The Deep Web: Big Data As A Risk Manag Tool

By **John Bigelow** - March 24, 2015

By Rick Draper

Managing security-related risks requires information. To manage those risks effectively rec information; available at the right time; presented in a meaningful format. How do you get i

Open source intelligence, or OSINT, has long been used in risk management by governmen around the world; well before the internet was even conceived. However, the World Wide W ridiculous amounts of information available to everyone. It is just a matter of defining your knowing what you want to do with the information you obtain so that you can turn that info worthwhile intelligence.

The Internet in 3D
The internet, like most human sources of information, has a number of dimensions. Inform happy for others to know, and may even want to publicise; things that we are happy enougl qualified way; and, of course, those dark secrets that should never be publicly known. The t the internet that are relevant to our search for data to inform risk management are the Dail the Dark Web.

The Daily Web, or more commonly referred to as the "surface web" or "indexable web", is h content on the internet every day. If we are interested in finding information on a specific su certainly turn to Google, Yahoo or Bing. There are over 45,000 Google searches every secon

Ever wondered how they determine what gets displayed in the search results and what doe link to a webpage to be shown at all in the search results, it had to have been 'indexed' by th means that someone told the search engine about the page directly (there are techniques f was available as a link on another page that was itself indexed. There is a whole industry a indexed and appearing first in the search results – Google "Search Engine Optimisation" if y

The Deep Web, is a term coined by the founder of BrightPlanet, a company that pioneered the internet. The "Deep Web" is that layer of the internet that is not indexed or accessible di search engines. It is impossible to reliably estimate the size of the Deep Web, but it is thou thousands of times the size of the surface web. It includes, for example, web content acce logging into paid subscription or membership accounts – such as www.asisonline.org, asi www.spaal.com.au.

There are many approaches that can be used to restrict Deep Web content from being inde available search engines, or accessed by links in other webpages that seek to expose the c called deep linking). However, it is important to note that just because content has not bee mean that it is not able to be harvested using tools designed for the purpose. There are tec unlock a substantial amount of Deep Web content to supplement OSINT from the surface will be discussed later in this article.

The Dark Web, is sometimes referred to as a subset of the Deep Web; and to the extent tha Dark Web is not indexed by commercial search engines, this is valid. However, the Dark We intentionally) more difficult to access, unless you know the techniques needed to reach the a publicly accessible webpage might appear innocuous enough on first inspection, but clic page may reveal an otherwise hidden form field. Entering a valid passphrase into that form the page to change completely, revealing the hidden secrets. Welcome to the Dark Web, wh content is hidden in plain sight.

Some Dark Web content is even further obscured through anonymising networks, such as Router) Network. TOR uses a series of virtual tunnels to conceal information about both th which would otherwise be available over conventional internet routing. TOR was originally deployed for US military purposes, but is now known to be widely used to provide the anon engaging in illegal or otherwise questionable activities.

Law enforcement agencies invest a great deal of time and effort tracking down the dark w effect, supporting crime. Probably the most famous of those taken off line by the FBI was appeared again not long after that as Silk Road 2. As you might expect, these sites facilitat drugs and firearms, distribution of trade secrets, and money laundering, along with enablin human depravity. However, there are other dimensions of the Dark Web that are important corporate security perspective, including issues around the sale of counterfeit goods and d property, and fraud. These will be discussed in more detail below.

It would be remiss not to point out that there are legitimate uses for TOR and the dark web overshadowed by the nefarious activities that it supports.

What is Big Data and what is in it for me?

The term "Big Data" is used to describe a collection of information that is so large or compl challenging to process and use in a meaningful way. What is "big" to some organisations others, so the term is context dependent. For the purposes of this discussion, big data is si large, and mostly unstructured, datasets that have the potential to reveal linkages and relat understanding and inform further analysis.

The data and information available on all three dimensions of the internet comes in many f traditional websites and web-enabled databases, through to streams of social media. Mos being used to varying extents by organisations in managing security-related risks. But ther benefits to be gained by leveraging insights available through harvesting data from multiple

Public and private sector organisations are taking advantage of deep web harvesting servic operate in parallel with the traditional search engines. These services go much further thar by actually extracting surface web and deep web content so that it can be analysed on the made of content over time. In some cases, it is even possible for these services to harvest sources.

The risk management uses for this type of big data collection and analysis range from dete disease outbreaks so that staff travel advisories can be issued, through to identifying relate counterfeit designer brand products, so that targeted action can be taken. The power of be from literally tens of thousands of sources on a daily, or even hourly, basis should not be ur

The key to being able to use all this information effectively is inherent within the stages of t intelligence cycle:

1. Planning and direction.
2. Collection.
3. Processing/collation.
4. Analysis and production.
5. Dissemination.

While you might not know what information you are actually going to get, having a very cle for harvesting the data is essential. When it comes to big data, the value comes through se analytics and the application of visualisation tools that enable the important relationships t attention of a human who can take the analysis further.

While big data is not something that every security manager needs for their risk managem important to become familiar with what all three dimensions of the internet have to offer.

What about Social Media?

The next article in this series deals specifically with social media and how it can be used in management. For now, it should be recognised that for the most part, social media is a par can provide insights into a wide range of security-related risks.

Many organisations now require staff, and even contractors, to provide details of their soci Naturally, there are privacy concerns that are often raised in relation to such requirements, that utterances by staff on social media can have implications for employers.

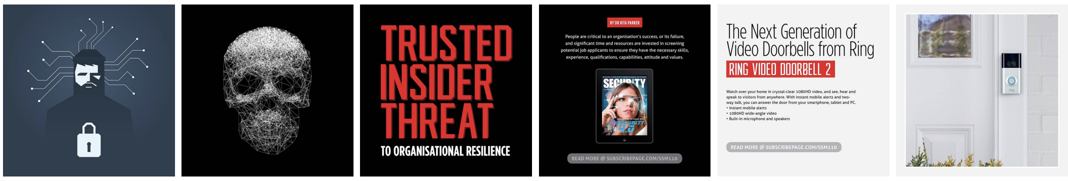
Security managers should familiarise themselves with social media and deep web harvesti use tactically for situational awareness, and as sources for OSINT to support their risk mar employing any of these strategies, it is essential that effective policies and procedures be c implemented to ensure that OSINT and social media are leveraged in the most effective ma regard to human resource and reputational risks.

Rick Draper is the Principal Advisor and Managing Director at Amtac Professional Services 30 years of experience in the security industry – the last 21 years as a consultant. He is als *lecturer in security management and crime prevention at Griffith University, and a member Prevention and Crime Prevention Council. Rick Draper has been involved in the developmer and data management since the 1990s, including the development of a range of tools to as managers. You can contact him on* [*rick.draper@amtac.net*](mailto:rick.draper@amtac.net)

John Bigelow

https://www.securitysolutionsmedia.com/

FOLLOW US ON INSTAGRAM @SECURITYSOLUTIONSMEDIA


TRUSTED INSIDER THREAT
TO ORGANISATIONAL RESILIENCE
SECURITY
The Next Generation of Video Doorbells from Ring
RING VIDEO DOORBELL 2