2017

Balancing Integrity with Privacy Interests: Fighting Cyber-Corruption with Background Checks

Robin J. Kempf

Chelsea Binns

Balancing Integrity with Privacy Interests:

Fighting Cyber-Corruption with Background Checks

Authors: Robin J. Kempf and Chelsea Binns

Robin J. Kempf has been an Assistant Professor at the John Jay College of Criminal Justice, City University of New York since Fall 2014. She teaches in the Public Management Department.

Chelsea Binns is an assistant professor of criminal justice, legal studies, and homeland security at St. John's University.

Cybercrime is a serious threat to the public sector, especially as more of the public's business is automated. In recent years, malicious actors have successfully infiltrated systems at the U.S. Department of Defense, the Navy, and the Environmental Protection Agency. Yet despite all the media attention on external hackers, especially those coming from foreign countries, employees remain the biggest cyber risk to governments. While background checks may promote employee integrity among those in public service, privacy concerns exist. This brief discusses how background checks are utilized to mitigate employee risk of cybercrime in the financial industry. The practices of this heavily regulated industry serve as an ideal example for the public sector, which is increasingly targeted by a highly dangerous form of public corruption: internal cybercriminals.

Introduction

Workers in the United States are estimated to be responsible for 80 million cybercrimes each year against their own employers. In the public sector alone, employees perpetrate over half of all cybercrimes, including cyberespionage, which is now the most common attack in the public sector. Such cyberespionage attacks are facilitated with "spear-phishing" emails that steal electronic data. In 2016, Charles Harvey Eccleston, a former Department of Energy (DOE) worker, was arrested after pursuing a spear-phishing cyberattack against fellow DOE employees. Eccleston also attempted to sell top secret DOE data to an undercover operative. The risk of employee-perpetrated cybercrime is something public managers must take seriously.

One method used to proactively reduce the risk of corruption – whether cybercrime, embezzlement, or other corrupt acts – is to perform background checks on job applicants; however, overly intrusive background checks may compromise applicants' rights to privacy. Further, employers run the risk of perpetuating discrimination against disadvantaged applicants. It can be challenging to balance those competing considerations, especially when hiring public sector workers who will have access to sensitive computerized information.

For lessons on how to balance these competing interests, we turn to the financial sector, an industry critical to the world economy, and one with experience in the kind of cybersecurity issues now confronting the public sector. Although both sectors are targets for cyberattacks, in 2016, the financial industry was subject to more cyberattacks than any other sector. As a result, hiring in the financial industry has become heavily regulated, with a particular focus on background checks of applicants. An examination of how background checks work in the financial sector can help illuminate how public employers may want to approach background checks and better balance the interests of applicants, employers, and society at large.

Balancing Interests when Using Background Checks

Employers have an interest in compiling information about an individual to help determine his or her eligibility and fitness for employment. Why? For one thing, surveys have found that over half of people lie on their resumes. Background checks certainly do not guarantee a problem-free workplace, but they are a time-tested, proactive step to pinpoint and prevent potential problems. At a minimum, background checks help employers make better, more informed hiring decisions. Typically, background checks include verifying applicants' claims of education, past

employment, and military service. Yet, more extensive processes may explore items of an applicant's past which could shed light on his or her character or potential to commit a crime on the job. Studies have confirmed that criminal history is one of the strongest predictors of future bad acts.[1,2,3] As a result, a background check may include a person's criminal history, along with past civil court cases, such as divorce and bankruptcy proceedings, or relevant regulatory and licensing requirements and any past violations thereof.

In the United States, background checks are generally legal and widespread. Some types of jobs, such as those in which employees work with vulnerable populations, require background checks by law, but one study found that 96 percent of organizations in all sectors use some minimal type of background check as an investigative tool whether required or not.[4] Generally, the decision to conduct a background check is up to the employer.
While an important component of the background check is a criminal history search, such searches are not always conducted. According to the Society of Human Resource Management (SHRM), 73% of employers conduct a criminal check on applicants.

Private sector employers are highly incentivized to perform criminal checks to avoid legal liability for negligent hiring or retention. In fact, avoiding liability is the justification most employers use for conducting criminal history checks on job candidates. Yet the extensiveness of these background checks has limits. Courts have stated employers must demonstrate that the information collected in a background check is directly related to the responsibilities of the position and consistent with a business necessity.

On the other hand, job applicants, like all individuals, have an interest in keeping their personal affairs private. In fact, the Fourth Amendment to the U.S. Constitution provides individuals with a right to privacy in their personal information. In a world of ubiquitous social media usage and easy access to information online, privacy can be harder to protect than ever; yet, ideally, job applicants should be judged based on their professional qualifications, rather than on their private backgrounds unrelated to the job needs.

In 2016, the financial industry was subject to more cyberattacks than any other sector.

Also problematic is the fact that over-zealous background checks may compromise other societal priorities. Scholars and practitioners suggest that background checks may provide a pretext for discrimination based on class, race and ethnicity, or gender identity. As such, background checks are limited by the constitutional and legal protections on applicants' privacy, which are enforced by common law torts or civil rights suits. Under Title VII of the Civil Rights Act of 1964, employers are prohibited from treating similarly qualified applicants differently because of their race, natural origin, or other protected characteristic. If discrimination based on criminal record has a disparate impact on protected classes, the employer must show the exclusions are job related and consistent with business necessity. The EEOC provides guidance for all industries on how criminal records are to be utilized by employers to prevent discrimination.

Additional laws provide applicants with more protections. Under federal law, employees and applicants have the right to be informed before an employer asks any third party to perform a background check on them (although the employee or applicant need not be informed if the employer performs the check). Also, several local and state jurisdictions have decided that asking applicants to check a box on a job application indicating a past criminal conviction may unfairly stigmatize ex-offenders trying to reintegrate into society. For this reason, many jurisdictions have passed "Ban the Box" laws to limit how employers can ask about applicants' criminal records. Specifically, government employers are encouraged to reserve the criminal history check until the end of the application process, to avoid inadvertent discrimination.

In the public sector, the background check process is inconsistent. In the federal government, a basic criminal history check is always included in the hiring process. However, the federal government recently instituted a "Ban the Box" rule requiring all federal employers to ignore the results of that research until later in the hiring process. At the state and local level, a "fragmented patchwork of laws" exists concerning the use of criminal background checks.

Given this complicated legal landscape, how do public employers balance their need to prevent internal cybercrime with applicants' rights to privacy? Reference to the financial industry provides lessons about how the public sector might approach the use of background checks in the hiring process.

Background Checks in the United States Financial Industry

Applicants in the financial industry are legally subject to heightened scrutiny, because of their fiduciary responsibilities and potential to inflict widespread economic harm. Evidence has also demonstrated that applicants in this industry often lie on their resumes. Regulators specifically require financial industry employers to consider the criminal background of employees during the hiring process. The stringent background checks in this industry allow employers to preemptively reject potential workers who may pose cybersecurity threats. Employee privacy is considered secondary to this mission. As a result, this industry has been made exempt from "Ban the Box" laws.

Several laws, regulations, and universal practices, summarized in the following table, govern the background check process. The table illustrates two significant elements to hiring in the financial industry. First, background checks are required for all applicants. Second, several types of past crimes provide a complete bar to employment to many types of finance jobs: dishonesty, breach of trust, money laundering, drugs, or other financial crimes.

Table A: Background Check Laws in the U.S. Financial Industry

Applicable Law or Regulation	Requirement
Federal Deposit Insurance (FDI) Act, Section 19	FDIC-insured depository institutions may not hire individuals who have been convicted of criminal offenses involving dishonesty, breach of trust, money laundering, or drugs without the prior written consent of the FDIC.
Financial Industry Regulatory Authority (FINRA) Rule 3110(e)	FINRA-member securities broker-dealers "shall ascertain by investigation, the good character, business reputation, qualifications and experience of an applicant before the member applies to register that applicant with FINRA." Under the rule, for new hires, firms must conduct a search of "reasonably available public records" to include criminal history, bankruptcy, civil litigation, liens and business records.
Gramm-Leach-Bliley Act (GLBA), also known as the Finance Services Modernization Act of 1999	"Financial institutions," which are companies that offer financial products or services such as loans, investment advice, or insurance, conduct "pre-hire risk assessments" of applicants for positions that have access to "consumer information."
Secure and Fair Enforcement for Mortgage Licensing Act of 2008 (SAFE Act)	SAFE Act employers, i.e., state-licensed mortgage loan originators, are required to conduct a credit background check on applicants for the position of loan officers. SAFE Act employers must also submit applicant fingerprints to the FBI for a criminal background check. A license will not be granted to applicants who have been convicted of a financial crime, such as fraud, theft, or bribery, including those using technology in a manner that would be considered a cybercrime.

What Public Managers Can Learn from the Financial Industry

There are two practical lessons offered by the financial industry's approach to background checks, which can be considered by the public sector to balance the interest of the applicants and also address risks of employee cybercrime.

First, while the public sector wants to avoid discriminatory practices as a model employer, it also needs to recognize the heightened risk of cybercrime, which suggest greater scrutiny of applicants who want to work with computerized data. The public sector is lagging behind the financial industry in this way. The identification in job descriptions of the extent to which an employee will be required access to data is the first step in determining what should be added to the hiring process.

Second, unlike in the public sector, the background check process in the financial industry is highly regulated and is consistently applied. This consistency is favorable to the applicant, employer, and society. The regulations set expectations for the applicant, which apply regardless of where an applicant resides. The disqualifying crimes are set forth in writing and can be reviewed by all. Candidates who do not meet certain criteria can decline to apply, preventing embarrassment, which also saves the employer from interviewing unsuitable candidates. This regularized approach would serve public managers who are hiring for positions that deal with sensitive data.

Although a comprehensive legislative model utilized in the financial industry is unlikely to be imposed in the public sector, especially in a uniform manner on the state and local levels, public sector managers should voluntarily consider implementing a more vigorous and consistent background check process as is used in the financial industry. This should at a minimum include:

- Recognizing which positions require access to sensitive electronic data
- Identifying the types of criminal conduct, such as fraud or misuse of technology, that would disqualify a candidate from being hired for those positions
- Assigning an individual who will not make the hiring decision or supervise the position to collect the background information and only pass on information that might disqualify the individual

Ultimately, with careful thought and execution, the interests of all parties can be served in a hiring process that includes a thorough background check. In this way, applicants' rights to privacy will be protected as will the public's data.

References:

[1] Gendreau, P., Little, T., & Goggin, C. (1996). A meta-analysis of the predictors of adult offender recidivism: What works! *Criminology, 34*(4), 575–608. Retrieved from http://onlinelibrary.wiley.com/doi/10.1111/j.1745-9125.1996.tb01220.x/abstract

[2] Cummings, A., Lewellen, T., McIntire, D., Moore, A. P., & Trzeciak, R. (2012). *Insider threat study: Illicit cyber activity involving fraud in the US financial services sector* (No. CMU/SEI-2012-SR-004). Carnegie-Mellon University Software Engineering Institute. Retrieved from https://resources.sei.cmu.edu/asset_files/SpecialReport/2012_003_001_28137.pdf

[3] Kowalski, E., Cappelli, D., & Moore, A. (2008). *Insider threat study: Illicit cyber activity in the information technology and telecommunications sector*. Carnegie-Mellon University Software Engineering Institute. Retrieved from https://resources.sei.cmu.edu/asset_files/WhitePaper/2008_019_001_52266.pdf

[4] Brody, R. G. (2010). Beyond the basic background check: Hiring the "right" employees. *Management Research Review*, *33*(3), 210-223. Retrieved from http://www.emeraldinsight.com/doi/abs/10.1108/01409171011030372; Clifford, W. (1976). *Crime control in Japan*. Aero Publishers Inc., US; Komiya, N. (1999). A cultural study of the low crime rate in Japan. *British Journal of Criminology*, *39*(3), 369-390. Retrieved from https://academic.oup.com/bjc/article-lookup/doi/10.1093/bjc/39.3.369; Braithwaite, J. (2014). Crime in Asia: Toward a better future. *Asian Journal of Criminology*, *9*(1), 65-75. Retrieved from https://link.springer.com/article/10.1007/s11417-013-9176-0

Integrity in Brief Series

This publication is part of an ongoing series of contributions from practitioners, policymakers, and civil society leaders in the public integrity community. If you have expertise you would like to share, please contact us at **CAPI@law.columbia.edu**.

The series is made possible thanks to the generous support of the Laura and John Arnold Foundation. The views expressed here are solely those of the author and do not represent the views of the author's organization or affiliations, the Center for the Advancement of Public Integrity, Columbia Law School, or the Laura and John Arnold Foundation.

Published: July 2017