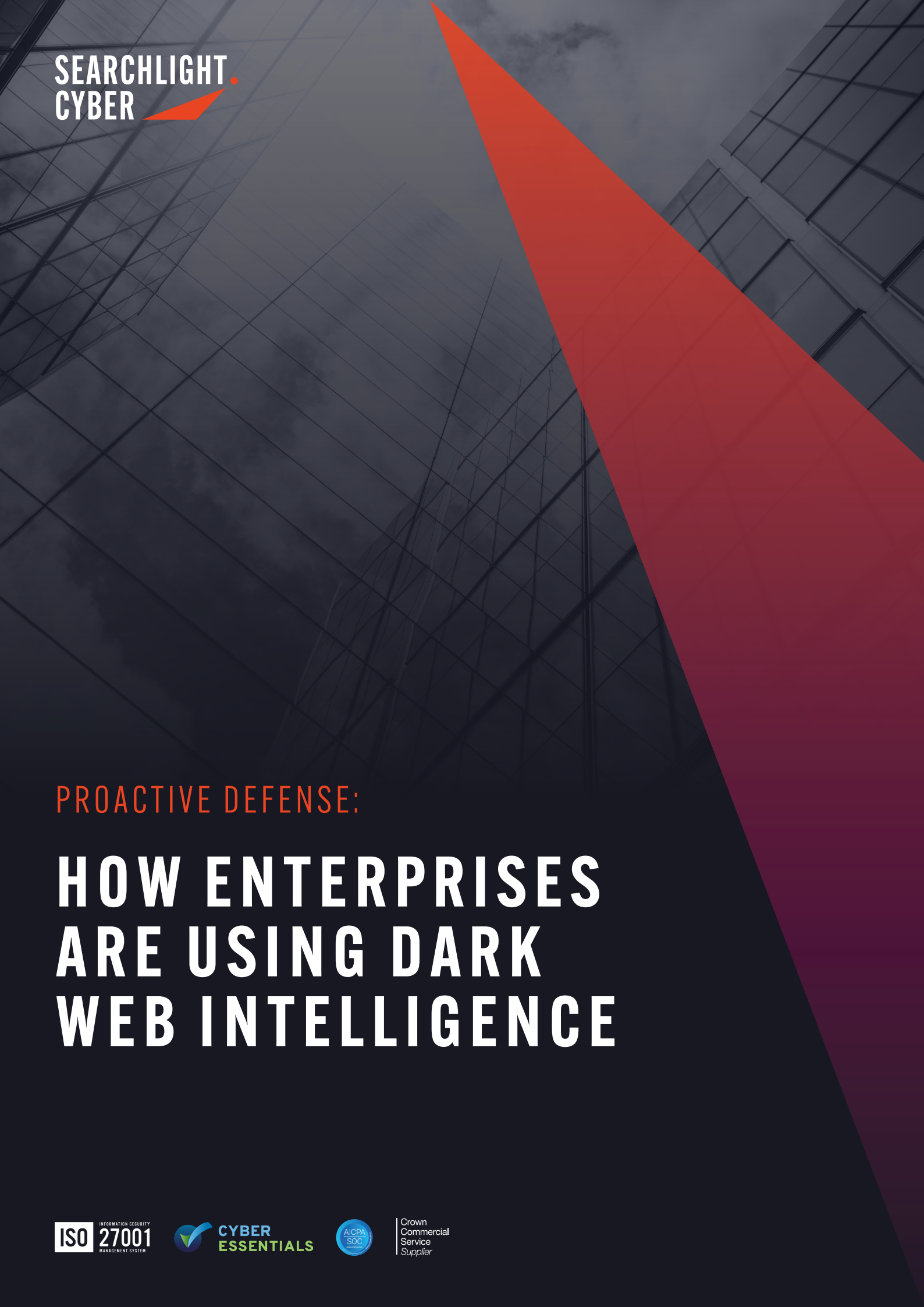


SEARCHLIGHT CYBER

PROACTIVE DEFENSE:

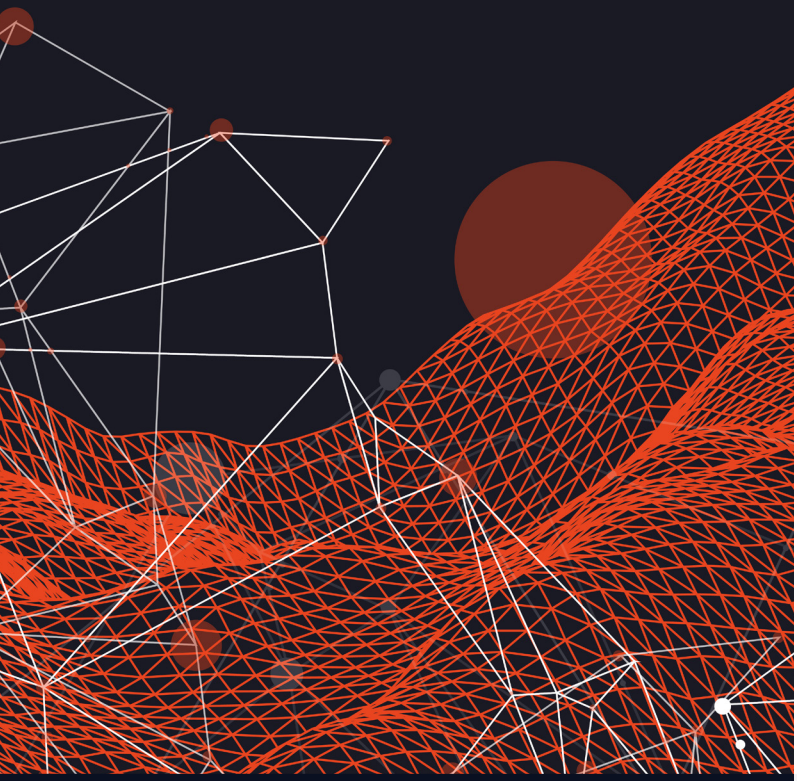
HOW ENTERPRISES ARE USING DARK WEB INTELLIGENCE

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

CYBER ESSENTIALS

AICPA SOC

Crown Commercial Service *Supplier*



SEARCHLIGHT. CYBER

Searchlight Cyber provides organizations with relevant and actionable dark web intelligence, to help them identify and prevent criminal activity. Founded in 2017 with a mission to stop criminals acting with impunity on the dark web, we have been involved in some of the world's largest dark web investigations and have the most comprehensive dataset based on proprietary techniques and ground-breaking academic research. Today we help government and law enforcement, enterprises, and managed security services providers around the world to illuminate deep and dark web threats and prevent attacks.

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

CYBER ESSENTIALS

AICPA SOC

Crown Commercial Service *Supplier*

CONTENTS

INTRODUCTION

Over the past few years cybersecurity professionals have been increasingly turning their attention to the "pre-attack" stages of a cyberattack. This refers to the time when threat actors are effectively in the "planning" stages. Or, to use the technical terms, undertaking their reconnaissance against organizations and developing the resources they need to execute their attacks.

This stage is critical for cybersecurity professionals because it is the only part of the attack that takes place off their infrastructure. If they can spot threat actors targeting them in this phase, they can prevent them from ever breaching their network in the first place. It is a much more proactive approach to security but it requires visibility into the dark web, the space that cybercriminals use to plan their attacks.

The objective of the research was to understand how far large enterprises - the ones who have the biggest budgets, resources, and motivation to protect themselves - have come in gathering pre-attack intelligence from the dark web, and the impact it has had on their security posture. To do this, we commissioned the research company Censuswide to conduct a survey of CISOs working in large enterprises with more than $200 million in revenue and more than 2,000 employees. In total, 1,008 CISOs were interviewed across the US and UK.

What we discovered is a clear correlation between the CISOs that are gathering threat intelligence, pre-attack intelligence, and gathering data from the dark web - and a better security posture. Those that have invested the most in these areas are more confident that they understand their adversaries and are more likely to have identified an attack before it hit their network - i.e. in the pre-attack phase.

While the adoption of threat intelligence and use of dark web data is high among this sample, our research shows that it is not equal. CISOs in the US are ahead of their UK counterparts in this area, and the finance industry emerges as the most "cyber mature" sector.

Our hope is that this research, which demonstrates the positive impact of gathering pre-attack intelligence, will help CISOs learn from the successes of their peers. Across the board, there is more opportunity that can be seized from gathering dark web intelligence, which can be used for everything from identifying historic breaches, to threat hunting, to monitoring the risk exposure of the supply chain. The evidence is compelling: unlocking these data sources can help enterprises to take a more proactive approach to cybersecurity.

BEN JONES
CEO and Co-Founder
Searchlight Cyber

METHODOLOGY

The following findings are from a survey conducted by the research company Censuswide. In total, 1,008 CISOs were surveyed between November 18, 2022 and January 16, 2023 - 502 in the US and 506 in the UK. All of the CISOs in this sample come from large enterprises with more than $200 million in revenue and more than 2,000 employees.

TOP LINE FINDINGS

ALMOST ALL CISOs IN LARGE ENTERPRISES ARE WORRIED ABOUT THE DARK WEB

93 percent of the CISOs said they are concerned about dark web threats.

MOST CISOs ARE USING THREAT INTELLIGENCE TO ADDRESS THIS THREAT, INCLUDING DATA FROM THE DARK WEB

79 percent of CISOs say they are currently gathering data from the dark web.

HOWEVER, THERE IS MORE WORK TO BE DONE TO MAKE SURE ALL LARGE ENTERPRISES ARE ON THE SAME PAGE

More than a fifth of CISOs have no threat intelligence capability at all.

IN PARTICULAR, US ENTERPRISES ARE AHEAD OF THEIR UK COUNTERPARTS IN GATHERING PRE-ATTACK INTELLIGENCE

And, as a consequence, 85 percent of US CISOs feel confident that they understand the profile of their adversaries compared to 70 percent of CISOs in the UK.

INDUSTRIES SUCH AS FINANCIAL SERVICES ARE ALSO FURTHER ALONG IN GATHERING INTELLIGENCE FROM THE DARK WEB

Almost all (85 percent) of finance organizations are gathering data from the dark web, compared to 57 percent of healthcare organizations.

CISOs VS DARK WEB THREATS

AWARENESS OF DARK WEB THREATS

The dark web is a part of the internet that is purposefully obfuscated, requiring a user to download specialist software such as The Onion Router (Tor) to access. While there are some ethical uses for the dark web - such as its use by whistleblowers - the vast majority of activity is explicitly illegal, with criminals taking advantage of the ability to browse and host websites anonymously.

Among other criminal activities, such as the sale of drugs, arms, and forgeries, the dark web is the home to cybercriminal activity. This includes (but is not limited to): marketplaces for buying and selling malware, exploits, and stolen corporate data; forums where cybercriminals discuss their tactics and share techniques; and ransomware leak sites where cybercriminals threaten to publish stolen data unless their demands are met.

Naturally, this makes the dark web a topic of interest for the CISOs' who are ultimately responsible for protecting the organization from cyberattacks. Indeed, almost all (93 percent) of the CISOs we surveyed said that they are concerned about dark web threats, demonstrating that this is very much at the top of the list for security leaders in some of the biggest companies.

93 PERCENT OF CISOs ARE CONCERNED ABOUT DARK WEB THREATS

72 PERCENT OF CISOs BELIEVE THAT INTELLIGENCE ON CYBERCRIMINALS IS "CRITICAL" TO PROPERLY DEFEND THEIR ORGANIZATION

76 PERCENT OF CISOs USE THREAT INTELLIGENCE AS PART OF THEIR SECURITY STRATEGY

HOW CISOs ARE TAKING ACTION

The next question is how CISOs are taking action on this concern. Our survey found that Cyber Threat Intelligence has been identified as a priority by CISOs in most large enterprises. Almost three quarters (72 percent of them) believe that intelligence on cybercriminals is "critical" to properly defend their organization, and 76 percent are already using threat intelligence as part of their security strategy.

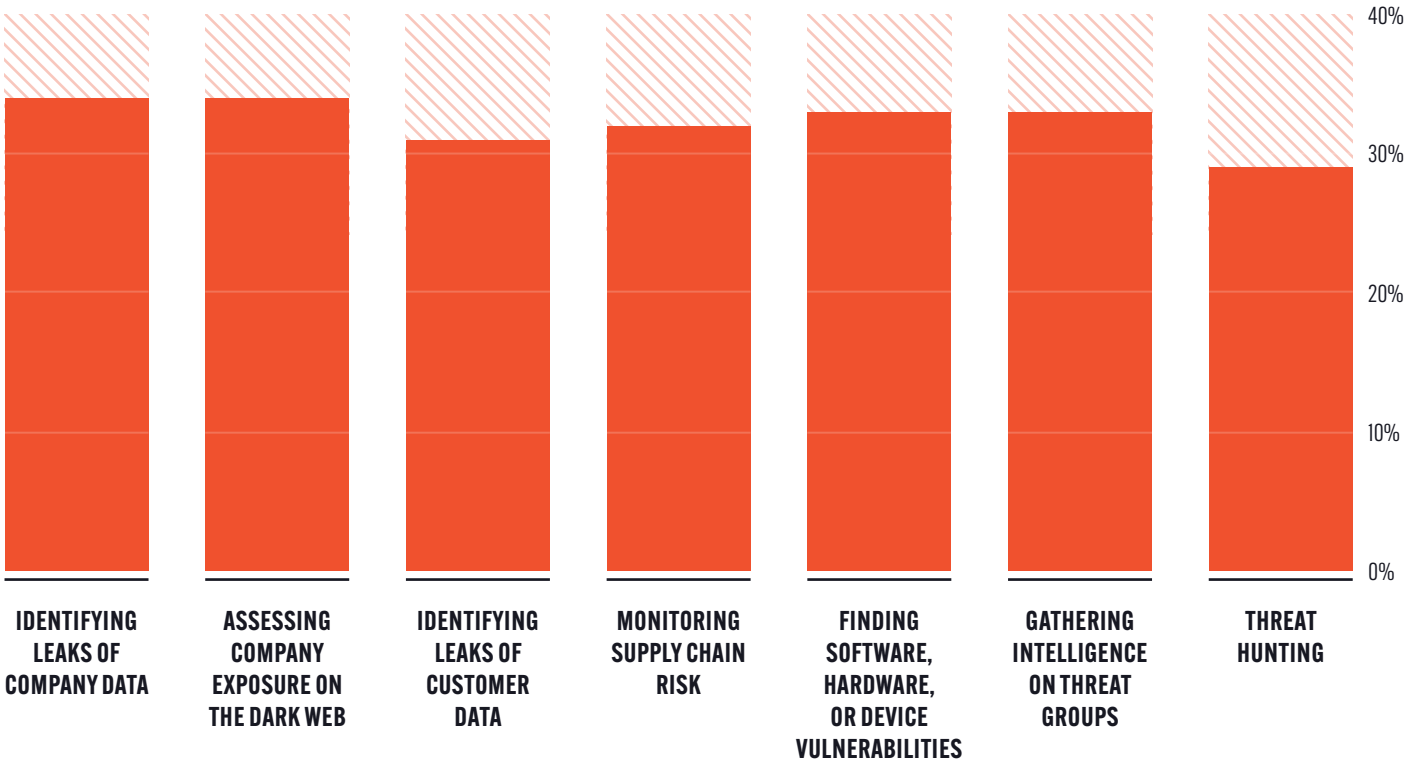
While this widespread use isn't entirely shocking, as threat intelligence has long been established as a staple of cybersecurity defense, what is interesting is how many CISOs (64 percent) claim to be gathering "pre-attack intelligence".

As the name suggests, this is a specific type of threat intelligence that relates to the actions of cybercriminals before they launch their attack on an organization, and breach the network. As defined in the MITRE ATT&CK Enterprise Matrix, pre-attack intelligence concerns threat actor's Reconnaissance (TA0043) and Resource Development (TA0042) tactics.[1]

[1] https://attack.mitre.org/matrices/enterprise/

This activity - where criminals choose their target, plan their attacks, and build their tools - predominantly takes place in the dark web, which is where security teams need to gather their "pre-attack" intelligence. In fact, 79 percent of CISOs say they are currently gathering data from the dark web, and they use it for a number of different purposes:

FIGURE 1: HOW THE CISOs THAT COLLECT DARK WEB DATA USE IT (N. 800).



In terms of how they gather this data, most CISOs reported that they used a dark web intelligence platform, followed by a feed, and a consultant service provider.

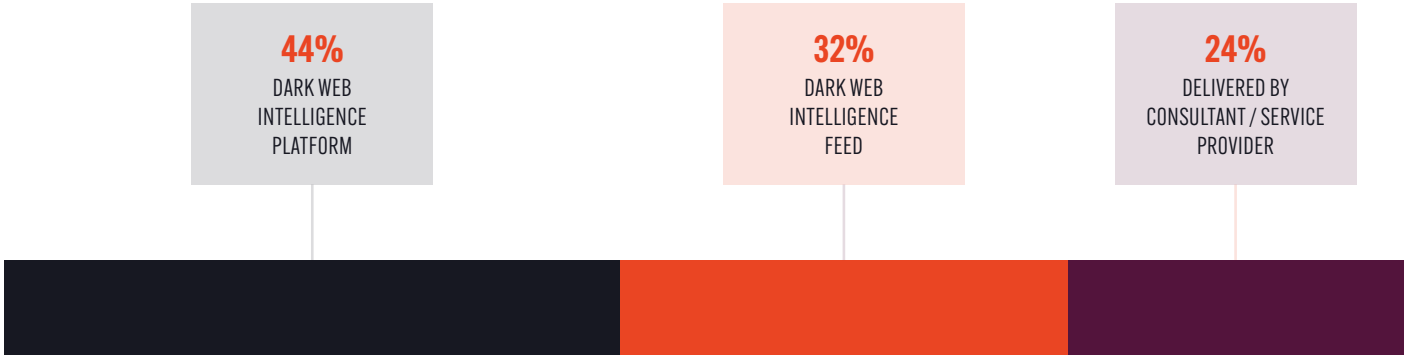


FIGURE 2: CHART SHOWING SOURCES OF DARK WEB DATA, FOR CISOs WHO SAID THEY GATHER DARK WEB INTELLIGENCE (N. 800).

MORE WORK TO BE DONE

Although these adoption rates are high, the research also demonstrates that there is room for improvement both in understanding of dark web threats and in the gathering of threat intelligence, even among this sample of cyber mature organizations.

For example, while the vast majority are using threat intelligence to some degree, less than a quarter of CISOs (24 percent) have a dedicated threat intelligence team.

More concerning for the size of organization we are discussing, more than a fifth (21 percent) have no threat intelligence capability at all.

Furthermore, when it comes to understanding the possible impact of dark web threats, almost a fifth (18 percent) of respondents believe that criminal activity doesn't have an impact on their business. A further 18 percent "neither agree or disagree", suggesting a lack of understanding between the relationship between the dark web and cybersecurity attacks.

BEN JONES, CEO OF SEARCHLIGHT CYBER COMMENTED:

"There is no doubt that the general adoption of threat intelligence and, in particular, pre-attack intelligence among these CISOs is high. The sample we are surveying are from large organizations, so we would expect them to be ahead of the curve in their use of threat intelligence and understanding of dark web threats. However, even among this group we have identified some organizations lagging behind, which goes some way to explaining why more than a quarter of CISO (26 percent) reported that they have never identified a legitimate threat before it hit the network.

"Figure 1 (page 7) also suggests that enterprises are not yet using dark web data to its fullest potential. While many organizations are using it in some way, these stats show that few are using it across the board for everything from finding vulnerable devices to gathering intelligence on threat groups. This is resulting in missed opportunities to solve some of their biggest cybersecurity challenges.

"For example, 71 percent of total respondents told us they would like the ability to see if their suppliers are being targeted on the dark web, but Figure 1 shows us that only 32 percent of those that are gathering dark web data are using it to monitor their supply chain risk. Gathering intelligence from dark web forums and marketplaces offers a brilliant chance for enterprises to spot cybercriminals targeting their suppliers."

ONLY **24 PERCENT** OF ENTERPRISES HAVE A DEDICATED THREAT INTELLIGENCE TEAM

ONE IN FIVE ENTERPRISES HAVE NO THREAT INTELLIGENCE CAPABILITY AT ALL

71 PERCENT OF CISOs WANT TO SEE IF THEIR SUPPLIERS ARE BEING TARGETED ON THE DARK WEB

DARK WEB DISPARITIES

Splitting the survey by geography and industry uncovers imbalances in understanding of dark web threat and use of pre-attack intelligence. Analyzing these results demonstrates a clear correlation between those enterprises that are gathering threat intelligence and data from the dark web, and improved security posture.

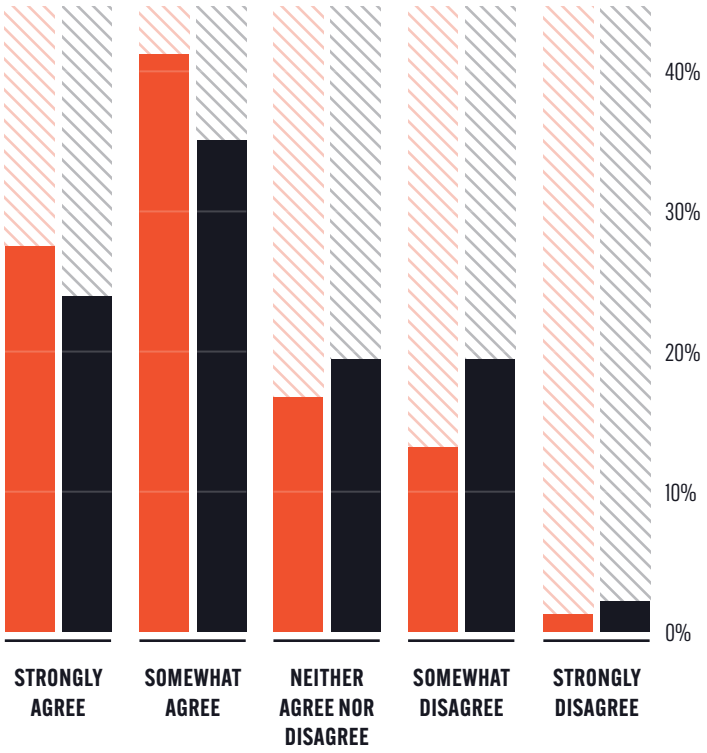
US AHEAD IN PRE-ATTACK INTELLIGENCE

Starting with geography, a major finding of this research was that the US-based CISOs are ahead of their UK counterparts in terms of understanding of dark web threats. For example, 69 percent of US CISOs understand that criminal activity on the dark web can have an impact on their company, compared to 59 percent in the UK.

Moreover, more US CISOs (77 percent) believe that intelligence on cybercriminals is critical to properly defend their organization, compared to 66 percent in the UK. US CISOs are also more interested in intelligence on whether their supply chain is being targeted (76 percent US vs 66 percent UK), and if their executives are being targeted (76 percent US vs 62 percent UK).

As a consequence, US organizations are more likely to have a threat intelligence capability, more likely to capture "pre-attack" threat intelligence, and more likely to gather data from the dark web (**Figure 4**).

FIGURE 3:
MORE US CISOs "AGREE" OR "STRONGLY AGREE" THAT CRIMINAL ACTIVITY ON THE DARK WEB HAS AN IMPACT ON THEIR COMPANY.



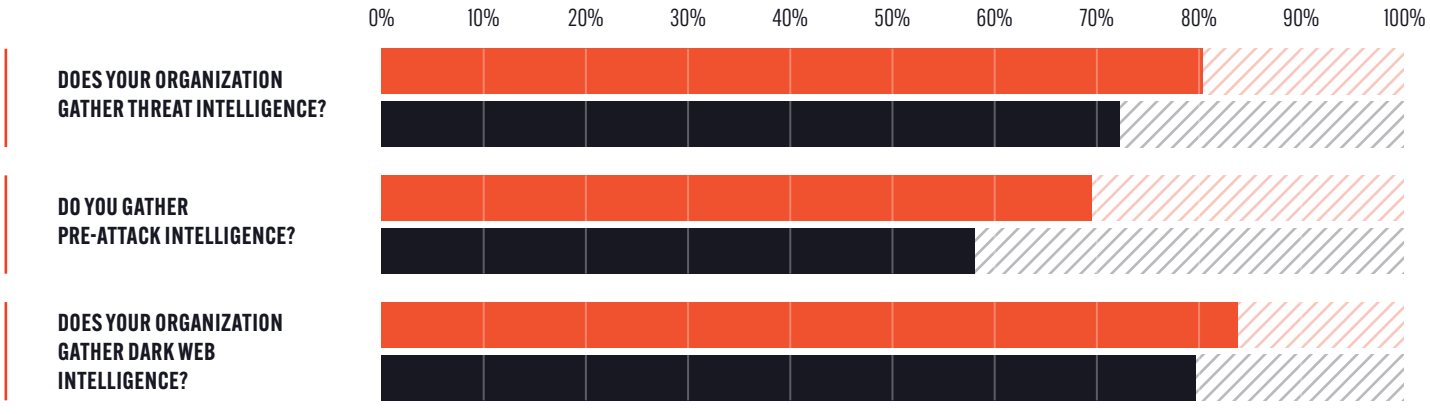


FIGURE 4: THESE DATA POINTS DEMONSTRATE THAT THE US IS AHEAD OF THE UK IN TERMS OF ADOPTING THREAT INTELLIGENCE, PRE-ATTACK INTELLIGENCE, AND DARK WEB INTELLIGENCE.

Perhaps unsurprising, US CISOs feel far more secure in their cybersecurity posture. For example, only 85 percent said that they feel confident that they understand the profile of their adversaries, compared to 70 percent of CISOs in the UK.

Most significantly, US enterprises are more than 20 percentage points more likely to identify a threat before it hits their network (54 percent vs 75 percent). This demonstrates that the use of pre-attack intelligence has a material impact on the ability of US CISOs to identify and prevent emerging attacks.

BEN JONES, CEO OF SEARCHLIGHT CYBER COMMENTED:

"Our survey suggests that the US is slightly ahead of the UK in the adoption of pre-attack intelligence. What is significant is the clear pattern that emerges between gathering more threat intelligence and data from the dark web, and a better security posture. Many UK enterprises have clearly already identified the opportunity of dark web intelligence but, for those that haven't, these results make it crystal clear: gathering pre-attack intelligence will help them gain a better understanding of their adversaries and increase their chances of spotting an attack."

80 PERCENT OF US ENTERPRISES ARE GATHERING THREAT INTELLIGENCE, COMPARED TO **72 PERCENT** IN THE UK

75 PERCENT OF CISOs IN THE US REPORT THAT THEY HAVE SUCCESSFULLY IDENTIFIED A CYBERATTACK BEFORE IT HITS THEIR NETWORK

85 PERCENT OF CISOs IN THE US FEEL CONFIDENT THAT THEY UNDERSTAND THE PROFILE OF THEIR ADVERSARIES

FINANCE LEADS ADOPTION OF DARK WEB INTELLIGENCE

There are also variations in how different industry sectors are responding to dark web threats. Often assumed to be the most "cyber mature" sector, it is perhaps unsurprising that financial services organizations perform highly across most categories. However, not all "high risk" industries are tackling dark web threats as effectively and the same pattern emerges: the more pre-attack intelligence that is being gathered the better the security posture.

The graphs in **Figure 5** shows where a selection of the industries we surveyed stand in their adoption of threat intelligence and dark web data.

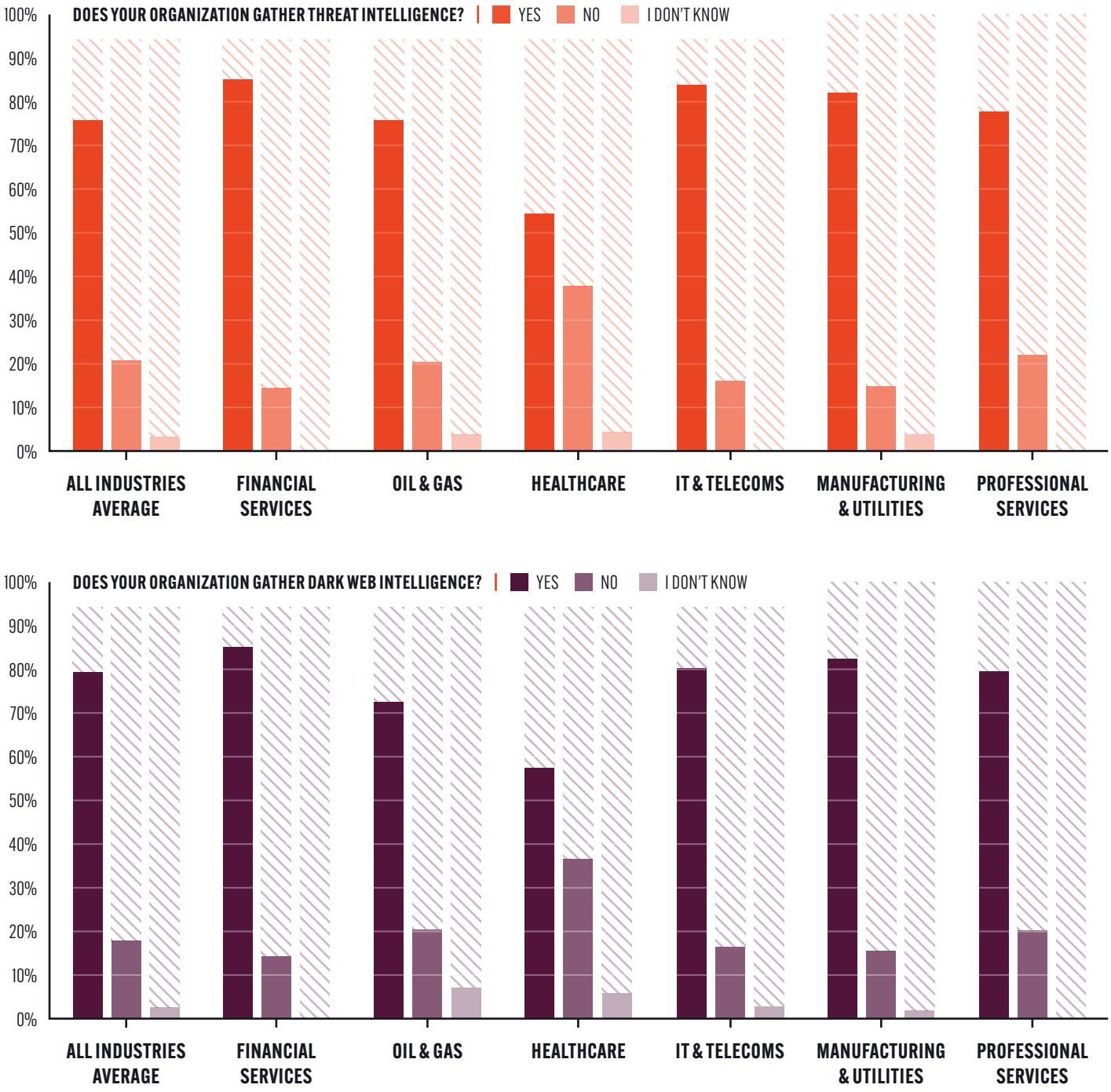


FIGURE 5: A COMPARISON OF SAMPLE INDUSTRIES IN ADOPTION OF THREAT INTELLIGENCE AND DARK WEB DATA.

Finance performs best in both categories but is followed closely by IT & Telecoms, manufacturing, and professional services. Unfortunately, the survey results indicate that the healthcare industry is behind its peers, with more than a 20 percentage point gap between its results and the average in gathering threat intelligence (54 percent) and gathering data from the dark web (57 percent). These findings also show that oil and gas organizations are below the average in terms of adoption of threat intelligence and dark web intelligence.

Once again, disparities in the use of threat intelligence and - in particular - dark web coverage is reflected in CISO's perception of their security posture (**Figure 6**). For example, only 60 percent of CISOs at healthcare organizations and 74 percent at oil and gas enterprises feel confident that they understand the profile of their adversaries, compared to 77 percent on average. They are also both less likely to have identified a legitimate threat before it hit the network, which is especially concerning considering that these industries fit squarely into the category of critical national infrastructure. On the other hand, industries such as manufacturing, financial services, and professional services report a stronger security posture.

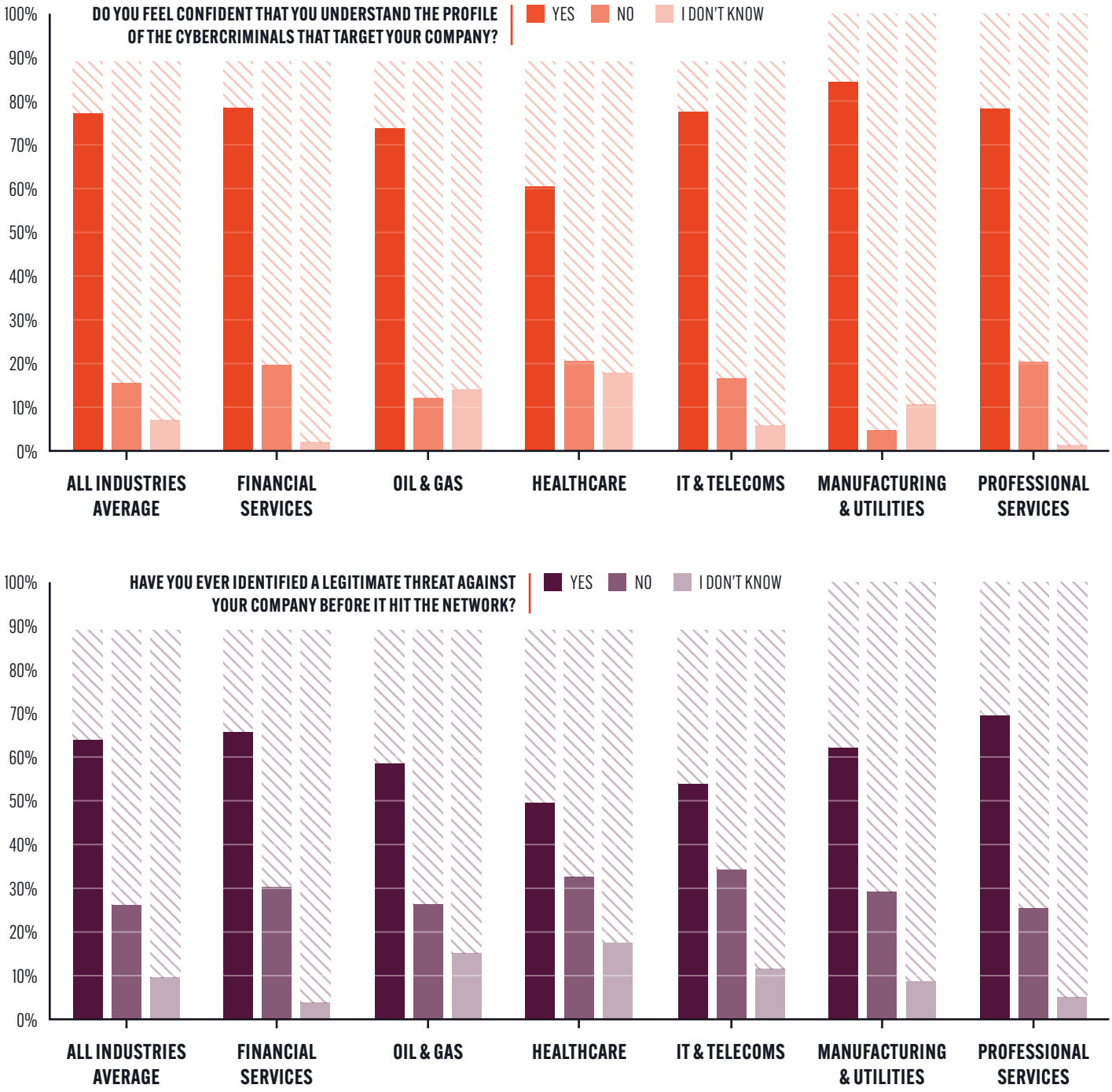


FIGURE 6: CISOs IN HEALTHCARE AND OIL AND GAS ORGANIZATIONS ARE LESS CONFIDENT THAN THEIR PEERS THAT THEY UNDERSTAND THEIR ADVERSARIES AND ARE LESS LIKELY TO HAVE IDENTIFIED A THREAT BEFORE IT HITS THEIR NETWORK.

A lack of understanding of threats emanating from the dark web could be a contributing factor for why healthcare and oil and gas are falling behind other industries. For example, only half (50 percent) of CISOs at healthcare organizations said they believe that criminal activity on the dark web has an impact on their company (compared to the 64 percent average) and only 53 percent believe intelligence on cybercriminals is critical to properly defend their organization. Similarly, more than a quarter (27 percent) of oil and gas CISOs stated that criminal activity on the dark web has no impact on their company.

One of the most surprising results of the research (displayed in **Figure 7**) was that only 50 percent of healthcare CISOs and 66 percent of oil and gas CISOs are interested in seeing if their suppliers are being targeted on the dark web. Once again, this suggests a lack of understanding of where cyberattacks against their enterprises are originating.

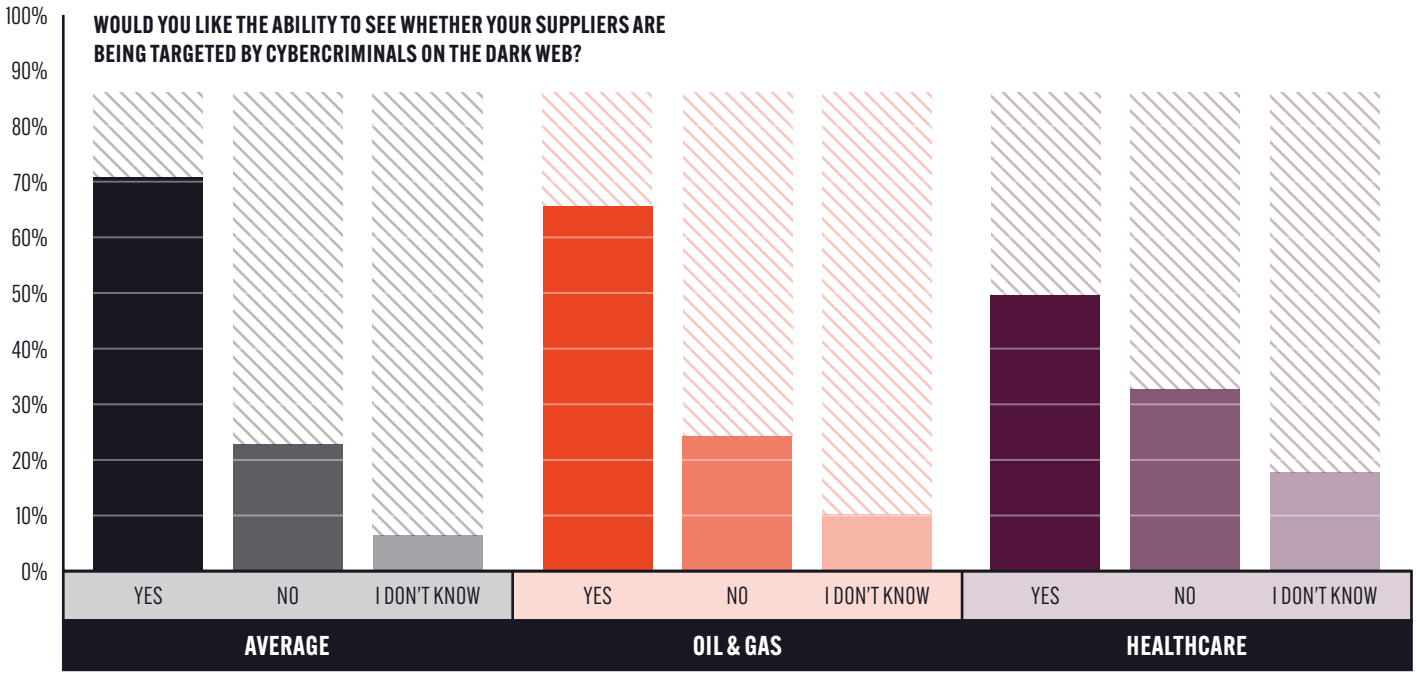


FIGURE 7: CISOs AT HEALTHCARE AND OIL AND GAS ORGANIZATIONS ARE LESS LIKELY THAN THE AVERAGE CISO TO WANT THE ABILITY TO SEE IF THEIR SUPPLIERS ARE BEING TARGETED ON THE DARK WEB.

BEN JONES, CEO OF SEARCHLIGHT CYBER COMMENTED:

"There are a number of possible explanations as to why oil and gas companies and healthcare organizations are behind in the adoption of pre-attack intelligence. Both of these industries have large, complex, and legacy infrastructure, which means they may be prioritizing other security challenges such as vulnerability patching. It is also likely that, unlike enterprises in the finance sector, health and energy organizations may not have historically considered themselves the primary target for financially-motivated cyberattacks emanating from the dark web.

"However, the cybersecurity landscape has changed dramatically over the past few years. Cybercriminals are no longer just focusing on asset-rich organizations like banks and insurance companies. They are increasingly targeting enterprises in industries such as healthcare, oil and gas, and manufacturing, and leveraging the critical nature of these companies to extort ransoms.

"In both the healthcare and energy industries we have seen high-profile examples of these kinds of attacks - often targeting their supply chains. In the US, the 2021 ransomware attack on Colonial Pipeline led to the White House declaring a state of emergency after the oil pipeline was shut down for several days.[2] In the UK, incidents such as the 2022 ransomware attack against the NHS supplier Advanced demonstrates that nothing could be more vital to healthcare organizations than identifying if their suppliers are being targeted online.[3]

"Research from our own threat intelligence team has found that companies are routinely targeted on dark web forums. For example, we often observe threat actors auctioning initial access to oil and gas organizations through compromised VPNs - which is the exact technique that the ransomware gang DarkSide used to compromise Colonial. Visibility into this cybercriminal reconnaissance would help CISOs in the healthcare and oil and gas sector to identify likely paths of attack, inform defenses, and help them prioritize imminent threats."

[2] https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know
[3] https://techcrunch.com/2022/10/13/advanced-nhs-patient-data-ransomware/

> THE CYBERSECURITY LANDSCAPE HAS CHANGED DRAMATICALLY OVER THE PAST FEW YEARS. CYBERCRIMINALS ARE NO LONGER JUST FOCUSING ON ASSET-RICH ORGANIZATIONS LIKE BANKS AND INSURANCE COMPANIES.

GATHERING DARK WEB INTELLIGENCE

There is a clear correlation between the organizations that are gathering pre-attack intelligence and the CISO's perception of their own security and ability to spot and stop attacks before they hit their network. Often this capability comes down to access to dark web sources, which provide the best chance of spotting a criminal in the early stages of planning a cyberattack.

With the right dark web data, organizations can see exactly what is happening on dark web forums, marketplaces, and leak sites. They can observe cybercriminals discussing exploit techniques, buying and selling the latest malware, and even spot them discussing their organization or talking about their suppliers.

This access enables security teams to identify the early warning signs of some of the threats that keep CISOs awake at night, including: ransomware attacks, cybercriminals targeting the supply chain, and even malicious insiders connecting with threat actors via Tor.

At Searchlight Cyber, we are committed to furthering organizations' understanding of how they can gather and use threat intelligence gathered from the dark web. Our threat intelligence team is continuously researching activity on the dark web and developing models of how organizations can act this pre-attack intelligence into their security posture and respond to imminent attacks.

THE TOP THREE RECOMMENDATIONS FROM OUR DIRECTOR OF THREAT INTELLIGENCE

1. USE DARK WEB INTELLIGENCE TO PRIORITIZE THREATS

Most enterprises will already be undertaking a combination of first party and third party threat intelligence collection, which means some readers may be wondering what dark web data offers in addition - other than more alerts. The answer is that dark web intelligence should be drawn into the security operations center and cross-referenced against other intelligence sources to identify the most pressing threats based on the pre-attack activity of criminals. While other threat intelligence sources mostly tell enterprises what has happened in the past, and therefore what might happen again, dark web data helps enterprises identify what is most likely to happen next.

Remember, a threat is indicated by a conversion of three factors: capability (the tools and resources of the adversary), opportunity (the ability to attack at that time), and intent (the motive behind the attack). By providing unique visibility into cybercriminal reconnaissance, dark web intelligence gives enterprises the best chance of spotting an attack before it hits the network.

2. BUILD THREAT MODELS

Threat modeling is a process by which potential threats can be identified, enumerated, and prioritized – all from a hypothetical attacker's point of view. The intent is to provide defenders with a systematic analysis of the probable attacker's profile, most likely attack vectors, and the assets most desired by an attacker. Threat modeling aims to answer questions such as: "Where are my high-value assets?", "Where am I most vulnerable to attack?", "What are the most relevant threats to me?", and "Is there an attack vector that might go unnoticed?".

It is critical that enterprises remember that threat modeling isn't a one and done exercise - attackers change what they are doing, new actors join the party, some actors aren't even seen again - so at a minimum it should be conducted annually.

3. UTILIZE THE MITRE ATT&CK FRAMEWORK

The MITRE ATT&CK framework is a popular resource with security professionals for a good reason. The pre-existing database of MITRE ATT&CK TTPs, possible countermeasures available with MITRE ATT&CK Mitigations, and detection opportunities with MITRE ATT&CK Data Sources - provides organizations with a fantastic foundation for them to build their company-specific threat models in a common and well documented lexicon. The evolving nature of cybercrime is reflected in the granularity of MITRE ATT&CK and allows the threat model to describe the nuances seen in attacks and guides in how these can be mitigated. It helps the threat model live.

JIM SIMPSON
Director of threat intelligence
Searchlight Cyber

SEARCHLIGHT. CYBER

DARK WEB INTELLIGENCE
FOR ENTERPRISE

COLLECT PRE-ATTACK INTELLIGENCE WITH SEARCHLIGHT CYBER

Our dark web investigation and monitoring products give cybersecurity professionals unprecedented visibility into cybercriminal activity on hidden forums, marketplaces, and leak sites. Updated live, with an archive of more than 15 years of historic data, security teams can search and be alerted to threat actor activity that might indicate a group is in the "pre-attack" stage of attack against their organization.

CERBERUS
DARK WEB INVESTIGATION

UNCOVER DARK WEB ACTIVITY

Cerberus uses proprietary techniques developed by world-leading researchers to deliver the most comprehensive dark web dataset on the market, providing access to intelligence that was previously unobtainable.

UNCOVER THE CYBERCRIMINAL UNDERWORLD

Understand the scale of criminal activity on the dark web to inform resourcing and investigation.

IDENTIFY ACTORS

Investigate individuals and groups with the ability to pivot on usernames, aliases, and historic activity.

EXTRACT THREAT INTELLIGENCE

Uncover the activity of cybercriminals in the pre-attack phase, to inform cyber defenses.

DARKIQ
DARK WEB MONITORING

SPOT CYBERATTACKS. EARLIER

With DarkIQ, you can identify cybercriminals while they are still in the reconnaissance stage of their attack, so rather than just responding to attacks, you can prevent them from happening.

INCREASE SOC EFFICIENCY

Prioritize alerts based on dark web intelligence that indicates an imminent threat.

BUILD THREAT MODELS

Based on dark web intelligence on the capability, opportunity, and intent of threat groups.

ENHANCE SUPPLY CHAIN SECURITY

With visibility into the dark web exposure of suppliers and cybercriminals targeting third parties.

SEARCHLIGHT CYBER

VISIT **WWW.SLCYBER.IO** TO FIND OUT MORE OR BOOK A DEMO NOW.

UK HEADQUARTERS
Suite 63, Pure Offices,
1 Port Way, Port Solent,
Portsmouth PO6 4TY
United Kingdom

US HEADQUARTERS
900 16th Street NW,
Suite 450, Washington,
DC 20006
United States