A Study of Doxing, its Security Implications and Mitigation Strategies for Organizations

Roney Simon Mathews
Information Systems Security
Concordia University College of Alberta
Edmonton, AB, Canada
roney.s.mathews@gmail.com

Shaun Aghili, Dale Lindskog
Information Systems Security
Concordia University College of Alberta
Edmonton, AB, Canada
{shaun.aghili, dale.lindskog}@concordia.ab.ca

***Abstract*—This research paper focuses on the impact of intentional and unintentional exposure or leakage of sensitive personal data elements that- when aggregated and used or disclosed in an unauthorized manner- could impact the employees of an organization. Doxing usually escalates to hacking, espionage and harassment. Such impacts could damage the reputation or competitive advantage of the organization; especially if the targeted employee is a senior management executive. Threat agents use doxing to collect data undetected, from targeted victims. Doxing is a mode of Open Source Intelligence (OSINT), aimed at launching sophisticated attacks on individuals or employees of an organization, through the collection of personal information over time; as such, doxing is considered an Advanced Persistent Threat (APT). Some risk management strategies today, may not consider the risk associated with doxing; the objective of this research is to create its awareness and recommend methods for its mitigation.**

Keywords— Advanced Persistent Threat; Doxing; Open Source Intelligence (OSINT); Sensitive Data; Risk Management

I. BACKGROUND

People and data are critical assets of an organization. Any compromise of data can be considered as a threat to business continuity. Doxing generally, a means of vigilantism, is defined as the overt collection, aggregation and publication of information of a targeted individual (without his/her consent) on the internet for public consumption, with the intention of causing embarrassment, humiliation and damages, in a way that threatens the victim's privacy and possibly those around the victim (friends, family members etc.) [1]. The doxed information could enable further escalations like espionage, hacking, blackmail and other attack vectors that could potentially cause harassment, embarrassment and economic losses to the targeted individual. Information stored on webpages, documents and databases are made accessible via the internet to employees, clients and the public using a myriad of devices giving doxers (individuals involved in doxing) an opportunity to surreptitiously access information and compromise pieces of this information, if adequate access control methods have not been implemented. As the endpoints of a corporate network are extended beyond its physical location and mobile devices, doxers use the internet and the mobile device's information gathering and correlation of information from multiple sources. In this context, the collection, publishing and use of personally identifiable information (PII) [2] by doxers, cause privacy implications. Addressing these risks and mitigating them is challenging to both individuals and organizations. As such the focus of this paper is on incorporating dox mitigation strategies, within an enterprise's risk management framework.

Personal information discussed in this paper refers to the exclusive containment of pieces of data (identifier, quasi-identifier or sensitive) that an individual may share on the internet with a restricted group of people. These may be shared on blogs, social networking websites, surveys, and websites that require collection of user information for creating a registered account or for providing services, as defined in each website's Terms and Conditions. Individuals generally restrict the availability of certain types of information to a certain group of people on social networking websites; however, there are instances when an individual may accidently share this personal information to a larger audience aside from the restricted group to which it was originally intended. This also occurs due to software misconfiguration or bugs in a website, accidently revealing personalized information of individuals. This is seen in the case where a bug in Facebook's "Download Your Information" application shared phone numbers and email addresses of 6 million users [3]. Information about an individual may also be available from meta-data present in documents and pictures, already available doxing dossiers and the availability of an individual's or an organization's communications. The information published can include confidential information of the organization, an employee's PII, corporate programs, sensitive and strategic corporate information linked to the employee etc. One might argue that the disclosure of personal information, meta-data in documents and pictures that were published overtly (though accidental) on the internet is still considered public information. This paper aims to create awareness on how doxers could use this information and also the privacy risks that are associated with such publications overtly on the internet.

Doxing is not a random act. A doxer selects a target and begins to dox the target by collecting basic information (name, address, family members, gender, email addresses, user names, registered websites etc.). Doxers use a myriad of sources (news media, social networking, applications installed on mobile devices, Government websites etc.). Applications (with unsecure privacy settings) installed on mobile devices share data among other users of the same application, and additionally help form information records for the application developer's database. The doxer creates an aggregated document referred to as the victim's dossier. Dossiers can include published information and hacked communications from websites such as WikiLeaks. This is published in pro-doxing websites such as AnonBin, DoxBin and PasteBin. The process involved in doxing is outlined in Fig. 1; however describing each of the stages is beyond the scope of this paper.

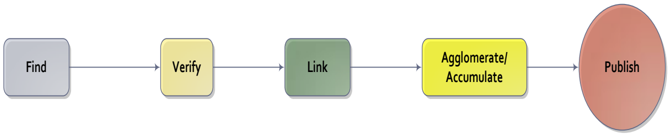

Fig. 1. Demonstrates the process flow involved in doxing

Hactivists use computers and computer networks to rally against a political agenda or voice concern about an issue. An attacker may use this doxed information in performing other attacks like social engineering and hacking; to gather and plan intrusive future attacks against an organization. Doxers may be motivated by financial gain, revenge, mischief or a special cause.

The purpose of this paper is to provide information security professionals with:

- An awareness of the risk-impacts of doxing to individuals and organizations;
- A review of related findings that tailor towards building up a case for the need of a risk model to mitigate doxing;
- An ISO/IEC 27005 compliant proposed risk model which can be integrated into an organizational risk management framework. This proposed risk model should be capable of aligning itself to existing risk assessment frameworks;
- Recommendations aiming to enhance the mitigation strategy against doxing;

The current section provides an introduction to the concept of doxing and a review of related researches and articles that assist in understanding the terminologies and concepts that will be used in this paper. Section II describes that proposed risk model that will be used towards mitigating the risk of doxing to an organization and which can also be integrated into an organizations existing risk management framework. The final section of this paper provides conclusions based on the proposed risk model, for it to be effective.

As mentioned before, doxing involves the overt collection, aggregation and publication of information of a targeted individual (without his/her consent) on the internet for targeting an individual publically to cause embarrassment, humiliation and damages, in a way that threatens the victim's privacy and possibly those around the victim (friends, family members etc.) [1]; it is primarily used by hactivists (against an organization's political or social agenda) to create and publish dossiers on the internet; thus damaging the reputation of the organization and also centring the organization to be victim to other threats like social engineering, hacking, financial crimes etc. (refer to TABLE II in APPENDIX: that show recent data disclosures of several organizations). The key factor to mitigate the effects of doxing involves actively monitoring the information disseminated via social-media networks, emails etc. [1].

On August 2nd 2011, the Federal Bureau of Investigations Intelligence Bulletin on Cyber Intelligence broadcasted a bulletin among law enforcement agencies alerting law enforcement officials to a high exposure rate to harassment and identity theft through doxing [4]. This bulletin was circulated based on law enforcement agencies activities against Anonymous and LulzSec members. Doxing is a means of retaliation by hactivists. The Bit9 US Global survey of IT Professionals report that: sixty two percent (62%) of respondents in North America and fifty seven percent (57%) from Europe categorized hactivists as the primary attackers of organizations; rated higher than corporate competitors, disgruntled employees, nation states and cyber criminals [1] [5]. As such, doxing should be considered as a major threat by organizations due to its effectiveness and relative simplicity.

Open Source Intelligence (OSINT) involves intelligence gathered from overt sources that are used by security services and law enforcement agencies and can be shared amongst friendly agencies [6]. Analyzed OSINT reports can become classified and are never shared with the public [6]; however, doxing involves publishing to the general public (creating a larger audience) and a cause for security concern. There are privacy risk impacts caused due to unauthorized use, disclosure and retention of personal information. This gathering of information overtly is done by performing inference attacks over quasi-identifier (birthdays, address, zip codes, city, gender etc.) and sensitive (anniversary dates, vehicle registration numbers etc.) attributes of an individual [7]. By using background knowledge (common sense and domain knowledge), a doxer performs inference attacks to connect and match information elements together, gaining more personal information when combined. Although these information elements on their own do not provide for neither meaningful information, nor sensitivity, nor impact [6] [7]; through the use of data mining methods, doxers are able to develop correlations between pieces of information gathered from several sources and individuals, related to communications, projects, activities etc. Data utility means the weightage of piece of data about an individual on the overt web which could enable inference attacks about that individual's online presence and their related personal information. Data about an individual that is found on the overt web must have a low data utility, in order to ensure greater overall privacy for that individual [7].

Private data that is stolen and posted on file-sharing networks and other online forums by hactivists and hackers are rich in information resources that assist in doxing and enable eminent hacks against an organization [1]. The use of social-media networks, public records and information on private, public and government entities assists hactivists to gather information about targets [1]. Doxing is a form of reconnaissance attack against an individual or an organization, as it involves collecting information from overt sources from a limited set of information that is initially available to a doxer. The geo-location sharing feature available on social-network, forums and photographs assist doxers in establishing references to current address/location, places visited, hometown etc. which enable doxers to refine their search results for the targeted individual [1]. The ramification of doxing extends to the victim's friends, family, co-workers, organization and those acquainted to the target, which includes harassment, public humiliation, threats to life, identity theft, fraud and the disclosure of their private lifestyles [1].

The Defence in Depth solution [1], deals with discussions related to providing personnel training on social engineering, implementing technology solutions like firewalls and Intrusion Detection and Prevention systems (IDPS), developing policies and security assessments on the existing system in general. It majorly calls attention to the problems and consequences of hactivists using doxing against individuals, public and private organizations and law enforcement agencies. While very useful, security bits and pieces are no real substitute for an integrated, comprehensive framework model for an organization to protect, detect and react against the threat of doxing.

Enterprise data must be controlled are in 3 loss-modes, namely [8]:

- Data at Rest: A state where the data resides in computers and other electronic devices, including databases and other storage centres.
- Data at the Endpoint: The state where data exists on end devices like storage devices, laptops, mobile devices.
- Data in Motion: Data being transmitted across a network via chat, email and other communication mechanisms.

Metadata present in documents reveal a wealth of information about an individual and the organization's technological set-up, and can be utilized for various purposes. Using Data Loss Prevention (DLP) tools like MetaShieldProtector, OpenDLP etc. prevent data loss from happening by removing critical metadata present in documents, which would enable an attacker to fingerprint an organization's assets and network infrastructure [8] [9]. The use of Data-at-Rest and Data-in-Motion solutions further improve sanitization, securing and accidental employee disclosure on the internet [10].

In 2005, the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information was established, to set a guideline for all US government, civilian and military personnel, consultants, vendors and other individuals who require access to classified information [11]. One of the strategies proposed in the research paper "New technologies and emerging threats: Personal security adjudicative guidelines in the age of social networking", was to incorporate cyber-vetting into the background investigation process, which would result in an increase in security clearance denials [12]. It looked into 11 categories that could help identify an individual whose access needs to be removed and to mitigate espionage involving cleared personnel with access to classified information. Lax security habits which could be harmful to an individual's personal information and could put that individual at a greater risk for blackmail or coercion were also discussed in the same paper [12]. The author suggested including doxing as a threat in the personal conduct and handling protected information guidelines, as it involves behaviours that are damaging or malicious to others (reduces trust) [12].

Aaron Barr- then CEO of HB Gary Federal who reported that he was successfully able to infiltrate the hactivist collective known as "Anonymous", and was on the verge of exposing its members was retaliated against by Anonymous as the malicious group hacked into the private servers of HB Gary Federal to expose sensitive corporate emails, in addition to launching a massive doxing attack on Aaron Barr [1]. This resulted in very severe organizational reputational losses.

II. PROPOSED RISK MITIGATION MODEL

Although most organizations have a risk management plan, these may not include specific mitigation strategies against the risk of doxing. This section discusses controls that need to be implemented in order to integrate doxing risks into an organization's risk management strategy. The proposed risk model consists of proactive and reactive controls to ensure business continuity. The defense in depth strategy (people, technology and operations) of information assurance must be considered with people as the weakest link to achieve this objective [1]. The defense in depth strategy revolves around providing multiple layers of security for an organization to detect, deter and respond to a situation.

The proposed risk model on doxing (Fig. 2) can be integrated into the organization's overall risk management process. It provides for a well formed risk approach on doxing and helps to mitigate its impacts from further escalations.

The proposed risk model is ideal for small sized businesses (Statistics Canada defines small businesses as those having an annual total revenue between $30,000 and $5,000,000, with employees between 5 and 100). Specifically, the authors of this paper propose that this model can best be used on small businesses that meet certain criteria, such as those:

- Organizations that are about to go public (IPO).
- Organizations that are targeted for acquisition.
- Organizations vulnerable to above average reputational risk.
- Organizations that have a larger number of high profile employees.
- Organizations targeted by hactivists.
- Organizations with high revenues that can afford to implement additional mitigation controls against doxing.

TABLE I shows the mapping of this proposed risk model to ISO/IEC 27002, an alignment to the applicable domain controls listed in ISO/IEC 27002. Factor Analysis for Information Risk (FAIR) standard [13] developed by The Open

Group, is a suitable plugin for risk assessment that may be used with various frameworks, such as COSO, ITIL, ISO/IEC 27002, COBIT, OCTAVE, etc. to analyze risks and determine the appropriate risk treatment plan. Services such as Recorded Future can assist in estimating probable Threat Event Frequency (TEF) for the organization targeted by hactivists. TEF can also be obtained by contacting law enforcement agencies and monitoring the threat of doxing to the same or similar organizations in the past. The FAIR plugin could be one such approach an organization can use to perform risk assessment for an organization (if the organization does not have one already in place).

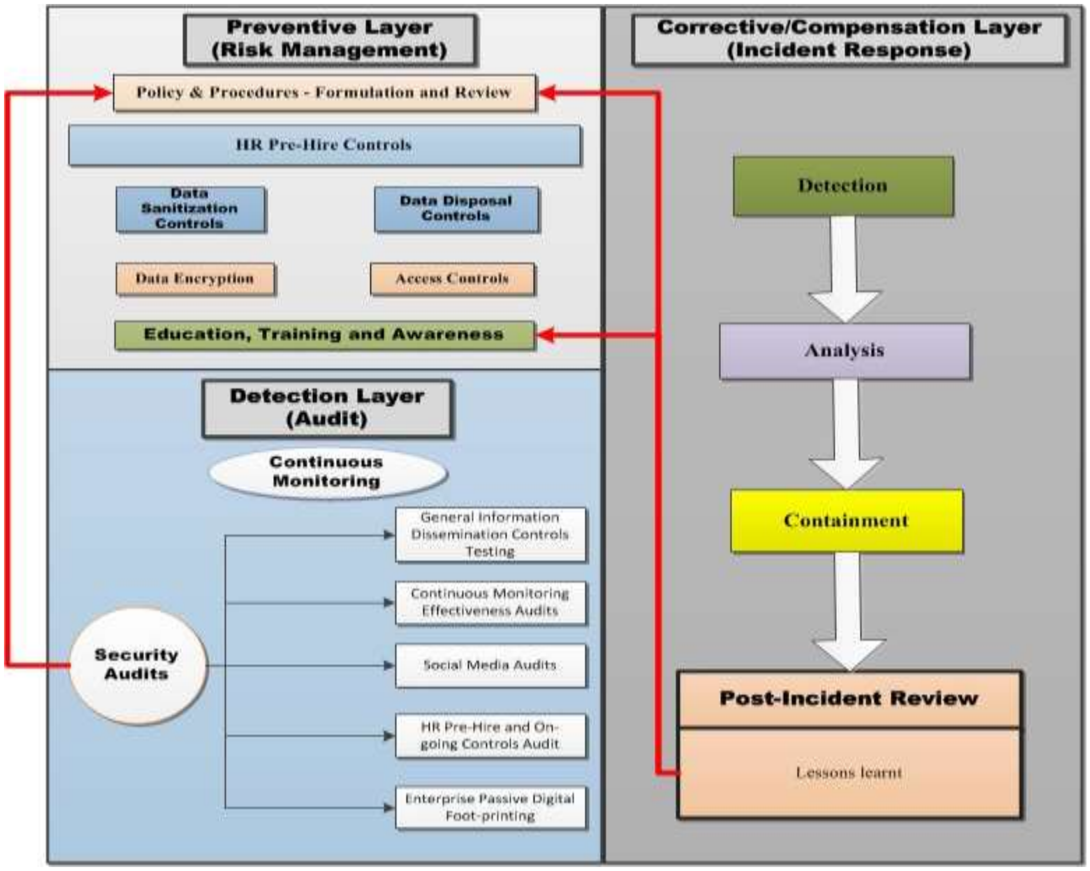
Preventive Layer
(Risk Management)
Policy & Procedures - Formulation and Review
HR Pre-Hire Controls
Data Sanitization Controls
Data Disposal Controls
Data Encryption
Access Controls
Education, Training and Awareness
Detection Layer
(Audit)
Continuous Monitoring
General Information Dissemination Controls Testing
Continuous Monitoring Effectiveness Audits
Security Audits
Social Media Audits
HR Pre-Hire and On-going Controls Audit
Enterprise Passive Digital Foot-printing
Corrective/Compensation Layer
(Incident Response)
Detection
Analysis
Containment
Post-Incident Review
Lessons learnt

Fig. 2. Proposed risk model for small businesses

TABLE I. TABLE ALIGNING THE DOMAINS OF ISO/IEC 27002 WITH THE PROPOSED RISK MODEL

No.	ISO/IEC 27002 ISMS Controls	Features of Proposed Model enabling these controls*
1	Risk Assessment and Treatment	Policy & Procedures - Formulation and Review (A.1), HR Pre-Hire Controls (A.2), Continuous Monitoring (B.1), Security Audits (B.2), Detection (C.1), Analysis (C.2), Containment (C.3)
2	Security Policy	Policy & Procedures - Formulation and Review (A.1), Security Audits (B.2), Post Incident Review (C.4)
3	Organization of Information Security	HR Pre-Hire Controls (A.2), Data Sanitization (A.3), Data Disposal (A.4), Data Encryption (A.5), Access Controls (A.6), Continuous Monitoring (B.1), Security Audits (B.2)
4	Asset Management	Data Sanitization (A.3), Data Disposal (A.4), Data Encryption (A.5), Access Controls (A.6), Security Audits (B.2)
5	Human Resource Security	Education Training and Awareness (A.7)
6	Physical and Environmental Security	N/A
7	Communications and Operations Management	Data Sanitization (A.3), Data Disposal (A.4), Data Encryption (A.5), Access Controls (A.6), Security Audits (B.2)
5	Access Control	Data Encryption (A.5), Access Controls (A.6)
9	Information Systems Acquisition, Development and Maintenance	Data Sanitization (A.3), Data Disposal (A.4), Data Encryption (A.5), Access Controls (A.6), Continuous Monitoring (B.1), Security Audits (B.2)
10	Information Security Incident Management	Detection (C.1), Analysis (C.2), Containment (C.3), Post Incident Review (C.4)
11	Business Continuity Management	N/A
12	Compliance	Policy & Procedures - Formulation and Review (A.1), Security Audits (B.2)

*Note: The features of the proposed model are denoted in the above table in the format (*x.y*) where *x* represents the layer in the description below and *y* represents the control or feature of that layer. For instance, Continuous Monitoring is part of Layer B (Detection) and is discussed as control or feature 1 of that layer; hence denoted as Continuous Monitoring (B.1).

This risk-based methodology divides the employees into upper management, middle level managers and lower grade employees to assist in dissecting the flow of information and the consequences to the organization in each level. However, even though lower level employees or middle level managers may have access to more information, it must be understood that as information flows up the ladder, the format of the information becomes more concentrated, yet more comprehensive.

This risk model is broadly classified into 3 main categories which provide for different layers within it. A segregated team of employees consisting of members from IT, HR and Legal should form the IT Security and Compliance Unit (ITSCU) for the organization.

A. Preventive Layer

This first layer provides critical controls for a strong security infrastructure against the threat of doxing and ensures business continuity and security posture for the organization as a whole. It, essentially requires the organization's employees, vendors and contractors to undergo certain rigor, as described below:

1) *Policy & Procedures - Formulation and Review:* A security policy should be introduced to the employees of the organization, with regard to the threat of doxing by addressing the security objectives to information, namely confidentiality, integrity and availability. Policies and procedures must adequately cover all departments, technology operations and technological configurations of the organization. Related policies must be simple, concise, easy to understand and must undergo periodic review. Procedures must provide clear directions related to the appropriate use of storage devices, handling of sensitive information, return and maintenance of mobile devices laptops for all employees, including those on leave, on disability or on vacation [14].

2) *Human Resources (HR) Pre-Hire Controls*: The HR department should be actively involved with employees in the organization to safe-guard employees against the threats of doxing. This can be achieved in the following ways:

   - *Information Control and Hire*: This control should involve procedures to control access to employee information outflow by classifying the various types of roles and information based on a stipulated guideline and then using administrative (policies, procedures and physical protection) and technical controls (access, identification, authentication and communication controls) that best serve employee privacy and the business goals of the organization [15].

   - *Digital Foot-print Analysis*: This process involves HR analyzing the online exposure of prospective employees (provides for a digital baseline for each employee). This practice must be disclosed to all applicants, as a prequisite for employment. Prospective employees with little social media boundaries are at a greater risk to doxing. Such analysis can be part of cyber-vetting /background checks for employment and can also serve as the basis for determining access to sensitive information [12].

   - *Proactive HR Supervision*: This control will help ensure that employees who require or have access to sensitive information cannot be easily manipulated to leak out sensitive information about an organization. It also helps flag employees who may be involved in or are susceptible to fraud. HR can perform this by identifying employees who are prone to commit fraud due to financial, personal or family pressures. HR should proactively monitor developing negative financial trends or recent display of unconventional behavior of key employees. Credit report analysis of key employees by HR during the hiring process, and on a routine basis -with upfront disclosure- will help mitigate this risk of fraud arising from financial motives. HR should individually notify those key employees regarding the nature of information and its data utility that was found during routine digital foot-print analysis. This helps in providing feedback to key employees on the risks to the organization and the privacy impacts to these individuals. The main idea behind these controls is to serve as the first line of defense to deal with a huge vulnerability; namely internal employees with managerial-level access control privileges.

3) *Data Sanitization Controls:* Sanitization must be done automatically for all documents, images and various other file types that are transmitted electronically. Policies and procedures must be in place to automatically sanitize all documents and images that are created, used or transmitted both at a system and a network level. Encryption of sensitive information should be considered for additional precaution against doxing. System usage policies regarding the use of systems for non-work related activities should be strengthened such that users do not transmit files containing metadata to external recipients unless the information is approved and sanitized for external distribution and secured. The integration of Data Loss Prevention (DLP) tools, Data-at-Rest and Data-in-Motion solutions further improve sanitization, securing and accidental employee disclosure on the internet. Furthermore, controls that enable remote wiping of information from mobile devices, when reported stolen, must be in place.

4) *Data Disposal Controls*: Controls that address the archiving, retention, de-duplication, sanitization and disposal of stored information must be in place. This

assists in preventing loss of data due to security breaches and helps ensure adherence to existing regulations. The Electronically Stored Information (ESI) and Confidential Electronic Stored Information (CESI) retention and disposal models discussed in reference [16] are achieved by categorization of information and with the use of a meta-data vault (Fig. 3 in Appendix), which results in ESI being routed for storage or disposal.

5) *Data Encryption*: An industry accepted standard of encryption must be deployed for all modes of organization communication, transmission and storage. Full Disk Encryption (FDE) must be enabled on all devices (desktop, laptop, mobile devices etc.) that store data-at-rest or process organizational information. Data-in-Motion must always be encrypted using Advanced Encryption Standard (AES) or other robust algorithms. This practice must also be supplemented with the use of a tunneling protocol such as Secure Socket Layer 3.0 (SSL) or Transport Layer Security 1.2 (TLS) for communication, or the use of Virtual Private Networks (VPN) for remote access using Internet Protocol Security (IPsec). Wireless security policies must be enabled on organization-provided mobile devices restricting connection to unsecure wireless access points.

6) *Access Controls*: Access controls should be based on business needs, and should never be given to an individual who isn’t required to have access to a particular asset. The Adjudicative Guideline for Determining Eligibility for Access to Classified Information [11] should serve as a baseline before providing access rights. By performing an access privilege audit on employees on a regular basis, it is possible to assess not only if the access is required; but also ensure that the confidentiality of the information would be maintained (Digital foot-print analysis and HR supervision controls help in assessing if employees requesting access can keep the information confidential). Role-based access controls must be implemented across the organization, and the organization must have a Chief Information Security Officer (CISO) or Information Security Manager who is responsible for the categorization of information. Data owners should be accountable for the control and audit of the list of employees who have access to a shared resource every 90 days, and access should be removed as soon as the need for a particular employee’s access is over. Access should also be revoked based on non-usage and termination.

7) *Education, Training and Awareness*: The threat of doxing to employees of an organization should be included in the organization’s security training and awareness program; and, must educate employees on a regular basis about the potentially devastating impacts of doxing. Conducting short training events that demonstrate the ease and manner in gathering information overtly over the internet without the need for any specialized skill set or advanced computer knowledge could be beneficial in two ways: it helps employees understand the threat better; and, it can show employees how to track their own digital foot-print on the internet. The latter helps modify employee behavior regarding the use of the internet and privacy issues for the individual on the internet.

Educate employees on the use of Social Media: Employees need to be educated on the proper use of social media and the dangers posed by doxers using social media as a resource. This also leads to understanding privacy settings and implications of posting images with geo-tagging data, privacy implications arising from the ability to tag people on social networking websites, sharing and exposure of posts to friends and the public. The task of easily connecting people based on their posts on social networking websites made public allows for a wealth of information to be collected and aggregated by doxers. Employees must also be educated on phishing, data harvesting and the means to secure online browsing at home by using personal VPN applications like Hot Spot Shield, WiTopia etc. (that provide online privacy and secure access to the internet), the TOR Project, the use of secure search engines like Start Page that do not store or track a user’s online search results. Educate employees to understand the need to question before submitting personal information on the internet, by asking the following questions: who is asking for the information? why is it needed? how will this information be used [17].

As a supplement to reinforce ongoing training, the distribution of flyers, posters and brochures inside the organization can act as constant reminder of the threats of doxing

B. *Detection Layer*

This layer brings together many elements of technology into a single monitoring and analysis engine. This layer works by utilizing organizational monitoring of reputation and threat vectors to the organization, along with analyzing and performing security audits to the existing system in place against an upcoming threat of doxing to the organization.

1) *Continuous Monitoring:* This involves the ITSCU of the organization, to actively monitor all the employees of the organization, and also assess threats against the organization by hactivists. This process is based on monitoring the digital foot-print left on the internet by employees which could be harmful to the reputation of the organization, privacy of employees (due to the publication of dossiers of employees) and analyzing the use of organizational information resources that could serve as indicators to fraud and other means of mischief by employees or attackers on the web. This can be achieved by using specific OSINT products like Maltego, FOCA, etc. in combination with services from Reputation.com and Brand.com that manage

organizational reputation, monitors and establishes management and reporting features on the go. It should also monitor pro-doxing websites such as PasteBin, AnonBin etc. for employee information and hactivist web pages for information to attack their organization.

However, the use of services such as Recorded Future would be a more enhanced approach to continuous monitoring for an organization. Recorded Future provides a source for web intelligence (OSINT) that formulates or enables business decisions using predictive analysis of past, planned and predicted events on the web. Some of its features that stand out for predictive analysis include planning for upcoming threats and threat agents in real-time, keep up to date with social unrest, follow warning and threat indicators against company assets, analyze trends based on historic data available and its ability to investigate business and personal relationships or geographical trends [18].

2) *Security Audits:* The role of internal audit activity is to provide assurance that the risks associated with doxing are appropriately mitigated. The internal audit activity is to be supplemented by an external annual security audit to provide a non-biased, third party opinion on the effectiveness of anti-doxing controls in place. Management should let the external audit team know that anti-doxing controls have been implemented within the organization's risk management structure and ask the external audit team to test the effectiveness of such controls as part of the team's overall controls testing. In general, such security audits should include the following:

- *General Information Dissemination Controls Testing*: This refers to an audit test that assesses the communication and nature of information transmitted. Information flow must be bi-directional (top-down and bottom-up approach). This information security audit consisting of technical, physical and administrative controls that validate information dissemination, integrity of information transmitted, functioning of strategic communication and isolation of confidential information. This audit requirement helps ensure that access controls and communication strategies implemented are functioning properly.

- *Continuous Monitoring Effectiveness Audits*: These audit tests are designed to test the effectiveness of the continuous monitoring system in-place in the organization. An appropriate testing procedure checks to see the ratio of detected potential threats versus successful threats by hactivist. Of those identified, how many were false positives and false-negatives? The goal is to configure the system to generate the least number of false negatives.

- *Social Media Audits*: This type of test procedures aims to identify if employees are -intentionally or unintentionally- leaking out sensitive or confidential information. It also assesses the policies and procedures effectiveness of the organization related to social media use by the organization itself, as well as its employees. This can provide for identification of offenders, as well as, the effectiveness of appropriate access controls and information dissemination procedures. It can also account for detecting possible areas of improvements for policy, education, training and awareness and steps for minimizing the impact of such disclosures.

- *HR Pre-Hire and On-going Controls Audits*: The goal of this audit is to ensure the accuracy of background checks for employment, and controls to assess HR supervision effectiveness in identifying employees who may engage in fraud. This is done by performing routine baseline examination of employees (reference checks, credit report checks, annual performance evaluations, access control review, etc.).

- *Enterprise Passive Digital Foot-printing*: This serves as an extension to security audits by being the initial phase of a regular penetration test. The intelligence information gathered here is obtained to perform future attacks against the organization. This helps in conforming to the organization's risk appetite by revealing the risks that are present for the organization and helps build stronger security policies and/or improve the use of the existing controls.

C. *Corrective/Compensation Layer*

This final layer forms a contingency shell by formulating an incident response approach when an organization is targeted for doxing or when an employee reports a security incident to the ITSCU. This unit should have a specialized email and contact number for employees to be able to report a security incident.

1) *Detection*: Based on digital foot-print analysis and routine baseline examination in the preventive layer of this defense in depth model, ITSCU can alert employees with information of their online presence that could be used by a doxer to target both the individual and the organization. This can also be based on a reported incident by an employee. Digital foot-print analysis and continuous monitoring establish if an organization is being targeted by hactivists and doxers. When the ITSCU is notified, the notified person should check the seriousness of this threat to assess if it is an organization wide attack. As soon as multiple employees report identity theft or the presence of dossiers causing harassment to multiple employees then an Incident Response Team should be activated. When detected, an incident should be raised which includes details

regarding the employee, contact information, department information, where the dossier was found etc. Using services such as Recorded Future, the organization would be better able to assess and outline a strategy to deal with a current, ongoing doxing attack against an organization.

2) *Analysis*: A detailed analysis should be done by members of the Incident Response Team to determine who was affected, the nature of the threat, what kind of information was revealed and how the information was obtained. Once it is determined that the threat is real, the executive team of the organization must be notified officially.

3) *Containment*: Aside from the regular IT policies and procedures to contain data loss and reduce its impact, it is probably a good idea to consider monitoring the targeted employee's network and physical access including remote access privileges until the threat to the organization has been adequately contained. This ensures that the ability to coerce or use the resources of those employees to gain additional access to information on the organizational network is thwarted. The implementation of formal communication channels between the Incident Response Team, ITSCU, the executive team, and the general public will ensure that organizational partners, investors, customers, suppliers and vendors do not lose confidence and are better prepared to work together, until the threat is adequately contained.

4) *Post-Incident Review (PIR)*: After these stages are completed, a review process must be conducted in order to identify how an identified threat was initiated and map the existing vulnerabilities that were used on the existing system and the digital foot-prints that were available to hactivists to execute this threat. This stage revolves around planning to patch the vulnerabilities found, process improvement (what is working and what is not, how to avoid repeating this mistake, how did it impact the organization) and closure of the security incident. This PIR should be done by technical experts. External specialists could be used to get a fair and unbiased assessment of the existing process. This would amount for lessons learnt; to better improve the quality of the security policy of the organization and provide for enhanced education, training and awareness.

III. Conclusion

The risk of doxing the employees of an organization could impact the reputation or the competitive advantage of the organization. Furthermore, it has been known that doxing could lead to further escalations like hacking, fraud, espionage etc. Many organizations are not aware of the risks associated with doxing. In this regard, such risks are not included in the organizational risk management framework. This paper seeks to generate awareness on the risk-impacts of doxing and its escalation; by briefly describing the process of doxing including examples and statistical information.

Through the analysis of doxing methodologies and strategies, this research has outlined some of the ways in which organizations can secure and help prevent information leakage overtly and from further escalations. Additionally, this paper included a proposed risk model that is appropriate for certain enterprise profiles, such as those highly vulnerable to reputational losses. The proposed risk management approach primarily focusses on upper and middle management, as it is often too impractical to monitor every single employee on a routine basis.

With the rise of cyber-crime and the rise of hactivists to expose targeted organizations, governments and individuals; the proposed risk model demonstrates how an organization can ensure adequate controls are in place to mitigate the risk of doxing. Mitigation of doxing should be integrated into the existing risk management program of organizations. Although a number of mitigation controls against doxing have been suggested, educating employees regarding the proper use of internet services, such as social media is key to the prevention of disclosure of personal information. Lessons learnt and strategies used for building a stronger security policy for the organization should be well documented and should be shared among security professionals to build a standard to mitigate the risk of doxing.

Acknowledgment

This research was supported by the Faculty of Graduate Studies of Concordia University Collage of Alberta. The first author is very grateful to this research paper's supervisors: Dr. Shaun Aghili and Dr. Dale Lindskog for their valuable guidance during this research. Special thanks to Dr. Ashish Thomas for his constant encouragement throughout the research. Additionally, the first author wishes to acknowledge and thank his parents, family, friends and his eldest brother Roshan Simon Mathews for their endless love and understanding.

REFERENCES

[1] Ingrid N. Norris, “Mitigating the effects of doxing”, A Capstone Project Submitted to the Faculty of Utica College, Dec 14, 2012 [Online]. Available: http://www.utica.edu/academic/library/Norris%20IN%202012.pdf.

[2] NIST, Special Publication 800-12: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), U.S Department of Commerce.

[3] Facebook, “Important Message from Facebook’s White Hat Program”, June 21 2013 [Online]. Available: https://www.facebook.com/notes/facebook-security/important-message-from-facebooks-white-hat-program/10151437074840766.

[4] Federal Bureau of Investigation, "Law Enforcement at Risk for Harassment and Identity Theft through "Doxing"", Aug 2 2011, Intelligence Bulletin, Cyber Intelligence Section [Online]. Available: info.publicintelligence.net/FBI-Doxing.pdf.

[5] Bit9, “2012 Bit9 Cyber Security Research Report” [Online]. Available: https://www.bit9.com/research/cyber-security-research-2012.

[6] Clive Best, “Web mining for open source intelligence”, 2008, IEEE Explore, Information Visualization, 2008. IV '08. 12th International Conference. pp.321-325 [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4577966.

[7] Chiemi Watanabe, “Privacy risks and countermeasures in publishing and minning social network data”, Oct 15-18 2011, Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2011 7th International Conference, pp. 55-65 [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6144789.

[8] Simon Liu and Rick Kuhn, “Data loss prevention”, March/April 2010, IT PRO pp 10-13 [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5439507.

[9] Sudhanshu, "Metadata Extraction using FOCA", March 1 2013 [Online]. Available: http://blog.kaffenews.com/?p=2676.

[10] IdentityFinder, “Data Loss Prevention: Data-at-Rest vs. Data-in-Motion” [Online]. Available: http://www.identityfinder.com/us/Files/WhitePaper.pdf.

[11] The White House Washington, Adjudicative Guidelines for Determining Eligibility for Access to Classified Information [Online]. Available: http://www.fas.org/sgp/isoo/guidelines.pdf.

[12] James P. Festa, “New technologies and emerging threats: Personnel security adjudicative guidelines in the age of social networking”, Dec 2012, Naval Postgraduate School [Online]. Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a576171.pdf.

[13] The Open Group, Technical Guide FAIR – ISO/IEC 27005 Cookbook, October 2010 [Online]. Available: http://www.businessofsecurity.com/docs/FAIR%20-%20ISO_IEC_27005%20Cookbook.pdf.

[14] Jennifer L. Bayuk, Jason Healey, Paul Rohmeyer, Marcus H. Sachs, Jeffrey Schmidt, Joseph Weiss, Cyber Security Policy Guidebook, Wiley.

[15] Kashif Syed, “Proposed control procedures to mitigate the risks of strategic information outflow in the recruitment process” Sept 3-7, 2012, Trust, Privacy and Security in Digital Business, 9th International Conference, TrustBus 2012, pp. 50-64 [Online]. Available: http://link.springer.com/chapter/10.1007%2F978-3-642-32287-7_5.

[16] D. Fernando, “Secure decommissioning of confidential electronically stored information (CESI): A framework for managing CESI in the disposal phase as needed”, June 10-12, 2012, 2012 World Congress on Internet Security (WorldCIS), pp. 2018-222 [Online]. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=628018.

[17] Javelin Strategy & Research Inc., “More than 12 Million Identity Fraud Victims in 2012 According to Latest Javelin Strategy & Research Report”, Feb 20, 2013 [Online]. Available: https://www.javelinstrategy.com/news/1387/92/More-Than-12-Million-Identity-Fraud-Victims-in-2012-According-to-Latest-Javelin-Strategy-Research-Report/d,pressRoomDetail.

[18] Recorded Future, “White Paper: Cyber Security Insights from Web Intelligence” [Online]. Available: http://go.recordedfuture.com/cyber-security-insights-from-web-intelligence.

[19] Privacy Rights Clearinghouse, “Chronology of Data Breaches” [Online]. Available: www.privacyrights.org/data-breach.

APPENDIX

TABLE II. COLLATED TABULATION FROM PRIVACY RIGHTS CLEARINGHOUSE'S DATA BREACHES FROM UNINTENDED DISCLOSURE OF 2013 [19] AND IDENTITY FINDER'S REPORTS OF 2011-2012 [1]

Date	Hactivists	Organization	No of Individuals affected	Names	Date of Birth	SSN	Address	E-mail Address	Credit Card	User Names	Passwords	Phone
11 Jul 2013	-	Page High School Greensboro, North Carolina	456	456	-	-	456	-	-	-	-	456
03 July 2013	-	Indiana Family and Social Services Administration	187,533	187,533	187,533	3,926	187,533	187,533	-	-	-	187,533
21 Jun 2013	-	Facebook Menlo Park, CA	6,000,000	-	-	-	-	6,000,000	-	-	-	6,000,000
21 May 2013	-	Lifeline, TerraCom Inc., YourTel America Inc.	44,000	44,000	44,000	44,000	44,000	-	-	-	-	44,000
01 Jun 2012	AntiSec	Toronto Police Service	664	-	-	-	-	3,692	-	2,848	2,848	1,045
29 May 2012	AntiSec	American Pharmacists Association	Unknown	-	-	-	-	28,659	-	-	-	-
29 Dec 2011	Anonymous	Stratfor	860,000	75,000	-	-	50,618	859,311	68,063	860,000	860,160	50,569
28 Dec 2011	Anonymous	specialforces.com	40,000	-	-	-	-	40,854	7,277	36,368	36,368	-
06 Sep 2011	Anonymous	26 Texas Law Enforcement Agencies	Unknown	-	6,182	647	4,631	39,419	42	-	174	14,701
30 Aug 2011	ObSec	UGO Entertainment	Unknown	-	-	-	-	21,548	-	-	23,389	-
08 Aug 2011	AntiSec	U.S Law Enforcement	Unknown	-	2,058	1,923	7,165	1,531,638	8	-	4,661	17,105

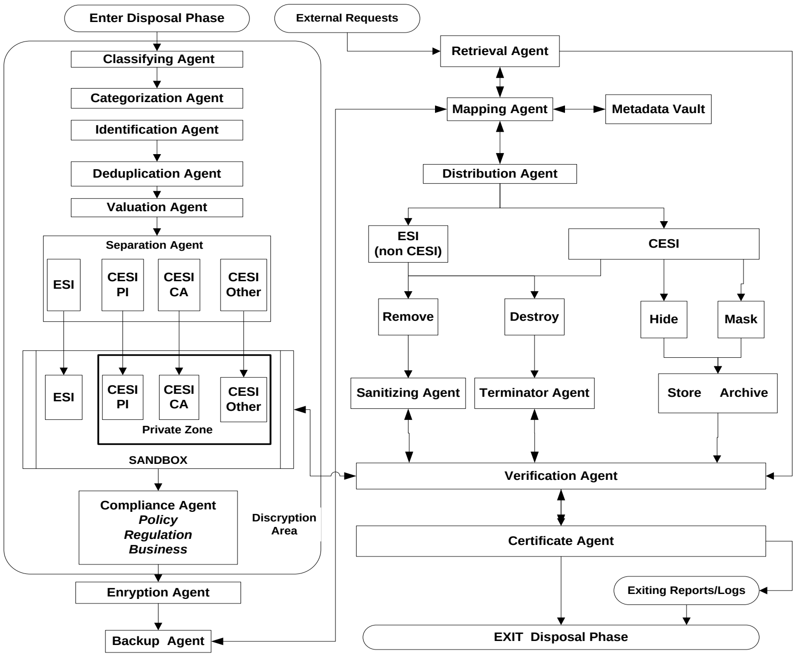

Fig. 3. Flow diagram of ESI/CESI within the disposal phase [16]