

The background of the slide is composed of several overlapping geometric shapes, primarily triangles, in various shades of blue. These shapes are arranged in a way that creates a sense of depth and movement. On the right side, there is a dark, diagonal band that contains faint, light-colored text resembling hexadecimal code or data strings, such as "32C20616E6420", "206C6974746C65", "Data BreachE20", "3686573204C6974", "ack696EA1", "206E61C", "2AA261736E", "B4FA01774", "5697D01", "52756E", and "em S".

THE DARK WEB:

A PRIMER FOR TAX REPORTING PROFESSIONALS

This white paper is based on an interview with Randy Johnston, CEO and founder of Network Management Group Inc., who recently spoke with Sovos about the dark web and its impact on tax reporting security. This paper also offers some perspective on how Sovos protects tax information.



The dark web is the online Wild West: A mostly lawless place full of black-market vices, clandestine meetings and battles between good and evil. And your customers' 1099 information might already be for sale on it.

For many tax professionals, and for most users of the web, the dark web – sometimes called the deep web – is more a vague concept than a tangible destination. But it is, in fact, very real, and it's the most likely place for a would-be thief to sell or acquire stolen tax information, including W-2 and 1099 forms. As such, tax professionals should at least understand what the dark web is, how it functions, and how to avoid being victimized by it.

What is the Dark Web?

At least six times larger than the web that's home to Facebook and Amazon, the dark web is a semi-secret place accessible through a browser anybody can download. Guesses on its precise size vary widely; some estimates peg the dark web as being 500 times larger than the standard web. Maybe 5 percent of total internet users are on the dark web, but the number is likely far lower than that. Just about anything is available there, from the vilest of indecent material to credit-card numbers, weapons and government secrets.

IT'S THE MOST LIKELY PLACE FOR A WOULD-BE THIEF TO SELL OR ACQUIRE STOLEN TAX INFORMATION, INCLUDING W-2 AND 1099 FORMS.

It's not all black market contraband and illicit videos, though. The dark web is home to security experts trying to protect average Internet users from would-be attackers. It's also a place where journalists can converse with sources who need to stay completely hidden—think someone like Edward Snowden. Like the consumer web, the dark web is full of communities and debate, although the tone there tends to be stronger than it is on standard social-media sites.

They now have to repaper their entire client bases to get FTINs from customers who haven't given them. This is an expensive and time-consuming process that came as an unwelcome surprise.



How Does the Dark Web Work?

Most users of the dark web access it through a browser-like application called “Tor,” an erstwhile acronym for The Onion Router. Tor was a creation of the CIA, the U.S. military and the Israeli government and was intended as a network for military communications. But it leaked somehow—possibly intentionally on someone’s part, but nobody knows for sure—and now it’s freely available as a download.

There are search engines on the dark web, the most prominent of which is Duck Duck Go, which doesn’t track user activity the way Google does but does index websites to the extent indexing is possible. One characteristic of the dark web that makes it dark, though, is that many sites are so deeply hidden they are not indexed. Those sites do not show up in search engines and are extremely difficult to find.

A dark web user who does find what they are looking for and wants to pay for it will almost assuredly use Bitcoin. The digital-only currency has no physical iteration and is extremely difficult to track. Bitcoin exists only in online repositories, and hiding transactions made with the currency is relatively simple. It’s easy, in other words, to avoid leaving a paper trail when there is no paper involved.

ONE CHARACTERISTIC OF THE DARK WEB THAT MAKES IT DARK, THOUGH, IS THAT MANY SITES ARE SO DEEPLY HIDDEN THEY ARE NOT INDEXED. THOSE SITES DO NOT SHOW UP IN SEARCH ENGINES AND ARE EXTREMELY DIFFICULT TO FIND.



What is Available on the Dark Web?

A better question might be, “what isn’t?” The usual suspects are there—weapons, drugs, pornography, credit-card information, stolen identities, bomb-making recipes...and, yes, stolen tax forms. Information from Wikileaks often appears on the dark web before it goes mainstream.

It is possible that every American has had personal information exposed on the dark web at some point. For instance, a massive data breach of the Republican National Committee database put at risk the personal information of nearly 200 million Americans—virtually every registered voter in the country. Astonishingly, the leaked information wasn’t even protected by a password. Those big data breaches at retailers and financial institutions? That information very likely goes straight to the dark web.

Of course, tax information is not immune to exposure. A recent data breach of a company consumers use to file taxes exposed sensitive information. A data thief got directly into the company’s systems and pulled data out at a slow enough rate that the company did not have appropriate systems management to monitor it.

But it gets worse: There’s more than just bait for identity theft. Consider, for instance, Assassination Market, a kind of Kickstarter for having people killed. And then there are far less nefarious offerings, such as all the documentation to get out of a parking ticket in Los Angeles. A Slack bot generates all the information an illegal parker needs. The person then submits the documentation, and the city waves the ticket.

A similar method exists for getting back into the good graces of the IRS. Let’s say a company forgets to pay its payroll taxes one year—or file its 1099 forms. That slip could lead to trouble with IRS auditors for a decade or more. On the dark web, there is information on how to seek revenge on that auditor —much of it straightforward and actually legal. But if the auditor still hangs around, there’s a “how-to” out there with information that can ruin that person’s life. The dark web goes from relatively innocuous to extremely dangerous very quickly.



Who is on the Dark Web?

There is no definitive answer to the question of how many people are on the dark web. An estimate of 5 percent of all Internet users might be aggressively high. The number certainly is not larger than 5 percent. That could still be millions of people, but anybody who has not heard of the dark web should not worry about being the last to know about it.

Of course, there is a collection of characters on the dark web that includes would-be thieves, smugglers and other criminals. But there are also whistleblowers, law-enforcement officials, security experts and journalists. Many of them, both doers of good and evil, are very well disguised. They need to be given the nature of some of the activity on the dark web.

For instance, one of the first five global responders to virus outbreaks is carefully hidden under a series of handles on the dark web. So are hackers—in the original sense of the word, people who want to play around with technology and make it work better—who offer knowledge on how to detect and thwart attacks. Security innovations such as OpenDNS sprang from the dark web.

In a story that reflects the unpredictable nature of the dark web, Marcus Hutchins, who shut down the WannaCry virus, was well known on the dark side for his positive work as a security researcher. But the virus-killing hero was also arrested in August 2017 on charges of creating and selling malware. People on the dark web are rarely all good or all bad, which goes for people on the standard web, too.

What people on the dark web are, though, is brutally honest and straightforward. There's no room for politeness or diplomacy when the stakes are high. Anybody who thinks Facebook debates get heated would be shocked by the heated discourse on the dark web. Many users are there with clandestine and anonymous identities, so there is no need to be nice. But people do need to get what they want, so brutal honesty wins out in most interactions.

Is It Possible to Protect Data from the Dark Web?

Most data breaches come about as a result of an error, often a change-management error. The error opens a hole that thieves use to access and steal data. There is only so much software developers can do to eliminate errors. Generally, for every 1000 lines of code in an application, there are between 10 and 50 errors.

The typical app for Apple iOS, for instance, has 10,000 lines of code, which means it likely also has somewhere around 500 bugs. Data thieves can exploit those errors to steal critical information and sell it on the dark web. And the number of lines of code is not shrinking. The new F-35 fighter jet, for instance, runs on 120 million lines of code, but a Ford F-150 pickup runs on 150 million lines.

Software will always have bugs, so companies have to find other ways to protect information in the products they produce. Organizations that use software—so, all of them—also need to take precautions. All it takes is for one user in an organization to download malware through, say a Microsoft Word document or a printer driver, and a data breach is off and running.

**MOST DATA BREACHES COME ABOUT AS A RESULT OF AN ERROR,
OFTEN A CHANGE-MANAGEMENT ERROR.**



How Can Tax Professionals Avoid Data Breaches?

But there are steps tax professionals can take to protect their data. The most important step they can take is not doing all of their tax reporting themselves. Tax operations departments aren't in the security business and shouldn't have to be. But handling tax information reporting in-house, especially with the urgency that now surrounds it given new deadlines, invites errors and exacerbates risk.

Tax professionals need a partner that can automate reporting processes and minimize security risk; they need to find an organization that is in the security business. In fact, security needs to be perhaps the highest priority in the search for a reporting partner. What should organizations look for, then? There are several factors to consider.

- » **Defense in depth.** Every organization talks about this but few actually practice it. A single failure should not open access to data for a breach. There should be multiple levels of failover for security. That means a partner should do more than just adhere to a minimum set of standards; it should be constantly updating and monitoring security measures.
- » **Constant monitoring for vulnerabilities.** The right partner should have rigid and robust control over who can access data and which data is available for access. A tax-reporting partner needs to constantly look for vulnerabilities within its apps and servers as well as monitoring with multiple third-party applications. Most vendors will do vulnerability scanning once a quarter or once a month. A partner that's serious about security will do it more frequently.
- » **Extensive background checks of employees.** Every organization should implement background checks, but it's essential that tax professionals choose a reporting partner that also takes security very seriously in its hiring practices. Sovos, for instance, has set the industry standard for background checks and performs periodic rechecks for all employees. accompany the truck to ship goods.



What is the Future of Tax Reporting and the Dark Web?

Data breaches in the field of tax reporting aren't yet as prevalent as they have become in the consumer tax-preparation market. However, B2B tax reporting – including 1099 and W-2 filings – is very much at risk of becoming the next vector in data theft.

The effects of having data stolen and sold on the dark web could be devastating. The loss of confidence by clients alone could derail a business, as could financial losses due to IRS penalties and settled lawsuits. Many organizations are still using outdated, manual processes to handle tax information reporting. Not only are those processes insufficient for meeting new deadlines and avoiding new penalties, they also pose huge security risks.

Centralizing and automating tax reporting, and finding the right partner to facilitate both, is the best way for organizations to keep their data safe. The dark web is only going to get darker, so tax professionals need to do all they can to keep critical data off of it.

TAX PROFESSIONALS NEED A PARTNER THAT CAN AUTOMATE REPORTING PROCESSES AND MINIMIZE SECURITY RISK; THEY NEED TO FIND AN ORGANIZATION THAT IS IN THE SECURITY BUSINESS.



To learn more about the security measures Sovos takes, visit this page:
sovos.com/why-sovos/about-us.

Or read more on sovos.com/product/tax-information-reporting/ about how Sovos 1099 reporting protects customers from both IRS penalties and security breaches.