Issue #32
December 2015

GREAT AMERICAN and LOWERS & ASSOCIATES

Fidelity / Crime Observer

The Black Sheep Grill Room Gets Fleeced

The Hemlock Hill Restaurant Group owns thirty-five restaurants in seven states. Gross sales reach $150M. One restaurant, The Black Sheep Grill Room is located in the financial district of a major city. The restaurant is open for lunch and the after work commuter crowd. They also operate a bakery/coffee shop in the adjacent space.

Vicky Morgan was the longtime bookkeeper for the restaurant and bakery/coffee shop. She arrived at the shop early each morning to do the books from the night before. She was a single parent, raising a teenage daughter.

Hemlock Hill Restaurants have all their properties report daily business into the home office via the corporate accounting reporting system to track all of the locations from one source. The individual restaurant locations maintain their records in an accounting sales system, a separate accounting system from the corporate system. The sales system is tied to the cash registers at the individual locations. Customer checks are rung into this system that records food and beverage sales, tips, taxes, and payment methods (cash or credits cards). The information is captured in a Waiters Report. Certain home office employees have access to the restaurant sales systems.

The two systems do not “talk” to each other. The bookkeeper for each restaurant was required to manually input the information from the sales system into the corporate accounting system. Ms. Morgan’s job was to print the Waiter Reports reflecting the amount of business done the day before, input that information into the corporate accounting system, and then prepare the daily deposit. The home office staff relied upon the information reported manually by the individual restaurants into the corporate system. If a question was raised about a particular restaurant, they would look at the second system but for all intents and purposes they did not have the time to review thirty-five different systems each day.

On March 18, 2015, Ms. Rogers, a home office accounting employee reviewed the sales information for the prior day, St. Patrick’s Day. She thought the numbers were going to be higher so she conducted further review. In looking at the information, she noticed a discrepancy regarding net sales—the restaurant system reported net sales were $14,922.17 while the bookkeeper reported $9,840.06 into the corporate system. When asked about the discrepancy, Ms. Morgan explained that one report included taxes while the other did not. She said that she needed to back the tax out of the sales figure.

After spending time going over the reports, Ms. Rogers could not reconcile the difference. She brought the matter to the attention of her boss who said that both net sales figures on the reports are net of taxes and should be equal. He had her run a complex sales report from the restaurant sales system to confirm the correct amount. Looking at the two reports he saw that the amount of the deposit on the corporate accounting report was $5,082.11 less than what the restaurant sales system said it should be. The deposit was $5,082.11 short. They pulled the previous five days reports and discovered more discrepancies.

The next morning they confronted Ms. Morgan at the restaurant. They asked her to explain the shortage on March 17. Morgan told them the discrepancy was caused by a problem with the credit card machine. They then asked her about the previous five days’ shortages. She had nothing to say other than to admit that she had stolen the money.

The forensic investigation revealed she stole $1.2M over a five year period.

Continued on Page 4

Contact List

Great American Insurance Group

Dennis Burns, SVP
Fidelity / Crime Division
212.513.4017
dburns@GAIC.com

Lowers Risk Group

Steve Yesko, ARM
Director, Business Development
540.338.7151
syesko@lowersriskgroup.com

Inside This Issue

Hackers Gonna' Hack: Recap of Theresa Payton, Former White House CIO, at the SCTA Conference

October 1, 2015
By: Lowers Risk Group

True or False: 95% of all security breaches are due to sophisticated cybercriminals that we could not defend ourselves against. Believe it or not, the answer is false. In fact, we are most often victims of breaches due to human error which is linked to poor security design.

The recent Secure Cash & Transport Association (SCTA) Conference, which brought more than 200 cash management industry thought leaders to Chicago, was filled with insightful speakers and important discussions about the security, transportation, and management of cash in today's world. Foremost among them, was Keynote Speaker and former White House CIO, Theresa Payton, who stressed the need to design security "for the human psyche." As Ms. Payton so astutely pointed out, 95% or more of past breaches were a result of human error, this according to the 2014 IBM Security Services Cyber Security Intelligence Index. From clicking on a malicious link found in a phishing email, to running servers that are set up with the wrong settings, to lost laptops or portable media, human error is a huge concern.

95% or more of security breaches are a result of human error which is linked to poor security design and NOT a result of sophisticated cybercriminals.

To illustrate the point, Payton and her team conducted a geofencing test to show how a hacker might target companies through individuals. Similar to how a physical security team for a rock star might draw a circle around a venue and look at all the entrances and exits to the venue to ensure the safety of the rock star and the crowd, in the digital sense, geofencing was used to demonstrate how any of us, while connecting with loved ones through social media, could expose too many clues.

Payton explained the steps of her geofencing experiment, which involved drawing a "digital circle" around a physical location, using tools to see all social media being posted within or near the geofence, reverse facial recognition, geolocation tools, and demonstration of how all of the data collected could be used to trick the subject into giving access to a network of data.

The point of the experiment was to demonstrate why it is so critical that all security programs help design and manage through the human psyche, and not against it.

Designing Security for the Human Psyche: Evolutionary Change Required

Payton stressed the need to design applications under the assumption that your users will do everything wrong – they will share passwords, they will forget them, and they will do unsafe things to get their jobs done, such as use free, unsecure WiFi.

To make evolutionary change, Payton suggests we need to incorporate the following scenarios:

- ❑ Understand and educate the knowledge of human nature and psyche into the cyber security profession.
- ❑ Incorporate that knowledge into the design and implementation of all our systems.

Innovate cyber security technologies and policies that account for insecure human behaviors and incentives. Unless we do these things, she contends, our privacy and security will perish.

Continued on Page 3

Hackers Gonna' Hack: Recap of Theresa Payton, Former White House CIO, at the SCTA Conference

Continued from Page 2

How can you put these changes into action?

Payton suggests the following five steps:

1. Design security awareness and rules with your end user in mind.
2. Knowing users will break all the rules by accident, segment your most critical data elements away from every day access (different credentials, limited access, expiring passwords).
3. Use expiring and limited credentials. In a recent study, 70% of people polled said they have access they don't really need and many admitted they peak at the data because they have access!
4. Implement "digital shredding." Just like you wouldn't keep overstuffed paper files and cabinets, Payton suggests getting rid of unneeded data in the digital sense.
5. Reward reporting. Make it easy and recognize and reward employees who report malware, strange emails, or other suspicious files or network activity.

Payton stressed the need to design security applications under the assumption that your users will do everything wrong.

The US Director of National Intelligence has ranked cybercrime as the top national security threat, higher than that of terrorism, espionage, and weapons of mass destruction. A threat of this level is bound to impact everyday organizations. Payton made the impactful statement that at some point technology will fail and process is all that will remain. This is why she says it is so very important to design for the human psyche.

Is your organization on the offense when it comes to addressing cybersecurity and the human psyche? We'd like to hear from you.

The US Director of National Intelligence has ranked cybercrime as the top national security threat, higher than that of terrorism, espionage, and weapons of mass destruction.

Great American Insurance Market Advantage Quick Facts

- **The Great American Insurance, Fidelity/Crime Division was established in 1995 and has grown to be the 4th largest crime insurer in the U.S.**
- **A.M. Best rated "A+" (Superior) Class XIII and Standard & Poor's Rated "A+" (Strong).**
- **A.M. Best Rating of "A" (Excellent) or higher for over 100 years.**
- **Licensed in all 50 states and Canada.**
- **$50 million in capacity for Commercial Crime and tailored coverages to meet the specific needs of our clients.**
- **$65 million in capacity for Kidnap, Ransom, & Extortion coverage. $0 deductible applies.**
- **7 regional offices in 3 countries.**
- **Partnership with highly-regarded global risk mitigation firm.**
- **Experienced claim staff only handling Fidelity/Crime claims.**

For more information please visit our website at www.crimeinsurance.com | Applications | Brochures.

To Hire An Ex-Offender or Not: Evaluating Your Risks

Should you hire an ex-offender? The easy answer is "it depends," but in the real world you can't just peer into your applicant's eyes and get the answer. The employer's dilemma is that the choice you make exposes you to potential risks of competing types.

The socially-beneficial choice is to hire ex-offenders, and right now there is a lot of pressure on employers to do just that. (Assuming, of course, there are not very legitimate reasons to exclude them based on the risks inherent in the role.) The threads in the conversation on this issue range from feel good stories about employers who have had great successes hiring ex-offenders to organized movements working to get more job opportunities for them. These mostly positive stories are backed up by the legal mandates of employment law rooted in anti-discrimination concepts.

Yet employers are still responsible for the safety of their customers and workers. To the extent that having committed a crime in the past is a predictor of future anti-social actions, ex-offenders seem to pose extra risk. If these risks materialize, the employer is potentially liable for negligent hiring or retention.

A common response to the risks associated with hiring ex-offenders is for employers to adopt a "blanket" exclusion policy and simply reject all applicants who have a criminal history. Unfortunately, neither hiring every ex-offender who walks in the door nor rejecting every one of them is an effective way of managing the competing risks. The better course involves making decisions on individual applicants; taking the relevant factors into account. Read this complete blog and get our free guide below. Proforma Screening Solutions is a Lowers Risk Group company.

The Black Sheep Grill Room Gets Fleeced

Continued from Page 1

How did she steal for so long before she was caught? There are several reasons. First, the home office had the ability to review the information from the restaurant sales system directly but failed to do so. Instead they relied on the corporate accounting system that contained the manually input data. Staffing was lean. It was less time-consuming to use the corporate system that contained the data for all locations rather than looking at thirty-five different systems. Second, updating the computer system was expensive and Hemlock Hill was not about to change something that in their mind was not broken. Third, Ms. Morgan was good at her job and developed a high level of trust with management. It never crossed their minds that she would steal. Fourth, internal or external audits did not include review of the restaurant sales system. Fifth, there was no separation of duties. The person reporting the numbers was the one responsible for the deposit. Lastly, Ms. Morgan tested the waters when she contemplated stealing by reporting small discrepancies. There was no response from the home office. She soon came to understand nobody was looking at the restaurant sales system and she was off to the races. She gradually increased the amount of theft to a level so as not to raise any questions. Like most embezzlers however her undoing was greed. The large amount of cash after St. Patrick's Day was too tempting and proved to be her downfall.

What motivated Ms. Morgan to embezzle from her company? It turned out the thefts started around the time her daughter began equestrian lessons. As the teenager became more proficient, Ms. Morgan felt the need to fully support her endeavor. She quickly learned how expensive the equestrian sport can be. Her daughter went from riding a horse provided by the riding academy to one her mother purchased. Stable fees, feed, veterinarian care, transportation to competitions and other expenses were well beyond Ms. Morgan's bookkeeper salary.

This is a loss that could have been avoided. Unfortunately, the company failed to establish adequate controls. Even though the home office staff had access to the source information it was largely ignored. Ms. Morgan realized this and took advantage. In the end the Black Sheep Grill Room was out $1.2M.

By Thomas E. Maloney, Vice President
Great American Insurance Group—Fidelity / Crime Division