Part Human Resources, Part Superhero: HR's New Role In Our Digital Era

5 tips to guide you through the journey

By Ammon Curtis

It's raining in Baltimore.

Janice is stuck on the Jones Falls Expressway, lost in thought. Should she switch slide 5 with slide 9? How are the new trainees doing? Were reservations for 7pm or 7:30pm?

The phone rings. Janice normally wouldn't answer, but she recognizes the ringtone. It's the CEO of her company, and he is panicked.

There was a data breach, and there's reason to believe every employee record was compromised. They've brought in an outside party to investigate, but the data may already be on the dark web. Many of the details remain unclear, but she should brace herself for a worst-case scenario.

It would be understandable if Janice was paralyzed in the moment. After all, most people would be. Luckily, Janice isn't most people.

She is an HR professional, one who understands the threats of today's digital era. And she committed long ago to protecting her employees from the hackers, cybercriminals, and identity thieves that mean to cause them harm.

In short, Janice is a superhero. And the good news is, she's not alone.

HR Professionals Understand the Danger of Identity Theft

When you're in the identity protection industry, giving presentations becomes a part of your DNA. We spend a great deal of time educating the public on a wide range of topics — from the rise of botnet attacks to employee privacy settings and everything in between.

Last year, we decided to do things a bit differently. When hundreds of HR decision makers signed up for our presentation on emerging cybersecurity threats, we knew we were presented with a unique opportunity.

In addition to arming HR professionals with the knowledge they need to protect their employees and company, we could also survey participants to better understand how they use technology, gauge their knowledge about employee identity theft, and identify what steps their employers are taking to protect their workers.

The data revealed a number of key insights, and it reinforced something we've known to be true for quite some time: HR workers are among the most knowledgeable of all employee groups. For example, 85 percent of respondents understood human error poses a greater risk than hackers and cybercriminals combined.

Image credit: InfoArmor

Our findings also highlighted the number of challenges HR workers face when it comes to protecting their employees and company.

Despite the fact that 73 percent of HR professionals personally know a victim of identity theft — or have been a victim themselves — just 35 percent of organizations currently offer employees the protection they deserve.

As we explained to the audience that day, this doesn't have to be the case. There are immediate actions you can take to raise awareness, gain C-suite buy-in, and protect your employees.

Not Every Superhero Wears a Cape

You don't need x-ray vision, a magical lasso, or an invisible jet. But, you will need superhuman focus. While this might seem overwhelming at first, the following tips are designed to guide you through your new journey.

#1 Educate Yourself and Others

Arm yourself with the knowledge you need to secure leadership buy-in. You can find a number of great resources on identity theft and employee data protection. Just keep your audience in mind.

Discussing the financial impact identity theft has on a victim works well for raising employee awareness, though it might not be as effective when discussing the topic with your CEO or CFO. Instead, a data-driven approach will likely work best.

Consider offering the following stats:

- As much as 50 percent of identity theft cases begin at a victim's workplace, increasing employer liability

- Employee identity theft can quickly lead to a disengaged workforce, often causing employers to experience:
  - 20 percent fewer sales
  - 17 percent less productivity
  - 21 percent lower profitability
  - Between 24 and 59 percent higher turnover
  - 70 percent more employee safety incidents
- Americans now rank criminal hacking as the greatest threat to their safety, and 60 percent of millennials expect their employer to protect them

#2 Create a Data Breach Response Plan

For most organizations, it's not a matter of if a data breach will occur. The better question is, when? Hackers, cybercriminals, and identity thieves are targeting businesses like never before, and companies benefit from adopting a proactive approach to risk management.

One of the most important steps you can take is to create a data breach response plan.

Keep in mind, this isn't something you can do in isolation. You'll need to work with key leaders across all departments, especially IT. If budget allows, you might want to consider working with an external organization that specializes in corporate data breach preparedness.

#3 Analyze Current Data Collection Policies

It's critical to routinely analyze your data collection policies and evaluate who has access to employee and customer records. This often means conducting both internal and external audits. In our poll, more than two-thirds of respondents said their organization shares employee data with at least one outside party.

#4 Offer Robust and Ongoing Training

As we discussed in our first tip, education will play a key role in protecting your company and its employees. Just remember that a one-and-done approach doesn't work. You should offer training to all employees, including senior leadership, on an ongoing basis.

Topics might include:

- How to avoid phishing scams and malware attacks
- Best practices for privacy and sharing settings
- Accessing sensitive corporate and employee data
- The benefits of employee identity protection
- Department-specific risks and opportunities

#5 Stay Vigilant

Nearly every week, there are reports of some new, widespread data breach — from the hotels we visit, to the doctors we see, and the social media accounts we use to connect with friends, family, and associates.

It's easy to grow fatigued in our current climate. That's why the most powerful step you can take is to always stay vigilant.

This can be challenging. If you're like most HR folks, you chose this profession because you wanted to help employees unlock their full potential, protect them and their families from danger regardless of where it might arise, and make a difference in your company, community, and the world.

Even if this doesn't describe you, you probably didn't enter the HR field because you wanted to combat cybercrime. Yet, that's what the role requires in our digital era — and there's no one better suited to handle the challenge.

You might not have a cape, but the good news is you don't need one. You're already a superhero.

• • •

Ammon Curtis is the Executive Vice President of Product, Marketing, and Design at InfoArmor.

Would you like to comment?

Submit Your Articles

InfoArmor

Not every **superhero** wears a cape.

Defend your organization with PrivacyArmor®, the most advanced identity theft protection available.

In-house **24/7** resolution

Seamless integration with **140+ platforms**

99% client satisfaction rate

Schedule your free demo