How to Avoid Becoming a Security Breach Headline

HR's Unique Role as a Cybersecurity Partner

businessolver

Introduction

Nearly every week, we hear about a company's security system being breached. Social Security numbers are stolen. Credit card accounts are hacked. Customer and employee information is compromised. The headlines reporting security attacks are so commonplace, you almost begin to wonder what you'll do when, not if, it happens to your company.

Unfortunately, we seldom hear about the attacks that were prevented, which is too bad. HR professionals often deserve much of the credit.

By working with your IT department and senior leaders, HR professionals like you can help keep your company safe from some of the most dangerous criminals out there. All it takes is a commitment to building a culture where cybersecurity is a natural part of everything you do.

In this guide, you'll learn strategies to help you:

- Build a Cybersecure Workforce
- Select Secure Benefits Administration Technology
- Keep Your Employees Safe at Work and Home

Culture Collaborator:

Your IT department and senior leadership need your help in creating a cybersecure culture across the organization.

Building a Cybersecure Workforce

As an HR professional, you know that one of your organization's greatest assets is your people. That's why your role is so important when it comes to protecting your organization against cyber threats. As a recruiter, educator, and culture creator, you are uniquely qualified to help your IT team develop a "human firewall" to keep the bad guys at bay.

Like a technical firewall that blocks unauthorized access to your data from external hackers through email filtering, gateways, antivirus software, and other tools, your human firewall introduces a layer of security for which humans are uniquely qualified. It's all about being watchful and taking appropriate action to prevent and respond to threats.

Just as your employees are among your organization's greatest assets, certain individuals also represent your greatest threats. Without a well-trained human firewall in place — one in which every "brick" is equally strong — your entire organization can be compromised by the simple click of a mouse. All it takes is one employee clicking, downloading, or sending the wrong thing to the wrong person, and you've become a security breach headline.

Most of the time, the actions that lead to employee-based breaches are unintentional. Like all "accidents," however, they can be prevented by following some basic strategies. In this section, we offer the five most important.

Asset Activator:

Your employees are your greatest asset. By working with your IT team, you can help develop a "human firewall."

1. Train Early and Often

Off-the-shelf cybersecurity training modules are a great place to start. Look for one that addresses the unique security threats your company faces. A trucking company will have different needs than a hospital. After you have identified the most appropriate curriculum, find a way to introduce it during new employee orientation.

Most importantly, reinforce the teaching points or expand upon periodically. Cyber-attacks have no season. This will help you develop a sustainable cybersecure culture that is on-call 365 days a year. As you execute on your training plan, make sure to get feedback from leaders to determine whether staff have internalized the practices you've advocated. Ask them, for example, how often the issue of security is raised when employees are speaking with one another.

If your teaching points appear regularly and in the context of protecting the company, keep doing what you're doing. If not, consider increasing the frequency of your educational efforts or look for more impactful teaching methods. Remember, culture is not created overnight.

2. Test Your Employees

One way to develop an intrinsically driven cybersecure culture is to allow employees to learn from their mistakes. **The best teacher is experience, but the landscape of cybersecurity is no playground.**

At Businessolver, we regularly test our employees by sending them fake phishing emails — messages purporting to be from a reputable sender that persuade the recipient to share information such as passwords, bank account information, and the like. Every so often, we randomly select a portion of our employee base to receive an email that looks legitimate but that has certain tell-tale signs of a phishing attempt.

If an employee falls for the stunt, they receive a message telling them they made a mistake but, fortunately, did so in a safe environment. Those who report the message receive a reply recognizing their vigilance at identifying a security threat and taking appropriate action.

3. Develop Policies

Providing employees with realistic opportunities to practice their skills can build habits that last a lifetime. But, those strategies take time. The bad guys move fast, making a strong case for non-negotiable cybersecurity policies.

Some tasks can be hard-wired into certain applications. Individual employees should, for example, get periodic prompts to change their password or be prevented from accessing certain applications until they complete a multifactor authentication process (e.g., physically entering a code delivered through a secondary medium such as text messaging).

At the programmatic level, however, policies are sometimes misinterpreted or reprioritized. A manager may forget to demand periodic audits from their vendor or update their technology for storing data. **As an HR professional, part of your job is to ensure that all policies are followed, whether they impact 100% or 1% of your employees.** Remember, a cybersecure workforce is only as strong as its weakest link.

4. Monitor All End-Points

As you go about creating a cybersecure culture, you'll need to understand some, not all, technical aspects. One such detail is endpoint security. Also called endpoint protection, this concept pertains to protecting all "endpoints" (e.g., servers, laptops, smartphones, etc.) connected to the corporate IT network. **Endpoint security allows your IT department to monitor employee activity with respect to their job duties.**

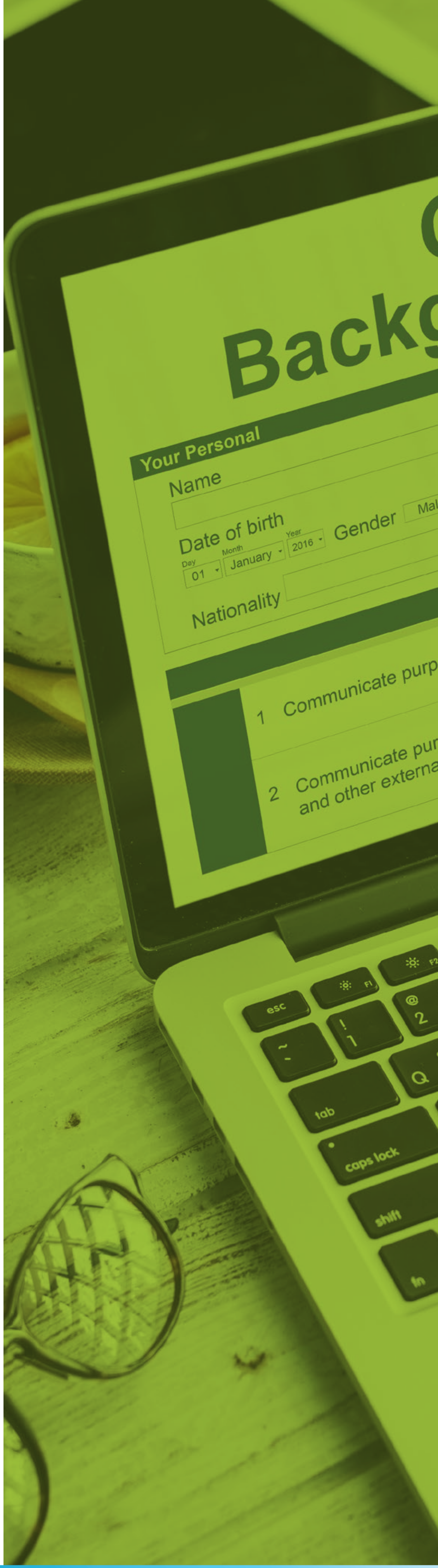
If, for example, a service center representative is doing something on an endpoint that is not normal given their job description, your security team is alerted. When that happens, it's easy to get caught up in the moment.

When approaching employees about possible misuse, take a "trust, but verify" approach. Start by assuming positive intent but be thorough in your investigation and follow-up.

5. Screen Your Employees

Background checks are now considered a standard part of the pre-employment process. Some companies, such as Businessolver, conduct background checks on every employee annually. **Regardless of how often you screen your employees, find a vendor that suits your unique business needs.** Find out their level of flexibility and whether they have a menu of services that allow you to select the right level of screening for each job description.

Also consider how connected the vendor is in terms of their established integrations with critical information sources, including those outside the U.S. Data privacy should also be on your checklist as well as the vendor's ability to integrate with your existing HR systems.



Choosing Secure Benefits Administration Technology

HR leaders are increasingly being asked to dive into the murky waters of HR technology and data security. And, they must somehow be able to discuss what they find with their IT team and the C-suite, especially when considering a new benefits administration technology vendor.

As software-as-a-service (SaaS) platforms grow in popularity, it becomes increasingly tempting to gravitate toward vendors with a certain degree of brand recognition and assume that other companies have already done the work of evaluating these solutions from a cybersecurity perspective. That, unfortunately, is a common misconception — and one that could result in your becoming a security breach headline. **Ultimately, you must evaluate your options based on your organization's unique security threat model.** What worked for one company, may not work for yours.

Due diligence in selecting an HR technology provider starts by writing a request for proposal (RFP) that will get you the information you need. Although writing an RFP can be a daunting task, it can also be exciting. **After all, it's really a wish list — a grown-up letter to Santa about everything you need (and deserve) to do your job and impress your boss.** But before you start listing up all the bells and whistles you've been dreaming about, start with your non-negotiables, like security.

In this section, we offer five tips to help you plan, research and select a benefits administration platform that best suits your needs.

Consultative Coordinator:

Don't go it alone. Listen to your IT team. Involve them in creating your RFP. And, invite them to review the submissions you receive.

1. Involve Your Security Team

When security is a non-negotiable, IT needs to be at the table. The last thing you want is to narrow your search to three finalists after months of searching only to find that none meet your security team's requirements. **By involving risk management specialists early and often, you'll get more than an idea of their minimal security requirements; you'll also gain a deeper awareness and appreciation of the risks associated with collecting, storing and accessing benefits information.**

Your discussions might even prompt these subject matter experts to revisit security issues they haven't considered in a while, thereby strengthening their value as a partner in your RFP process and the overall security of your organization. Also, make sure to include your risk management specialists on your review team. They'll know the follow-up questions to ask.

2. Demand Cyber Insurance

Didn't know this existed? It does and it's worth it. Vendors who carry cyber insurance protect their customers against internet-based risks such as data destruction, extortion, theft, hacking, and denial of service attacks. Coverage often includes losses due to errors and omissions, failure to safeguard data, defamation, post-incident public relations expenses, investigative fees, and even criminal reward funds.

It is important to note that not all benefits administration platforms offer cybersecurity insurance. The reason for this is the increasingly stringent requirements insurance companies place on vendors to qualify them for coverage. If the vendor cannot demonstrate they are a good risk, they can't get coverage.

3. Ask for Proof

Just as an insurer would ask your vendor to prove that they are a good risk, so should you. **When going to market for a new benefits administration platform, make sure your RFP requires the applicant to concretely demonstrate their skills, experience and practices.** Examples might include evidence about how they protect your data when it isn't moving through systems, what kind of technical controls they use to ensure appropriate data acquisition and use, or how they vet their employees.

Once the proposal comes back to you, ask the risk management specialists on your review panel to pay special attention to the voracity of any security-related claims made by the vendor. If you need more or different kinds of evidence to back up the vendor's claims, ask for it in your follow-up questions.

4. Confirm Resources

As you consider a benefits administration solution provider, resources like customer service are almost certainly near the top of your list of requirements. It's easy to imagine what "great" looks like because your experience has provided you with some context. **Security works in the background though, making it a little more difficult to determine how your needs will be met.**

Again, engage your IT team to determine the kind of resources you'll need from the vendor to ensure that all your security needs will be met, including the number of people who will be assigned to your account, their qualifications, their length of time with the organization and other details that will give you the confidence to move forward.

5. Determine Stability

Considering the pace at which technology and the business of technology moves, partner stability deserves special consideration when going to market for new HR solutions. **Make sure your RFP helps you determine the applicant's long-term viability during the life of your contract with them.**

Consider factors such as financial strength, staff turnover rates, growth history, plans for expansion, and other factors. Also ask yourself whether you might be impacted by any disruption caused by recent or potential mergers or acquisitions.

Keep Your Employees Safe at Work and Home

Ultimately, cybersecurity comes down to personal accountability. Your role as an HR professional is to ensure employees know what is expected of them to keep your organization from becoming a security breach headline. You also bear some responsibility to ensure your employees' cyber habits at home or on their personal devices prevent them from running into trouble that could jeopardize their work life. Stolen identities and hacked bank accounts can cause stresses that have a major impact on personal and team productivity.

Your role as an HR professional makes you uniquely qualified to offer the kind of training your employees need to stay safe at work and home. But, where do you begin? In all honesty, there are hundreds of tips you could offer your employees. But that would be overwhelming and result in very few changes in employee behavior. Worse, it could turn them off completely and make them care even less about cybersecurity.

But 5 is a manageable number. Here are our top recommendations:

Partner in Protection:

As a trainer and natural communicator, you are a valuable partner in protecting your employees at work and at home.

1. Slow Down and Think

Whether on the clock or off, technology hasn't done us many favors in getting us to slow down. And the bad guys know this. That's where employer-sponsored fake phishing expeditions, as introduced in chapter 1, can help.

Failure to slow down and think can spell disaster in the office and at home — and it can happen in the blink of an eye. You can't "unclick" the link that installed a virus on your company's network or "untap" the icon that sent your bank details to who-knows-where.

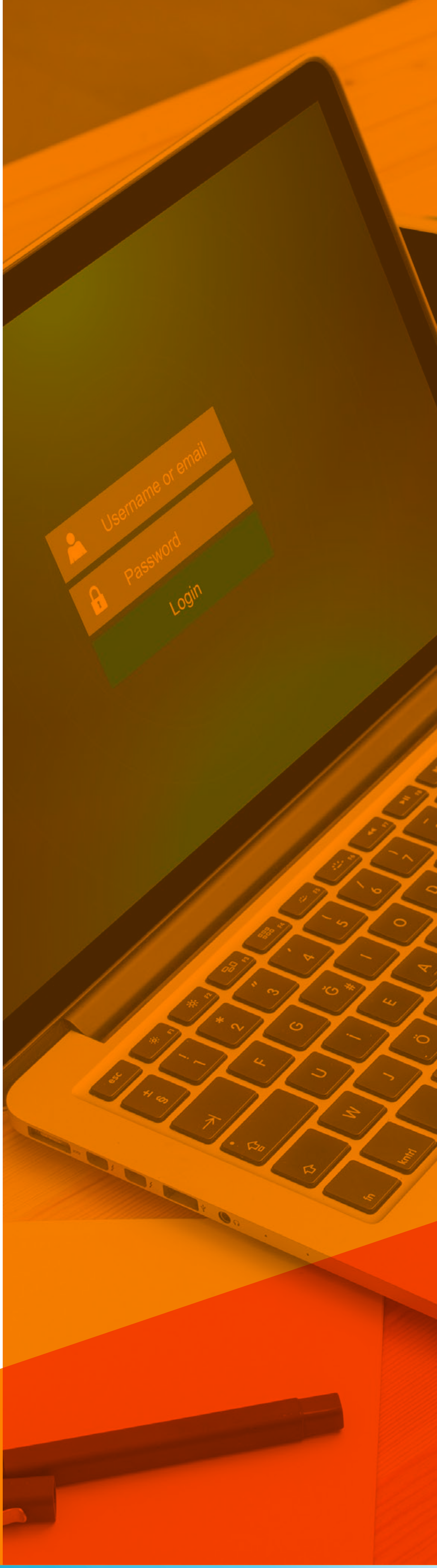
Slow down. Think.

Got questions? Ask before you act. Especially when the message sounds too good to be true, conveys a sense of urgency, or appears to come from someone you know. Slow down. Think. Ask.

2. Use Long Passwords

Here's something fun. **Google "correct horse battery staple" for a great comic strip about password length and complexity.** Spoiler: it would take a computer 550 years to guess that string of four simple words is the key to your work email.

By comparison, a password of 11 characters, including numbers and symbols, could be guessed in just three days. In fact, it's more likely you'd forget that password before a computer could guess it. But "correct horse battery staple"? You probably wouldn't even need to write that one down.



3. Keep Your Passwords Safe

The safest place to keep a password is in your head. Using the same password for multiple accounts, however, is risky, leaving us with the challenge of having to memorize dozens upon dozens of passwords at work and in our personal lives.

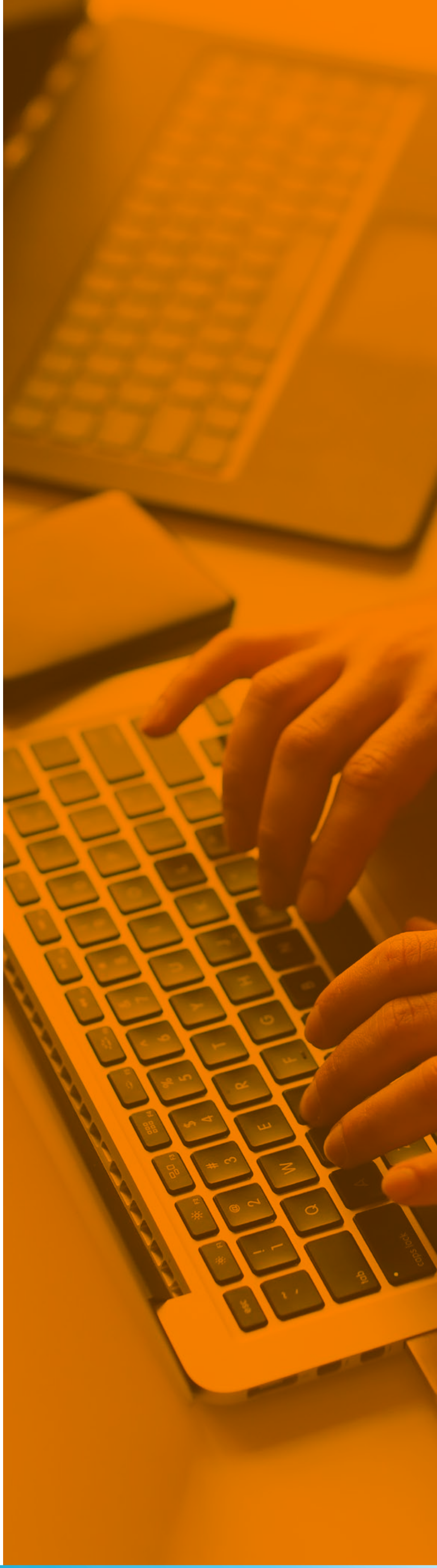
Using a password manager can help. These simple yet secure applications act as a vault for all your passwords that can be opened and accessed using a key or master password. If your employer won't allow you to use a password manager for your work accounts, decide where to store your passwords based on your unique security threats. For example, handwritten notes kept in a locked office may work, but not if the night cleaning crew has access to that physical space.

Whatever you do, do not store your passwords in a spreadsheet or email them to yourself. One hack, and all your accounts are compromised.

4. Consider a Credit Lock

When a bad guy gets hold of your personal information, they're usually looking for a way to monetize it. Opening a credit card in your name is one of the most common ways in which this is done.

While it's always better to prevent your information from being accessed in the first place, locking your credit is a great safeguard. Also called a credit freeze, the idea is simple and federally mandated as a free service from all three credit bureaus: Equifax, Experian and TransUnion. After confirming your identity, each credit bureau will provide you with a code you can use to freeze and unfreeze your credit report as needed, thereby preventing anyone else from opening an account in your name.



5. Protect Yourself on Social Networks

Taking the family to Switzerland next week? Put that on Facebook and you just might come home to a house that has been burglarized in your absence. **It sounds like common sense, but people share this information all the time without thinking.**

Again, slow down. Think.

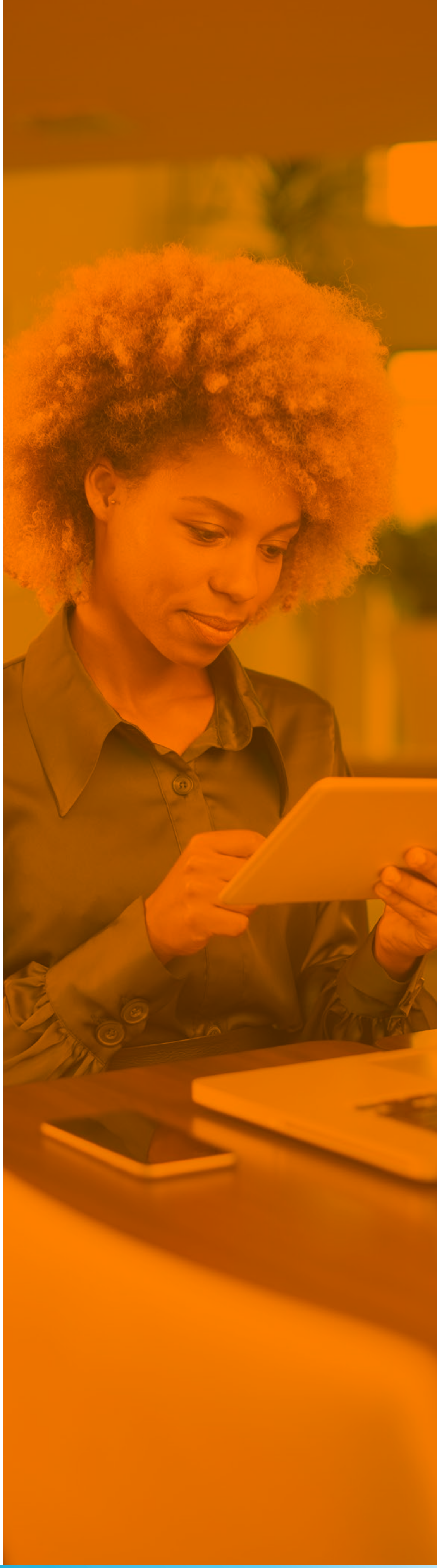
Other tips to keep your employees safe on their professional and personal social media accounts include accepting friend requests only from people you know in the "real world," managing your privacy settings, turning off the GPS function on your smartphone's camera and closing old accounts you don't use anymore.

Conclusion

Technology moves fast and so do the criminals. To avoid becoming a cybersecurity headline, your HR and IT teams will have to make a long-term commitment to protecting your organization by understanding your unique security threats, training your workforce, selecting the right technology, and empowering your employees with the knowledge they need to keep them safe at work and home.

As you continue developing your business acumen around cybersecurity, remember to keep the communication lines open. Your IT department is an important partner and they will appreciate the skills you bring to the table as a culture creator. The executive officers and decision makers also need to be engaged; failure to do so could result in a headline you don't want and a conversation you'd rather not have.

Lastly, you and your vendor must have a shared interest in the security of your data and system. Make sure you choose one who knows your unique security threats and can prove to you that they can provide you the level of service you need.



Wrap Up:

To avoid becoming a security breach headline, remember these basic principles and follow these simple steps.

Build a Cybersecure Workforce:

- Train Early and Often
- Test Your Employees
- Develop Policies
- Monitor All End-Points
- Screen Your Employees

Select Secure Benefits Administration Technology:

- Involve Your Security Team
- Demand Cyber Insurance
- Ask for Proof
- Confirm Resources
- Determine Stability

Keep Your Employees Safe at Work and Home:

- Slow Down and Think
- Use Long Passwords
- Keep Your Passwords Safe
- Consider a Credit Lock
- Protect Yourself on Social Networks

Additional Resources

Check out “**Password Protected: A Cybersecurity Toolkit for Employers”** for more tips and best practices.

Password Protected:

CYBERSECURITY

Toolkit for Employers

77%
of organizations lack a cybersecurity plan

A successful **online hack occurs every 39 seconds**[1], and human error—including insecure usernames and passwords—account for about 90%[2] of the blame for breaches. Yet, with more employees working remotely than ever before due to the pandemic, **77% of organizations lack a cybersecurity plan**[3].

During **Cybersecurity Awareness Month** (October), Businessolver offers employers tools and resources to keep employee and business data safe year-round—with a three-pronged approach to cybersecurity:

Technology

Culture

Partnership

businessolver®

Market-Leading Benefits Technology +
Innovative, High-Touch Services

businessolver.com