Big Data, Cyber Threats and Relocation: How to Keep Your Organization's Data Secure in Times of Transition

There are few buzzwords more commonly heard these days than "big data" (okay, maybe "millennials"). The promise and hype of big data has led companies to believe virtually any question about their customers – or employees in the case of HR – can now be answered with enough data mining and analysis.

The problem? While there is more data being captured than ever before, which can be tremendously useful for improving business functions like corporate relocation, too many companies focus on the "big" and not the "data," going down a seemingly endless rabbit hole.

On top of that, the deluge of data and ways for employees to access and share online documents also has put many companies at an increased risk for data hacks. While there isn't a guaranteed way to prevent a breach, educating your staff and taking the proper steps to secure information – particularly during high-risk times like relocations – will significantly enhance your organization's defense against cyber threats.

The following white paper highlights:

- how to use big data to support and enhance your relocation strategy,
- the current state of data security and the common reasons companies experience a data breach,
- how to implement security best practices at work, and
- how to protect your organization's data during both corporate and commercial relocations.

Corporate Relocation in the Age of Big Data

Too much data

According to an IBM study, 90% of all the data in the world has been created in the past two years, with people generating 2.5 quintillion bytes of data every day. (That's 2.5 billion gigabytes, enough to fill 78.1 million base-model iPhones.) The amount of data captured every day, frankly, is too vast to comprehend, and few companies are collecting, analyzing and securing it all in an efficient manner.

And these bad data analyses can hurt your company's bottom line in a significant way. A second IBM study estimates that poor quality data, in the U.S. alone, cost $3.1 trillion in 2016. That's approximately a quarter of the combined annual revenue of all the companies on Fortune's 500 ranking.

Big data analysis isn't an inherent profit-loss activity. There are countless examples of it being used to save companies money and improve the quality and efficiency of work across an organization.

Only 6% of HR departments believe they are 'excellent' in analytics and more than 60% feel they are poor or behind.

Big Data in HR: Why It's Here and What It Means
By Deloitte

So how do you go about developing a big data strategy that has a positive impact – without adding to the next deficit study?

What are your goals?

Depending on how much data your company is gathering about its employees, it might seem daunting figuring out where to start. Again, too many companies hear "big data" – or to be more HR specific, "workforce analytics" – and think they need to start gathering life-changing insights immediately.

Not surprisingly, starting too fast or too big is a recipe for failure. The best way to make your data efforts manageable is to start

Big Data, Cyber Threats and Relocation: How to Keep Your Organization's Data Secure in Times of Transition

with your company or department's goals that your relocation strategies support. This, in turn, will help you determine the data specific to those goals you should capture and analyze.

Some common relocation goals that lend themselves to being improved by data:

- Policy benchmarking to ensure your standard relocation offer is competitive for your industry
- New employee/transferee job satisfaction following the move
- Employee retention

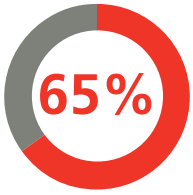
For example, if there's a company goal to increase efficiency and productivity, you could start with minimizing the time spent reviewing exceptions to your company's relocation policy. To do so, you could track those requests throughout the year and identify the most common ones, along with the amount of time your HR department spends on them. While there might be a cost to adding these benefits, it could ultimately save money by improving productivity, as well as making your relocation package more competitive within your industry.

There are other common issues like failed assignments, retention rates and recruitment success that a simple data strategy can help address. If you're not sure how your relocation efforts relate to your company's overarching goals, this could be a great opportunity to meet with leadership to make sure they are aligned.

How to share the data?

Many executives and those in upper management prefer to make decisions based on data – hence, part of the reason why big data has grown in prominence. But that doesn't mean they want a 20-page report of numbers and charts to read through and decipher. People are far more likely to understand and recall your findings and recommendations when the data is "translated" into a visual like a graph or infographic.

65% of people are visual learners, according to the Social Science Research Network.



Why We're More Likely to Remember Content with Images and Video by Fast Company

Keeping it all safe

Big data can do a lot to improve your organization's operations and relocation efforts, but it's important that you're collecting, storing, analyzing and distributing it all in a secure way. Too many companies have had their customers and employees' trust diminished because of a data hack. And while some hacks are entirely the result of a malicious external cybercriminal, many breaches at least partly stem from employee negligence. Educating your employees on how to keep company information secure is a critical first step.

Current State of Data Security

"Credit card and personal data are the lifeblood of every hacking scheme," said Kris Monaco, managing partner at Level ETF Ventures, in a CBS News interview about the Equifax data hack. According to a report from IBM Security and the Ponemon Institute, a cyber attack costs the average U.S. business $3.62 million per year.

Although certain industries like health care and financial services have shown to be at a higher risk for data hacks, no company is completely immune in this day and age. While the nuts-and-bolts of data security are more IT's domain, HR managers should play an active role in helping educate employees of proper data management, onboarding and exit processes, and staying safe during a relocation.

hilldrup.com
800.476.6683

Hilldrup

Big Data, Cyber Threats and Relocation: How to Keep Your Organization's Data Secure in Times of Transition

Common employee data security problems

Contrary to many TV shows and movies, most data hacks aren't solely the work of a computer mastermind. One of the biggest risks a company faces is from those employees who have access to sensitive information like customer records.

Two common causes of data hacks:

- Employee accidentally releases malware
- Third-party partner comprises your data

[Infographic] Stop Insider Threat by IBM

While some data security incidents can be caused by a disgruntled employee who maliciously steals and/or releases the information, two common causes of data hacks are from an employee accidentally releasing malware into your system and third-party businesses and partners who compromise the data.

According to a 2017 Dell survey, nearly half (45%) of employees engage in some amount of unsafe behavior during the workday. These actions can include connecting to unsafe WiFi or a personal email to access confidential work and losing a company work device.

Nearly 5% of company devices are lost or stolen each year.

Kensington

Which countries and industries are most prone to data breaches?

Not all countries approach internet security the same, and because of varying security standards and privacy laws, some are more susceptible to cyber attacks than others. Depending on the extent of your company's global operations, it's important to understand which international offices may be more vulnerable than others.

Countries most vulnerable to cyber attacks:

- Belgium
- Dominican Republic
- Hong Kong
- Samoa
- China
- Afghanistan
- Tajikistan
- South Africa
- Australia

Similarly, certain industries face a higher risk of cyber attacks. Those with extensive online records of personal information or business and/or governmental details are often at the top of a hacker's list of viable targets.

Top five industries at the highest risk of a cyber attack:

- Health care
- Financial Services
- Manufacturing
- Government
- Legal

Laws regarding company breach notifications

Not only are incidents of corporate data hacks becoming more common, the laws mandating how a company responds to a breach are becoming more prevalent as well. Although there is no federal law regarding security breach notification, all but two states (Alabama and South Dakota) have a state statute on breach notifications.

The European Union has enacted a new law, as of May 2018, by the name of The EU General Data Protection Regulation (GDPR), to require companies to report breaches faster and establish more stringent processes to handle personal information. The regulation not only applies to companies with a physical presence in the EU, but also those with employees, suppliers or clients working there. Penalties can be as high as 20 million euros ($23.6 million).

The IoT Dilemma

IoT (Internet of Things) may not be a commonly understood expression, but virtually everyone interacts with these devices. IoT represents the network of internet-connected devices that exchange data (e.g., vehicles, home appliances, building

hilldrup.com
800.476.6683

Hilldrup

Big Data, Cyber Threats and Relocation: How to Keep Your Organization's Data Secure in Times of Transition

automation, thermostats). In many ways, IoT devices are behind so much of the big data boom. Intel estimates that there will be 200 billion IoT devices by 2020 – up from 2 billion in 2006.

And at the same time, these "smart devices" pose a tremendous data security threat. With so much automated exchange of data, it can be easier for a hacker to intercept that flow undetected. While there isn't as much that individuals can do to prevent against this type of cyber attack, it is important for businesses to be aware of all the IoT devices they currently use and ensure that security updates are installed quickly.

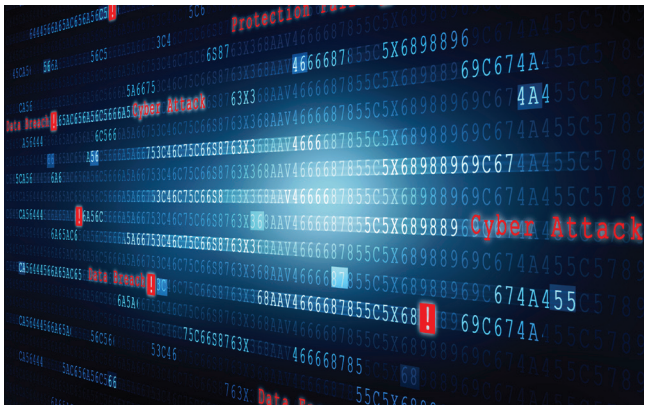
How to protect your organization

After all this, it might seem like a forgone conclusion that a data hack is imminent for your company. While no company should consider themselves immune from one, there are a number of steps and safeguards organizations can implement to protect themselves from cyber threats. These include having a formalized data security policy and incorporating data security best practices into your employee onboarding and ongoing training.

Implementing security best practices at work

With all the talk about data hacks and cybersecurity, you'd think the biggest threat to your organization is a team of foreign hackers surrounded by high-tech computers and gadgetry. However, if you're reading this at work, you might be surprised that you've already seen your company's biggest potential threat to a data breach – your employees.

One of the most common causes of a data breach is an employee sharing sensitive information. Certainly, some of these cases stem from a disgruntled employee with malicious intent, but surprising to many, most employees who share sensitive information do so unknowingly, believing that with whomever they are sharing the data needs it for a legitimate business purpose. In fact, 72 percent of employees, for one reason or another, are willing to share sensitive information with someone who does not have access to it.



How to make training effective

New employees, especially those who've recently relocated for their job, have a lot of information to retain throughout their onboarding process. Contrary to how your IT department may feel about this, it is often better to focus on the highlights of your data security plan during their first few days, and then use ongoing training and messaging to reinforce their understanding with additional details and best practices.

Most common phishing scams

According to Symantec's 2017 Internet Security Threat Report, email remains the most common entry point for malware into an organization. Some of the most common "tricks" for hackers that employees should look out for include:

- *Dangerous attachments and links – particularly invoices:* One of the ways hackers are most successful in gaining access to a company's network is by sending employees emails with fraudulent links or attachments that appear to be about important business matters – most commonly, invoices. It's not a surprise, no one wants to be late on an invoice. However, these often include an .exe file that runs a program designed to give a hacker remote access to the computer.
- *Slightly "off" email addresses:* The general rule of thumb is to only open messages from known contacts. So, naturally, hackers are now attempting to have their messages appear to be from someone the recipient already knows or a seemingly reputable organization. They'll do so by changing a letter or adding a hyphen to the email domain. For example, an email domain may normally appear as "@companyname.com," whereas the fraudulent version would appear as, "@company-name.com." If the tone or content of a message appears off, look to see if the email address is a fake one.
- *"You've been hacked" popup:* Another common trick are popups alerting a person of a hack. They look and read like an official warning, urging the user to either click on a link or install a program to resolve the problem. What this

Big Data, Cyber Threats and Relocation: How to Keep Your Organization's Data Secure in Times of Transition

really does is give a hacker access to the computer, and subsequently, the network to which it is connected.

Report possible breaches ASAP

It's critical to stress the importance of reporting a possible breach – or even an attempted one – as quickly as possible. According to a report from the Ponemon Institute, breaches that took more than 100 days to identify cost $550,000 more ($4.38 million total) than those reported in less than 100 days ($3.83 million).

First, employees need to be able to recognize signs that a breach might have occurred. These can include:

- Their antivirus software has been disabled.
- Other colleagues are receiving random messages and emails that include unusual links or attachments from them that they never sent.
- They are encountering an excessive number of random popup windows.
- They experience an unexplained drop in network performance.

Second, employees need to feel safe in reporting a potential data breach. Not to say that there shouldn't be any consequences to a breach that stems from employee negligence, but if there's a no-tolerance policy in place, some employees may opt to try and hide a potential breach rather than report it. Several security experts even suggest offering incentives for proactively reporting a potential hack or breach.

Other steps to make data security part of your training process include:

- *Focusing on the essentials during the onboarding process:* Again, there's a lot of information being thrown at new employees, so try to focus on the key aspects of your company's data security plan during their initial training.
- *Considering monthly campaigns for other issues and reminders:* Whether an employee has been with the company for two months or two decades, everyone needs to be updated on new issues and policies regarding data security. A monthly email, newsletter or town hall discussion are great ways to continually remind and educate employees.
- *Making the materials easy to understand:* The average person cannot understand all the technical jargon used among IT professionals. Take the time to "translate" the training materials into language that's easily understood. Not only that, consider developing graphic materials or a video to relay this information. One study shows that people only remember 20% of text without a visual.

How to prevent employees from taking sensitive data with them when they leave/move

During an employee's tenure with a company, and especially after they've announced their resignation, you need to have a policy and systems in place to ensure sensitive information cannot be taken with them.

A formal policy, at the very least, should outline acceptable use of company devices and information, identify which data and information is considered confidential as well as how long it should be retained, and how devices will be set up and decommissioned upon an employee's hiring and resignation.

While these policies will formally state what employees can and can't do, that, obviously, isn't a foolproof plan. Additional steps your IT department should consider is restricting computers with access to confidential files from accepting portable storage devices (e.g., a flash drive), allowing single-computer printers and restricting access to certain files based on specific employee need.

Big Data, Cyber Threats and Relocation: How to Keep Your Organization's Data Secure in Times of Transition

Keeping Company Data and Employees' Identity Safe During a Move

Relocations – whether they are residential, corporate or commercial – create certain challenges around data security. With all of the changes and updates to information during a relocation comes a heightened risk of hackers, identity thieves or simple employee negligence.

Securing Corporate and Employee Data During an Office Move

If you've ever been involved in an office move, you know how many moving parts are involved. It takes a tremendous amount of coordination and vendor support to orchestrate everything in a way that doesn't negatively impact the company's productivity. It's not uncommon that people's attention is more focused on getting things from Point A to Point B – and less on making sure sensitive information is relocated in a secure manner.

Because there's so much going on that is out of the ordinary, without proper planning, your company data – including data concerning employees and customers – could be at risk. To help mitigate any potential risk, consider the following:

- *Make data security procedures a priority ASAP:* Early on, your organization should form an internal move team to coordinate all the logistics, timelines and vendors. As early as the first meeting, make your data security procedures one of the top priorities of your move plan.
- *Identify the full scope of your sensitive information:* Dedicate some time to outline any and all sensitive information that needs to be secured – both electronic data and hard copies. Depending on your organization, this may include bringing in those individuals in charge of HR, IT, operations, and customer service – just to name a few. When in doubt, ask yourself what information do we possess that would be a major security issue if it was maliciously obtained?
- *Consult staff on how to secure their personal files:* Your staff may keep certain personal records at their desk, which also need to be transported securely. Generally, it's best that employees handle those themselves to limit the company's liability. Still, it's important to make them aware that they should personally transport any sensitive personal files.
- *Use a reputable commercial mover:* There is quite a bit that goes into an office move, and few, if any, companies can pull it off alone without sacrificing their employees' productivity. At some point, you'll need outside help, so make sure those vendors demonstrate integrity and competency. Beyond that, there are measures you should consider requiring your vendors abide by, including:
  - » Using the same crew members throughout the move to ensure continuity
  - » Providing background and drug screenings for all crew members involved
  - » Only using locks for containers and trucks that you provide
  - » Maintaining line of sight for crew members while on company property and line of sight for any transport vehicles holding company documents

These requirements should be seen as reasonable requests to any professional, reputable commercial moving company. If they can't abide by them, consider someone else.

Helping Transferees Stay Secure During Their Move

Not only are companies at an increased risk of cyber attacks, the average person similarly faces greater risk of identity theft during a relocation. This is because so much of the move process includes creating new accounts for utilities, updating addresses with the bank and credit card company, and a laundry list of other tasks that involve sharing personal details with a variety of individuals. It's easy to understand how relocating can put your employees at greater risk of identity theft.

hilldrup.com
800.476.6683

Hilldrup

Big Data, Cyber Threats and Relocation: How to Keep Your Organization's Data Secure in Times of Transition

It's important to know how you can help your employees protect their identity throughout their relocation. Some tips to keep in mind:

- *Make sure they pay close attention to their bank and credit card statements:* While this might seem daunting with all the extra expenses stemming from a move, it's important to regularly scan financial accounts to see if there are any charges they can't account for.
- *Place a security freeze on their credit report while they relocate and settle:* This is a low-cost service ($3-$10) employees can set up with the three main credit bureaus (Experian, Equifax and TransUnion) that prohibits any loans or credit accounts from opening without their consent. It does so by "freezing" access to their credit history, which is a required step when setting up a credit account. If they need to apply for a loan or open a new credit card, they can request a temporary or permanent lift at any time.
- *Order a credit report:* On top of a credit freeze, this can be a good time to review their credit report. By law, everyone is allowed one free report from the three major credit bureaus each year. These reports list all credit accounts in their name, so they can see if there are any fraudulent ones. Each bureau also allows you to add a fraud alert if they believe they're at a higher risk of identity theft, which stays in effect for 90 days.
- *Update mailing address:* In addition to friends and family, it's important they notify organizations they do business with such as banks and health care providers of their move and new address. This will make sure personal and financial information is sent directly to their new home.
- *Vet your moving company:* Movers have access to many of your employees' belongings that might have personal data that could be used against them. It's important to research your moving company to ensure it is reputable and trusted (like Hilldrup).

If you'd like to offer your employees an additional layer of identity-theft protection while they move, United Van Lines offers an Identity Theft Protection service in all of its Straight Talk Advantage packages.

Some of the features the protection service provides include:

- Credit monitoring
- Full restoration services
- Legal and emotional care
- Reimbursement for expenses and lost wages
- Member resources

We hope this white paper on data security was helpful and enlightening. It's an unfortunate reality, but with the right help, there's a lot companies and individuals can do to protect themselves.

hilldrup.com
800.476.6683

Hilldrup