Business Horizons (2018) xxx, xxx—xxx

Available online at www.sciencedirect.com

ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

www.elsevier.com/locate/bushor

Open-source intelligence for risk assessment

Darren R. Hayes [a,b], Francesco Cappa [c,*]

[a] *Seidenberg School of Computer Science & Information Systems, Pace University, New York, NY 10038, U.S.A.*
[b] *Sapienza Università di Roma, Roma, Italy*
[c] *LUISS Guido Carli University, Viale Romania 32, 00197 Roma, Italy*

KEYWORDS
Open-source intelligence;
Critical infrastructure;
Cybersecurity;
IT risk assessment

Abstract Advances in information technology (IT) have prompted tremendous growth in security issues for companies. Increasingly, cyberattacks represent a threat to companies and national security; to prevent them, firms should routinely perform risk assessments of their IT infrastructure and employees. This article highlights the importance of open-source intelligence (OSINT) tools in conducting risk assessments to prevent cyberattacks. More specifically, we performed a vulnerability assessment on the critical infrastructure of a company operating on the U.S. electrical grid. We successfully profiled the company's network software, hardware, and key IT personnel—using OSINT—and detailed potential vulnerabilities associated with these findings. The results of our study provide empirical evidence for the efficacy of OSINT in improving the security posture of organizations. Our research findings were subsequently used to produce tactical and strategic recommendations for organizations based on the use of OSINT to identify vulnerabilities, mitigate risks, and formulate more robust security policies to prevent cyberattacks.

1. Open-source intelligence: An introduction

Advances in information technology (IT) have prompted tremendous growth in security issues for companies (Bayrak & Brabowski, 2006; Genge, Kiss, & Haller, 2015). From the early 2000s, the number of organizations reporting cyberattacks rose to around 50% (Shackelford, 2012). In 2011, almost 80% of IT corporate executives reported that their firm had been the target of an attack (McAfee, 2011; Shackelford, 2012). These attacks are primarily due to IT vulnerabilities, lack of employee awareness, and the availability of personal information that can ultimately be used to *social engineer*: leveraging technology and human emotion to gain access to a target's

* Corresponding author
E-mail addresses: dhayes@pace.edu (D.R. Hayes), fcappa@luiss.it (F. Cappa)

0007-6813/$ — see front matter
https://doi.org/10.1016/j.bushor.2018.02.001

computer (Abraham & Chengalur-Smith, 2010; Krombholz, Hobel, Huber, & Weippl, 2015; Mouton, Leenen, & Venter, 2016).

Today, websites and social networks can produce a treasure trove of personal information and behavioral attitudes of employees, and can even be used to identify a company's IT infrastructure; in turn, this identification may later be used to identify potential system vulnerabilities (Amichai-Hamburger & Vinitzky, 2010; Kandias, Gritzalis, Stavrou, & Nikoloulis, 2016). The World Wide Web maintained almost 2 zettabytes (i.e., 2 billion terabytes) of data in 2011, and this data content is predicted to grow to approximately 90 zettabytes by 2020 (Alharthi, Krotov, & Bowman, 2017). The retrieval of data from websites and online social networks has become commonplace and the information obtained is extremely valuable for cybersecurity planning (Sapountzi & Psannis, 2016; Stavrou & Gritzalis, 2015). Publicly available information can be exploited to analyze a firm's IT infrastructure and employees through the use of *open-source intelligence (OSINT)*, which is data produced from "publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement" (U.S. Army, 2010).

OSINT is a fast and effective way to perform in-depth analyses for strategic security planning, and is increasingly used by a range of governmental agencies like the Federal Bureau of Investigation, the Central Intelligence Agency, and Europol for criminal intelligence purposes (Quick & Choo, 2016). This growing interest in OSINT relies on the ability to mine websites and online social network information to determine the software being used by a company and to profile staff in critical positions. Unfortunately, there has been a disconnect between the search methods of employers—who often rely on social media accounts like Facebook (Brooks, 2017) or search engine results to screen employees for employment—and the OSINT available to adversaries. Furthermore, some state laws prohibit employers from seeking access to employees' social media accounts (NCSL, 2018), which means that new techniques must be developed by employers that seek to protect their employees and the organization. However, in this research, OSINT is seen as a powerful tool for counterintelligence so as to improve a company's cybersecurity posture. Based on the aforementioned foci, we pose this research question: Can OSINT be used by firms to perform a risk assessment in order to identify vulnerabilities before cyberattacks occur?

To answer this question, our goal was to analyze the extent to which a company's IT infrastructure and personnel could be profiled using OSINT and subsequently identify potential vulnerabilities. The objective was not to single out any particular company for deficiencies in their security posture but to explain how OSINT can be used to perform a risk assessment by identifying exposures, while ultimately providing recommendations to improve security and mitigate the risk of cyberattacks. In this case study, we provide empirical evidence that demonstrates the efficacy of this technique for companies, policymakers, and practitioners who need to improve organizational security and national security. Furthermore, we contribute to the academic discussion regarding the capabilities and potential of OSINT.

2. Methodology

We set out to profile the IT infrastructure of a specific company and gather personal information on key employees. Our case study focused on a critical infrastructure company operating in the U.S. (which we refer to as Company XYZ) as a relevant case study in determining the value of information garnered through OSINT. Critical infrastructure efficiency and safety are among the major efforts of national governments because so many stakeholders are involved and critical infrastructure has major implications regarding human welfare, the environment, and economic wealth (Bayrak & Brabowski, 2006; Cappa, Del Sette, Hayes, & Rosso, 2016). Studies on critical infrastructure networks have increased in number recently but primarily have been focused on performance, technical reliability, and network security (Bayrak & Brabowski, 2006; Gyires, 2017; Quijano, Ríos Insua, & Cano, 2016). Meanwhile, risk assessment methodologies for organizations to prevent cyberattacks have been overlooked in the literature.

Information retrieved from OSINT can be used to (1) highlight existing technical vulnerabilities and identify vectors of attack, and (2) social engineer key employees. Our approach, based on OSINT, utilized a combination of business and social networks, technical job postings, and an analysis of network domains. In this research we retrieved data using web-scraping scripts, which is the harvesting of structured data from the web (Boeing & Waddell, 2017), and largely relied upon several open-source applications. In particular, we utilized the Yahoo search tool, the Maltego open-source link analysis tool, and other free tools as detailed in Section 3. We also used a user-scripted tool, based on Python 3.6.0, to automate the collection of data; however, to avoid violating the terms of service for online third-party companies, the