Daniels Fund Ethics Initiative
University of New Mexico
http://danielsethics.mgt.unm.edu

**Debate**

# Using Predictive Analytics for Detecting Insider Risk

*Issue: Should firms use predictive analytics to monitor employee emails for insider risk?*

Many firms are turning to predictive analytics to analyze or predict employee behavior. Predictive analytics use statistics, modeling, data mining, and more to apply big data toward predicting future events. For instance, some firms are using predictive analytics to aid with staffing decisions. Big data allows organizations to identify trends and connections that are hard to see with traditional research methods. The more information a company is able to get about a prospective employee, the more likely it is able to determine whether he or she would be a good fit.

Predictive analytics is also being incorporated into risk management. In a world where hacking and cybercrime have become commonplace, firms are focused on external threats to their intellectual property and sensitive information. However, a recent cybercrime survey shows that 27 percent of electronic attacks on organizations come from within the firm. Even the largest firms are not immune—Morgan Stanley and Goldman Sachs were both hit with internal attacks. Disgruntled employees may decide to try and harm the company's reputation or steal customer data if the opportunity arises.

Not every employee who is frustrated or dissatisfied with his or her organization will commit a cybercrime against it. But some employees might. The problem is that email communication reduces the ability of managers and employees to observe co-workers' behavior. According to Ed Stroz, a former FBI agent and co-founder of security firm Stroz Friedberg, our dependence on email communication has reduced the kinds of face-to-face interactions in the workplace that indicate potential issues with problematic employees. Less interaction means fewer opportunities to observe warning signs. As a solution to this problem, he believes firms can analyze the language in employee emails to detect employees who may pose an internal risk. Yet with massive numbers of emails being sent and received by businesses every day, it impossible for most organizations to track every email without sophisticated technology.

Ed Stroz's solution is SCOUT®, a tool that uses psycholinguistics to monitor the language in employee emails. Psycholinguistics involves the use of algorithms to identify how each employee uses language and determine if there are major changes. A negative change in language could indicate a problem with an employee. For instance, phrases like *I loathe my job*, *he's a zero*, and *you're awful* all suggest discontent or anger with the firm. Additionally, employees who log on to their work computers at strange hours or when nobody else is working could also indicate a problem. SCOUT® looks for these patterns. By examining an employee's email over time, SCOUT® can determine (1) what constitutes normal language for the employee, and (2) sudden changes in language to signal a change in morale or satisfaction. Tests of the technology indicate that it can be highly effective in predicting possible cybercrimes or other forms of employee sabotage.

The monitoring of emails is not new. However, because it is usually infeasible to analyze every email sent every day from work computers, random samples are usually analyzed to determine if there is a problem. This leaves many emails unaccounted for. SCOUT® is able to handle this vast amount of email and will only alert managers to

emails that appear suspicious. Stroz believes this still affords employees privacy because most emails will not be brought to the manager's attention, but only those that might be suspicious. As an example, one client organization that used this tool experienced flagged messages that constituted only 0.0008 percent of all email sent. The company claims that 30 out of the *Fortune* 50 have used this product.

There are enormous benefits to being able to anticipate insider risk. First and foremost, if managers are able to identify angry or disgruntled employees with the potential to commit cybercrime, they can take steps to stop these individuals before they are able to commit misconduct. Additionally, the information SCOUT® offers can be used to determine problems in the organization's culture, such as failures in leadership or conflict between employees. These practical uses of the technology have the potential not just to mitigate risk but to actually improve employee morale and interactions between co-workers and managers. SCOUT® has also been used to indicate extreme stress among employees. In one case, company officials were able to able to prevent a suicide because they were alerted to the employee's stress and were able to address it.

On the other hand, employee privacy becomes a big issue in using this technology. From a legal standpoint, companies have the right to monitor emails if they inform employees beforehand that the computers belong to the company and they may be monitored. Stroz claims the tool respects employee privacy because it only flags suspicious emails for further review. However, although this is the way the product is *supposed* to be used, companies may not use it in this way. Some privacy advocates believe the data collected through predictive analytics has the potential to be exploited by employers. Additionally, there is always the possibility that an employee whose emails are flagged might not have any intention of harming the firm, meaning that the monitoring has created a false positive with potential harm to the employee's career. Critics believe that algorithms cannot replace humans in making these types of decisions, and some legal experts feel that even with implied consent from the employee, employees who feel they are being unfairly treated may try and seek legal recourse for tracking their emails.

## There are two sides to every issue:

## 1. Predictive analytics used to detect insider risk in organizations is an ethical way to detect employee problems before they occur and respect employee privacy.

## 2. Predictive analytics used to detect insider risk in organizations cannot replace the human element and can be misused to retaliate against employees.

**Sources:**

Ben DiPietro, "'Psycholinguistics' Used to Identify Troubled Employees," The Wall Street Journal, June 18, 2015, http://blogs.wsj.com/riskandcompliance/2015/06/18/psycholinguistics-used-to-identify-troubled-employees/?cb=logged0.8254254915588222 (accessed July 20, 2016).

Julia Gorham, Anita Lam, and Paul Jackson, In An Era of Cyber Anarchy Is It Time for Enhanced Employee Monitoring, December 15, 2015, https://www.dlapiper.com/~/media/Files/Insights/Events/2015/12/DLA%20Piper%20TechLaw%20HK%20%20In%20an%20era%20of%20cyber%20anarchy.pdf (accessed July 20, 2016).

Stroz Friedberg, "Organizational Health in the Face of Insider Threat," https://www.strozfriedberg.com/wp-content/uploads/2016/04/SCOUT-Organizational-health-in-the-face-of-insider-threat.pdf (accessed July 20, 2016).

Roger Parloff, "Spy Tech That Reads Your Mind," Fortune, July 1, 2016, 72-77.