SECURITY IN HR

BROUGHT TO YOU BY workbright

TABLE OF CONTENTS

ABOUT THE AUTHOR

WorkBright's (formerly All4Staff) mission is to empower companies to be great employers by equipping them with HR technology that makes life easier and employees happier. Currently, our products help businesses that are rapidly, seasonally, or just plain constantly hiring by taking the cumbersome and paper-heavy process of onboarding and putting it all online! New employees can fill out documents (W4s, I9s, and more), upload photos of licenses or certifications, and digitally sign from any web-enabled device before they arrive for their first day. Learn more at www.WorkBright.com.

LET'S START WITH A TRUE STORY

ALL NAMES HAVE BEEN CHANGED TO PROTECT THE IDENTITY OF THE PARTIES INVOLVED BUT EVERYTHING ELSE IS 100% FACTUAL AS TOLD BY THE VICTIM

Diane had been the Chief Financial Officer for a major industry trade organization for 10 years when she went to file what seemed like a very normal tax return. So you can imagine her surprise when her refund was rejected because it had *already* been filed. She called the IRS and they quickly agreed she had been *the victim of identity theft!*

The very next day, one of her staff members briefly said in passing, "the weirdest thing happened, we got a check in the mail from the IRS and we haven't filed our taxes yet". **RED FLAGS** shot off in her mind and she quickly sent an email to all staff asking if there was anyone else that had experienced something similar. Her intent was to lend a helping hand having just learned quite a bit about the scam. However, when dozens of employees came forward to say they had the same thing happen, Diane knew there was something bigger going on and it was time to get the authorities involved.

ATTEMPTS HAD BEEN MADE TO FILE FRAUDULENT RETURNS ON BEHALF OF NEARLY ALL OF THEIR 100+ STAFF MEMBERS

By the time it was over Diane and her company were involved with the IRS Criminal Investigations Unit, the FBI, the Secret Service, and a few local authorities who determined that attempts had been made to file fraudulent returns on behalf of nearly ALL of their 100 staff members. It was late in the tax season so most were rejected due to the rightful party having already filed, but they were able to determine that whoever was responsible for the breach **had access to the employees W2s.**

What was the scheme?

It's called Tax Identity Theft, and in 2014 there was a 66% increase in the number of criminal investigations linked to this type of scheme. In fact, the IRS recently increased the number of staff working to identify and prevent tax identity theft to over 3,000 employees. In total they've caught 14.6 million suspicious returns since 2011.

In this eBook, we will go through some of the steps Diane took to investigate how her employees' W2s were compromised. She and her staff have spend countless hours working out the details, but - *spoiler alert* - because these schemes are very complicated and there are so many breaches happening every minute, her case is still unresolved.

One interesting thing to note is that with the help of the IRS Scheme Development Center, which works to identify patterns in identity theft related crimes, she was able to narrow down the likely vulnerability to a particular filing that was made - an energy credit used to bump up the refunds. This same vector was used to steal information from 5 other companies, meaning **whoever stole the information from Diane's staff, likely did this same thing to thousands of employees nationwide.**

The worst part: even though the case has been opened for over a year, the effects of the breach are ongoing. Even after Diane instructed employees to file form 14039, showing they were victims of identity theft, many of them did not. And the next year when these employees went to file their 2014 returns - the same thing had happened!

AND THE SCARY PART IS

YOU COULD BE RESPONSIBLE

To put it frankly, **the last 3 years have sucked for data security and privacy.** We all heard about the super high-profile breaches:

- Target lost 40M financial access records (2013)
- Home Depot lost 109M financial records (2014)
- Ebay lost 145M financial records (2014)
- Anthem lost up to 80M records (2015)

And that's just the tip of the iceberg! Goodwill, Jimmy Johns, Chase, Neiman Marcus, Michaels, Dairy Queen, PF Changs, UPS, Kmart, and Staples were all on the list along with hundreds of others. If you're thinking "Yeah, but those are all retailers losing credit cards...", Then let's talk about one of the most highly publicized hack of them all - Sony.

Sony "only" lost 47,000 records and "only" had $15 million dollars in damage, but what makes it unique to all the others above was that the Sony hack was **primarily HR files.** And the HR managers at Sony, while not responsible for the hack itself, may share part of the blame for unwillingly providing the stepping stones which allowed the hack.

Many people were hurt personally and professionally by the breach; from A-list celebrities who are clients of Sony, to everyday employees in each department. One of the hacked employees reported her credit card number was being used to buy handbags on Rodeo Drive; another was told his bank information was being used to apply for new credit cards. And over the course of the next several months up to **38 million files** were released including personal information, social security numbers, profit-and-loss statements, pilot scripts, emails and more.

Over half of attacks last year were identity theft. And the sad truth is that "more and more organizations are accepting the fact that despite their best efforts, security breaches are unavoidable." But there IS hope. The 2014 Breach Level Index Report states, "If organizations know how the attacks were conducted and by whom, they can take proactive steps to better protect themselves against similar intrusions and loss of data." So stick with us and read this guide to help you better prepare against security breaches in your organization and in your life.

2014 DATA RECORDS LOST OR STOLEN BY FREQUENCY

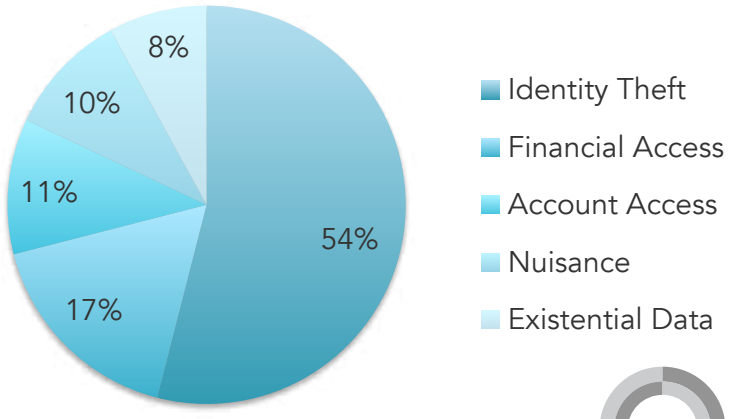
EVERY DAY
2,803,036

EVERY HOUR
116,793

EVERY MINUTE
1,947

EVERY SECOND
32

Incidents by Type in 2014



THE HR PROBLEM

As HR professionals, we are DEFENDANTS of vast amounts of personal and sensitive data (see the image below). And how many HR professionals have received prior training in Information Security Awareness? Our polls indicate that it's less than 10%. Unfortunately, this gap comes from historic thought processes that security and data privacy are largely IT issues. As we have started to illustrate, that is no longer the case. **It only takes ONE piece of personally identifying information to steal an identity**... and think about how many social security numbers you've seen!

IDENTITY THEFT

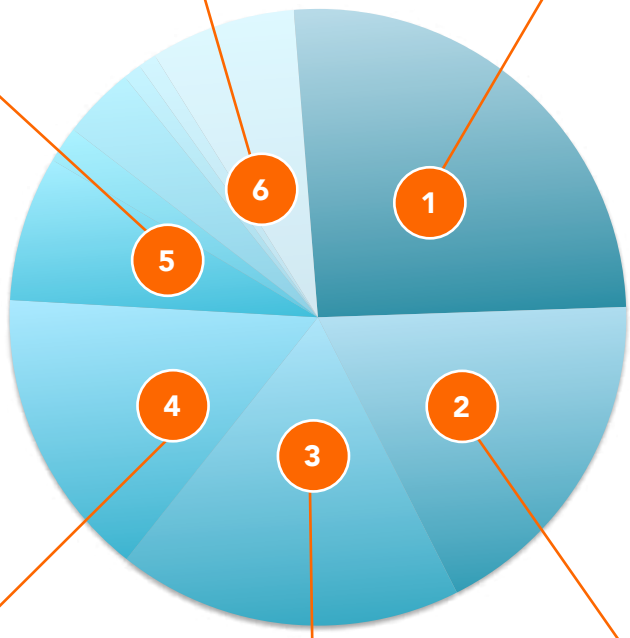
Ask most people HOW identity theft happens and the response will be "hackers." According to the 2014 Verizon Data Breach Investigations Report, 92% of the incidents seen over the last 10 years (and 94% of the breaches in 2013) can be described by nine simple patterns. And the most used methods just might surprise you...

OTHER - 11% COMBINED

Types of breaches include: DoS Attacks (2%); Card Skimmers (1%); Cyber-Espionage (1%); POS Intrusions (1%); and Everything Else not included in these forms listed.

WEB APP ATTACK - 8%

Feel like you have to change your password every time you log-in? That's because there are password cracking programs that can try over 1,000 password combinations PER SECOND to guess your login information to the financial and personal systems you use everyday. More on passwords later.



MISC. ERRORS - 27%

The most common way that personally identifiable information is released is through Miscellaneous Errors. And if you think your safe because you keep hard copies of files - think again! 49% of miscellaneous errors involved PRINTED documents. Here are some examples:

- Emailing the wrong person on accident or mistyping info
- Leaving paper in the photocopier
- Reciting confidential data in a public setting
- Throwing confidential information in the recycling
- Forgetting sensitive hidden columns in a spreadsheet

THEFT & LOSS - 16%

When something like your personal cell phone gets lost or stolen, your first reaction is probably to think about the personal inconvenience. But consider this: if your item gets in the wrong hands, it may be used as a stepping stone to access work accounts, bank info, friends information, and more. This past year, 43% of theft/loss happened at work. Ask yourself, if a personnel file goes missing from a filing cabinet, how long will it be before you notice?

CRIMEWARE - 19%

Also known as Malware, Viruses, Phishing scams, etc. While new crimeware pops up everyday, this is actually one of the more straight forward vectors you can protect yourself against (we'll cover this in more detail in Best Practices). For now, just know that the majority of crimeware installations happen via WEB ACTIVITY, not links or attachments in your email inbox. This is a complex issue so see the next page for more details on types of crimeware.

INSIDER MISUSE - 19%

Insider misuses occurs when you share an account to a critical business system or loan someone a key. To paraphrase a great post from HRHero, "Even for all the increased reliance of networked computing, the most common scenario appears to be when a single employee gains access to the hard, paper version of personal information about the company's other employees or customers."

IDENTITY THEFT CONTINUED

Before we jump in to best practices, we want to spend a little more time on malware, viruses, and phishing scams. Crimeware may be targeting your HR files, but it can be brought in to your organization from any employee, simply browsing the web. It is crucial you understand how these work so you can educate your staff about safe web (and phone) activity. To begin, let's think of the crimeware on a scale of sophistication. The more targeted the crimeware, the more sophisticated it gets:

NOT SOPHISTICATED ——— **VERY SOPHISTICATED**

On the low end of the scale, we have phone phishing scams. Con artists use auto-dialers to dial hundreds of numbers per hour until someone picks up and they tell you a lie like, "this is your bank, we see fraudulent activity and need you to verify your credit card information". It's simple, but in 2014 the phone was the #1 method of contact coming in with 36% of all complaints according to Fraud.org.

In the middle, we have an internet phishing scam which injects a new tab to your internet browser that LOOKS like (for example) it's your bank's login page. Once you enter your information, it directs you to your bank's homepage. "Weird", you think to yourself. But you ignore it and log back in to the real bank page unknowingly having just given away your login information to a malicious source.

If those don't scare you, have you ever gone to a coffee shop and connected to the store's WiFi? Even though the network name is (for example) "Starbucks" it could be posing as an "Evil Twin", recording every keystroke you make. This means if you log in to Facebook, email, bank, anything while connected to that WiFi, your information may be compromised. Lesson: ask a barista for the WiFi name.

A LIFE THREATENING KIND OF IDENTITY THEFT

Your health insurance information or Social Security number is used to get health care & treatment

Crimeware or personal theft can be used for a newer kind of identity theft: Medical. This is the fasted growing type of identity theft, and an AARP study found that stolen health insurance cards and information are being sold on the black market for $500 - $600 a piece. In Medical Identity Theft, your health insurance information or Social Security number are used to get health care and treatment. This can potentailly be LIFE THREATENING because it alters your medical history. For example, if the person who stole your card has a different blood type and you are later in a trauma related incident, you could be unknowingly transfused with the wrong blood type.

BEST PRACTICES TIPS & TRICKS

If you've used the table of contents to skip ahead to this section, then stop - go back - and read the first 5 pages of this book. We are thrilled to provide you with actionable, practical tips and tricks to protect yourself and your staff against security breaches. However, as we illustrated on the previous page, over half of all breaches are covered by three simple patterns. Understanding WHAT are the stepping stones to identity theft, and HOW these types of breaches occur is your first line of defense against an attack.

MAINTAIN A MINDSET OF SECURITY

If you are still with us, then great! We are so excited to show you some real world examples from HR professionals like yourself. You should use these and implement them with your staff TODAY! Before reading these, we want you to understand that this is not a catch-all. Even if you follow every trick in this book and are the most secure HR professional out there, a breach can still happen. Every person who holds sensitive information could be responsible, even if they have NO malicious intent whatsoever.

What do we mean? This is a true story from our CTO that happened just last month. While ordering Chinese food over the phone, the woman taking the order kindly said, "Can you hold please?". Of course he obliged, but instead of actually being put on hold, the woman simply put the receiver down and picked up a second phone at the restaurant. At that point, he could hear every word from the busy kitchen staff, the clanging of pots and pans, and of course, the woman on the second phone. On that second line, after taking the order, the woman proceeded to REPEATE aloud every single digit of their credit card (expiration and all) to the point where the kitchen staff, our CTO, and anyone else in ear shot could have easily written it down. The unwitting customer was none-the-wiser that their credit card information was mishandled and may now be compromised.

Imagine the damage that could do if that were your office administrator ordering lunch for a staff meeting. It could take months to recoop money spent before the breach was discovered and many headaches reissuing cards, changing recurring billing statements, and identifying other information about your Company or employees that had been compromised. That's why these following tips and best practices are so important. They will not only help you be proteced against an attack, they will help limit the reach of a breach if one should occur in your organization.

BEST PRACTICES
PASSWORDS

"Sorry, your password must contain a capital letter, two numbers, a symbol, an inspiring message, a spell, a gang sign, a hieroglyph, and the blood of a virgin"

Ever feel like the password policies have gotten ridiculous AND you have to change your password just as soon as you started to remember what it actually was? You're not alone, but if you're thinking that we are going to write about how important having complexity in your password is, we just may surprise you. Take a look at these two passwords, which one do you think is more difficult for a hacker to break through? Psst... don't cheat and read ahead, just play the game:

Option 1: **Tr0ub4d0r&2**
Option 2: **batteryhorsestaplecorrect**

If you've been paying attention to the password policies implemented on most sites you would probably say Option 1 is more secure. However, remember the automated web attack programs we discussed on page 5 that guess thousands of combinations of passwords per second? It would take one of those programs just 3 days to crack Option 1 (at 1000 guesses per second - and that's conservative). Option 2, however, would take 550 YEARS to crack (at the same rate of 1000 guesses per second)! Why? The answer has to do with the mathematical notion of entropy (randomness), but effectively it comes down to the length: Option 2 has 25 characters vs Option 1 has a mere 11. So there are two big tips from this example:

Tip 1: Length beats complexity
Tip 2: Think about PassPHRASES not PassWORDS

Think that sounds even more complicated to remember? It doesn't have to be. We are HUGE fans of Password Managers. There are lots of options out there (1Password, LastPass, Dashlane, to name a few) and they are all easy to use and highly secure. The most important advantage password managers give you is the ability to assign different passwords to each of your online accounts. Then, if one of your accounts is compromised, the damage is limited in its scope - hackers will be unable to use that same password to gain entry to other accounts.

If you choose not to use a password manager, at the very least, assign a separate password to your email accounts. Your email is the gateway to resetting your password on just about every other service you sign up for (via "Forgot your password"). Don't let your email get compromised.

Tip 3: Use a Password Manager
Tip 4: AT THE VERY LEAST use a unique password for your email

BEST PRACTICES
2 FACTOR AUTHENTICATION

Wouldn't it be great if intruders couldn't access your bank account or email account even if they stole your password? Turns out, there is a way: 2-factor authentication (or sometimes: multi-factor authentication or MFA/2FA). You've likely used it when already when a service (such as your bank account) sends you a text message with a security code that needs to be entered before logging in! It's usually turned off by default, but you can enable it on most major web applications, including email, banking, finance, file storage and more (full list at twofactorauth.org). It works is by requiring two pieces of identification instead of just one: your password (something you know) and your phone (something you have). So, even if a hacker stole your password, they wouldn't be able to access your account (since they don't have your phone to receive a text message). Plus, you would be alerted that sometime was trying to login as you.

Tip 5: Use 2 Factor authentication & favor websites that offer 2FA

BEST PRACTICES
YOUR DEVICES

Speaking of your devices, you really need to be locking your screen! As we learned earlier, 16% of identity theft cases started from personal theft or loss. Putting a passcode on your cell phone and laptop could be the difference between a minor inconvenience and a life-shattering identity theft case. Some companies even require that passwords be set on both company issued AND personal devices because of the constant connectivity employees have with their work accounts. Consider it.

Tip 6: Lock it down!

Most people use "Find my iPhone" or "Device Administration" (on Android) to be able to locate their phones in the event of theft or loss. And that's a great reason to use it! But not many people know that these features can also be used as a REMOTE KILL SWITCH. This means you can completely erase all data on your phone from a remote location the minute that you realize your device is missing.

Tip 7: Turn on remote kill switch

There is a feature built in to all Macs and Windows 8+ devices which automatically encrypts your files so that even if your laptop is stolen, hackers can't rip out the harddrive and access your files. To enable it, search for FileVault on Mac and BitLocker on Windows.

Tip 8: Turn on encryption

STORAGE & DELETION

Copy from a real email we received at All4Staff:

"Hi, I don't have any checks on me to upload for the direct deposit portion so here is my routing and bank account number fo use for payroll."

And then the employee WROTE OUT their entire routing and bank account number! There are a lot of issues with the message, the most obvious of which is that you should never send your bank account information over email! Put yourself in the hackers shoes for a second. If you have maliciously stolen someone's email password and are looking for information to commit identity theft, what is the first thing you are going to search for? A simple Ctrl+F for "SSN", "Social Security Number", "Bank", "Routing" should do the trick! Consider th amount of similar HR emails you probably have archived in your own email client. Scary isn't it?

Same goes for **emails marked "CONFIDENTIAL" or "IMPORTANT"**. It's a double edge sword: even though you're telling the receiving party the content is secret, you're also shining a bright light for hackers to see.

Tip 9: Don't request or send sensitive information via email

But now that you have you've received this sensitive information in your inbox, do you know how to properly dispose of it? Most email inboxes (like Gmail) will not actually delete messages, but rather **store them for up to 30 days** in a "Trash" folder, giving unathorized parties that much bigger of a window to dig up sensitive messages. However, you can go in to your "Trash" and choose to permanently delete either individual emails or the entire contents of the folder. Find out how your specfic email provider works, and make sure you are disposing of this information correctly and permanently.

BEST PRACTICES

PAPER FILES

As previously discussed, keeping sensitive information in paper files - even if it's in a locked cabinet - can be a huge liability. With digital systems, you can have **fine-grained permission controls** to limit what users can and cannot see. Plus, top-tier HR systems will have full-blown **audit trails** that can tell you exactly when files are accessed or modified.

Remember Diane's story fom the beginning of this eBook? Using digital audit trails from her payroll system, she was able to eliminate an internal source from her tax fraud case. Here is an actual email she sent to her boss during the investigation:

From: [redacted]
Sent: Friday, September 12, 2014 9:53 AM
To: [redacted]
Subject: Payroll System

Hi there,

[redacted] and I have been narrowing down the systems and places where the employee SSNs and W-2s live. I have some knowledge of who has access to the payroll system as administrators but [redacted] and I figured out last night that administrators, which we both are, have different levels of access.

We are in the process of selecting a new payroll system. Under the guise of [redacted] and I examining access controls in preparation for implementation of the new system, I am going to ask [redacted] P / [redacted] S to give us full access to the company set up so we can see not only who has access but when they accessed the system.

If they push back on this, I may need to you back me up. Will you?

[redacted], CPA, CFE
Chief Financial Officer
[redacted]

Tip 10: Use secure digital systems to store files

If you insist on keeping hard copy files, make sure you have some sort of access log. For instance, anytime someone needs the key, or asks you for a file, have them sign a Check-In/Check-Out sheet. It may sound old school, and it won't protect from someone picking the lock if they really want the data, but it could be your saving grace should you need to pinpoint a source like Diane did.

Also, keep a close eye on what you do and do not need to hold on to limit your exposure. Check out our blog to learn more about the I9 storage rules and more.

BUT ABOVE ALL ELSE, REMEMBER THESE

TAKEAWAYS

Key Takeaway 1: Minimize Access!

We're talking minimize access for your department, your staff, and even yourself! Use our simple tricks and use a cloud-based solution set up for storing sensitive information. It is much safer to have 1 copy of a file in a cloud based system than in a dropbox account where files can be downloaded and saved anywhere, insecurely. But most importantly take a hard look at who really needs access to information and how often they need it. We recommend starting with a no-access policy and go up from there. And for each piece of sensitive information you come across, **ask yourself these three questions:**

> *"Start with a no-access policy and go up from there"*

*Q: Do I really need **immediate** access to this?*
If no, put it in an encrypted, secure place and delete or shred from everywhere else. If yes, get to the corresponding task as quickly as possible so you can get rid of the information as soon as it's done to limit your exposure.

*Q: Do I really need to hold on to this **forever?***
Check with your local state and federal laws to create a record retention policy & stick to it! For example, did you know that you **do NOT need to keep social security numbers on file for "medical purposes"?** The hospital may ask for this information but that is purely for insurance and biling purposes. A patient will never be denied care for not having their SSN on them.

Q: Do I really need to share this with...?
Before we talk about explicity sharing files and folders with colleagues - make sure you're not inadvertently sharing folders publicly via your network setup. Ask your IT team to double-check that your drives are locked down and that you're not sharing anything you shouldn't be through Airdrop, Dropbox, or network sharing preferences.

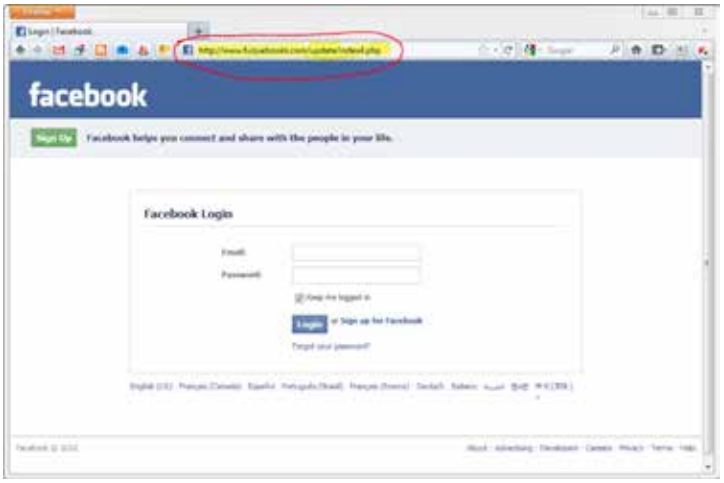
When you do need to share a document, whether hard copy or digital, **give the specific document alone, directly.** Don't merely lend your key out or give access to an entire folder for just one file. And take the time to check for hidden columns or other potential leaks in the document.

Make sure that you deprovision access appropriately and in a timely manner! You need to assume that even if *you* are being secure, others may not be. Removing access when it is not needed anymore is crucial to avoiding a security threat. If you DO loan out your key, make sure the person knows when it is expected to be returned.

At WorkBright, we have interns that will help transfer legacy employee files - and although we run background checks, know them personally, and trust them very much - we only give them access to one account at a time and remove access immediately upon completion of a job. It costs us more money and more time, but we think the minor overhead of doing this is worth it to keep our customers and their files secure.

BUT ABOVE ALL ELSE, REMEMBER THESE TAKEAWAYS

Key Takeaway 2: Slow Down!



When it comes to sensitive information and your identity, it pays to slow down. We discussed how most phishing scams could be avoided if we just took a few seconds to question the source. Did your ex-neighbor whom you haven't spoken to in 10 years really email you a link of a cat video? If you even have the slightest doubt in the back of your mind, just don't bother clicking it. Yeah, you might miss out on the next great viral video. Or you might protect your entire identity.

Even the more sophisticated scams can be avoided if we just slow down to check for obvious red flags. Take a look at this tab injection attack, asking you to log in to Facebook. You can see that while it looks like Facebook, the URL is actually "Fuizebook". Bam-phisihing scam averted!

Key Takeaway 3: Train Your Team!

On the next page you will find a one-page sheet which summarizes the tips and tricks we've outlined here. Print it out and distribute it your employees, especially your HR department. Better yet, forward them this eBook and hold a group discussion about identity theft in the real world. We bet more people in your office have been affected than you might know about. Data security is no longer an IT responsibility - it's everyone's responsibility. Just like in the Dilbert cartoon below, it only takes one uneducated person to be a stepping-stone to penetrating your entire organization. Take the time to train them, and make sure everyone is on the same page!

ONE PIECE OF INFORMATION CAN CAUSE A SECURITY BREACH

DON'T BE THE LEAK

10 DATA SECURITY TIPS TO PROTECT YOURSELF AND YOUR COWORKERS

With passwords, LENGTH beats COMPLEXITY
Longer passwords (over 20 characters) are exponentially more difficult to crack.

Use passPHRASES instead of passWORDS
Using other personal information (like dogs name) makes it easy on hackers.

Have a UNIQUE password for your EMAIL
Your email is the biggest stepping stone to data breaches for our organization.

Use a password MANAGER
Tips #1-3 are much easier and more secure with the help of a password manager.

Use 2-factor authentication
It's easy to do and the added level of security is second-to-none.

LOCK your phone, tablet, computer, etc. with a PASSCODE
Just like you lock your house or your car, your unattended device should be locked. Set your automatic lock on your computer for a reasonable time - like 10 minutes.

Turn on the REMOTE KILL SWITCH on your phone & tablet
In the event of theft, this will allow you to remotely delete all of your data.

Turn on ENCRYPTION & password protect sensitive files
Make sure your computer's automatic encryption is activated for all files and if you use excel or other programs for sensitive information make sure they are password protected!

Don't discuss sensitive information VIA EMAIL
If you need to transmit sensitive data, do it in person, over the phone, or on a channel the IT department has deemed safe.

Use SECURE digital systems to STORE sensitive files
Don't keep sensitive files on paper unless you have a locked filing cabinet. If storing personal information on your computer, store in a locked, secure, unshared file.

IF YOU DON'T KNOW WHAT OR HOW TO COMPLETE ANY OF THESE ACTIONS, PLEASE CONTACT YOUR HR DEPARTMENT

THANK YOU
FOR READING OUR EBOOK

SECURITY IN HR: *HOW SECURE ARE YOUR FILES... REALLY?*

If you're ready to take the next step in data security, then consider WorkBright for storing all of your employees personal information and records electronically. Our security precautions are listed to the right but we do so much more than that!

With WorkBright you can get rid of paperwork from day one with our 100% digital onboarding solution! We save you time and money on your onboarding so you can get back to interacting with people, not pushing paper.

Learn more by visiting www.WorkBright.com
Or contact us by phone at (844) 370-1783 or by email at info@workbright.com to start your free trial today!

A special credit and thank you to the brilliant minds that helped us as sources for this eBook. If you'd like more information on security and/or identity theft, please visit these links:

"2014 Year of Mega Breaches & Identity Theft" By gemalto and SafeNet

"2014 Data Breach Investigations Report" By Verizon Wireless

"Identity Theft and the Workplace" By HRHero

"Scammers switch back to phone calls to target victims" By CNBC

"Password Strength" By xkcd

WorkBright keeps YOU secure with best-in-class security infrastructure and privacy controls:

- Data is transmitted and stored using encrypted, bank-grade, 256-bit SSL certificates.
- Each customers' data is sandboxed in a unique, protected database environment.
- Account passwords are stored using one-way encryption so they can never be accessed in plain text (even by us).
- We maintain comprehensive audit logs covering all customer and user transactions, system access, and network operations.
- Production data is automatically and continuously backed up to multiple, separate locations.
- Our application is built and maintained entirely in-house by our core engineering team. Outside vendors never have access to any part of our code, databases, or application infrastructure.
- We eat our own dog food. We trust our sensitive HR information to our application, making sure our security and privacy priorities never become misaligned with our customers'.

To read more about our security precautions, visit this page.