CW technology

LEARN HOW IT WORKS

DARK WEB

What is It & Why Should It Matter to Me

Bill Kimbler
Leader of Business Development

TABLE OF CONTENTS

AUTHOR'S NOTE

Bill Kimbler is a partner and Business Development Lead at CW Technology.

Being with the company for over 13 years now, his role is centered on discussing the dynamics of IT support an the managed services model.

In such a way, Bill has impacted quite few thousand businesses over the years...

Bill's belief that the "CW Technology" way of mixing the IT support with management and business process needs of an organization is where the answer lies. This provides the complete solution for any SMB orgnization that relies on technology to meet its mission and objectives.

Outside of work, Bill is an avid runner and has competed in various half and full marathons, including the *Grandmas Marathon* in Duluth. He also enjoys spending time with his wife Teresa and his two teen sons - Noah and Jonah.

INTRODUCTION

You have probably heard the ominous name that describes the uncharted corners of the Internet: the "Dark Web." But what is it, really? Why should you be aware of it? And what should you do to protect yourself and your business from being a victim to its inhabitants?

WHY IT MATTERS

The fact is that there is high chance your business or corporate information is currently available for sale as a subset of a larger group of information on the Dark Web.

Passwords, log-in credentials, financial information, credit card numbers, and other confidential information is out there and you can’t stop it from proliferating to those with criminal intent.

You can choose to ignore this and go about your way, hoping that your particular information is not exploited. And yet, don't be surprised each time you come across countless stories about companies and people that fall victim to a Dark Web threat, such as identity theft.

You can roll the dice, but with such a threat increasing at alarming rates, it's better to stay safe than sorry...

CHAPTER 1

WHAT IS THE DARK WEB

The Dark Web is a term coined to describe the part of the Deep Web that is not indexed by search engines (i.e. Google). The Deep Web, on its own, is not inherently bad, but the Dark Web is *exactly* what it sounds like.

The Dark Web is a shady, unregulated part of the Internet where any individual can purchase a variety of illegal information and products, such as credit card numbers, drugs, guns, and counterfeit money.

Looking to purchase login credentials to a $50,000 Bank of America account for $500? How about a hacked lifetime subscription to Netflix for $6?

It’s all here, in the Dark Web, and it's all *very* illegal...

LET'S TALK STATISTICS

So, how expansive and detrimental is this so-called Dark Web?

A study by Kings College (London, 2015) classified the contents of 2,723 Dark Web sites over a 5-week period and found that over 57% host illicit material.

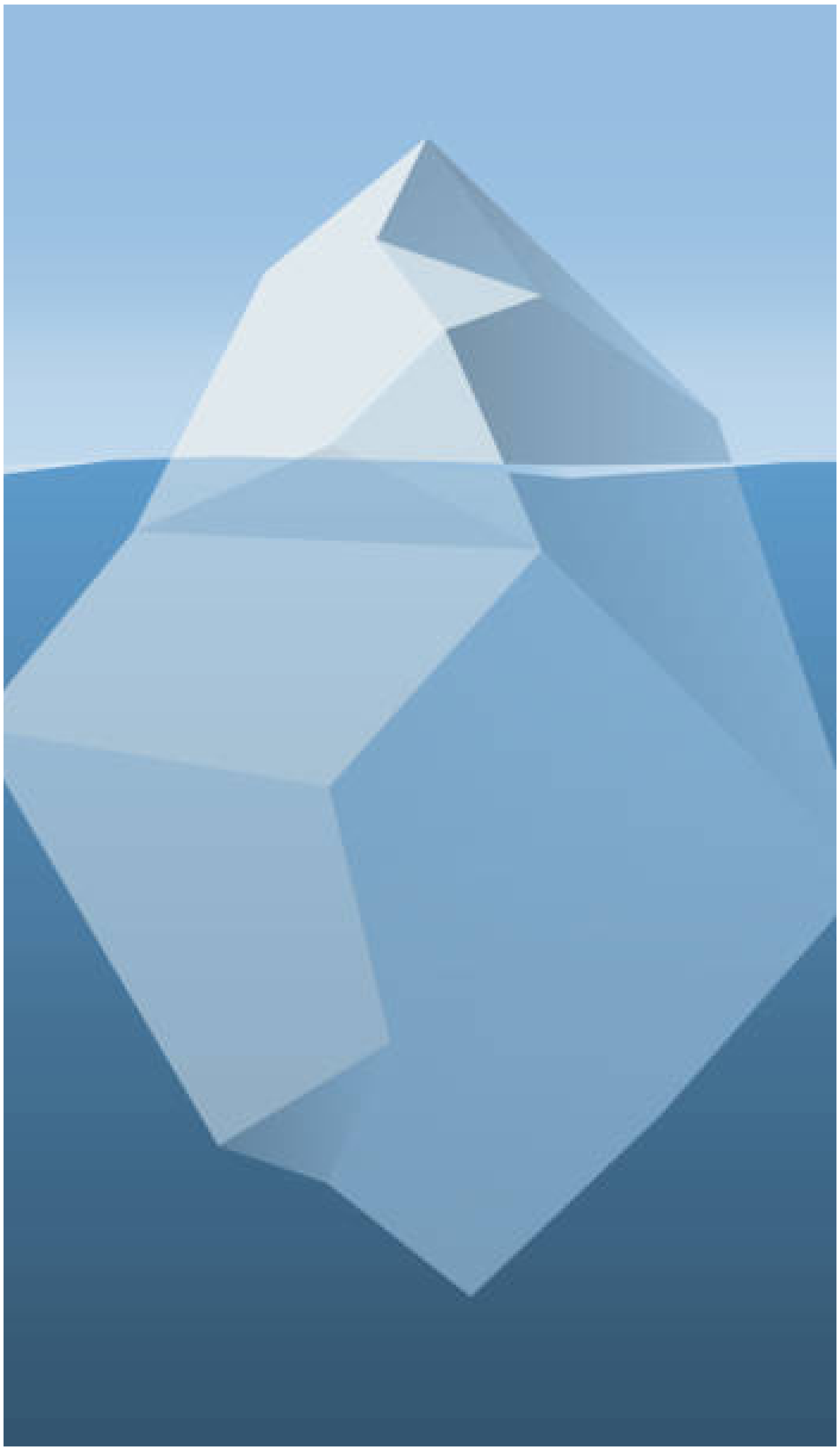
A recent study (University of Surrey, 2019) - **Into the Web of Profit** - by Dr. Michael McGuires showed the following:

- The number of Dark Web listings that harm an enterprise has risen by 20% since 2016.
- Of all Dark Web listings (excluding those selling drugs), 60% could potentially harm enterprises.

CHAPTER 2

BEWARE OF THE BOTTOM OF THE ICEBERG

Picture the Internet as an iceberg. The part above the water is the "Surface Web," where you can find webpages using search engines such as Google or Bing.



The part of the iceberg under the water is the "Deep Web."Search engines won't bring you to the pages here. This is where you are when you sign into your bank account online with your username and password. It's where the content is beyond paywalls.

It's where you communicate with other people through social media, chat services and messaging platforms. The Deep Web also houses large databases and many other things. It is a significantly bigger chunk of the internet than the Surface Web.

The "Dark Web" is a small part of the deep web. Mozilla Firefox, Internet Explorer, Google Chrome and other commonly-used web browsers won't get you there; you need a special browser such as Tor.

One of the features of Tor is that it disguises the computer that is being used to reach the internet, providing a high degree of privacy. While Tor can be used to go anywhere on the internet, if a website address ends in ".onion" it's in the dark web and only accessible via Tor.

CHAPTER 3

WHAT CAN I DO TO PROTECT MY BUSINESS & MYSELF

FOR YOUR BUSINESS

The answer is to deploy dark-web monitoring and response tools. The typical small and mid size business (SMB) will not have the resources, expertise, or time to do this themselves.

That is why working with an IT managed service provider that offers solutions for third party services that do these tasks is your primary solution.

A managed service provider is able to parse the data and work with you to develop a plan to remediate threats, as well and develop processes - both technical and training - focused to lower your exposure going forward.

The fact that more than a few small-business owners and their employees were unaware of the dark web becomes a good argument that additional training is needed.

FOR YOURSELF

For personal needs, identity theft services look for signs that that your personal information may have been used fraudulently. They usually check your credit reports, and some will monitor your financial accounts as well. They may also look at public records, commercial databases, and the Internet.

They have tools that the average person doesn’t for accessing places that are hard to reach, such as sites that sell stolen personal information on the dark web. If they find something suspicious, they’ll let you know.

You can correct, and in some cases remove, information about you in commercial and public records that has resulted from identity theft. That’s because you’re dealing with legitimate companies, agencies or organizations that will cooperate with fraud victims.

The Dark Web, however, is another matter. The people who trade in stolen personal information there won’t cooperate with an identity theft service or anyone else, so it’s impossible to get the information removed, stop its sale, or prevent someone who buys it from using it.

What Dark Web and other types of monitoring can do is alert you so that you can take action to avoid or limit the damage that the fraudulent use of your personal information could cause and remedy any problems that have already occurred.

CHAPTER 4

WHAT STEPS SHOULD I TAKE TO START?

PASSWORDS

Regularly change passwords for internal network access as well as third party services and applications. Ideally, these should be changed every 3-6 months.

MAIL FILTER & MALWARE SCREENING

You should also make sure that you have proper mail filtering and malware scanning tools deployed on your network to help identify threats that can pilfer this information from your network.

TWO-FACTOR AUTHENTICATION

Look into services that provide two-factor authentication (2FA) for verification of log in requests. These services will send you a code or link to your email that you need to enter or click to ensure it is you logging in.

Many services you may already use (Apple, Google, Microsoft, etc.) offer this type of service. It should also be part of your internal network and hosted services log in as well.

CYBERLIABILITY INSURANCE

Look into Cyberliability Insurance for your business. These policies will help with the clean up and remediation in the event of an issue but typically do not cover business loss.

These policies have become more widely available and your current insurance provider should have information on these types of plans.

DISASTER RECOVERY PLAN

Finally, have a disaster recovery plan for your business, in writing, that you can refer to in the event of a business impacting breach or data loss.

Having a plan that incorporates all areas of your business and prioritizes needs and services will help keep your business afloat.

CONCLUSION

The Dark Web has, and will continue to, be around for quite a while. Protecting yourself and your business doesn't just start with taking preventive measures in avoiding the Dark Web... It begins with an outlined cyber security strategy, and this is where a managed services provider comes in to help.

At ***CW Technology***, we are your dedicated IT partner, working with you to protect and support your business at all times.

If you're looking to gain greater value from your technology and establish greated security, then contact us today to discuss how we can implement the optimal cyber security processes and tools for you!