Red River

DARK WEB THREAT IMPACT REPORT

UNDERSTANDING THE TRUE COST OF HAVING YOUR COMPANY'S DATA ON THE DARK WEB

YOU'VE SEEN THE HEADLINES. IT SEEMS LIKE EVERY WEEK SOME BIG-NAME ORGANIZATION MAKES THE NEWS BECAUSE A CYBER-CRIMINAL BREAKS INTO A SERVER AND STEALS CONSUMER DATA.

HERE ARE SOME OF THE LARGEST DATA BREACHES WE'VE SEEN RECENTLY:

- Equifax – 143 million records stolen in July 2017.
- Yahoo – 3 billion in September 2016.
- Anthem – 78.8 million in February 2015.
- eBay – 145 million in May 2014.
- JP Morgan Chase – 76 million in July 2014.
- Home Depot – 56 million in September 2014.

According to CSO, 58 records are stolen every second and sold by criminals on the Dark Web. That's almost five million records every single day. Yet these headlines represent just the big and most publicized companies. How many more records are stolen from small to mid-sized companies that aren't as newsworthy? What is the Dark Web and what are criminals doing with the data they steal? This report will help you understand the dark web and how it can impact your business.

THE DARK WEB DEMYSTIFIED

The internet, which most of us think of as any website our Google search engine can find, is made up an interconnected network of computers, servers, and devices. But it can actually be divided into two elements: the Surface Web and the Deep Web. The Journal of Cyber Policy says the Surface Web is the tip of a digital iceberg and what lies beneath is as potentially treacherous as that chunk of ice that sunk the Titanic.

What's contained in the Surface Web includes search engines and any site that is easy to access with the click of a button. Underneath is a secondary layer of sites called the Deep Web. Like an iceberg, the Deep Web is surprisingly large; a report from the Congressional Research Service suggests that it is up to 5,000 times larger than the Surface Web.

What may surprise you is that 90% of user activity on the Internet regularly accesses the Deep Web. These are sites that aren't typically reachable by a search engine, such as a Gmail account or other sites that require registration, such as Facebook. Basically, anything that isn't reachable through a commercial browser such as Google, Yahoo, or Bing is considered Deep Web sites.

Housed within the confines of the Deep Web is the Dark Web. Wired says the Dark Web makes up only .01% of the Deep Web, but it is widely used by hackers and other nefarious types for illegal activities like child pornography, sales of weapons, illegal drugs, and buying and selling personal and corporate data stolen from individuals and companies.

The Dark Web is harder to reach, requiring a special browser and sometimes a password. It is an unregulated, murky cyber world. Websites characterized as residing in the Dark Web can only be found through a special browser service called The Onion Router (Tor). This downloadable service encrypts your IP address and the data you send, routing it through three computers chosen anonymously from thousands on the Internet. This hopscotch makes your identity and the information you're sending or receiving very hard to track.

Users navigate the Dark Web via Wikipedia-like directories that organize sites by name. These sites have a different URL; instead of .com or .net, Dark Web domains end in .onion.

What's interesting about Tor is that these free tools were designed for good. They are also currently being used to fight censorship, help whistleblowers remain anonymous, and enable members of the media to keep their sources anonymous. Only about 1.5% of Tor users are accessing the Dark Web; most are simply seeking to increase their privacy when surfing the web. NPR had a story a few years ago on how Tor helps political dissidents communicate without being censored by their government.

But most tools can also be used to harm - and that's the dark side to The Dark Web.

The anonymity of the Dark Web has spawned a number of websites like the Silk Road, a marketplace of illegal drugs, guns, and other contraband. In 2013 Interpol and U.S. federal prosecutors seized the site, along with hundreds of others, in a sweeping raid to clean up human trafficking, child pornography, drugs, illegal gun sales – and more. But the clean sweep was quickly undone just a few years later as new sites cropped up that shared consumer and corporate data.

An article in the Journal of Cyber Policy states that just a few weeks after the big publicized data breach in Target stores that affected 40 million consumers, stolen credit card numbers were being sold on the Dark Web for $20 to $100 per card.

A REPORT TO CONGRESS STATED:

Evidence suggests that the Islamic State (IS) and supporting groups seek to use the Dark Web's anonymity for activities beyond information sharing, recruitment, and propaganda dissemination, using Bitcoin to raise money for their operations.

This isn't to say that TOR is used exclusively for illegal activity. Internet privacy advocates use Tor and the Dark Web to retain a measure of confidentiality. However, a significant portion of the activity on the Dark Web is both illegal and dangerous to your company and customers.

GOING RATE – HOW MUCH IS YOUR DATA WORTH?

“Twenty-first century criminals increasingly rely on the Internet and advanced technologies to further their criminal operations.”

JOURNAL OF CYBER POLICY

What kind of data is on the dark web and what is it worth to thieves?

Hackers go after the data on private servers to glean any information they can to make a buck. Brokers on the Dark Web sell the data, which could include bank and credit card information, social security numbers, and personal information that criminals can use to set up fraudulent credit card accounts or take out loans.

ZDNet reports the Dark Web is “awash” in stolen credit cards such as American Express, Visa, and MasterCard. They confirm that the average cost of a stolen credit card number on the Dark Web is between $10 to $12. But the credit limit on the card changes the price.

THE CURRENT DARK WEB STOLEN CREDIT CARD MARKET LOOKS LIKE THIS:

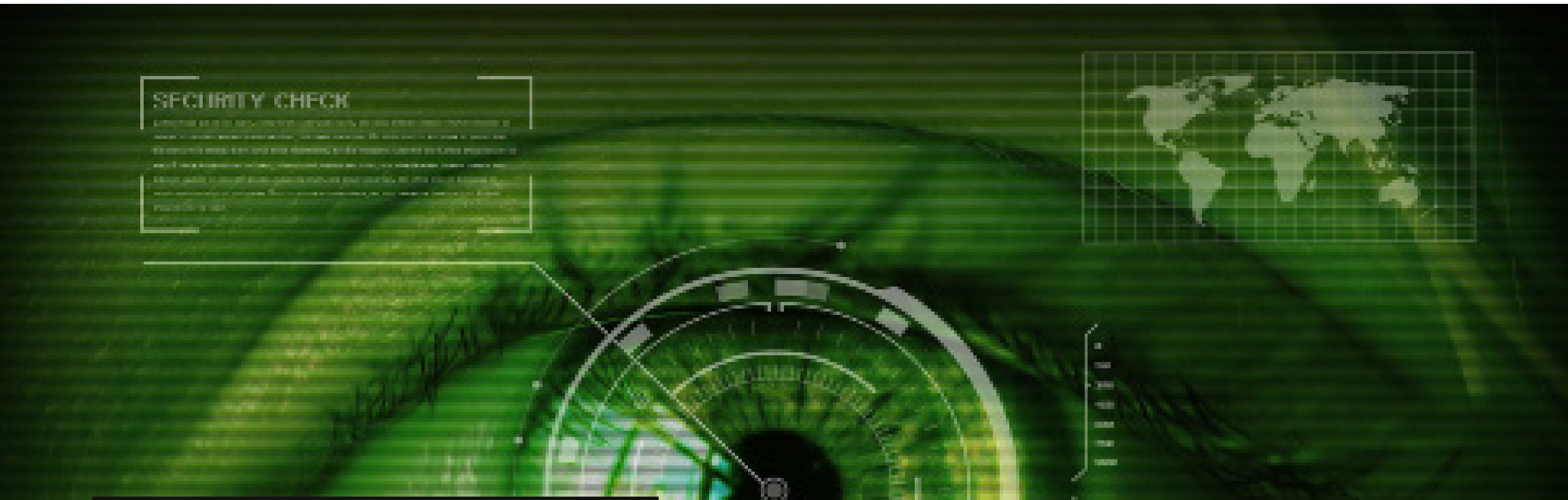
- **Low-limit stolen credit card numbers sell for around $12.**
- **Cards with $5,000 limits are selling for $450.**
- **Cards with a $10,000 limit are going for $800.**
- **Cards with a $15,000 limit are around $1,000.**

For somewhere between $200 and $1,000, a credit identity thief can pick up a “new” credit line of up to $15,000 at JPMorgan Chase or Wells Fargo. Most of this stolen information is from accounts in the United States.

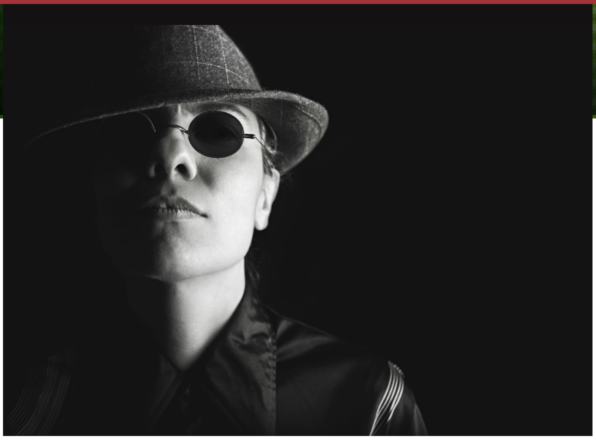
But that’s not all. The Dark Web has counterfeit identification documents, stolen IDs, passports, and more. You can pick up a US green card or drivers license for around $2,000 according to ZDNet.
You can purchase 1,000 Instagram social media accounts for $15. Or, pay a hacker $12.99 to break into your enemy’s Facebook account and wreak havoc.

How about an American social security number, address, dates of birth, and a whole identity package for around $40 a record? Imagine a cyber-criminal stealing login credentials for employee emails as well as email addresses. Then imagine our entire corporate database involved in an embarrassing phishing scam that infects your clients – and you – with ransomware.

Here's a phenomenon that will cause even the most unflappable security team a few sleepless nights: ZDNet is reporting that the Dark Web is selling remote access credentials to corporate computers in industries like retail, healthcare, education, and government. One login costs about $3 to $9. The implication is that hackers can dial into corporate servers remotely and observe daily operations. It's all business as usual on the Dark Web



THE IMPACT OF HAVING YOUR COMPANY'S DATA ON THE DARK WEB



Data breaches are a real and increasing threat. They're a massive disruption for companies when the headlines hit the media. These breaches can cost executives their jobs and damage corporate reputations. Quantifying all of the damage into a financial figure can be difficult because the cost of each cyber theft depends on a variety of factors.

Fortunately, there's a calculator for that. IBM teamed up with Ponemon in 2017 to create a free interactive calculator to determine individualized costs. But these two powerhouse organizations worked together to calculate and extrapolate the average global cost of a cyber breach as $3.6 million per incident or $141 per data record. Again, that's the global cost.

In the United States, the average cost of a data breach is higher, at $7.3 million. For attacks that steal data from less than 10,000 records, the average cost is $1.9 million. If the number of records stolen goes to 50,000 or more, the average increases to $6.3 million.

But can these studies really calculate the costs of reputational damage? Deloitte did a study in 2014 on the correlation between a cyber attack and the long-term damage to a company's reputation. In terms of risk, cyber hacking was in the top three risk categories for reputational damage in the marketplace. Mitigating the damage done by a data breach means putting a disaster recovery plan in place that includes vigilance around security awareness. Establishing an incident response team, according to Ponemon, can lessen the cost of a data breach by up to $19 per file stolen. Taking action quickly and responding with an established plan are all important to mitigating your risk.

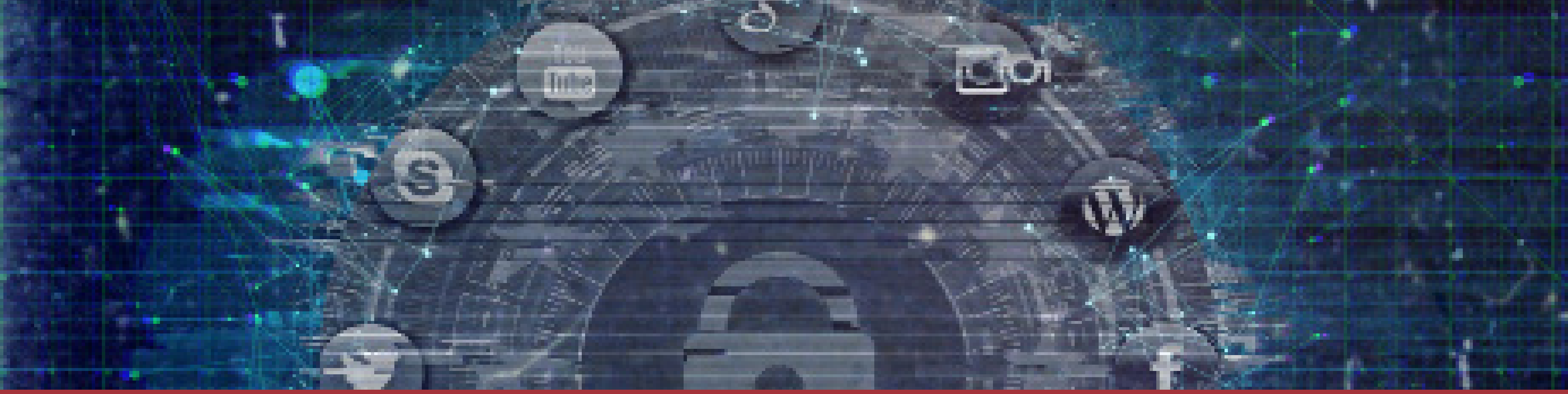
But what about small to medium-sized businesses (SMBs), which are increasingly targets of ransomware and other cybersecurity threats? Kaspersky Lab and B2B International released a report in 2017 showing that the cost of these attacks is increasing. CSO reported that cyber attacks on SMBs almost doubled from 2016 to 2017 in the U.S.

In the survey of more than 5,000 businesses across 30 countries, they found that the average cost of a data breach for an SMB was $117,000 per incident.

THE AVERAGE COST OF A DATA BREACH VARIES. FOR EXAMPLE:

- The Kaspersky Lab report said a targeted attack geared specifically to that business cost more to repair, at around $188,000.
- Attacks that affected non-computing hardware (Internet of Things devices) cost around $152,000 on average to repair.
- Lost devices with sensitive data cost SMBs on average $83,000 to mitigate.
- Staff errors that utilized IT resources inappropriately leading to a hacker event cost $79,000 per incident.
- Virus and malware infections cost SMBs $68,000 per incident.

The problem with SMBs is that they typically cannot afford an internal IT team to handle cybersecurity issues. They also typically struggle with cash flow, making the cost associated with a cyber attack especially difficult to overcome. In fact, CSO says 60% of SMBs who were cyber terrorism victims never recovered, and shut down within six months.



STAYING PREPARED IN THE DARK WEB ERA

CSO points out three reasons SMBs are struggling to mitigate the risks of data breach and the subsequent sale of critical data on the Dark Web:

1. SMBs are unable to afford a technology staff to monitor and mitigate these risks. Even corporate enterprise organizations often have a limited IT team – and rarely do they have technology experts dedicated to cybersecurity.

2. SMBs do not have ongoing cybersecurity training for staff. Given that the majority of data breaches occur from human error, creating a culture of cybersecurity is crucial for any company. This means creating awareness of email phishing scams or other opportunities for malware or cyber breach to occur.

3. The reputational damage an SMB can undergo when experiencing a cyber breach is particularly harmful. Customers feel betrayed when a company fails to keep their data secure. For a small business building their customer base, any instance of bad press can close their doors forever.

How can SMBs develop a robust, effective cybersecurity strategy to protect themselves against Dark Web threats?

The answer for SMBs lies in a new Dark Web Monitoring and Identity Protection Service offered by the team at Red River. We've partnered with ID Agent to deploy an affordable subscription service that can protect your crucial client data in minutes.

Keep your data from falling into the wrong hands or hurting your business. Contact Red River for dark web monitoring and other tools to enhance your cyber security strategy.

ABOUT RED RIVER

Red River brings together the ideal combination of talent, partners and products to disrupt the status quo in technology and drive success for business and government in ways previously unattainable. Red River serves organizations well beyond traditional technology integration, bringing 25 years of experience and mission-critical expertise in security, networking, analytics, collaboration, mobility and cloud solutions. To learn more, visit redriver.com.