SKURIO

Risks of the Dark Web for business

SKURIO

It seems that every other day, we hear of a new breach in the news or through our security grapevine.

Knowing whether your personal or business information has been compromised in these breaches can take days or even weeks to figure out. By which time, it is too late.

Large companies losing our information and data remind us to keep our eye on the ball in the field of cybersecurity. Still, a lot of the time, data dumps can be compilations of older breaches. Understanding the provenance of these breaches can help organisations estimate the risk they pose, avoid wasting resources on unnecessary investigations and help determine changes needed to Data Leakage Prevention (DLP) and Data Risk Protection (DRP) plans.

How are criminals using the Dark Web?

As an IT leader, you have likely heard of the Dark Web, but maybe you aren't quite sure how it's relevant to your business or your cybersecurity plans?

We've all seen the iconic iceberg graphic, showing the different levels of visibility and accessibility of the internet as a whole. The surface and deep web are the most commonly accessed by a standard user. The Dark Web is a section of the internet not readily found on Google or other search engines. It is not even accessible through your regular internet browser.

A specific type of browser such as a Tor browser is required to access this part of the World Wide Web, and usually, the user needs to know exactly where they want to go. You need the specific address for what you want to find. There's no search engine there.

The Tor browser, for example, uses several complex systems and VPNs to disguise the IP address of the source user, anonymising the location and metadata usually associated with browsing the web. Because of this, it has made the Dark Web the modern-day speakeasy for dodgy dealings and the illegal trading of goods.

It's a common misconception that the 'GDP' of the Dark Web is just that: guns, drugs and pornography. Goods these days are just as likely to include your business information, credentials, and credit card details.

SKURIO

According to the Dark Web Price Index,[1] a valid US social security number can cost as little as $2.

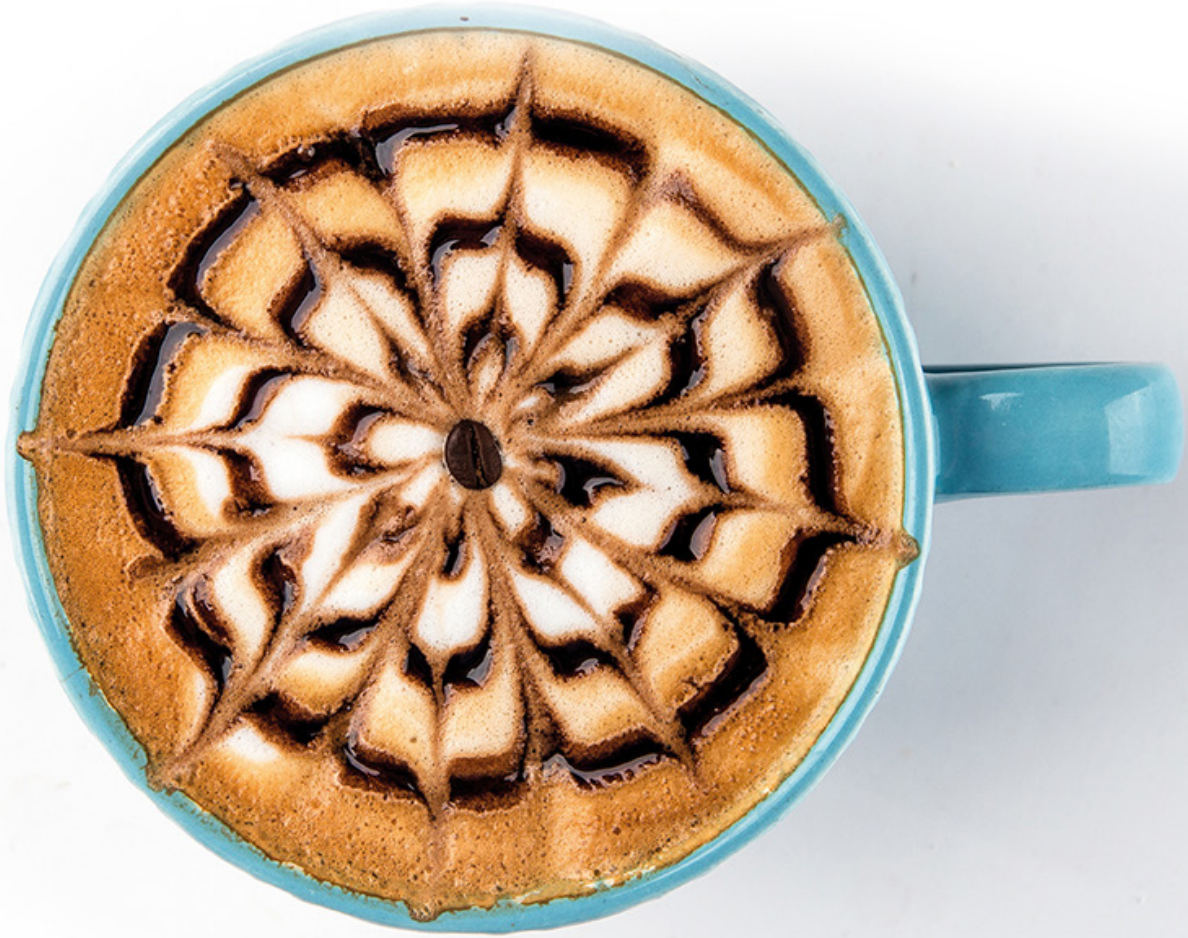
That's about the price of a cup of coffee.

Marketplaces and forums make up most of the content on these sites, with a whopping 90% of posts on Dark Web forums from buyers looking to contact someone for cyber-crime.[2]

The number of sites and pages on the Dark Web is as uncountable as those on the surface web, making policing it a large-scale job.

But it is not all bad news.

Sites such as the New York Times and the BBC have web pages on the Dark Web to allow easy reporting by those whose country could punish them for sharing information with the rest of the world. The anonymity given when using a Tor browser provides a safe and secure platform for whistle-blowers and citizens threatened with persecution to speak to reporters and journalists without compromising their safety.



1. Dark Web Price Index
2. Positive Technologies: Custom hacking services

What information could be on the Dark Web?

So, we've established this is a large, secretive information platform, as big as the surface Web, that could potentially be a dangerous place to be browsing.

Anonymity allows people to do unspeakable things they wouldn't normally consider, and they often use that freedom provided. But what could be lurking on these forums and marketplaces that could affect a business?

"Credentials to access our systems" was likely the first thought of any cybersecurity leader. Business plans could be at the top of a C-level exec's mind. Payroll information is probably the most significant worry for the finance team. But have you considered the impact of other internal documents? Personally Identifiable Information (PII) of customers and staff, and sensitive data should also be of concern - and that's not all.

While that information is usually digital and stolen from behind the company firewall or leaked, intentionally or not, consider the knowledge gained from a simple recon mission conducted by an outsider. What time does your office shut? Is access to the office easily attained? Is there a time the building is left unlocked or minimally staffed? Is the Wi-Fi accessible from outside the building boundary?

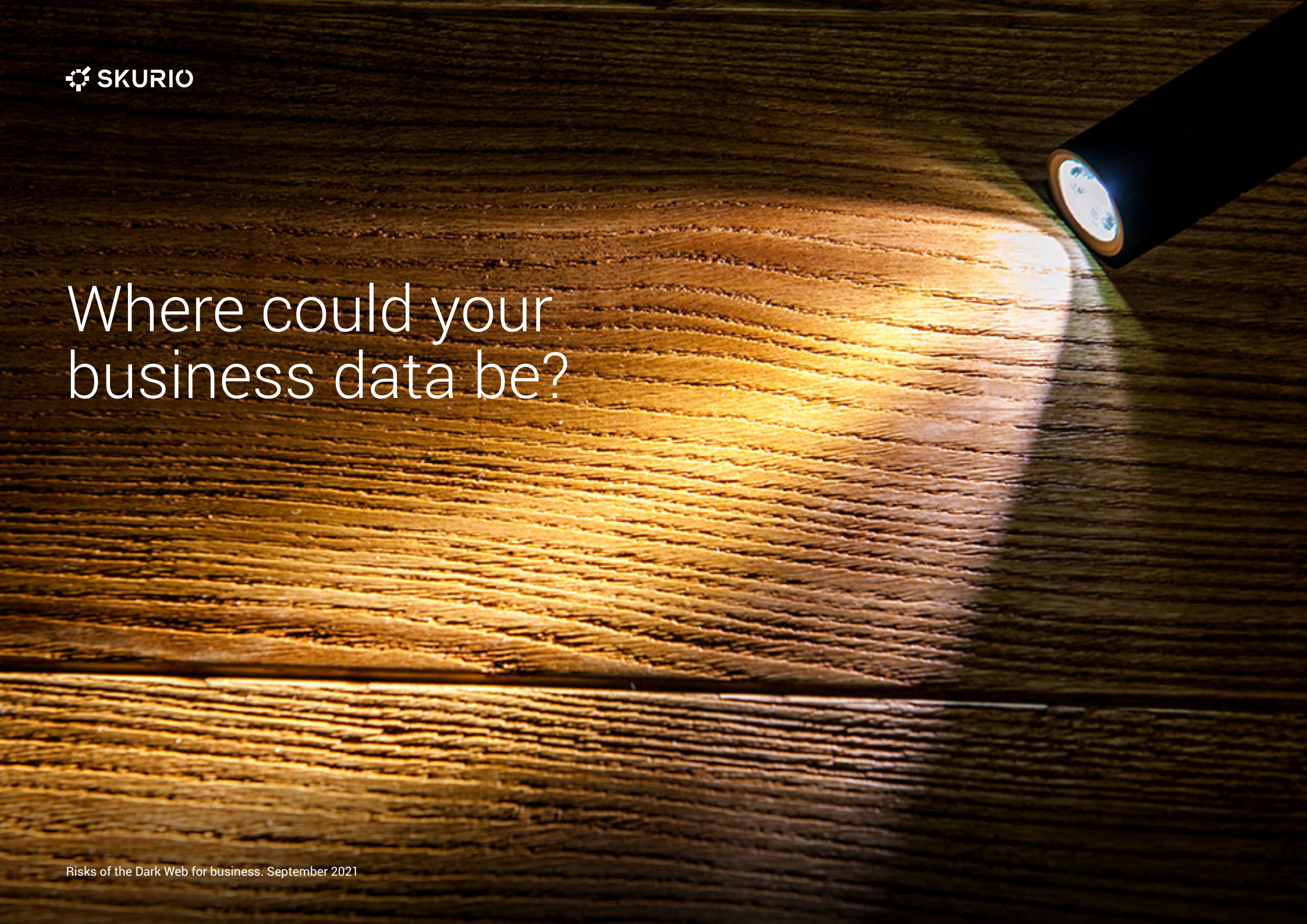
SKURIO

Threat actors will spend time compiling lists of businesses to target. They can dedicate hours researching those known to have vulnerabilities in equipment, outdated systems, or click-friendly users to use as ammunition in an attack.

Finding publicly available information of yours compiled into a step-by-step hack guide could be troubling for sure, but not finding it could be worse. In finding this information, you can be aware of and ready for an impending attack, or at least, potential attack.

DRP and DLP plans usually include monitoring codes, phrases, or keywords within critical documents and, in some cases, blocking them from leaving the network. This practice can assist your team in tracing any leaks back to the source. Regularly scanning the Dark Web for these keywords and phrases can be a great way to monitor your presence there and reduce your risk vector.

The sad truth is, most businesses will not know when they have had a breach until they have found sensitive information online, a public breach is announced, or the hackers contact you attempting to use the knowledge gained to exploit.


SKURIO
Where could your business data be?
Risks of the Dark Web for business. September 2021

We've explained that the Dark Web is hard to navigate, and you must know where you're looking.

Marketplaces and forums like eBay and Amazon are live, selling many nefarious items, including guns, illegal substances, and secret business information. The most famous black-market site you may have heard of, called Alpha Bay, was shut down by the FBI in 2017, and its moderator was given eleven years in prison. While that's a deterrent, it hasn't stopped others from setting up new markets in its place. These, often password-protected, marketplaces are frequented by threat actors looking for an easy way to make some cash.

While the Dark Web is the main topic of this whitepaper, it's not the only place to find stolen business and personal information. Posts and links showing snippets of data, and adverts pointing to Dark Web sites, can be found on common sites found on the surface web.

Google searchable sites such as Reddit, Telegram and other social media (yes, Facebook and Instagram) are often used for advertising the authors' illegal wares. Some accounts are created purely for this advertising task.

Scanning the Web automatically for similar posts can help link accounts and is the first step to identifying who is behind these criminal activities.

On top of these promotional posts, to prove their authenticity and give a flavour of what they have to offer, threat actors and hackers holding valuable business information may post snippets from their collection on other surface websites such as Paste Bin. Keeping a lookout for your domain, information, or your in-document codes and keywords on these sites, as well as the Dark Web, is imperative to any DLP or DRP plan.

Generic threat intelligence, is that enough?

As the weight of cybersecurity rests firmly on your shoulders, we know breach prevention and identification is high on your list. You will want to ensure you keep a balance between knowledge of breaches within your industry and their relevance to your business and current situation.

Most threat intelligence is broad, looking at breaches and sending alerts to you without much investigation into whether it is relevant or old information being re-shared or compiled.

Alert fatigue is prevalent in our industry and can make us complacent. And complacency and inaction in critical areas can lead to hacking opportunities.
If you can ensure only relevant information in the alerts, you can stay engaged where it matters.

That's where Skurio comes in.

SKURIO

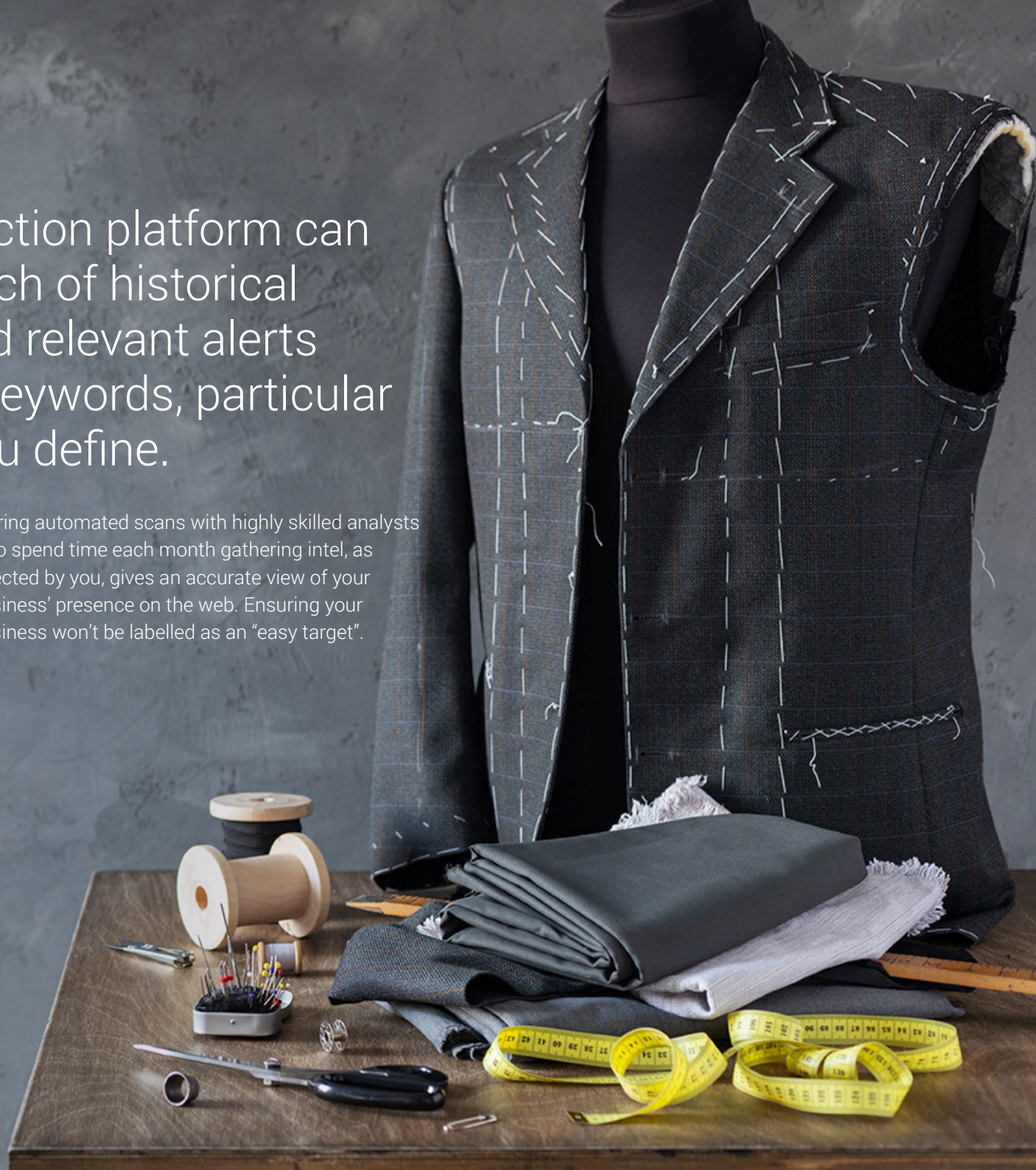
Skurio's Digital Risk Protection platform can be used for a one-off search of historical breaches or set up to send relevant alerts based on email, domain, keywords, particular vendors, or any criteria you define.

Skurio tailors the experience specifically to your business along with your employees and assets.

Its intuitive interface helps you search as granularly as you need, showing its working and its sources. Any alert or manual search results provide details relating to the breach with additional metadata, helping you determine what action you need to take.

Automating information scans of the surface, deep and Dark Web is time-efficient for everyone, including us! You won't have to wait for our analysts to find every detail across the web, and our analysts can use that time to analyse your data, research the Dark Web for more marketplaces, and optimise the system features.

Pairing automated scans with highly skilled analysts who spend time each month gathering intel, as directed by you, gives an accurate view of your business' presence on the web. Ensuring your business won't be labelled as an "easy target".



Can I do this in-house?

Reading this, it may be tempting to see if your team can accomplish this alongside their regular duties.

As we mentioned before, the Dark Web is vast and operates like a black market. Goods and services are sold to those who know where to look. To get into the marketplaces, you need to know the right people, chat them up on the forums, and get your in.

Even if you find a marketplace to enter, often other markets will pop up, sometimes for just a few hours. The names, web addresses, and passwords of sites are ever-changing and, without warning, will disappear into the ether.

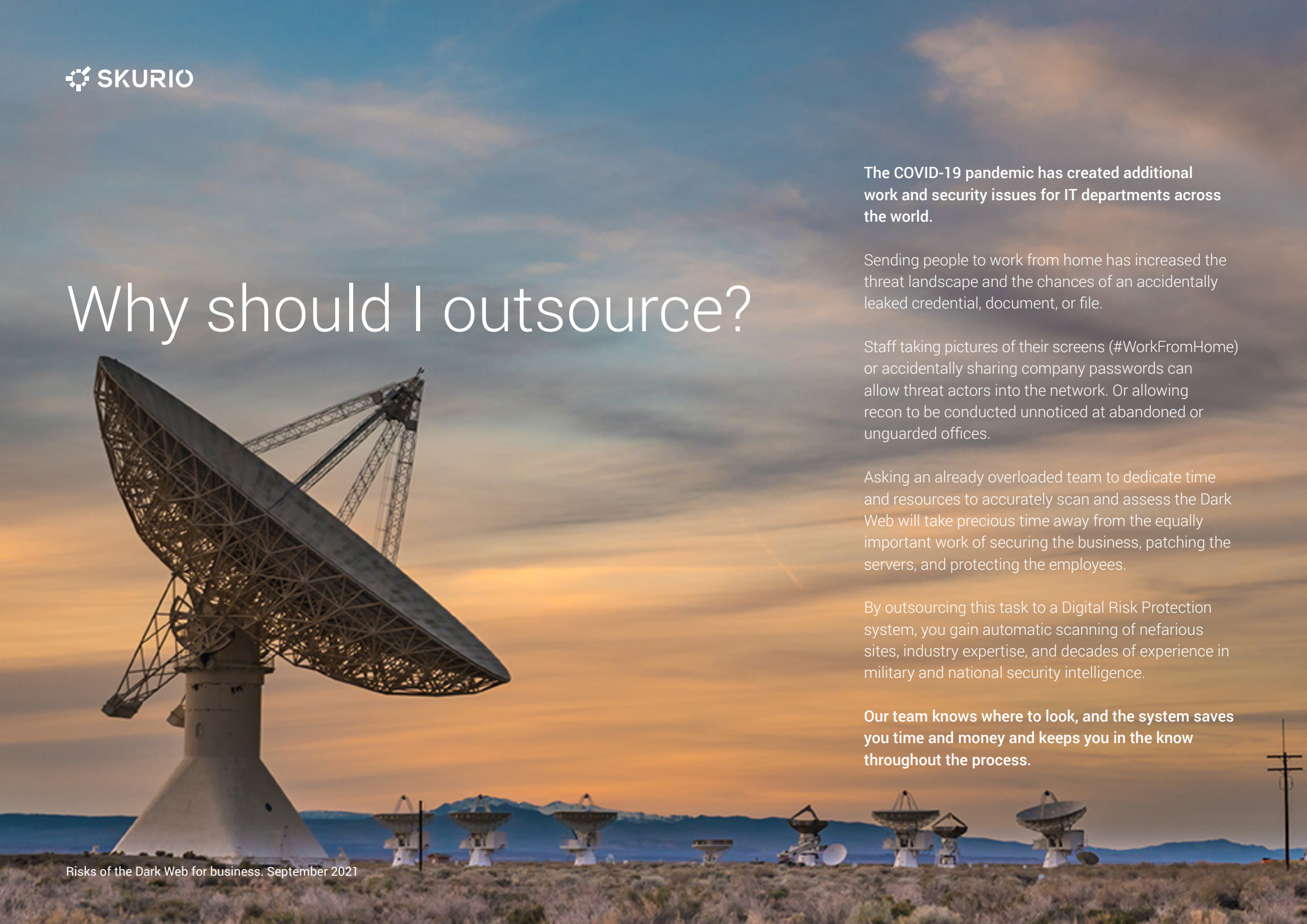
Knowing and accessing these marketplaces is only the beginning. Illegal activity, explicit pornography, weapons, and drugs are just a few of the disturbing things you can find on the Dark Web markets. Offensive conversations and discussions of illegal goings-on are regular content on the forums. Just viewing some of the images and market offerings without knowing what you are doing can legally implicate you and your staff. Mentally, the impact of traumatic and horrific content shown can be extremely disturbing for your employees.

Keeping on top of this kind of work would be tough.A business would need a team of highly skilled workers with knowledge extending to all corners of the unknown Web, working around the clock to catch the pop-ups.

Even with that team, it's too much work without the automation that Skurio can provide. You need to spend your time investigating breaches and threats, not searching for them.

SKURIO

Why should I outsource?



The COVID-19 pandemic has created additional work and security issues for IT departments across the world.

Sending people to work from home has increased the threat landscape and the chances of an accidentally leaked credential, document, or file.

Staff taking pictures of their screens (#WorkFromHome) or accidentally sharing company passwords can allow threat actors into the network. Or allowing recon to be conducted unnoticed at abandoned or unguarded offices.

Asking an already overloaded team to dedicate time and resources to accurately scan and assess the Dark Web will take precious time away from the equally important work of securing the business, patching the servers, and protecting the employees.

By outsourcing this task to a Digital Risk Protection system, you gain automatic scanning of nefarious sites, industry expertise, and decades of experience in military and national security intelligence.

Our team knows where to look, and the system saves you time and money and keeps you in the know throughout the process.

SKURIO

Should I be worried?

Let us worry for you.

It has been a tough 18 months for everyone, but IT and Cybersecurity have had it especially hard.

The pressure has been raised to quickly provide a secure and workable remote solution with little to no time to test it. The goalposts of DLP and DRP plans have moved way past the budgetary limitations previously given.

Working from home can also mean you haven't been switching off as much as you should. We don't want to add any more to your plate!

We want to take this time to congratulate you and your business for a job well done this past year. By reading this whitepaper and learning about the dangers of the Dark Web, you're taking all the proper steps to secure your business.

SKURIO

Skurio's Digital Risk Protection platform has options for companies of all sizes – with built-in security and GDPR compliance, and smart automation that takes the headache out of proactive monitoring.

Importantly, our experts are always here for a straightforward, no-fuss conversation to help you work out what measures you really need. If you'd like to explore the subject further – or if you have questions about anything in this guide – feel free to call us for an informal chat.

Call us today on **+44 28 9082 6226** or email **info@skurio.com**

www.skurio.com

SKURIO LTD | ARTHUR HOUSE | 41 ARTHUR STREET | BELFAST | BT1 4GB
+44 28 9082 6226 **info@skurio.com** **skurio.com**