The Ladders®

The Most $100k+ Jobs

RESUME

Resume Insecurity

Resumes are a treasure trove of personal information. What security steps do employers take to protect your identity from being lifted?

By Lisa Vaas

"PROPER STORAGE of employee and applicant records." It was just another item on the human resources audit checklist, right after "display federal, state and OSHA labor law posters."

See INSECURITY Page 2

ILLUSTRATION:Chip Buchanan

Be Careful Out There

By Matthew Rothenberg, Editor-in-Chief, TheLadders.com

LET'S FACE IT: A job search is not easy on introverts. The whole process of polishing up your personal brand and putting it on the open market is an exercise in self-exposure that can test the nerve of even the most outgoing candidate.

In a market saturated with job seekers, the personal information you provide will be scrutinized by a battery of software and human gatekeepers. The more opportunities you pursue, the more places that data will travel.

And in this age of identity theft and data piracy, that raises the chances that your information will take a bad turn and end up in the wrong hands.

In this package, veteran technology reporter Lisa Vaas speaks with security and HR experts about how to safeguard your resume and other personal documents to maximize their exposure to good leads and minimize their accessibility to bad guys. On this planet, there's no absolute guarantee of data security; nevertheless, understanding the threat and using some precautions should make your job search both successful and secure. ■

IN THIS PACKAGE:

What did you think of this package? Got a story of your own to tell? Have ideas for future coverage? Please write Editor-in-Chief Matthew Rothenberg at **matthewr@theladders.com**.

INSECURITY

After checking off a few other items on her checklist, Ellen B. Vance, an HR consultant and auditor, asked to see the storage room. The client led her to an unlocked storage closet in the middle of the old building, surrounded by half of the nonprofit's 40 employees.

When she opened the door, Vance encountered 15 large file-folder boxes. "When we moved to this new location, we just put this stuff in there," said the client.

Vance and the client started opening boxes. As they did, it became clear that "this stuff" included photocopies of birth certificates; Social Security cards; driver's licenses; and I-9 Employment Eligibility Verification forms that listed employees' Social Security numbers, dates of birth, addresses, maiden names, signatures — everything a criminal needs to perpetrate identity theft. "I was about ready to pass out, seeing all this stuff," said Vance, senior consultant and advisory services practice leader at **Titan Group**, an HR consultancy in Richmond, Va.

Why should you care about the poor compliance procedures at a nonprofit in Virginia? If you've applied to a job there or anywhere in the last decade, your resume may be equally exposed, your personal information similarly vulnerable to identity theft should anyone gain access to an unlocked closet and a stack of file folders. With the advent of e-mailed resumes, electronic storage and online applications, the thief need not even get so close; your resume may be open to attack from an unscrupulous recruiter or hacker.

Too few companies employ the safeguards necessary to protect applicant data, and almost none inform clients of their security practices before requesting a resume and applicant information. The economy has made matters somewhat worse, according to HR managers who said the employers' market has left job seekers feeling compelled to hand over information they would normally be reluctant to reveal and distribute it to dozens of sources in the hopes of finding a job. Criminals have even been known to post fake job listings to capture the data of unsuspecting job seekers.

But help is on the way: Employers are on notice to improve resume data protection after data breaches precipitated several lawsuits and government action. What's more, job seekers can implement their own safeguards to avoid being the putting their resume in the wrong hands.

Fumbled data

Interviews with hiring professionals confirm the anecdotal evidence: Even recruiting agencies that use sophisticated applicant tracking system (ATS) software to store and protect job applications often leave the applications open to theft by allowing access to anybody and everybody who walks by an unsecured terminal; companies leave sensitive information moldering in unlocked closets accessible to all; and job applicants' data gets left on laptops that get stolen and on USB thumb drives that get misplaced.

In her experience, Vance said that small firms without formal HR departments are most likely to fumble data. But make no mistake, large corporations with entrenched HR processes are still liable to mishandle job-applicant or employee data: In June, U.S. Insurer **Aetna was sued** after allegedly failing to protect personal information belonging to employees and job

How to Protect Your Resume from Identity Theft

Get the job without exposing your personal data. There are times when it's OK to withhold sensitive information.

By Lisa Vaas

"JOB CANDIDATES ARE WILLING in this market to give any information they can that would help them get a job," said Ellen B. Vance, an HR consultant and auditor who advises companies on how to safeguard applicant and employee information.

The instinct is natural, but it can leave you vulnerable to identity theft. Lax security by some employers has left resumes and job applications full of sensitive, personal data such as Social Security numbers, maiden names and drivers' licenses easily accessible to computer hackers and identity thieves.

Government regulations and lawsuits have motivated employers to take the issue seriously, but many employers' resume databases remain vulnerable to data breaches, and it can be hard to tell which ones are safe.

To protect yourself from becoming the victim of a data breach, sometimes it's best just to say no. For example, Vance, senior consultant and advisory services practice leader at **Titan Group**, an HR consultancy in Richmond, Va., recommends that, before receiving a job offer, job seekers should omit any fields on forms that ask for sensitive information such as Social Security numbers.

"It's OK to leave that blank and say you'd be happy to provide that at time of hire," said Vance. "There's noth-

applicants. This was direct fallout from an incident in which the company's job-application Web site was breached by cybercriminals, as Aetna disclosed on May 28. For its part, **the Gap lost personal information**, including Social Security numbers, for some 800,000 U.S. and Canadian job seekers, the company admitted in a September 2007 press release.

Several lawsuits that followed major breaches like the ones at Aetna and Gap and some action by Congress and state legislatures have put employers on notice that they need to improve resume and job-application date protection.

Can we blame the ATSes?

Job-application information is walking out the door in a number of ways, but often, insecure software is to blame. Research firm Forrester Research recently found that more than 62 percent of 200 surveyed companies **experienced a security breach** in the previous 12 months because of insecure software. Most were likely caused by a **SQL injection attack.**

> **"If you have an application publicly available on the Internet with form fields, people could potentially execute database statements if proper input filtering is not performed."**
>
> **—Anonymous security analyst**

In a SQL injection, a hacker uses a Web site's online form to gain control of the database. Security procedures are designed to filter and block such attacks, but hackers are constantly developing new codes and techniques and almost no database is safe, said a security analyst who works for one of the major ATS vendors. "If you have an application publicly available on the Internet with form fields, people could potentially execute database statements if proper input filtering is not performed," said the individual, who asked not to be identified.

How do ATS vendors fend off a SQL injection? With the exception of the aforementioned vendor, all of the major ATS vendors contacted for this article declined to participate out of fear they might encourage hackers to target their software. The ATS vendor who did speak to us said his company uses f**ilters to prevent a SQL injection and XSS (cross-site scripting)** to find and patch vulnerable code in the database software. The ATS vendor monitors activity logs for such types of attempted breaches against its Web-based applicant tracking and performance management software. In addition, the ATS vendor stores the resumes and applicant data for its clients at their own facility; only two people — the vendor's CEO and the security analyst himself — have physical access to servers that are accessed via biometric palm-print recognition.

A people problem

But technology is only part of the problem. All the software in the world won't protect applicant data if humans handle the technology recklessly.

See INSECURITY Page 6

ing a prospective employer needs that data for."

"I think the candidate is perfectly OK to say, 'The reason I ask that is I'm very cautious, based (on) what I see in the media, about identity theft.' " Vance said. "You can do it in a way that's not confrontational."

Lorne Epstein, a recruiter with 13 years of resume-review experience and creator of **InSide Job**, a Facebook community of job seekers, also suggests that job candidates who want to protect their confidential data should leave their home address completely off their resumes. "Mostly people are getting communicated with by e-mail and by phone" anyway, she said.

Another way to help protect your resume from identity theft is to stay away from sketchy job listings, many of which breed on unmonitored sites such as Craigslist, said Rachel Rice-Haase, human-resources and marketing coordinator for Oberstadt Landscapes & Nursery Inc., in Fremont, Wis.

To identify legitimate job postings, use reputable sites and look for job postings that identify the company posting the listing. "If you're not sure whether it's a bona fide (listing), don't apply," Vance recommended. "Or send a request for additional information."

Vance also encourages job seekers to use a separate e-mail account for their job search so they can isolate their e-mail, both for security purposes and to keep track of job correspondence.

Once a job offer comes, candidates should also avoid providing copies of documents used for I-9 purposes, such as passports or birth certificates. Employers can legally record the documents' information, but don't hand over photocopies that can be mishandled.

Oberstadt's Rice-Haase recommends that applicants using recruiting firms ask up front, "How much of my personal info is being given away?" And, "Do you really need to do a background check?" she said. "The recruiting company should have a sign-off, but they don't necessarily always (mind) all their Ps and Qs." ■

Who's Losing Data?

The Privacy Rights Clearinghouse keeps tabs on data breaches and provides some examples of how personal data gets into the hands of bad guys.

By Lisa Vaas

BEFORE YOU HIT "SEND" OR FILL OUT A JOB APPLICATION, do you ever wonder how careful a particular company is to protect your resume information? If so, you might consider checking to see whether it's had the dubious distinction of appearing on the Privacy Rights Clearinghouse's running chronology of data breaches.

The chronology lists data breaches that have been reported because the compromised personal information included Social Security, account and driver's-license numbers — all data used by thieves to steal identities. What follows is a selection from that list of some large, well-known companies and how their data stores were compromised:

Aug. 3, 2009

National Finance Center, Washington, DC

Number of compromised records: **27,000**

An employee with the National Finance Center mistakenly sent an Excel spreadsheet containing the employees' personal information to a co-worker via e-mail in an unencrypted form. The names and Social Security numbers of at least 27,000 Commerce Department employees were exposed.

Aug. 4, 2009

New Hampshire Department of Corrections, Laconia, N.H.

Number of compromised records: **1,000**

A 64-page list containing the names and Social Security numbers of about 1,000 employees of the state Department of Corrections ended up under the mattress of a minimum-security prisoner. The prison contracts with vendors to shred documents, and investigators are trying to find out why documents were not destroyed.

Aug. 13, 2009

National Guard Bureau, Arlington, Va.

Number of compromised records: **131,000**

An Army contractor had a laptop stolen containing personal information about 131,000 soldiers enrolled in the Army National Guard Bonus and Incentives Program. The data included names, Social Security numbers, incentive payment amounts and payment dates.

Aug. 14, 2009

American Express, New York, NY

Number of compromised records: **Unknown**

Some American Express card members' accounts may have been compromised by an employee's recent theft of data. The former employee has been arrested, and the company is investigating how the data was obtained. American Express declined to disclose any more details about the incident.

June 14, 2007

Lynchburg City, Lynchburg, Va.

Number of compromised records: **1,200**

Personal information of Lynchburg city employees and retirees was accidentally posted on the city's Web site, along with information about employees' prescription medications.

July 10, 2009

Northern California dumpsters, from San Francisco Bay area to Central Valley

Number of compromised records: **1,500**

A criminal complaint filed against a 30-year-old suspect claims that he made more than 1,000 fake ID cards that he used to rip off people, stores and banks. He also allegedly admitted to stealing the identities of more than 500 people all across Northern California, ranging from the Bay area to the Central Valley. Federal agents say the man said it was easy to find new victims: All he needed to do was visit the dumpsters outside a local business and dig for documents. Using the sensitive materials he found in the trash, he was able to use a computer to mock up fake identification cards and blank checks, according to authorities. He also allegedly confessed to stealing between

$1 million and $2 million dollars in cash and merchandise. ■

Where Companies Leak

Another casualty of the recession is data security, as a growing number of departing employees walk off with their former employers' data.

By Lisa Vaas

HOW EXACTLY DO JOB APPLICANTS' personal data manage to leak out of large, venerable companies?

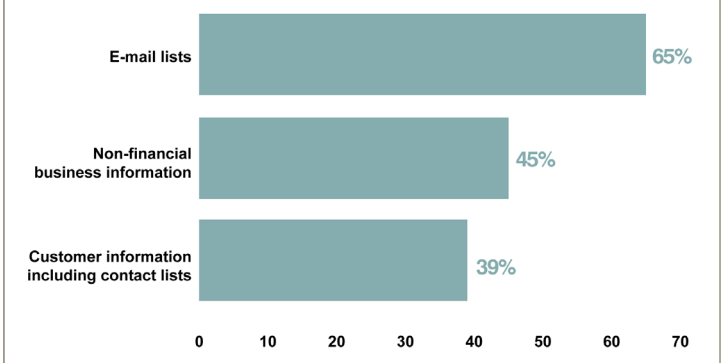
In many ways, it turns out. At Aetna, the large U.S. insurer **being sued** for allegedly failing to protect personal data, the hole was in a job-application Web site. At The Gap, where the personal information of **800,000 job applicants was exposed in 2007**, the problem was blamed on a third-party contractor that allegedly failed to encrypt the data on a personal laptop that was later stolen.

Of increasing concern in this dark economy is a third channel for data loss: files removed by employees who leave after layoffs or in pursuit of better opportunities.

A recent study from Ponemon Institute LLC, 59 percent of employees who quit or are asked to leave, walk out the door with company data. Of those respondents who left with company data, 79 percent admit they took the data without permission from their former employers.

The study, **"Data Loss Risks During Downsizing,"** sponsored by **Symantec**, polled 945 U.S. workers in January who left an employer within the preceding 12 months. All the people surveyed had access to a desktop or laptop computer for their jobs, and they all had access to proprietary information including customer data, contact lists, employee records, financial reports, confidential business documents, software tools and their employer's intellectual property. ■

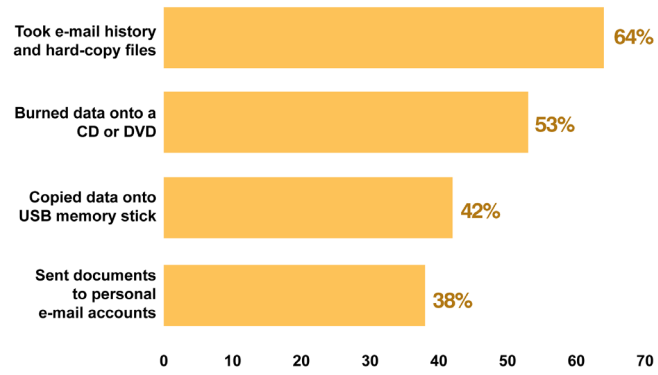
What did they take?



Source: Data Loss Risks During Downsizing, Ponemon Institute LLC

Chip Buchanan/TheLadders

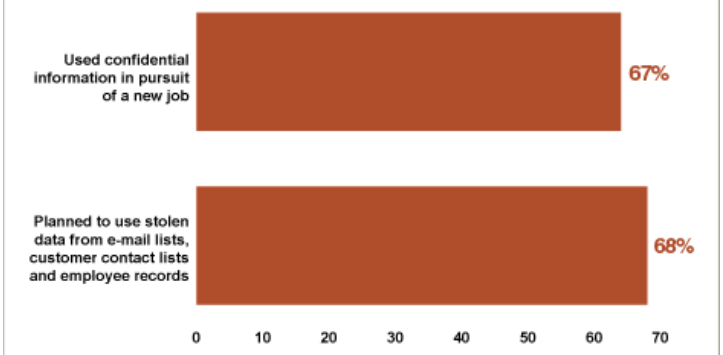
How did they take it?



Source: Data Loss Risks During Downsizing, Ponemon Institute LLC

Chip Buchanan/TheLadders

What did they do with the confidential information they lifted?

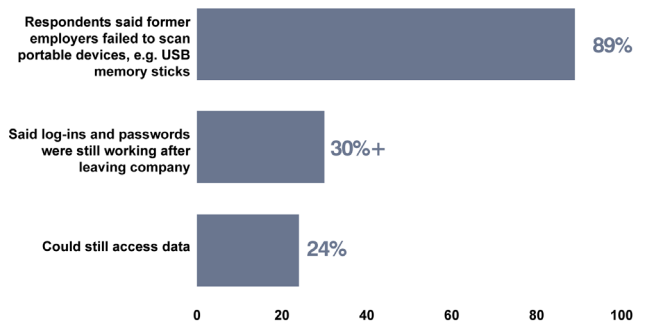


Source: Data Loss Risks During Downsizing, Ponemon Institute LLC

Chip Buchanan/TheLadders

Ponemon: Employers are doing little to stop this data exodus

Only 15 percent of companies bothered to conduct a review or perform an audit of the paper and/or electronic documents that employees took, and most of those were called superficial or incomplete.



Source: Data Loss Risks During Downsizing, Ponemon Institute LLC

Chip Buchanan/TheLadders

INSECURITY

Rachel Rice-Haase, human-resources and marketing coordinator for Oberstadt Landscapes & Nursery Inc. in Fremont, Wis., has witnessed that recklessness first hand. In a previous position at a recruiting company, recruiters used an ATS that Rice-Haase called "pretty up to date" to process applications. The company's help desk made sure to give tutorials to recruiters so they knew how to use the ATS applications. It all seemed "pretty advanced," Rice-Haase said. The software probably was sophisticated when it came to security and features, but the more she looked at it, the more Rice-Haase realized the company was using it carelessly.

"You had anybody, even people who weren't recruiters, going in and accessing applicants' information," she said. "You might have 10 recruiters, and they all have access to everybody's candidates. It's not just people you've interviewed. It's the person sitting across from you, down the hall, (they) can get in there and look at (any job applicant's information). That part was always baffling to me. Sure, you sign a little form saying, 'I won't take this information home with me.' But you have to wonder, when all this information is available to everybody at the recruiting center, how far that goes?"

It can go pretty far. As Rice-Haase describes it, the ATS collected information including Social Security number, date of birth, driver's-license number — "all this stuff you'd rather not have anybody and everybody have access to," she said, and that's typical of ATS software.

With the software, recruiters could create a resume for any candidate and e-mail it from the system. Convenient? Yes. Dangerous? Absolutely. Recruiters could e-mail out personal information or entire applications, whether by accident or for illicit purposes.

And sometimes a company doesn't have a clue — or perhaps doesn't much care — where its data is stored or how to prevent data loss. The Virginia nonprofit company with the unlocked storage room is another classic example of blissful ignorance: Even though the company is legally responsible for safekeeping of the confidential information stored on I-9 forms, the staff just didn't know what was in those 15 boxes.

Titan Group's Vance encouraged her client to go through the files, pull out the forms, put them into either a burn bin or a shredder, and to have a witness on hand to make sure the records were verifiably demolished. "She looked at me with a look of horror on her face," Vance said. "(She was) staring at these boxes. She didn't know how many contained employee files, so she had to go through all of them. They're a very conscientious client. It was one of those cases where they didn't know what they didn't know. They didn't have an HR person there to advise them on it."

People problem, technology solution

Many organizations fail to grasp the scope of data protection or understand that it goes beyond the technology, said Jenny Yang, senior manager of product marketing for data-loss prevention at **Symantec**, a security-technology company. They don't understand:

- Where the confidential data is
- Where it's going and how it's moving — for example, is it being e-mailed out as part of a monthly report to the vice president of human resources, or is it being casually e-mailed around by recruiters as was done at Rice-Haase's former recruiting agency employer?
- How to prevent it from leaving an organization

Companies like Symantec provide some technology solutions to the problem of managers who mishandle applicant data. Symantec makes a product that searches a company's entire network for sensitive data, like Social Security numbers, even if it's on a USB memory stick attached to someone's laptop. It will also ID and block such data from being transmitted outside the company's network, either by a negligent employee or a hacker.

But such software won't help job seekers unless until the unlikely scenario in which every single potential employer has opted to buy it, and few companies will tell applicants whether they use such technology.

Unlike e-commerce sites, which advertise their security practices to gain the trust of consumers about to hand over credit-card data, few employers advertise the steps they take to protect your resume and job application.

To protect your resume and sensitive data, the best practice, for now, Vance said, is to make less of it available. ■

Career Advice from TheLadders

- Resume, Meet Technology: Making Your Resume Format Machine-Friendly
- Where Does Your Resume Go? How Job Listings Are Filled
- How to Work with Executive Recruiters
- Prepare to be Quizzed: The Job Assessment