Vol.36, No.1 – 2020

Corporate downsizing: Where loyalty dies, dishonesty lurks

Anthony Luizzo, PhD, CFE, CST, PI (Ret. NYPD)

You can take a number of steps to avoid increases in thefts and other dishonest behaviors after companies cut jobs.

(Anthony Luizzo, PhD, CFE, CST, PI (Ret. NYPD), is a member of the board of advisors of Vault Verify, LLC. He is a former detective specialist with the NYPD and a former senior security executive with the New York City Mayor's Office of Economic Development and Business Services. He is the former Corporate Director of Security and Loss Prevention for the New York City Health and Hospital Corporation, the largest public healthcare system in the United States. Luizzo is a member of IAHSS and a frequent contributor to this journal.)

When business are in financial straits, some turn to downsizing, which the website Investopedia defines as "the permanent reduction of a company's labor force through the elimination of unproductive workers or divisions"—meaning the elimination of people or groups who do not bring in enough revenue [1]. When employees in an organization that has undergone downsizing feel betrayed or as if they or their co-workers are also at risk of being axed, they are more likely to engage in crimes such as theft than would be true if they felt more secure. Below, I offer suggestions for combating the increase in dishonesty that often accompanies downsizing.

TRENDS

According to a 2015 article at Fortune.com called "The 10 Biggest Corporate Layoffs of the Past Two Decades," the 10 companies that had the largest layoffs in that time collectively released

more than 400,000 workers [2]. Obviously, when statistics from small businesses are included, the numbers are staggering and a sad thing for American workers!

When it comes to hospitals, the data is equally staggering. According to an April 30, 2017, article by Casey Ross on the website STAT ("Facing a Financial Squeeze, Hospitals Nationwide are Cutting Jobs"), hospitals are cutting jobs amid a whirlwind of financial pressures and fears about future healthcare legislation [3]. The article goes on to quote an Ohio Hospital Association spokesperson who stated that many hospitals had managed to "make cuts using a scalpel instead of an ax," but they were "running out of options." Since that article was published, Congress has passed *no* serious legislation to deal effectively with the problem in healthcare. Moreover, many rural hospitals have had to close up shop, making it much harder for patients to access lifesaving medical services.

RELATION BETWEEN DOWNSIZING AND CRIMINALITY

In 1996, in an article titled "The Hidden Cost of Downsizing: Where Loyalty Dies, Fraud Grows," George Van Nostrand and I noted that, although no reliable authority had established a definitive link between downsizing and increased employee fraud in companies undergoing cuts, anecdotal evidence suggested such a link [4]. And there is a logical path between downsizing and fraud. From the turn of the 20th century through the late 1980s, many corporations had an unspoken contract with workers generally implying that if workers were loyal, did their jobs, and did not violate any major rules, they could expect to stay with the company for many, if not all, of their working years. This family spirit is long gone, and loyalty by owners and workers often seems to begin and end with each paycheck! In the absence of feelings of loyalty, it would not be surprising if employees who feared that they were becoming expendable would become more prone to stealing from the company or engaging in other dishonest behaviors.

WAYS TO HELP LIMIT CRIMINALITY

Forward-thinking security

executives, often called the "soldiers in the war against dishonesty," instinctively know that loyalty and honesty are the most important attributes that all new hires must bring to the table. Studies have shown that when employees feel themselves to be part of a corporate family and secure in their job, they also tend to feel that they have a stake in the success of the company and will usually keep a watchful eye over company assets. Conversely, if an employee believes there is *no* corporate family or loyalty code, he or she might feel disenfranchised and open to various forms of criminality (thievery, product-tampering, corporate spying, and so on). In the court of investigative consensus, many protection mavens believe that the first areas of the workforce affected by downsizing are those departments that *do not* directly increase company revenues, such as, security, internal audit, human resources, and others that fall within this continuum.

From a protection point of view, one method of maintaining optimum protection in the face of downsizing is to devise a series of innovative strategies to help keep criminality at bay. An excellent method of accomplishing this arduous task might be for security executives to begin thinking outside of the proverbial protection-specific toolbox and consider proactively reaching out to security specialists to conduct a security assessment that would ascertain any weak spots in the security curtain and devise strategies to mitigate these risks.

Several innovative protection-strengthening strategies might include the ones that follow.

Prepare a criminality impact assessment. Step 1 is to reach out to the company's CFO to ask for a list of existing and contemplated layoffs. Often, seasoned security executives have the expertise to internally evaluate whether layoffs will have a detrimental effect on facility protection. If the security executive does not have the expertise to conduct this evaluation, an outside expert should be consulted. It would be much more beneficial if this assessment were commissioned before cuts took effect, but an after-action assessment works well also.

Ensure that the security and

internal audit departments work effectively together. There is a long history of Security and Internal Audit not sharing information. It's important to remember that both functions are responsible for asset protection and should coordinate efforts when possible.

Implement low-budget security strategies. The Web is chock-full of low-cost strategies to help security executives stretch the security dollar. An excellent example might be to consider establishing a "security advocate" program, which involves positioning select employees at strategic locations within their offices who are charged with simply saying, "Can I help you?" to any and all unrecognized incoming visitors entering their areas of responsibility. Pertinent information on low-budget security strategies can be found in a recent article I wrote for *Texas Investigator Magazine* called "Squeezing the Most from the Security Dollar." The article lists several proactive security and safety strategies for deepening and strengthening a company's global protection envelope [5].

Include metrics in security and safety planning. A trilogy of articles that I wrote or coauthored in recent issues of this journal offers a roadmap for using metrics effectively to bolster facility security (see references 6, 7 and 8). Using metrics in security planning gives security administrators the ability to speak the language that CFOs understand and is especially valuable when it comes to seeking additional resources or justifying security and safety-related expenditures. One of the many benefits of applying metrics is that they can help to reveal fluctuations in service delivery and deteriorations in service levels, which are often breeding grounds for dishonest employment-related activities.

Devise an internal thievery-prevention data-sharing initiative. Following the age-old adage that "asset protection is every employee's responsibility," establish a data-sharing relationship among departments (human resources, internal audit, shipping and receiving, and so on) so that the security department becomes the repository of real and/or possible thievery-deterrence information. Often this data might include external di-

rectives from participating vendors about shipping and receiving fraud schemes, relevant terrorist information affecting other similar facilities, and the like. It is also important to establish a hotline for employees to use with anonymity.

Institute security- and safety-awareness workshops to deepen and strengthen facility protection. These seminars are designed to deliver the message that security is every employee's responsibility. Often these seminar programs are offered gratis by local law enforcement agencies and include personal-safety workshops and information about effective office security and safety strategies, etc.

Perform background checks on prospective employees. Volumes have been written about how to hire the right person for a given job, and human resources executives have developed a plethora of interview techniques to determine if an applicant is the right fit for a given job. The effort should include background checks. Further information on background checks can be found in a 2014 article I coauthored in this journal called "Background Checks: A Diagnostic Tool to Decipher Deception" [9]. The article outlines in some detail how the horrific terrorism-related tragedies hitting our shores, churches, synagogues, schools, and cities, coupled with the losses of protection advocates as a result of downsizing, has reinforced the need for and the value of background screening as a protection tool and job-applicant-verification strategy. The art and science of hiring trustworthy employees begins and ends with sitting down face-to-face with prospective candidates during the intake interview and then delving deeper into their backgrounds via performing a comprehensive background-surveillance check. The antiquated policy of only checking previous employer references is a prescription for disaster, especially since today's job applicant most likely has resided, attended, and worked in several geographical jurisdictions nationwide or perhaps even worldwide.

It is always important to study the rules governing due diligence before embarking on the journey of performing background checks. Federal and state rules limit the types of informa-

tion an employer may obtain and use concerning an applicant's background. Violating these statutes are corporate-reputation and bottom-line busters. Whether you perform the checking in-house or outsource these services to a third-party, you must still know and follow the law. Before performing any in-depth screening, take a moment and sit down with legal counsel to discuss what you can legally do and what you are restricted from legally doing. Next, begin reviewing federal and state statutes, including: Fair Credit Reporting Act of 1971, Privacy Act of 1974, Americans with Disabilities Act of 1990, and Health Insurance Portability and Accountability Act (HIPPA). Importantly, learn the mechanics of obtaining background records, such as educational records, criminal records, military transcripts, credit reports, and medical records. The Society for Human Resource Management (SHRM) (www.shrm.org) is an excellent resource.

Develop an interviewing procedure for assessing the integrity of all hires. An integrity interview is a one-on-one question-and-answer session between a seasoned loss-prevention investigator and a prospective employee to gauge the trustworthiness of the applicant. These interviews are usually held with people who have applied for a fiduciary position (such as cashier, bank teller, or shipping and receiving employee) and are designed to capture their views on honesty, thievery, and adherence to rules; they are also meant to champion corporate ethics. It is important to also consider extending these interviews to existing employees, especially when controversial information about the employee has been brought forward.

Initiate innovative revenue-generating initiatives to bolster the company's bottom line. Security executives need to show company management that security can be more than simply a cost contributor. One way to demonstrate such value is for the security administrator to reach out to the human resources administrator to ascertain how requests for employment and salary verifications are managed. Given that this task puts at risk a considerable amount of personal data, encompassing countless employees, it's important that

management cast an investigative eye on how this treasure trove of sensitive data is plied, disseminated, and safeguarded. When an entity does not have a corporate policy skeletonizing how the job must be done, the task may get completed in a variety of ways, some of which may not be in the firm's best overall interest.

As an example, many incoming verification requests list supervisory personnel as a contact. It is thus possible that, absent a corporate policy, these requests may end up being completed by former coworkers who may have developed a bias against the employee and/or had a previous work-related disagreement. To reduce liability and internal costs, some institutions choose to outsource this sensitive function to third-party entities that can perform the job effectively. Further information can be found in an article I co-authored in this journal [10], offering a roadmap for HR to follow.

A FINAL WORD

Hospitals understand all too well that in today's competitive global marketplace, they must run as efficiently as possible. One way that businesses sometimes try to achieve fiscal well-being is to reduce their workforce. Notwithstanding, it is equally important that business executives become familiar with the potential risks, as well as rewards, associated with downsizing, and the human toll that is being extracted. Profitability is great, but the trillion-dollar question that every business needs to ask is, *"Are these hard-earned profits simply coming into the company's front door and immediately leaving through the back door?"* Having comprehensive protection strategies helps keep that ever-important back door LOCKED!

References

1. "What is downsizing?" (2018, March 26 Update). *Investopedia.* https://www.investopedia.com/terms/d/downsize.asp

2. Zillman, C. The 10 biggest corporate layoffs of the past two decades. (2015, September 20). *Fortune.com.* https://fortune.com/2015/09/20/biggest-corporate-layoffs/

3. Ross, C. (2017, April 30). Facing a financial squeeze, hospitals nationwide are cutting jobs. *STAT.* https://www.statnews.com/2017/04/30/hospitals-layoffs-national/

4. Luizzo, A. & Van Nostrand, G. (1996, September/October). The hidden cost of downsizing. *The White Paper (from the Association of Certified Fraud Examiners), 10,* 23–25.

5. Luizzo, A. (2018, Summer). Security spot-

light: Squeezing the most from the security dollar. *The Texas Investigator,* 30–32. https://www.tali.org/assets/TTI/tti%20summer%202018%20issue%20.pdf

6. Luizzo, A. & Scaglione B. J. (2015). An alternative view in the development of security metrics. *Journal of Healthcare Protection Management, 31,* 98–104.

7. Luizzo, A. (2016). Resources available for applying metrics in security and safety programming. *Journal of Healthcare Protection Management, 32,* 27–33.

8. Luizzo, A. J. & Scaglione B. J. (2017). Applying metrics to 21st century healthcare security. *Journal of Healthcare Protection Management, 33,* 7–13.

9. Luizzo, A. J., Scaglione B. J., & Luizzo P. F. (2014). Background checks: A diagnostic tool to decipher deception. *Journal of Healthcare Protection Management, 30,* 57–65.

10. Luizzo, A., Roy, B., & Luizzo, P. (2016). A new approach to handling incoming verifications. *Journal of Healthcare Protection Management, 32,* 95–99.

Distribution by the Author for Educational Purposes

Anthony J. Luizzo, PhD, CFE