WeirFoulds LLP

WeirFoulds Technology Insights: "Dark Web: What's Underneath the Internet"

July 12, 2022

By James G. Kosa, Alfred Pepushaj

Overview

As data breaches have shown in recent years, the dark web can be utilized as a means to hack into organizations, compromising millions of people's information. Often, the compromised information is in turn sold for illicit purposes on the dark web. Organizations must therefore be aware of the dark web threats and, importantly, ensure that they have effective policies and safeguards to prevent or respond to the risks of the dark web. This is especially important at a time when Canadians are becoming increasingly concerned about their privacy

The Three Layers of the Web

The web is divided into three layers: the surface web, the deep web, and the dark web. Most of us are familiar with the surface web, which consists of websites indexed by commercial search engines (*e.g.*, Google, Yahoo, Bing) that are easily accessible. The deep web refers to content that cannot be easily accessed, as it is not indexed by commercial search engines. The deep web contains content like a person's banking or medical information. The dark web, unlike the surface web and the deep web, requires specialized software where users often operate in total anonymity. The dark web is described below in more detail.

Defining the Dark Web

The dark web is made up of dark nets, which are highly encrypted, non-indexed websites that cannot be accessed without special software, such as Tor. Tor, which is an abbreviation for "The Onion Router," is the primary software users rely on to access the dark web.

At its most basic, Tor sends a user's data through a series of computers—referred to as "nodes"— that are run by volunteer dark web users around the globe, making user IP addresses untraceable. In other words, Tor routes and encrypts user traffic through multiple servers, thereby enhancing user privacy.

Tor looks similar to a typical browser, but instead of using typical suffices like ".com" or ".ca," Tor users use ".onion" to access its websites. Generally, since websites on the dark web are not indexed, users seeking to access dark web websites are required to know the precise ".onion" URL. However, unsophisticated dark web users often rely on "Hidden Wiki" websites—accessible through commercial search engines—that contain links to dark web websites.

Dangers of the Dark Web

Dark web users generally include people with privacy concerns, people engaging in illegal activity, law enforcement and the

government, and activists. Thus, given its anonymity, the dark web can serve as an important space for, among others, political dissidents and whistleblowers—at least in theory.

The dark web can also be a haven for illicit activity. Users can trade, among other things, contraband (*e.g.*, opioids, weapons, body arts, etc.), as well as information pertaining to personal records (*e.g.*, medical records, social security numbers, etc.) and accounts (*e.g.*, e-mail accounts, bank accounts, etc.).

In particular, there are numerous privacy concerns that the dark web presents not only to its users, but also to large organizations. Organizations collect volumes of personal information, making them desirable targets for cyberattacks, as illustrated by recent cyberattacks, exposing the personal information of millions of people.

Organizations' Responsibilities under Privacy Legislation

Organizations have numerous privacy obligations under various statutory and regulatory regimes to keep personal information safe. Failure to comply can lead to significant consequences to organizations, including penalties under the applicable legislation and more broadly, reputational harm.

The *Personal Information Protection and Electronic Documents Act* ("***PIPEDA***") is the federal law that applies to private-sector organizations across Canada that collect, use or disclose personal information in the course of a commercial activity. Personal information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information such as age, name, identification numbers, ethnic origin, blood type, employee files, credit records, etc. Certain provinces have their own private-sector privacy laws that have been deemed substantially similar to *PIPEDA*.

Organizations subject to *PIPEDA* must follow the ten fair information principles to protect personal information. The principles form the ground rules for the collection, use, and disclosure of personal information. In turn, organizations must implement appropriate mechanisms and practices to avoid data breaches enabled by, among other things, the dark web.

1. **Accountability**: An organization is responsible for personal information under its control. It must appoint someone to be accountable for its compliance with these fair information principles.
2. **Identifying Purposes**: The purposes for which the personal information is being collected must be identified by the organization before or at the time of collection.
3. **Consent**: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
4. **Limiting Collection**: The collection of personal information must be limited to that which is needed for the purposes identified by the organization. Information must be collected by fair and lawful means.
5. **Limiting Use, Disclosure, and Retention**: Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected. Personal information must only be kept as long as required to serve those purposes.
6. **Accuracy**: Personal information must be as accurate, complete, and up-to-date as possible in order to properly satisfy the purposes for which it is to be used.
7. **Safeguards**: Personal information must be protected by appropriate security relative to the sensitivity of the information.
8. **Openness**: An organization must make detailed information about its policies and practices relating to the management of personal information publicly and readily available.
9. **Individual Access**: Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. **Challenging Compliance**: An individual shall be able to challenge an organization's compliance with the above principles. Their

challenge should be addressed to the person accountable for the organization's compliance with PIPEDA, usually their Chief Privacy Officer.

The *Privacy Act* is the federal legislation that governs the federal government's use, disclosure, retention or disposal of personal information in the course of providing services. Like *PIPEDA,* the *Privacy Act* also sets out various responsibilities that government institutions must follow to protect personal information.

Tips for Organizations

Organizations should have security measures in place to not only prevent possible data breaches, but also ensure, if a breach does occur, to respond quickly and effectively. What follows is a discussion of the various tips organizations should consider in seeking to avoid the threats of the dark web.

1. ***Keeping Information off the Dark Web***

One of the concerns for organizations, as illustrated by recent cyberattacks, is that personal information may end up in the dark web and, consequently, be used for illicit purposes. Therefore, as a precautionary measure, organizations should ensure that its data does not end up on the dark web. To prevent this from occurring, an organization and its members should, among other things, seek to:

- enable multi-factor authentication;
- install malware/antivirus software;
- use the appropriate software when accessing the dark web[i];
- store data locally on encrypted drives; and
- be aware of social engineering techniques.

2. ***Contracting with Third Parties***

When contracting with third parties, an organization should review its own privacy protection clauses to ensure that they are as rigid as those within third-party contracts. In addition, the organization should ensure that it fulfills any external security measures required by the contract.

3. ***Office of the Privacy Commissioner of Canada ("OPC") Recommendations***

In 2018, the OPC recommended cybersecurity remedial measures that organizations can take to protect their customer's personal information. The OPC recommendations came after a toy manufacturer experienced a data breach that compromised the personal information of over 500,000 people. The OPC approved of the following remedial measures performed by the toy manufacturer:

- **Testing/Maintenance**: Establish (i) a regular, multifaceted testing protocol to identify potential system vulnerabilities; and (ii) an update/patch management program to mitigate the risk of known vulnerabilities.
- **Administrative Access Controls**: Take steps to limit the number of individuals with administrative access, and limit the scope of access available via individual accounts (*g*., to limit cross-network access of local administrators)… Strengthen authentication controls (*e.g*., strong passwords) and put in place organizational measures to more strictly control the use of administrative accounts.
- **Cryptography**: Implement enhanced cryptography for stored information, as well as encryption for user information in transit via websites and apps.
- **Logging and Monitoring**: Establish increased and centralized log event retention to assist with detecting and investigating unauthorized activities on its network. Also restrict and monitor outgoing traffic to the internet.

- **Security Management Framework**: Implement a new comprehensive data security policy, which provides for the creation of a Data Security Governance Board to ensure, among other things: (i) staff awareness via annual training regarding the policy and data security; (ii) policy compliance; and (iii) annual risk assessments, best-practice benchmarking and reviews so that the policy and associated data security measures remain adequate.

Takeaway

Canadians are increasingly becoming more concerned about their privacy. Although the dark web serves as an important space for privacy, the dark web also presents various privacy concerns to both users and in particular, to organizations. As organizations collect significant personal information about their customers or clients, they should not only be aware of how the dark web may enable data breaches, but also be prepared to avoid such risks by implementing appropriate security policies and practices.

[i] Often, organizations may be required to access the dark web for brand management purposes to determine and monitor whether any harmful information about the organization is being shared, including personal information, related to organizational members or clients. However, while an organization may use Tor to access the dark web, organizations must be aware that Tor does not protect all internet traffic, as it only protects those applications that are properly configured to send their traffic through Tor.

For more information or inquiries:

James G. Kosa

Toronto
416.947.5043

Email:
jkosa@weirfoulds.com

James Kosa is a partner at WeirFoulds with a practice focused on information technology and intellectual property law. He is the Co-Chair of the firm's Technology & Intellectual Property and Privacy & Access to Information Practice Groups, and Co-Chair of the Blockchain and Digital Assets Practice Group.

Alfred Pepushaj

Toronto
416.619.6293

Email:
apepushaj@weirfoulds.com

Alfred Pepushaj is an Associate in the Commercial Litigation Practice Group at WeirFoulds LLP. He focuses on complex corporate and commercial litigation, including fraud, contract breaches, and shareholder disputes, as well as trusts and estates litigation involving will challenges, fiduciary breaches, and contested asset distributions.

WeirFoulds LLP

www.weirfoulds.com

Toronto Office
4100 – 66 Wellington Street West
PO Box 35, TD Bank Tower
Toronto, ON M5K 1B7

Tel: 416.365.1110
Fax: 416.365.1876

Oakville Office
1320 Cornwall Rd., Suite 201
Oakville, ON L6J 7W5

Tel: 416.365.1110
Fax: 905.829.2035