it’s safety. Usually, the area where they lack the most understanding and support is in cyber

defense. Every client of yours is a sitting duck for a hacker and you can help.

Traditionally, PEO offerings and services provided within the client service agreement (CSA) revolve around responsibilities such as workplace safety, hiring practices, human resources and employment-related insurance offerings such as workers’ compensation, health insurance and 401k. Employment Practices Liability Insurance (EPLI) associated services have grown substantially within the PEO model over the years for instance. An exponential number of client companies are provided EPLI whom either did not have it prior to meeting their PEO, or would never have bought on their own based on cost. While I do not have empirical evidence to back this statement, I believe the pick-up rate for



Cyber Insurance Market Growth in Direct Written Premiums ("DPW")

should always be assumed that a licensed agent must present quotations, discuss options, and bind premiums as these are insurance policies in the name of the client company.

### THE BENEFIT TO THE CLIENT COMPANY

AIG wrote the first internet security liability policy in the spring of 1997, so in terms of lines of insurance, it is a new entrant. A line of insurance that has transitioned from a "nice to have" to "vulnerable if not bought" over just the last 10 years. The main difference between cyber policies is that they are all different. Coverage, retentions, triggers, sub-limits etc. are all manuscript in nature by carrier, with many different types of products offered. For the most part, cyber insurance covers a range of basic cyber threats to include:

- Network security and privacy liability
- Social engineering
- Network business interruption
- Media Liability
- Errors and Omissions

While these are the main insuring agreements that provide actual limits of liability to clients, the services that are part of these offerings are paramount in their worth. After all, if you get hacked, who are you going to call? Services within the policy to protect the client company should include:

- Legal expenses to defend
- IT forensics
- Negotiation and payment of ransomware demand

- Data restoration
- Breach notification to consumers
- Setting up a call center after a breach
- Public relations expertise
- Credit monitoring and restoration

One of the items that is huge is notifications after a breach and maintaining compliance with all the different state rules on privacy. Laws in this realm are being enacted on such a rapid basis that it is virtually impossible to keep up with unless partnered with professionals that focus on this line.

### THE LANDSCAPE

Reports indicate that only 19% of the businesses you come across have "Cadillac" coverage, another 55% have some (<\$600k limit) and 28% are looking for something and normally unsure of what that may be. We can then surmise 83% of small businesses are bare or potentially is inadequate.

Prospects for cyber can be understood in three general buckets on this front:

#### Bucket #1:

Typical profile is <\$3m in sales and either has no current cyber coverage, scoring or hotline. Insurance policies may be in play with limits <\$600k and areas of concern such as ransomware sub-limited. Policies have basic limits and afford cyber "duty to defend" services.

#### Bucket #2:

These are accounts that are >\$10m in sales or have greater risks that should be

appropriately covered by higher end services and insurance limit. Examples of these types of firms are those that store large amounts of person information such as law groups, health care providers and financial sector groups. Policies have greater limits (\$1 million) and afford cyber "duty to defend" services. In addition, cyber scores, hotlines and sometimes threat-protect software are provided.

#### Bucket #3:

These are accounts >\$10m of sales and necessitate broader and excess limits in their programs. Offerings in this realm can provide limit up in excess of \$1m, a multitude of different retentions for differing causes of loss, more substantiated business interruption limits and in essence a cyber "special ops" team if a breach occurs. Post claim services such as forensics and rebuild of data sources. Cyber scores, hotlines and sometimes threat-protect software are provided.

### THE OPPORTUNITY

It is our role as salespeople to understand the greatest needs of our client and to bring products and services that address these needs. Cyber is a wave that is getting bigger by the day with event after event bringing it onto the front pages of our newspapers and therefore the front burner of our client's perceived enterprise risk. If something happens to them or their business, who are they going to call? Just like PEO has done with areas such as EPLI and 401K, we have the chance to educate and protect clients and sell some lives doing it. Let's go! ■

1 Freedman, David H. (2023, January 27). A Pandemic of Cyberattacks. Newsweek.

2 <https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html>

3 National Association of Insurance Commissioners ("NAIC"), "Report of the Cyber Insurance Market", 10.18.22, <https://content.naic.org/sites/default/files/cmte-c-cyber-supplement-report-2022-for-data-year-2021.pdf>



**PAUL HUGHES**

Principal  
Libertate Insurance LLC  
Orlando, FL

# FROM HR MANAGER TO PEO OWNER:

# CELESTE JOHNSON AND THE APPLIED COMPANIES

BY CHRIS CHANEY

**C**eleste Johnson leads Reno, Nevada-based The Applied Companies (TAC). A regional PEO that also boasts a robust recruiting services division, TAC is dedicated to serving northern Nevada as the premier workforce solution. Johnson's team is committed to high touch service and providing clients the custom tools they need to grow and thrive.

Today, she's the owner and CEO of the company, but her career path in the HR world began as a summer job while still in college.

## TAKING THE LEAP

While an undergraduate student at the University of Nevada Reno, Johnson took an opportunity to work at a hotel casino in an HR role. She admits that as a student she did not have specific or

set career plans in mind, so this seemed like a good opportunity to try something new.

The fast-paced, 24/7 nature of the casino industry made for a fun and exciting work environment. The unique nature of the casino industry encompasses some highly skilled positions like those in gaming finance, and some low-skilled ones like dishwashers. The broad group of people and employees



created a lot of HR issues which made the job interesting and engaging.

“I’m a farm girl from Iowa,” she says. “So working in HR in a casino was a really eye opening experience. I cut my teeth in frontline HR.”



*The fast-paced, 24/7 nature of the casino industry made for a fun and exciting work environment. The broad group of people and employees created a lot of HR issues which made the job interesting and engaging.*

Around this time, Reno businessman Jim Annis opened a staffing company called The Applied Companies. Two years later, in 2004, Annis added PEO services to his company’s portfolio; notwithstanding the fact that he did not have an HR manager on staff.

“After Jim had a few clients, he decided he probably needed an HR person, so he hired me to start doing handbooks for clients and helping with HR questions,” she says.

As is the case for many people when they learn about PEOs, Johnson had no idea what the business was about. No one in Reno did. Plus, she learned of the position by word-of-mouth so she didn’t even have much time to research PEOs or the industry before her interview. It all

worked out, though. The PEO industry is dynamic and interesting enough that Johnson has stayed with TAC since 2004, culminating in her purchase of the company in 2018.

Johnson and her husband purchased the company, with two small minority partners, from Annis as he was preparing to retire and leave the business. They relied on a Small Business Administration (SBA) loan for the bulk of the financing.

“We put our two homes on collateral, borrowed against our 401(k) and used our savings and took the leap,” Johnson recalls.

She says they did explore partnering with a private equity firm for the purchase, but ultimately her vision and plans for TAC meant she needed to have full control over the business and the decision-making process.

“The nice thing about an SBA loan, even though the process is nauseatingly painful, is that once it’s done, and so long as you make your payments, they leave you alone. Our team has full ownership,” Johnson explains.

Five years later, the company is strong and thriving. Even though Johnson did not start the company, she describes herself as having a lot of the energy and qualities of an entrepreneur. She likes to focus on vision and goals; creating big ideas, and letting others execute the details.

This spirit fueled a desire to continuously learn and grow. Before she even had the idea to purchase TAC, Johnson knew she wanted to expand beyond just her HR foundation.

“Jim was very supportive in letting me learn anything I wanted to,” she says. “I’d ask questions about the budget and financials to get out of my HR box. Prior to the purchase, I had been promoted to COO.”

This same desire to learn led her to return to school for her MBA at age 40 while also a mother to three kids.

“My husband took the kids out to eat a lot just so I could study,” she laughs. “Those were two really hard years.”

Earning an MBA was an important professional milestone that helped prepare her for leading the company when the opportunity arose.

### **PATHS TO SUCCESS**

Apart from offering a robust recruiting division, Johnson says that her company’s biggest differentiator is its commitment to high touch service that is nimble and customizable to client needs. Her team forms good relationships with clients and often visits their offices.

TAC operates on a hybrid model, but many employees come into the office most of the week. The team is also preparing to move into a new office space in the heart of Midtown Reno, an historic neighborhood that has been revitalized with shops and restaurants. Plus, fourth floor office space with large windows overlooking the mountains is pretty good for employee morale.

Employee morale is important to Johnson; she works hard to create and maintain an office culture that supports her employees. COVID’s workplace shockwaves are still being felt, she says, causing employee burnout to rise at alarming rates. She’s cognizant of this and tries to keep her employees engaged, motivated, and supported.

She also points out that many younger employees were not in the workplace during the 2008 recession and unemployment crisis. These employees have never experienced a workplace crisis, and so she spends a lot of time helping them through the ups and downs of the workplace.

Communication is always important which is one reason Johnson compiles a weekly internal employee newsletter. It's a way to reinforce the company's benefits package, and tout employee wins, and overcome losses.



*Employee morale is important to Johnson; she works hard to create and maintain an office culture that supports her employees. COVID's workplace shockwaves are still being felt, she says, causing employee burnout to rise at alarming rates. She's cognizant of this and tries to keep her employees engaged, motivated, and supported.*

Part of TAC's commitment to supporting employees goes beyond their workplace roles.

"Our benefits package includes 40 hours of paid time off for volunteer work as well as fitness and wellness programs. We spend a lot of time promoting physical and mental health," Johnson explains.

She even encourages her team to get up and take a walk at lunch instead of staying at their desks.

Of course, supporting employees also means empowering them to grow and succeed in their roles. To that end, everyone at TAC has his or her own path to success document. The blueprint was reinvigorated a bit post-COVID and includes individual and company-wide goals, career path initiatives, an updated job description, and a total compensation report. Each individual can also view his or her manager's document which fosters transparency and helps drive culture, Johnson says.

The total compensation report is important, she notes, because in today's highly competitive job market people are lured away by base pay.

"Not everyone understands that just because you're making \$5,000 more in base pay the grass is not always greener on the other side," she says.

**CONTRIBUTING TO THE INDUSTRY**

Johnson's path to PEO owner coincided with her path to getting involved in the industry and NAPEO. Before she took on leadership roles with TAC she was not very involved in association activities. She recalls struggling to break through the close-knit network. When she purchased the company, she decided that she needed to deepen association ties and form relationships with peers.

"I had to just start showing up, not just to the annual conference, but to other events, too," Johnson recalls.

She recalls first joining the Annual Conference & Marketplace planning committee. Now, she serves on NAPEO's Board of Directors, chairs the state government affairs committee, and works with our PEO Ambassadors group and Women in NAPEO (WIN).

"Once you get involved with NAPEO, it's really easy to get very involved," she jokes.

All of this involvement has paid off. She's developed a network of friends and peers who are battling the same challenges she is. Everyone brings different backgrounds and expertise, so being able to rely on a trusted network is important. Now when a tricky issue comes up she can shoot off a text or email and get help and advice, she says.

She's excited about the future for PEOs, especially now that more people are joining the industry. A few years ago, she notes, it was hard to identify a future generation of PEO leaders. Now, young and new people are taking on leadership roles and getting involved within the association.

In the meantime, though, she's focused on making TAC the premier workforce solution in northern Nevada. There's still a lot of PEO education left to do, but awareness and understanding of PEOs is much better than it was when she joined the industry.

"It took me a while to find my way, but it's been an exciting journey," she says. ■



**CHRIS CHANEY**  
Editor, PEO Insider  
NAPEO  
Alexandria, VA



# Risk Management Workshop

Omni Charlotte Hotel • Charlotte, North Carolina  
April 18-19, 2023

**NAPEO's Risk Management Workshop** has evolved into the largest gathering of PEO risk management professionals, carriers, brokers, and agents. Nowhere else will you find the PEO industry's top risk managers, key insurance executives, regulatory experts, and policy makers gathered for such an in depth look at PEOs and workers' compensation.

**Hotel Information:** NAPEO has reserved a block of rooms at the discounted rate of \$249/night at The Omni Charlotte Hotel. You must be registered for the workshop before you can reserve a room in the block. Once you register for the conference, you will be sent information to reserve your hotel room. Questions? Contact Ellie Rubalow, erubalow@napeo.org.

## This Year's Highlights

- The evolution of the risk manager in a PEO
- The risk management dashboard (including WC, EPLI, etc.)
- Recession and your PEO: what can the past teach Us?
- The Employer of Record model
- EPLI exposure and ways to manage
- An update on cybersecurity
- Much more!

## NAPEO Thanks its Sponsors for their Generous Support of this Event:

### Title Sponsors



### Partners



### Supporters



### Friends



## Who Should Attend?

- PEO risk managers
- PEO owners
- PEO senior managers with risk management responsibility
- Insurance and risk management service providers to the PEO industry



**Register Today: [www.napeo.org/rmw](http://www.napeo.org/rmw)**

**The National Association of Professional Employer Organizations**

707 North Saint Asaph Street, Alexandria, VA 22314 • 703/836-0466

# THE CYBER SEA: LESSONS IN LEADERSHIP, IDENTITY, AND HARD WORK

BY CHRIS CHANEY

**A**s Chief Information Security Officer at PrismHR, Dwayne Smith leads the company's cybersecurity efforts. He works to strengthen cyber defenses, and guard vital information from internal and external threats. A vast and evolving field, cybersecurity requires constant vigilance, training, and adaptation.

Smith may be a relative newcomer to the PEO industry, but his background boasts impressive cyber credentials from service in the United States Navy, consulting with government agencies, and leading cybersecurity efforts for Cummins, Inc., a large multinational company.

Underpinning his professional life, is a personal journey of hardship, hope,

service, grit, and success. He spoke with PEO Insider® to share his story.

## A DESIRE TO HELP

In his prior role as Global Director of Cybersecurity Engineering at Cummins, Smith says that he began to notice that many suppliers experienced cyberattacks. In many cases, large companies suffered

hacks because of small companies they had a relationship with.

This trend motivated Smith to think about how small companies could strengthen their cyber defenses. He realized that a cyber attack on a small company may seem like an isolated event, but it can be the stream that turns into a tributary that turns into a river.

“Like many people, I reflected a lot during COVID,” Smith recalls. “I was looking for something different, and when I learned about the PEO industry, I realized it supported small businesses.”

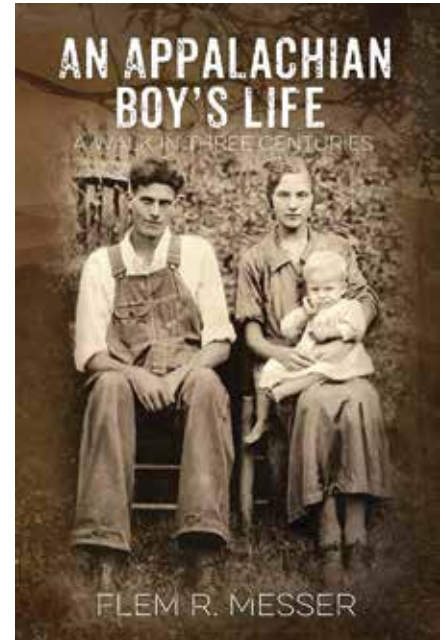
Smith found himself wanting to help small businesses bolster their cyber defenses and improve cyber hygiene. Joining the PEO industry offered him a way to put his skills and experience to use in this way. He notes that many PEO

leaders have learned cybersecurity the hard way. He hopes to use his background to influence the industry for the better.

He’s encouraged by the fact that more people than ever are undertaking cyber training, and that businesses are bringing people on board with cyber backgrounds to spearhead this effort. There will always be some level of risk, but appropriate safeguards and strong training can make a business a less than ideal target for hackers.

### LUCKY IN THE ORDER

Smith never intended to become a cyber expert. It’s just the way life worked out. Born and raised in a small Appalachian town, Smith knew he wanted to set out on his own course beyond the confines of his hometown.



Written by Smith's uncle, the book chronicles the struggle and perseverance of those living in Appalachia.

**AON**

## Building Sustained Cyber Resilience

Aon helps our clients mitigate, quantify and transfer their cyber risk to make better decisions and safeguard their balance sheets for sustained cyber resilience.

When an incident does occur, we help clients minimize the impact by driving operational and financial loss recovery.

[Learn more at aon.com/cyberloop](https://aon.com/cyberloop)



“I grew up in a very poor area of the country. A lot of my high school friends made the decision to stay there, but I knew I wanted to leave, I just didn’t know how,” Smith says.



*Smith’s upbringing has instilled in him a desire to help other people realize opportunities. He’s tried to do this whenever he’s had the chance. Whether in the military or in business, Smith has focused on bringing people in who others may have dismissed or overlooked.*

He attended Berea College in Kentucky, an experience that had a profound impact. College exposed him to many new ideas, perspectives, and cultures. His horizons broadened. He also began to develop what would become a lifelong commitment to diversity and inclusion. Smith recounts unfortunate incidents during which friends of his were mistreated due their backgrounds, and that’s part of the reason why focusing on Diversity & Inclusion is so important to him.

After his time at Berea, though, he was still unsure what sort of career he wanted to pursue. So, he joined the United States Navy which is what first led him to the world of cyber.

“I graduated from the Navy’s nuclear power program, and then found my way into cryptology,” Smith says.

“I worked with some 3-letter agencies studying networks and digital communication patterns. We didn’t even call it cybersecurity back then, it was called COMSEC, INFOSEC, and DATASEC.”

In the 1990s, unauthorized intrusions into government networks became a real threat. As the guy who knew about systems, Smith often found himself in the right place at the right time. He admits that he didn’t recognize cybersecurity as a career path at the time, but he pursued opportunities as they were presented and that’s what led him to where he is today.

His military training and experience taught him several lessons beyond his cyber skills that are still important. First, he says, if you’re the smartest person in a room, find a different room. Challenging yourself and taking risks is uncomfortable and hard, but it’s rewarding. You grow by pushing past boundaries and being willing to do the hard work.

The second lesson he learned can be captured by Isak Dinesen’s quote: The cure for anything is saltwater: sweat, tears, or the sea. At sea you’re isolated; for Smith, that was a calming influence. Being on a ship also forces you to be in constant contact with other people, you must learn to get along and work well with others.

The sea is also a good metaphor for the cybersecurity field. Some days are calm and peaceful, others are dark and stormy. Some days the course is clear, other days it’s uncharted. Smith sees his role as helping companies get where they need to go on the cyber sea.

### THE STRUGGLE FOR IDENTITY

You may be familiar with the National Institute of Standards and Technology’s (NIST) 5-part cybersecurity framework: Identify, protect, detect, respond, and recover. While all five components are important, Smith says a business should consider putting the bulk of its cyber investments behind identify, respond, and recover.

Protecting your systems from and detecting cyber-attacks are good, but cyber is an ever-evolving field and bad actors will never stop trying to penetrate systems. By focusing on identify, respond, and recover, a business can make it easier to limit the fallout from a cyberattack and get operations back to normal quickly.

Identity is the new boundary for cybersecurity, Smith says. It’s a hard concept for many to fully grasp. How do you ensure the person accessing the data is who they say they are?

“In the old school days, you were in an office on a network and the firewall basically kept you safe,” Smith explains.

“Now, with everything internet based, the password is the primary thing protecting you,” he adds.

And speaking of passwords, Smith’s not a big fan.

“They’ve outlived their time, but it is still important to have a strong password and not reuse that password,” he says.

Also, a good password manager is important to help eliminate password reuse.

He makes the point that within the confines of the English language there are a finite number of password combinations. To be sure, it’s a very large number, but he notes that computers are only learning to processing large amounts of data faster. Hackers just keep trying possible passwords until one works, he explains.

Even with multi-factor authentication enabled, if your password has been compromised, then you really only have one-factor authentication. Smith suggests that authenticator apps, certificates, or single use passwords should be considered.

This struggle with identity is deeply personal for Smith, too.

Growing up, many people took pity on him, he recalls. Expectations were not set very high, but he did not let that define him. He learned how to succeed. Tragedy struck early when his father was killed by a drunk driver over a Fourth of July weekend when Smith was just five years

old. It was a pain and hardship that still resonates today.

Smith says he sadly watched too many of his friends fall victim to the pill mill epidemic that has swept much of the country, but especially Appalachia.

These struggles and the plight that so many in the region deal with are chronicled in a book his uncle wrote, *An Appalachian Boy's Life: A Walk In Three Centuries*. One day, Smith hopes to write the sequel.

He's achieved a lot of success in his life, but it's come at a personal cost.

"I had to struggle with my background," he says. "I lost my accent and like many people, I had to re-invent myself. The saddest day of my life was my grandfather's funeral because a gentleman who I had known my whole

life did not recognize me because of how much I had changed."

"To be successful and grow, I had to leave some things behind."

Smith's upbringing has instilled in him a desire to help other people realize opportunities. He's tried to do this whenever he's had the chance. Whether in the military or in business, Smith has focused on bringing people in who others may have dismissed or overlooked. Diverse perspectives and backgrounds strengthen teams and help everyone grow, he believes. In one instance he describes how a team of diverse cultures was able to detect a widespread phishing scam in 30 languages. Bringing more women into the cyber field is a passion for him, too, since he is the father of two young daughters who are already learning to code.

He encourages people to set goals, but to think of them as way points, not end points. Goal setting requires introspection and reflection on where you want to go. He cautions not to stay hyper-focused on one goal or you may miss an opportunity on a different path.

As an industry, PEOs have made great progress in strengthening cyber defenses and improving cyber hygiene. Yet, hackers and bad actors learn and grow, too.

"Cyber needs to be a community and industry wide effort, we need the power of everyone working together," Smith says. ■



**CHRIS CHANEY**

Editor, PEO Insider  
NAPEO  
Alexandria, VA

  
**McHenry Consulting**

# THE PEO ADVISORS

Your Trusted M&A Partner.

**LET'S CONNECT**  
813-363-2270  
678-793-6693  
www.mchenryconsulting.net

*"McHenry Consulting exceeded ALL expectations in the handling of my transaction. If you are considering a transaction, reach out and speak to their team. Dan McHenry and Matt Claus were our champions navigating each phase of the process, and we could not be more pleased with the experience and outcome. Give them a call, they know how to get it done."*

**— Bob Burbidge**  
Founder of Genesis HR, now an Engage PEO company



# STATE PAID FAMILY LEAVE LAWS: WHAT PEOS NEED TO KNOW

BY TOM JACOBS, JD, MBA

**A**s more and more states adopt paid family leave laws, the PEO industry is confronted with both challenges and opportunities as we adapt and manage these laws on behalf of our worksite employer clients. Like the Americans with Disabilities Act (ADA) or the Family Medical Leave Act of 1993 (FMLA) or the Occupational Safety and Health (OSHA) Act, and other laws that have been bestowed on us, we are in a great position to use what we have learned and accomplished over the years to handle the challenges brought on by state paid family leave laws.

One of the first codified protections for a worker taking leave to address family or personal health was the FMLA passed in 1993. In a 12 month period, an eligible employee, public or private, can take up to 12 weeks of UNPAID leave for birth,

adoption, serious health condition of self or immediate family members, or for military exigency support. Employers are required to keep the same or similar jobs available and in some way have all previous benefits intact upon their return. When FMLA came out, NAPEO and member companies worked fervently to have FMLA be applicable to worksite employers (with over 50 employees) only, and not applicable to PEOs as a whole, which, of course, have far more than 50 employees on their W-2 payroll. The industry took similar action to have the ADA, OSHA Act, and other employment laws rest upon the worksite employer for responsibility, so the challenge relating to current paid leave situation is not new.

The next federal law to bolster the federal employees needing leave was to require the 12 weeks of leave to be paid during the leave. The Federal Employee

Paid Leave Act of 2019 (FEPLA) amended FMLA to provide for PAID leave for federal employees. While there is no requirement under the law for private employers to provide similar paid leave, they are encouraged to do so by claiming a tax credit of up to 25% of paid wages to qualified employees, through December 2025.

There are currently eight states with active paid family leave laws, and five more with paid leave laws that will be implemented over the next few years. More will follow. PEOs are learning to adapt to the paid leave laws. Some states are extremely organized and have developed a logical approach as it relates to co-employment, some other states need our help, and for those not yet implementing such laws we can be of assistance so that the notion of co-employment is considered as the new laws are promulgated.



States (including DC) with active laws as of this writing include: Massachusetts (effective 2019/2021); Connecticut (2021/2022); District of Columbia (2020); New Jersey (2009); New York (2018); Rhode Island (2014); Washington (2019/2020); and California (2004). States that have passed paid leave laws that will become effective in the near future are: Colorado (Jan. 2024); Delaware (Jan. 2026); Maryland (Jan. 2025); Oregon (Sept. 2023); and New Hampshire (2023). Of course these state paid leave laws are not uniform in eligibility, type of leave, timing of leave and more, creating a complex puzzle of



*There are currently eight states with active paid family leave laws, and five more with paid leave laws that will be implemented over the next few years. More will follow. PEOs are learning to adapt to the paid leave laws.*

administration for those PEOs with worksite employees in multiple states. While there is not enough space here to go over the details of each state's paid leave law, there are excellent online resources that summarize these. See <https://bipartisanpolicy.org/explainer/state-paid-family-leave-laws-across-the-u-s/>.

New York's law, for example, applies to all private employers and employees, full-time or part-time, who have worked 26 or more consecutive weeks for a covered employer. Public employers have the choice to opt in. Benefits include up to 12 weeks per year for birth of a child, placement of a child in adoption or foster care, caring for a family member with a serious health condition, or to assist loved ones when a covered parties are deployed abroad on active military service. The law provides leave to care for child, spouse, parent, parent-in-law, stepparent, grandparent, grandchild, sibling, domestic partner, or a person with whom the employee has or had an *in loco parentis relationship*.

California's law, by contrast, applies to private employees who have worked for an employer for at least 12 months, and who have 1250 hours of service during the 12 months prior to the leave. Benefits include up to eight weeks of paid leave to care for a seriously ill child, spouse, parent, or registered domestic partner, or to bond with a new child. The benefit amount is approximately 55% of an employee's weekly wage, from a minimum of \$50 to a maximum of \$1067. The program is funded through employee-paid payroll taxes and is administered through the state's disability program. The other active states have equally disparate

**Payroll Funding**

# Funding for PEO Clients at The Speed of Now

Got clients that are struggling to make payroll or need extra capital for growth? We specialize in providing same-day funding to businesses that struggle to get funding from traditional lenders.

✓ Fast Process   ✓ No Collateral   ✓ No More Floating Payroll

**609-516-5100**  
payrollfundingcompany.com/referrals

## LEGAL, LEGISLATIVE, & REGULATORY

provisions requiring PEOs to be prepared to address all.

To address the challenges of interacting and reporting to each state, there are different approaches PEOs are finding they need to undertake. Massachusetts for instance, recognizes the PEO client as the responsible employer and follows that state's unemployment insurance laws, and only requires employees of covered client employers to be included in paid family leave workforce calculations. I strongly encourage you to review the NAPEO member forum ([forum.napeo.org](http://forum.napeo.org)) conversations on paid family leave to learn what our members are experiencing with respect to how PEOs are

working with each state, and what processes are in place that benefit our position that the laws are applicable to worksite employer clients only. Some states are not similarly prepared. In Oregon, for instance, state officials are taking the position that the PEO is the responsible employer for Oregon's paid leave law. Reportedly, officials did not consider co-employment relationships when the Oregon laws and regulations were promulgated, and the state's internal systems have no way to address multiple employers in a reporting file.

For states such as Oregon, and for other states contemplating paid family leave laws, PEOs operating in those states need to work with applicable state agencies to

ensure that the interests of PEOs and of the worksite employers are protected. NAPEO is actively involved. Contact Jason Gabhart ([jgabhart@napeo.org](mailto:jgabhart@napeo.org)), NAPEO's senior director of state government affairs, for more information. ■

▼ This article is designed to give general and timely information about the subjects covered. It is not intended as legal advice or assistance with individual problems. Readers should consult competent counsel of their own choosing about how the matters relate to their own affairs.



**TOM JACOBS, JD, MBA**

*Principal  
PEO Auxillary  
Madison, WI*



## Barrow Group

INSURANCE BROKER

With more than 30 years of niche experience offering insurance solutions to the PEO industry, we are helping PEOs reduce the cost of risk.

Ask us about our Captive Insurance Program

- TALK TO US: 800-874-4798
- VISIT US: 110 E. Crogan St.,  
Lawrenceville, GA 30046
- CONNECT WITH US: [www.BarrowGroup.com](http://www.BarrowGroup.com)

# BUILDING STRONG RELATIONSHIPS WITH CLIENTS LEADS TO BETTER OUTCOMES FOR ALL

BY SAM RATHBUN

**A** PEO is only as strong as its client relationships. From ownership to worksite employees, we need to be engaged at every level of our clients' teams. Of course, strong connections between owners and executives build trust that is needed to develop successful relationships. Also, the quality of service we provide to worksite employees is essential to the PEO model being successful. However, it's often the relationships between our HR/client service managers and the clients' own supervisors and personnel managers that have the greatest impact on our effectiveness, efficiency, and ultimately our bottom line. There are examples in nearly every aspect of our service that outline how this dynamic can mean the difference between a profitable client and one that prevents you from growing.

When working with small businesses, it is common that the business owner themselves serves as the primary contact and worksite manager to the PEO. However, there are several hurdles in this setup. While the idea of allowing the PEO to take the administrative and HR burdens off the owners' plate is one of the reasons they pursue our services, it is not always that simple.

Many business owners have developed policies and practices that they may be reluctant to change, even after being informed of the legal and practical implications of why such change is needed. Facing this challenge, we always want our HR managers to keep the mindset of the business owner, to be able to empathize with their situation regarding a new law and how that will affect their operations. At the same time, it's important to help develop new

practices for the client to be compliant. If not handled correctly, a PEO can spend an immense amount of time cleaning up after the issues caused by some clients' lack of understanding.

It's important that HR and recruiting managers understand some of the opportunities for development in their worksite manager relationships. For example, over the past few years, the most common request we hear from clients is for new applicants. When looking at staffing services, it's easy to highlight the difference between an effective and ineffective client relationship.

Let's be honest, there's nothing more frustrating than fielding calls from clients needing employees, only for the applicants supplied to be denied by either slow responses, outdated practices, or narrow selection processes. When factoring the cost of job posting, the time

of your staffing associates, and the potential loss of quality applicants, it can be extremely detrimental to profit efficiency when the recruiting cycle is handled poorly. Many times, this inefficient cycle comes down to the effectiveness of the connection between the recruiter and worksite manager.

Managers who do not respond to applications quickly, don't host quality interviews, or provide feedback on applicants will hurt both the client and PEO. However, tight communication and responsiveness with the worksite

manager will lead to a quicker applicant-to-hire cycle, making the operation more profitable. Honest conversations such as how slow response times lead to a bottleneck of applicants, how to conduct better interviews, and initiate the onboarding process can help a worksite manager improve their business' hiring success. A strong relationship between the PEO and client makes honest conversations possible.

One of the biggest opportunities for improvement with many small business clients is their new hire training. If the



*There is a fine line between working with and working for the worksite managers. HR managers need to have the confidence in their expertise to make managers understand where there is opportunity, while developing real relationships so that the message is received.*

PEO can effectively help the client implement better onboarding practices, this will open up the recruiting target. By knowing they can properly train an employee, businesses are open to a wider selection of applicants opposed to needing someone to bring a particular skill from day one. In the increasingly competitive recruiting atmosphere, a PEO can help its clients implement long-term hiring solutions to stay a step ahead. Without strong relationships, a client will be much more reluctant to trust the development of long-term solutions in lieu of quick fixes.

For medium-sized businesses, the challenge becomes managing the relationships between the clients departmental and mid-level management.

**blr**

**ADDITIONAL REVENUE**

**MAXIMIZE BUSINESS PERFORMANCE**

**EXCEED CLIENT EXPECTATIONS**

**PEO'S PREFERRED PARTNER**

BLR simplifies HR, EHS, and training. Learn more about the true value BLR can bring to your business today!

**BLR.com**  
**800-727-5257**

BLR is proud to be a gold level NAPEO Medallion Partner

The PEO's HR team can easily become embroiled in inter-departmental conflict if it becomes too reactive in its service. Coaching managers on how to cooperatively lead their staff on the front end will lead to less issues needing to be addressed later.

Again, this comes down to the HR team being able to have honest and sometimes difficult conversations with managers about how they need to improve. The business owner chose to partner with a PEO to see the overall health and success of the business'

employee relationships improve. The PEO cannot do that by always being in adherence to worksite managers. There is a fine line between working with and working for the worksite managers. HR managers need to have the confidence in their expertise to make managers understand where there is opportunity, while developing real relationships so that the message is received.

It is our responsibility to help clients understand the importance of our services to the overall success of their business. The more engaged the business

owner is with the PEO service, rather than just a passive reliance, the more effectively we will be able to rollout improved processes. By creating a true partnership with clients, providing PEO services will feel more like skiing downhill instead of swimming upstream. ■



**SAM RATHBUN**  
General Manager  
KEENA  
Queensbury, NY

## Better together. Stronger than ever!



are now



**As the largest and most experienced insurance advisor to the PEO industry, we support hundreds of PEO'S in maximizing long-term profitability of their commercial insurance programs.**

**Contact us today to find out how we can help with your insurance and risk management needs.**



**Troy Reynolds**, Area Senior Vice President, PEO & Staffing Practice  
Troy\_Reynolds@ajg.com  
561-746-5027  
<https://www.ajg.com/us/>



**Jennifer Robinson**, President  
Risk Transfer Insurance Agency  
jrobinson@risktransfer.com  
407-230-6953  
<https://risktransfer.com/>



# EMPLOYER PRIORITIES FOR HEALTHCARE IN 2023

## BY ONE MEDICAL

**A**mployers are recognizing that virtual care has not fully eliminated barriers to access, and that an exclusively virtual strategy can fragment the care experience and lead to wasteful spending. In articulating priorities for 2023 during the Fall 2022 Roundtable session with One Medical, organized by the Employer Health Innovation Roundtable, over 4 in 1 employers named lack of access to care as a primary concern, and 1 in 4 employers expressed concern over fragmented care. A fragmented care experience is characterized by disorganization, poor communication, and/or general incoherence, all of which can compromise cost-effectiveness and create negative health outcomes.

While most employers anticipate that virtual care will continue to be important in the future of health care delivery, they also agree that combining virtual with in-person delivery will be essential to

designing successful and equitable health benefits strategies moving forward.

As a result, employers are now in a moment of examining, refining, and supplementing virtual health care options.

### THE IMPORTANCE OF PRIMARY CARE TODAY

Primary care, which accounts for about 35% of patient visits, is a key area of focus among employers as they work to assess the effectiveness of delivery strategies. However, primary care currently accounts for only a threadbare amount of total medical spending in the United States, estimated at 5%. To the detriment of many communities, as well as individual health outcomes, most hospital systems in the U.S. view providing primary care as unprofitable in the short term, and employees on corporate health care plans report having to wait about six months for primary care appointments.

Employers reported that one third to one half of their workforces haven't been able to access a primary care provider. These employers expressed concern about the serious risks and costs that problem poses. They noted that the stakes are high for both employees and payers, as timely, solid engagement with primary care is essential to the early detection of health problems and especially to effective cancer screenings and cancer care.

Without reliable primary care, employees can't address their health proactively; they can only react to symptoms, often after expensive problems have already developed and compounded. Conversely, investing in effective primary care leads to long-term savings and improved health outcomes. The California Health Care Foundation estimates that if commercially insured HMOs in California were to fully fund primary care services, the shift would

result in around \$2.4 billion in annual savings and 89,000 avoided ER visits.

Given the extensively documented human and financial costs of compromised primary care, as well as increasing awareness and demand for better primary care among employees and prospective hires, determining the most effective delivery strategy for primary care is central to employer priorities in 2023. The employers who spoke with One Medical reported that workers value access to primary care so consistently that including strong primary care options in benefits packages has become an important tool for recruitment and retention.



*Given the extensively documented human and financial costs of compromised primary care, as well as increasing awareness and demand for better primary care among employees and prospective hires, determining the most effective delivery strategy for primary care is central to employer priorities in 2023.*

#### ADVANCED PRIMARY CARE

Polling has found that 42% of EHIR members expressed that their biggest priority in offering primary care

benefits is to increase access to care among employees.

According to the same poll, 25% of employers are prioritizing the need to reduce fragmented care, and around 17%

of employers are primarily concerned with preventing duplication of services. Successfully addressing all three of these concerns—expanding access, reducing fragmentation, and preventing

## BROKERS and AGENTS JOIN US



**EnterpriseHR** works ONLY with brokers and agents. We make difficult prospects easy to place in Employee Leasing.

#### We make earning commissions easy:

- Small businesses, as little as one employee.
- Construction-related businesses.
- Hard to place businesses.
- Companies with previous bad losses.
- Startup companies.
- Our average commission is 2.13% of PAYROLL!
- Certs as fast as 1 day!
- 20 years in business with over 13,000 added in 2019

Contact:

**Tim Russell**

727.520.7676, ext. 206  
888.770.7676

[trussell@encorehr.com](mailto:trussell@encorehr.com)

700 Central Avenue, St. Petersburg, FL 33701  
**[www.enterprisehr.com](http://www.enterprisehr.com)**

duplication—would improve employee health outcomes and improve cost-effectiveness over time.

An integrated, advanced primary care solution that incorporates both virtual and in-person components addresses all three employer priorities head-on:

- Virtual delivery ensures that a majority of employees have wide-spread, easy access to providers.
- In-person options support employees without home access to broadband internet and ensure thorough, high-quality care for all.
- The well-coordinated use of both strategies ensures coherent communications and prevents unnecessary spending.

Fortunately, successful models have proven that it is possible to seamlessly integrate a virtual strategy with in-person options. With an integrated model, a wrap-around virtual care program can supplement in-person services at brick-and-mortar primary care facilities.

As distinct from urgent care facilities, primary care facilities provide ongoing, longitudinal services and enable patients to build relationships with providers. The integration of virtual care reinforces those in-person services and strengthens patient-provider relationships over time. An integrated, advanced primary care strategy therefore leverages technological advances

from the past several years to optimize patient outcomes; attract, retain, and support employees; and boost overall access to primary care. ■

### ONE MEDICAL

*References:*

- 1 **Employer Health Innovation Roundtable**
- 2 **One Medical** Insights Paper: “**Employer Priorities for Health Care in 2023: Addressing the Unmet Promise of Virtual Care**”, December 2022.

▼ This article is designed to give general and timely information about the subjects covered. It is not intended as legal advice or assistance with individual problems. Readers should consult competent counsel of their own choosing about how the matters relate to their own affairs.



## Retain your clients, even as they expand outside your market.

We can help your clients identify and hire their ideal talent anywhere in the world. We then put those professionals on our fully compliant global payroll – handling all corporate tax, legal, and HR matters so they don't have to. Learn more at [g-p.com](https://g-p.com).



# NAPEO UNVEILS LATEST PEO AWARENESS TRACKING SURVEY

**E**ach year, NAPEO conducts a tracking survey to measure the level of PEO awareness. The results from the December 2022 survey are encouraging and show that more and more business owners are aware of PEOs. Here are the key findings from the survey. The full report is available exclusively to NAPEO member companies at [www.napeo.org/marketresearch](http://www.napeo.org/marketresearch).

### KEY FINDINGS

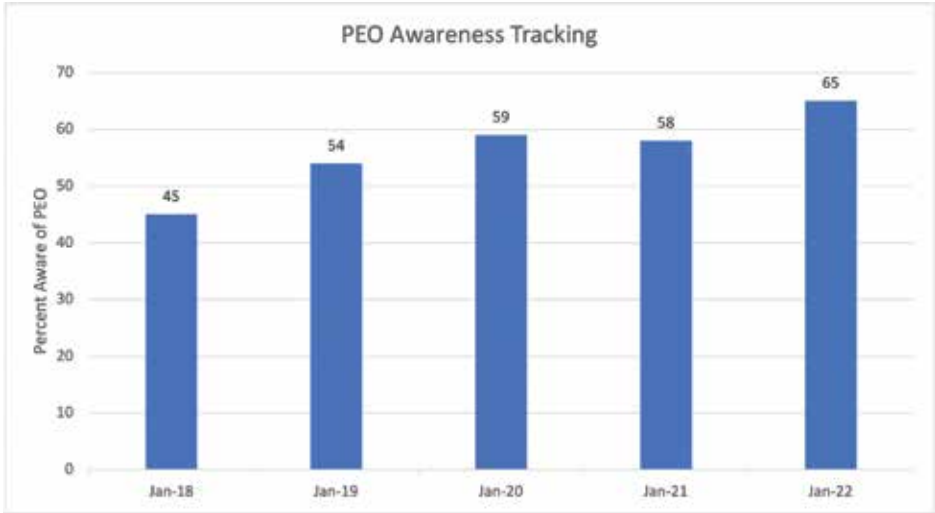
In 2022, all measures of awareness and familiarity increased, some significantly, as did reported PEO usage and interest in use among non-users.

1. Unaided awareness of PEOs increased significantly to 65% among decision makers in 2022 (+7 points over the past year and +20 points since tracking began in 2018).
2. Aided familiarity increased to 75% with three-in-four decision makers saying they are very or somewhat familiar with PEOs (+5 points over the past year

- and +14 points since tracking began 2018).
3. One-third (33%) of decision makers in this sample report using a PEO, a significant increase of nine points over the past year. This increase in PEO use most likely reflects a combination of true market growth as well as confusion regarding what a PEO is and does due to the increased familiarity with and availability

- of outsourced business function offerings in the current market.
4. Of those who do not currently use a PEO, eight-in-ten indicate interest in using one in the future (81%, +5 points over the past year).

While unaided awareness holds steady among younger decision makers (74%) and newer businesses (69%), there continues to be an increase in unaided awareness among middle-aged decision



makers (63%, +5 points), older decision-makers (62%, +15 points), and businesses that are more established (10-19 years: 71%, +15 points; 20+ years: 57%, +8 points) over the past year.

Decision makers are most likely to learn about PEOs from friends/colleagues (39%), reading about them in an article (38%), or discovering them online (33%).

## METHODOLOGY

### Objective:

The core objective of this research is to track the benchmark awareness, understanding, and use of PEOs to better

understand the impact of NAPEO's marketing efforts.

Further, this research looked to uncover/confirm core concerns among potential clients and understand which core PEO services are seen as most burdensome for business owners to handle in-house.

### Approach:

Method: online

Sampling: n=553 business decision makers

- 64% business owners
- 36% key decision makers

Field dates: December 8, 2022–January 5, 2023

Margin of error: ±4.2%

### Screening Criteria:

- In order to qualify for this survey, participants must have met the following criteria:
- At least 25 years old
- Business decision maker for hiring a professional services firm to help handle internal business functions
- At least 10 full-time employees
- Annual business revenue of at least \$500,000 ■

# Let's achieve your 2023 goals together

Here's how...



Intelligently connected, futureproof PEO Software.



Secure and stable technology with a modern architecture.



PEO-specific programs, processes, and people to maximize your success.

# PEOS CLOSE OUT 2022 WITH SOLID REVENUE AND GROSS PROFITS GROWTH

The results of NAPEO’s PEO Pulse Survey for the fourth quarter of 2022 show that PEOs closed out the year strong. Here are some of the survey’s highlights:

Revenue increased in Q4 of 2022, while WSE wages and WSE counts remained stable.

- PEO revenue growth had its largest increase of 2022, with 79% of PEOs experiencing growth vs. Q4 of 2021. Only 9% of respondents reported that revenue decreased.
- 31% of PEOs reported no change in WSE wages this quarter. Two-thirds saw wage increases, and only 2% reported any decrease.
- The sizes of clients (based on WSEs per client) remained steady during 2022, with most seeing their clients grow slightly versus 2021.
- In Q4, 40% of PEOs reported year-over-year increases in WSEs, 49% noted that their WSE count stayed about the same, and 12% reported a decrease (none categorized their decrease as significant).
- Client counts stayed positive, with 65% of PEOs having more clients now than in 2021. Only 12% of PEOs have fewer clients now than a year ago.

Gross profits climbed in Q4.

- In the final quarter of 2022, gross profits saw the most year-over-year growth since 2018.

- 76% of respondents indicated that their gross profit increased in Q4. 7% reported a slight decline, and 17% said that they stayed about the same.
- Operating profits were up for 65% of PEOs. A quarter noted no major change, and 9% reported a decrease in operating profits.

The number of internal employees remains elevated.

- 47% of PEOs have more internal staff now than in 2021, with 12% having significantly increased their internal headcount.
- 9% of PEOs reduced their staff size during the year, with most reductions happening in the second half of 2022.
- The amount of workers compensation claims reported to insurance carriers remained steady, with only 18% seeing more claims and a quarter of PEOs with fewer.

The confidence streak continues into 2023.

- 91% of PEOs are planning for growth over the next 12 months, with 29% expecting that the increase in WSEs will be significant.
- The PEO Expected Growth Index\* for Q4 is 4.17, which is consistent with the past 9 months and is in line with the typical index rating of 4.15 recorded over the past 6 years. ■

## NAPEO QUARTERLY PULSE SURVEY—Q4 2022 RESULTS: TYPICAL PEO

WSEs per Client **22**

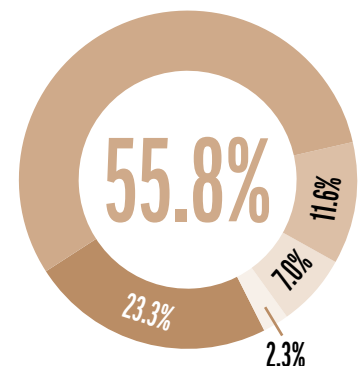
Clients per FTE\* **8**

WSEs per FTE\* **159**

## HOW DID THE 4TH QUARTER OF 2022 COMPARE WITH THE 4TH QUARTER OF 2021?

### PEO REVENUE

▲ INCREASED SOMEWHAT



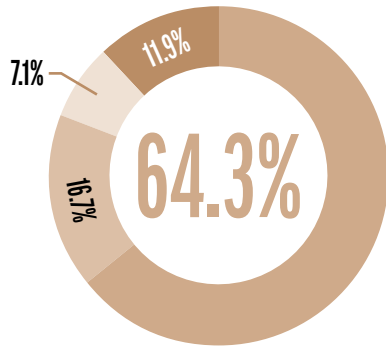
RESPONSE COUNT **43**

\* Expected Growth Index is based on the average score of a 5-point scale where 1 = Significant Decrease / 3 = No Change / 5 = Significant Increase.

NAPEO’s Pulse Survey was developed by the Accounting Practices Committee in 2016 and is conducted quarterly among members to take the pulse of the PEO industry through a series of easy-to-answer questions. For more information about NAPEO’s Pulse Survey, please contact Melissa Viscovich at [mviscovich@napeo.org](mailto:mviscovich@napeo.org) or 703/739-8161.

GROSS PROFIT (\$)

▲ INCREASE SOMEWHAT



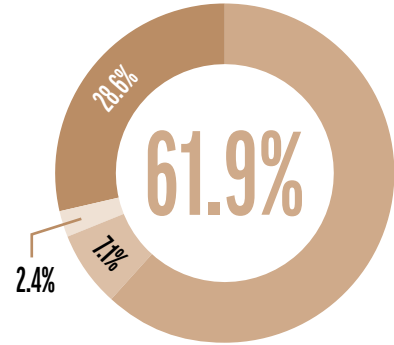
RESPONSE COUNT 42

WSE PROJECTION

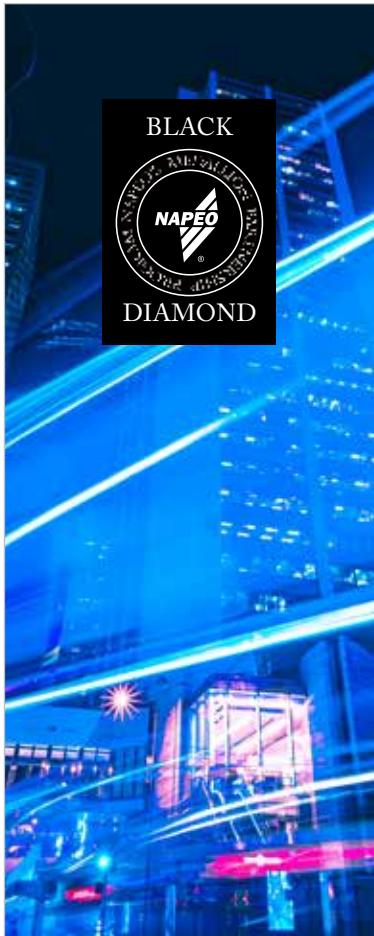
HOW DO YOU ANTICIPATE YOUR NUMBER OF WSES WILL CHANGE OVER THE NEXT 12 MONTHS?

▲ INCREASE SOMEWHAT

RESPONSE COUNT 42



■ Increased Significantly	■ Stayed About the Same	■ Decreased Significantly
■ Increased Somewhat	■ Decreased Somewhat	



PEO Velocity is a risk-management platform that will help your master-health plan thrive.

We go beyond underwriting by bundling:

- project management
- competitive benchmarking
- risk assessment
- new-business pricing
- performance dashboards
- high-tech tools
- actuarial support
- interactive team

All in one unique PEO experience that's actionable, collaborative, transparent, and specialized.

Contact Kym Porter, GBA, CBC  
Senior Vice President  
moreinfo@peovelocity.com  
610-428-7761

[peovelocity.com](http://peovelocity.com)

Accelerate your growth today through Velocity's deliberate, creative solutions.

# AD INDEX

Ameritas.....	9	G-P.....	48	Poster Guard® Compliance Protection.....	56
Aon.....	37	isovled Network.....	50	PrismHR.....	6
Barrow Group.....	42	McHenry Consulting.....	39	PRO Software, LLC.....	29
BLR.....	44	Normandy Insurance Company.....	53	Slavic401k.....	2-3
Enterprise HR.....	47	Payroll Funding Company, LLC.....	41	SUNZ Insurance Company.....	11
Gallagher–Formerly Stonehenge Insurance Solutions.....	45	PEO Velocity by Compass/PRM.....	52	ThinkWare Corporation.....	55

**Boldface type** indicates NAPEO Medallion Partner

Yes!  
We write  
**PEOs**



## Workers' Compensation for PEOs

- Master policies for as little as 10% down
- Monthly self-reporting online or via payroll template
- Available through your agency or broker
- 24-hour turnaround on 99% of submissions
- Guaranteed Cost, Small & Large Deductible Plans

"Normandy Insurance is the BEST of the BEST in the PEO Industry! Customer Service, Underwriting, Claims, Billing, no matter what subject, **they are amazing!**"

- Robin Lefebres, AAI, CLCS

Trustpilot Rated 4.8 by verified agents

Learn more at and get started  
[www.normandyins.com/PEO](http://www.normandyins.com/PEO)

# ENGAGING ON CYBER AND ERTC

BY PAT CLEARY

**W**elcome to the cyber issue! I don't know if there is any issue that is a bigger threat to the industry than cybersecurity, and it has exploded in importance just in the past few years. The arc of its prominence has gone almost straight up.

I remember several years ago when we invited John Carlin to speak to a CEO Forum dinner during PEO Capitol Summit. John was in private practice at the time, but he had been the first-ever US Assistant Attorney General of the National Security Division that oversaw cybersecurity and cybercrime. In that role, he dealt on a daily basis with global threats from China, Russia, North Korea, Iran...you name it. As we do with all our speakers, I called him in advance of his speech to give him some background on this industry. As I started to explain who we were, he cut me off.

"I know who you are," he said.

He went on to say that because of his government career, he knew PEOs well. In terms of cyber-attacks, he told me, "payroll is often the entry point."

So, the good news was that he knew who we were. Turns out, that was the bad news too.



*We need to keep the pressure on, and we intend to do just that. But we will need your help and engagement here, and that of your clients.*

Last year, our board set up a cyber task force chaired by Alex Campos of Vensure. It is by design a small group of hands-on experts and PEOs. They meet monthly to develop tools and best practices for our members. You can see the fruits of their labor at [www.napeo.org/cyber](http://www.napeo.org/cyber). It is regularly updated and has consistently been getting strong traffic. You'll see information and resources there on many different cyber-related topics. Check it out.

Another big issue occupying our time—and yours—is the Employee Retention Tax Credit (ERTC). It is confounding—and infuriating—that the IRS backlog is still north of 557,00 returns and

climbing. You know we've been pounding away on this issue, with repeated meetings with and letters to the IRS and members of Congress. In February, we sent a letter to every member of Congress, reminding them that this issue was threatening small businesses in their districts. We produced a letter in January that you should have received. It's intended for use with clients, to let them know the ERTC is a small business-wide problem with the IRS and not a PEO-specific problem. By the time you read this, you will have received a communication from us with a sample letter for you to send to Congress and a widget you can put on your website for your clients to use to contact their members of Congress directly. We need to keep the pressure on, and we intend to do just that. But we will need your help and engagement here, and that of your clients, if we hope to move the needle. This issue, this backlog, has been around far too long. It's time the IRS fixed it. I hope you will help us make that case. ■



**PAT CLEARY**  
President & CEO  
NAPEO  
Alexandria, VA

The logo for Cohesion, featuring a stylized icon of three horizontal bars in blue and red to the left of the word "cohesion" in a white, lowercase, sans-serif font.

# Complete PEO Software

...for your entire business

# Advanced Digital Services Get Your Clients in Total Compliance



All three services help satisfy New York's digital posting requirement.

No longer are labor law posters on a breakroom wall sufficient. Today, businesses need additional solutions to maintain complete posting compliance with onsite and offsite workers.

**Poster Guard E-Service** provides easy, online access to digital postings required at the federal, state, city and county levels and notifies employees by email.

**Intranet Licensing Posting Service** uses a link placed on a company intranet to provide access to all mandatory federal, state, city and county posters.

**Mandatory Employee Handout Service** provides online access to a comprehensive database of applicable employee notifications at the federal, state and local level, which can be downloaded as needed.

Our innovative offerings set the standard for the industry.

*Protecting your business is our business – no matter what.*



Learn more, call 954-970-5611 or visit [www.posterguard.com/PEO](http://www.posterguard.com/PEO).