

# LOUISVILLE BUSINESS FIRST

## An uncommon move

Jonathan Goldberg took a bold step by relocating his law firm to the suburbs

LUCY PRITCHETT, 24



## INSIDE

### Who are the winners in the Humana deal?

Based on stock ownership, we take a look at how key executives and board members will fare if the deal goes through. DAVID A. MANN, 5

### Breaking up now would be expensive

Billion dollar fees would come into play if regulators block the deal or if either party were to have a change of heart. DAVID A. MANN, 5

### Humana Foundation has a wide reach

The foundation, which will remain in Louisville, handed out more than \$10 million in cash donations across the U.S. in 2013. CAITLIN BOWLING, 8

### Humana's real estate footprint is substantial

Humana is one of the biggest office users in town as it owns or leases nearly 3 million square feet of office space downtown and in the suburbs. MARTY FINLEY, 6



## LONG-TERM CARE LISTS

Is some form of long-term care in your future? Statistics indicate that it's likely for a majority of Americans. Learn about facilities that offer long-term care in this week's lists. And gain insights into the costs of care in Kentucky and Indiana.

PAGES 16-19

COVER STORY, PAGES 4-9

## Aetna's acquisition of Humana rests in hands of regulators

### BUSINESS OF LAW

## BE PREPARED TO BE PROTECTED

Stites & Harbison attorney Ian Ramsey, at right, says Kentucky lags behind other states in the battle with hackers. "We are behind and therefore we are unprepared," he said. Ramsey and other attorneys weigh in on the fact that preparation and protection are essential to combat cybersecurity.

RACHEL REYNOLDS, 20



### TOOLS OF THE TRADE

TECH TOOLS HELP LAWYERS COMMUNICATE BETTER 26



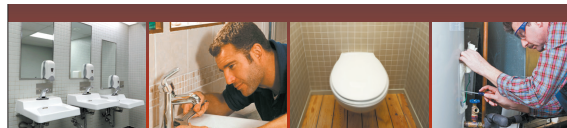
### LEGAL BRIEFS

FIND OUT RECENT HAPPENINGS AT AREA LAW FIRMS 28



### CONSUMER TRENDS

FIND OUT WHAT TYPE OF WINE IS FAVORED MOST IN KENTUCKY 12



PLUMBING AND REMODELING DONE RIGHT.

**TOM**  
SONDERGELD  
PLUMBING

For a free estimate contact us today at (502) 955-4451 or visit [www.tomsondergeldplumbingky.com](http://www.tomsondergeldplumbingky.com)



JULY 10, 2015  
VOL. 31, NO. 49, \$2.75  
455 S. FOURTH ST.  
SUITE 278  
LOUISVILLE, KY 40202



# PREPARATION & PROTECTION

## are essential assets for businesses' cybersecurity, local attorneys say



BY RACHEL REYNOLDS  
Correspondent  
Send comments to [bdaily@bizjournals.com](mailto:bdaily@bizjournals.com)

Kentucky was the 47th state to pass cybersecurity legislation with the 2014 creation of state law KRS 365.732 in 2014.

The date of that passage is a sign that Kentucky is lagging behind other states in the battle with hackers, said Ian Ramsey, an attorney at Stites & Harbison PLLC.

"We are behind and therefore we are unprepared," said Ramsey, who has worked closely with the FBI's cybercrime unit and gives presentations on cybersecurity nationwide. He is chairman of Stites & Harbison's Information Security Committee and a Certified Information Privacy Professional (CIPP/US).

"There will be many companies in the commonwealth who will have this problem ... You don't find out about a data breach the day it

happens. You find out months or years later."

### Responding to a breach

In the wake of recent high-profile cyber breaches at companies such as Target Brands Inc., The Home Depot Inc., Sony Pictures Entertainment and Morgan Stanley investment firm, U.S. companies are scrambling to create their own corporate cybersecurity plans, say attorneys at Louisville law firms interviewed for this report.

Companies in Kentucky and elsewhere that maintain information-rich consumer databases are increasingly uneasy as news of breaches becomes an almost daily occurrence.

"It's something that I do think is a big concern out in the community," said April Wimberg, an attorney at Bingham Greenebaum Doll LLP. She authored a January article titled "Electronic Data Breach Planning: 4



April Wimberg

Tips For Reducing Liability Risk" on the firm's website.

Amy Cabbage, an attorney with McBrayer, McGinnis, Leslie & Kirkland PLLC, said companies need to think through their response to a potential breach – who to call, who to mobilize and how to limit the damage.

Having a plan is important, said Bob Dibert, an attorney at Frost Brown Todd LLC. He said developing a customized cyber response plan is like "having the first 10 plays scripted in a football game."

Attorneys recommend that cybersecurity plans include a strategy on how to communicate to the public in the event of a breach.

"The quicker you respond, the better," Cabbage said. "Unless you come out with some kind of mea culpa in the first few hours of



Amy Cabbage

## FIVE KEY CYBERCRIME AND CYBERSECURITY ISSUES TO CONSIDER

A February National Law Journal article highlights five key cybersecurity issues to consider when formulating a federal legal approach to fighting cybercrime.

1. Legislate national notification standards.
2. Restore the effectiveness of the 1984 Computer Fraud and Abuse Act.
3. Create trade-secret remedies and protection.
4. Share cyber threat information among government and corporations.
5. Promote understanding and restore public trust.

SOURCE: THE NATIONAL LAW JOURNAL ARTICLE, FEB. 19, 2015

## STATS AT A GLANCE

The federal government spent less than \$1 billion on cybersecurity in 2000. For fiscal year 2016, President Obama requested a budget of \$14 billion for cybersecurity.

Analysts project that \$77 billion will be spent by corporations and others on cybersecurity this year alone.

Members of the U.S. Congress and congressional committees generally agree that comprehensive cyber legal reforms are necessary.

SOURCES: FOX BUSINESS, BEZINGA, THE HILL, MITCHELL S. KOMINSKY, REUTERS

## COMMON MISTAKES WHEN CREATING A CYBERSECURITY STRATEGY

1. You must have data backup for any plan to be worthwhile. Some companies have no meaningful computer backup, which makes response to a breach and remedial efforts much more difficult.
2. A plan is just a piece of paper. You must have the right people in place to implement a cybersecurity plan. Don't just list the title that each person holds, but list the name and contact info of the person who has the ability to solve problems calmly and quickly under pressure.

3. A security plan needs to be practiced and continually updated. Don't create a cybersecurity plan and then leave it sitting on a shelf. Review and update it periodically and hold practice drills.

SOURCE: IAN RAMSEY, PARTNER AT STITES & HARBISON PLLC



a breach, you're going to irretrievably damage your brand.

"If you step up and ask for forgiveness, people are pretty quick to forgive," she said. "If you flounder around and point fingers, people don't forgive that."

Attorneys said businesses also might want to purchase a cyber insurance policy to protect themselves in case they are sued. These cybersecurity policies are becoming increasingly popular, and a business can contact its insurance agency to find out more.

"We're seeing in the marketplace the emergence of information security insurance," Dibert said. "Big data means big targets."

#### A variety of risks

Most large breaches are committed by cyber criminals working for governments, organized crime, political movements or corporate espionage. But sometimes, breaches are caused by employee error, independent hackers or a disgruntled former employee.

"It might be that (cybercrime) is new to people in Kentucky, but it's not new to the criminals because they've been doing it for many years," Ramsey said.

The No. 1 person on the FBI's Cyber's Most Wanted List is a Russian man using the online moniker "lucky12345," Ramsey said. The suspect, Evgeniy Mikhailovich Bogachev, is wanted for his alleged involvement in a wide-ranging global racketeering enterprise in which bank account numbers and passwords were stolen, resulting in losses of more than \$100 million, according to the FBI website.

Cubbage reminds business owners that they need to protect not only the personal consumer information in their marketing databases but also their own internal corporate plans, emails and documents.

"It's not just about your consumer data," Cubbage said. "It's also about your company's data. The emails in the Sony breach were just humiliating."

The database of the Sony Pictures Entertainment movie studio was breached in 2014, resulting in widespread distribution of more than 6,000 internal memos containing comments about pay disparities, personal feuds, failed projects and gossip about movie stars.

Companies that need help formulating a plan might want to consult with firms that specialize in preventing cybercrime, attorneys interviewed for this article said. Such firms – FireEye Inc., CyberArk Software Ltd. and Fortinet Inc., among others – have become the darlings of Wall Street as investors snap up these stocks as breaches become increasingly common.

#### Privacy and politics

There is no overarching federal cybercrime law, though there are rumblings in Congress about it. Very little case law exists on cybersecurity either.

"There are a lot of state laws," Wimburg said, "and it's almost begging for a federal law for companies that operate in multiple states."

President Barack Obama urged congressional lawmakers to take action on federal cybersecurity legislation in his Jan. 20 State of the Union



address.

"No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets or invade the privacy of American families, especially our kids," Obama said. "If we don't act, we'll leave our nation and our economy vulnerable."

Ramsey said that European countries are light years ahead of the United States in the sophistication of their laws and cybersecurity measures.

"The U.S. model is very different than the European model," said Ramsey, who has worked as an attorney in Switzerland for Stites & Harbison.

Ramsey said that the idea of privacy is practically extinct in America, whereas countries in Europe firmly state that personal information belongs only to the person.

Ramsey said Europeans would find U.S. marketers' use of people's names, addresses, telephone numbers and detailed buying preferences an "outrageous" act.

European countries are much more strict in protecting personal privacy after enduring the horror of the Nazis during World War II, he said.

"(Europeans') response is that we can never let this happen again," Ramsey said. "We can never let a government use personal information against its own citizens."

#### Small and large targets

Doug Brent, an attorney with Stoll Keenon Ogden PLLC, said that not only do firms' clients experience cyber breaches, but he himself has been a victim.

"I have had three different cards that have been caught up in breach situations," Brent said.


In the past five years, Brent has been reissued a card after a national retailer had a cyber breach and was reissued another card because he had used it at Target and The Home Depot during periods when their breaches occurred.

A family member experienced attempted fraud on a card after it was compromised at a retailer and then used by a culprit at a grocery

story out of state.

Brent said that such experiences are very common and happen to even the most informed and careful cardholders. Credit and debit card issuers are now adding embedded chips and PINs to cards in addition to the existing magnetic strip to create systems that are harder to attack, he said.

Brent reminds businesses that cyber breaches can result from events other than Internet hackers. An employee in the payroll department whose work computer is stolen at a restaurant can wreak just as much havoc.

"That information could be highly valued by the bad guys," said Brent, adding that large and small companies alike need to be vigilant. "Some companies may think they don't have anything interesting to steal. That would be mistaken thinking." 

### 3 tips for preventing cyber breaches

1. Know your company by doing a data audit now. A company forgets, misplaces and loses things just as a person does. But unlike a person, there's not a single point of reference that can remember where everything is. Audit your data and create a map showing where all essential information resides.
2. Know your employees and train them now. A majority of data breaches occur because of human error. You cannot expect to protect your company's data when everyone doesn't know how to do so.
3. Listen to your IT adviser carefully. If you don't have one, find one now. Preventing a data breach is not just about having the right software to scan for malware or viruses, but a continual investment in technology and the people who understand how all of it works together.

SOURCE: IAN RAMSEY, PARTNER AT STITES & HARBISON PLLC