BLACK DRAGON CAPITAL

# CYBERSECURITY WHITEPAPER

Black Dragon Capital, LLC

**By Mohamed Abuagla,**

**Black Dragon Advisory Board – Media Technology & Ecommerce**

## About Black Dragon Capital

Black Dragon Capital, LLC ("BDC") is a minority founder led private equity firm making control investments in technology companies. BDC was formed by technology operating executives with a track record of building market leading companies and providing above market investment returns.

Learn more at https://blackdragoncap.com/

# About the author:

### Mohamed Abuagla

Mohamed Abuagla has more than 25 years of experience in business transformation and technology at established enterprises, government organizations, startups, and business ventures in the education, finance, healthcare, telecom, defense, and media industries. He has been recognized with numerous executive awards for his role in the digital transformation of the media industry in the Middle East and North Africa. At Black Dragon, he advises on media and technology investments and is involved in operational improvements within the media portfolio. Abuagla is an executive board member of the International Broadcast Convention Council, an advisory board member of the Grass Valley Customer Council, and an executive member of the SAP Advisory Council for Media. Previously, he served as the Chief Information Officer and Chief Technology Officer of Al Jazeera Media Network. Abuagla earned a degree in systems engineering from George Mason University.



©2020 Black Dragon Capital, LLC

# CONTENTS





©2020 Black Dragon Capital, LLC

# Summary

**The internet,** the global network we all rely on, has grown exponentially over the last few years, and our dependence on connectivity to it has grown accordingly.

**Virtually** all economic activity touches the Internet in some way, digital security becomes an ever more important function in the growth of an organization. As technology capabilities and choices evolve, so does the breadth of risk. Commercial survival mandates continuous focus on cybersecurity risk management and improved security defense mechanisms.

**Threats increase daily, yet the ones that dominate the headlines are only a select few. This white paper focuses on security implications to the media, e-commerce, and financial technology (fintech) sectors.**



©2020 Black Dragon Capital, LLC

# Global Cybersecurity Challenges

Nearly all organizations, regardless of how they conduct business are affected by growing cybersecurity threats. Media, e-commerce, and fintech organizations are the recipients of significant and costly security targeting that requires special attention in order to operate normally without service disruption.

## Cybersecurity Challenges in Media

Cyber criminals conduct cyber-attacks that continuously grow in size and severity on global media companies. Among the largest concerns for media companies are theft of sensitive information and intellectual property with consequences ranging from damaged reputations to the complete undermining of existing business models.

For years, media companies' defense against cyber threats was to stay off the grid. However, as more cloud and IP-based technologies are adopted, companies must be more vigilant against cybersecurity threats due to the interconnected nature of these new workflows. Media companies can no longer operate in silos or as disconnected technology islands. New strategies are needed to handle such new threats.

Attacks, whether sustained or ad hoc, can be triggered by news coverage and content disliked by the attackers. Such attacks may originate from state sponsors, activists, or political groups.

Operational disruption is the goal of most attacks. The attacker wants to prevent the media organization from fulfilling its service to society. Such attacks are not necessarily limited to content piracy or information theft and can have far greater and lasting economic effect on the targeted company.



©2020 Black Dragon Capital, LLC

## Cybersecurity Challenges in Fintech

Fintech is of paramount importance to the global banking and financial services industry. Ingenious and disruptive technologies provide financial services to people who never before had access to banking. It has also removed friction from the investment and loan processing sectors. Enterprises using fintech must address the cyber risks inherent in these solutions.

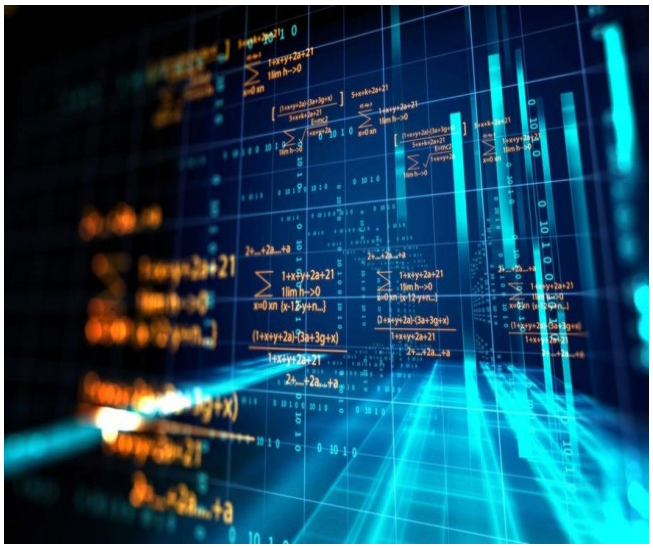
Fintech has led the digitization revolution with ATMs, Internet banking, and direct payments. Widespread adoption of mobile tools for core processing, loan origination and digital payments exposes new and profound vulnerabilities. Often regulators and law enforcement are slow to mitigate threats, failing to match the agility of cyber criminals.

Cloud-based fintech is so commonly targeted because it transfers monetary value directly. A fintech transaction deals with the world's most valuable asset - money! The vast amounts of personal and corporate data come along for the ride only to be sold on the dark web.

Companies providing fintech services face cybersecurity risks at the various integration points with legacy systems. Fintech solution providers collect huge quantities of customer data, including sensitive personal information, making them prime targets for cyber-attacks. Data privacy at these integration points is among the highest concerns.

Fintech brings access to core banking activities to people who could not access them previously. Many of these new bank customers have little or no former knowledge of cybersecurity risk and, therefore, may be more vulnerable to attack. Additionally, fintech providers connect to core banking services through application programming interfaces (APIs) developed to connect the banks to their fintech platforms. These points of contact provide additional opportunities for cyber-attack.

The complexities, technical dependencies, and myriad connection points that exist between thee integrated technologies in the fintech ecosystem make it a very lucrative target for cyber attackers.



## Cybersecurity Challenges in e-Commerce

**As e-commerce has seen extraordinary growth over the last few years, cybersecurity threats have been growing at a similar pace. Attackers normally target online commerce websites with the intent of stealing consumer data to be used for nefarious purposes. E-commerce attacks provide a goldmine for attackers seeking access to consumer information. Breaches can lead to severe business disruption, reputation loss, and in some cases, to complete business loss.**



©2020 Black Dragon Capital, LLC

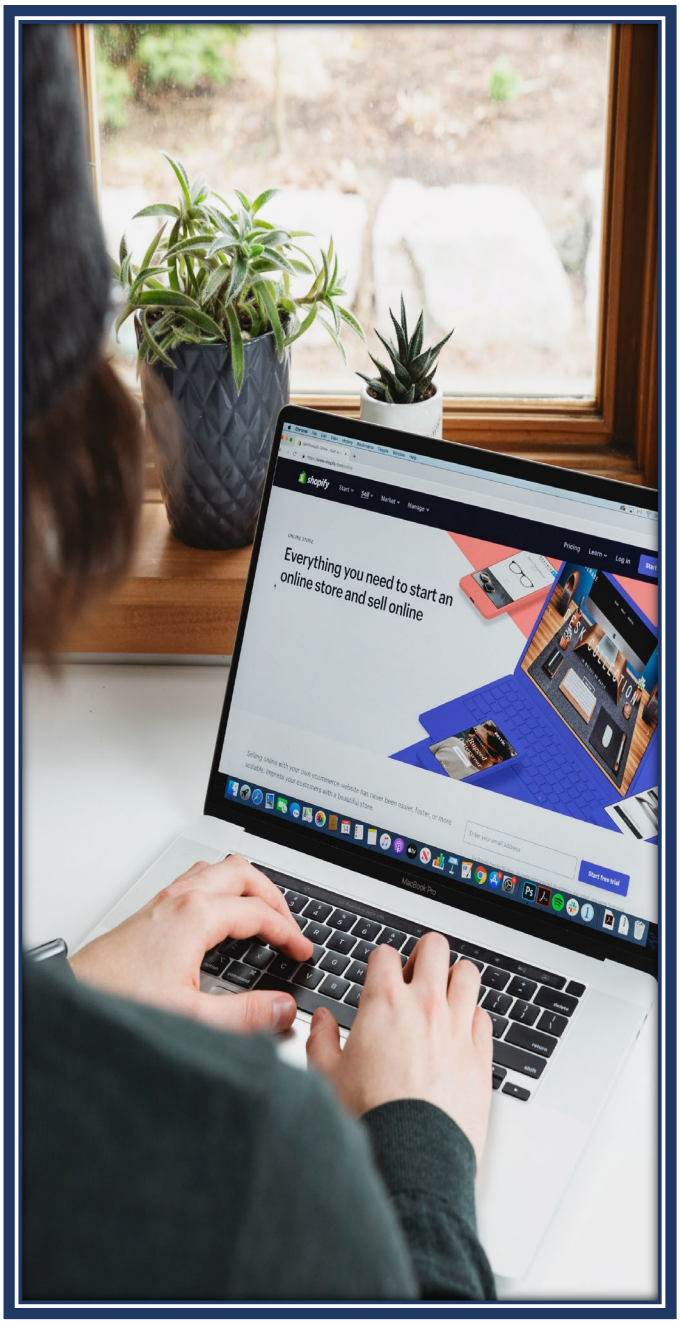
The convenience of online shopping makes it a practical necessity for millions of busy consumers. The unfortunate reality is that same convenience extends to criminals as much as it does to legitimate consumers.

Since almost all customer interaction for online retailers occurs via phone, social media, web or email, e-commerce sites are particularly vulnerable to social engineering attacks. An attacker on the other side of the globe can pose as a nearby teacher or accountant from New York.

Companies with online stores and human customer support reps must be particularly vigilant against this sort of manipulation. No amount of technology can prevent an employee from being tricked into giving up sensitive customer information such as addresses, birthdays and phone numbers, and even passwords that customers might use elsewhere. Instead, the job of any company's cybersecurity team is to provide the customer facing lines of business with procedures and safeguards to verify a customer identity before releasing confidential information. The challenge is to avoid tension between operations and customer service departments.

Further, e-commerce sites run a variety of backend shopping cart and transaction processing software. In cases where this software is developed in-house, security needs to be built into such software to reduce bugs and vulnerabilities at the coding level. Where external software, or cloud services, are used, thorough assessments and testing are required to validate the external vendors' security measures.

It is necessary to be mindful of which aspects of security can be outsourced safely and which must remain in-house.






©2020 Black Dragon Capital, LLC

# Leading Cyber Security Threats

The benefits of today's increasingly digitized and interconnected world come at a price: Cyber-attacks are a serious threat – affecting not only individuals' data, but their psychological wellbeing. Comprehensive security mechanisms and a security-oriented mindset throughout the entire organization are required to avert such risks.

New and evolving cybersecurity threats have put the information security industry on high alert. Evermore complex and sophisticated cyberattacks involving DDoS, malware, phishing, machine learning and artificial intelligence, cryptocurrency, and more place the data and assets of businesses, governments, and individuals at risk.

The following is a brief overview of leading cybersecurity threats with a direct and significant impact on the media, fintech & e-commerce sectors.

## Distributed Denial of Services (DDoS)

A Distributed Denial of Service (DDoS) attack is an attempt to crash an online system or web server by overwhelming it with data. DDoS attacks can be simple mischief, revenge, or hacktivism, and can range from a minor annoyance to long-term downtime resulting in loss of business.

DDoS attacks to all types of institutions increased significantly in recent years. Networks have been overwhelmingly flooded with terabytes of data. This type of attack can take online systems offline for several days. Beyond their damaging impact on uptime, they may also disrupt a company's transaction systems and banking services.

Unfortunately, it is easy to launch a DDoS attack. For $5 per hour someone without any technical knowledge can pay a DDoS for hire service to launch an attack. Often, the DDoS is used as a smokescreen to cover other criminal activity. The low cost and ease of DDoS make it obvious why there is such a surge in the number of DDoS attacks across all industries.



©2020 Black Dragon Capital, LLC

## DDoS attacks in Media:

With heightened political and trade tensions globally, media organizations find themselves the target of DDoS attacks. The recent attacks on Swedish media sites are an example. Though investigations failed to prove the attack was endorsed by the Russian government, it was proven to be a typical distributed attack originating from computers in Russia, among other countries. Quite likely the attack was executed through a botnet for hire service.

The BBC has also been recently hit by a DDoS attack. In fact, according to Newscycle Solution over 50% of media companies have been the victim of some sort of cyber-attack in the last two years. It's clear that media organizations are currently in the sights of attackers, activists, and nation state actors.

Traditionally vandalism and political or ideological disputes motivate attacks on media organizations. The DDoS attack on the BBC is the poster child of this -- providing a stage for attackers to flex their muscles and show everyone their strength and prowess.

More recent attacks have displayed the troubling growth of criminal extortion, data exfiltration and DDoS for Bitcoin. Media organizations report on all types of events, and often without taking a position, yet they become a target of an attack. Interestingly there is usually a correlation between political conflicts in the real world and online attacks – often called cyber-reflection.

## DDoS attacks in Fintech:

For financial institutions, a single attack is all that is required to create significant havoc and destroy the confidence of their customers. Financial losses can be significant too. A survey by Neustar indicates that more than 80% of financial services firms estimate a loss of $10,000 per hour during a DDoS-related outage.

It was also reported that 38% of DDoS attacks last more than 24 hours. For threat actors, no opportunity is too small or too big. All that's needed, is a single window of weakness and they can easily launch a DDoS attack.

Recently, attackers sent emails to Australian banks asking for large payments and threatened DDoS attacks if their demands weren't met. Their demands: Hefty ransom fees in cryptocurrency.

## DDoS attacks in E-commerce:

Nothing says "happy holidays" like a well-executed DDoS attack targeting your digital properties during the busiest shopping season of the year. Like holiday spending activity, industry DDoS attack metrics can be difficult to predict. Volumes can trend upward and then mysteriously die off. The trends are only obvious after the attack campaigns have ended.

Cybercriminals are just as keen to exploit the holiday shopping boom as anyone else, with DDoS attacks on eCommerce providers increasing by over 70 percent on Black Friday compared with other days in November. On Cyber Monday, attacks increased by 109 percent compared with the November average.

Forward-looking companies will benefit from investing in scalable, cloud-based protection solutions to counteract targeted overloads caused by DDoS attacks. Information about website and server failures spreads quickly across social platforms as well as complaints about long loading times, leading to lost revenue and long-term reputational damage.



©2020 Black Dragon Capital, LLC

## Phishing Attacks

Phishing is defined as the fraudulent use of electronic communications to deceive and take advantage of individuals within any organization. Phishing attacks attempt to deceive users to allow attackers to gain sensitive, confidential information such as usernames, passwords, credit card information, network credentials, and more. By masquerading as a legitimate individual or company via telephone, social media or electronic mail, attackers use social engineering to manipulate unaware victims into performing specific actions—like clicking on a malicious link or attachment—or willfully divulging confidential information.

### Phishing attacks in Media:

Today it seems the media is in the crosshairs as never before by people within the United States as well as those associated with its biggest global adversaries. Cleary, many state-sponsored actors spy on journalists or use cyber-attacks to try to further their agenda. According to Google, 21 of 25 top news organizations have been the target of state-sponsored attacks.

The media industry – categorized as major newspapers, radio, digital properties, and traditional television outlets – is increasingly targeted by phishing campaigns. Not only are criminals trying to break into the media websites and internal networks, but also associated accounts on social media are also under attack. The attackers fall into two general categories: groups or individuals seeking publicity or causing disruption, and state-sponsored attacks attempting to spy or steal information.

### Phishing attacks in Fintech:

It is no surprise that the fintech industry is a top target for phishing attacks to find ways to breach the organization's security of organizations. Although many security protocols are built into both internal and consumer-facing banking solutions, typically the human element is the weakest link in failing to detect the scam.

Cyber-attacks not only target traditional banking institutions' checking and savings accounts, but also credit cards such as Visa and MasterCard, as well as payment processing companies like PayPal and web payment technology providers such as Google, Amazon, Apple, Stripe, or Square. With the rise of Bitcoin and other cryptocurrencies, e-wallets are also being targeted by thieves.

### Phishing attacks in E-commerce:

Often referred to as the age of Amazon, Etsy, eBay and other industry giants, phishing took to targeting businesses' online transaction systems. Buyers and sellers have become accustomed to using the Internet as a storefront, boosted by unprecedented speed, efficiency, and convenience. These conveniences come loaded with unprecedented risk.

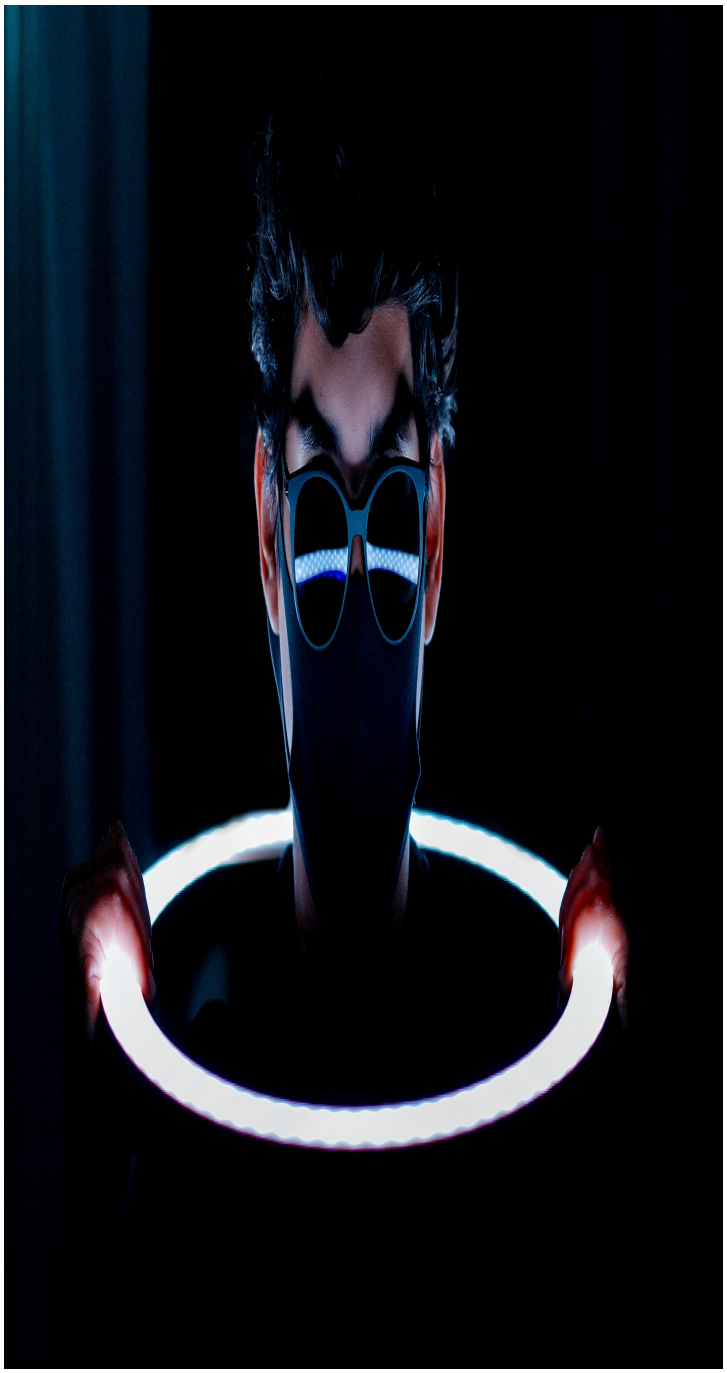
The success of such e-commerce in using the latest Internet and online credit card technologies is what makes them the crown jewels sought by phishing attackers

## Malware / Ransomware

Ransomware is a type of malware that encrypts computer files and is often deployed through links in fraudulent emails that act as a payload for successful phishing attacks. Once the malware is distributed into a network and begins locking up data on connected computers, cybercriminals demand a ransom in exchange for a decryption key to unlock access to such data.



©2020 Black Dragon Capital, LLC



Ransomware can have shocking effects on an individual or an organization with important data stored on their computer or network, including government or law enforcement agencies and healthcare systems or other critical infrastructure entities. Recovery can be a difficult process that may require the services of a reputable data recovery specialist, and some victims pay to recover their files. However, there is no guarantee that organizations will recover their files even if they pay the ransom.

Ransomware attacks have been growing in recent years against all types of government agencies and businesses, including school districts, doctors' offices, and even multinational corporations. But the COVID-19 pandemic has presented hackers with a once-in-a-generation opportunity to strike vulnerable targets as entire offices are working from home and information-technology staff are stretched thin. As an example, the Ryuk strain of ransomware was created by a Russian-organized crime ring that cybersecurity researchers have dubbed as Wizard Spider.



©2020 Black Dragon Capital, LLC

## Ransom attacks in Media:

The infamous Sony hacking revealed that the entertainment industry is a major target of cyberattacks. The leak ended up costing the company millions due to associated costs including legal fees, restoration fees, and system upgrades.

Not long ago, hackers obtained a copy of Netflix's original series Orange is the New Black and threatened to leak episodes of the new season unless ransom was paid. The company remained unresponsive, prompting the hacking group behind the threat to leak the episodes. While hackers did not compromise internal systems, such attacks have inspired cyber criminals to hold valuable assets, such an entire online series for ransom.

An interesting twist relating to media sites such as The New York Times, the BBC, MSN, and AOL is that they became victims of cyber-attacks by the injection of malicious ads into their sites that installed ransomware on the site visitors' computers. While the ransomware did not invade the computer networks of the big media sites, the ransomware attacks affected visitors through the malicious ads.

## Ransom attacks in Fintech:

Recently, the London-based fintech company, Finastra, which provides financial software to the global banking sector, disclosed suffering a ransomware attack that prompted the company to shut down its servers and lead to disruptions to its global operations. The relative success of the ransomware attack hints at overlooked weaknesses present in Finastra's security infrastructure, as well as the increasing prevalence of ransomware among attackers for targeting large enterprises.

Most attackers are motivated by financial rewards, so targeting organizations with money inevitably tops attackers' lists. The financial and business impact in fintech is significant because such trust-based businesses are vulnerable to customer loss, reputation damage and, of course, actual money loss.

## Ransom attacks in E-commerce:

The most obvious consequence of being a ransomware victim is the loss of money you are asked to pay to regain access to your system and/or data. The more money the attacker thinks you have, the more you will be asked to pay.

However, the greatest consequence for every commercial entity, e-commerce stores included, may be the downtime it suffers. A ransomware attack may put an e-commerce store out of commission for several days. In fact, the best-case scenario is a matter of days, and not weeks. Downtime can spell doom for an e-commerce business, so it's obvious how great a problem this can be.

**Regulations compel breached organizations to notify customers. Most organizations are required to report any type of compromise, though management may see it as an indication of weakness that further damages the organization.**



©2020 Black Dragon Capital, LLC


As per a recent report by Delliotte, The COVID-19 pandemic has forced organizations and individuals to embrace new practices such as social distancing and remote working. While the world is focused on the health and economic threats posed by COVID-19, cyber criminals around the world are without a doubt capitalizing on this crisis.

Cybercriminals are using the pandemic disruption for commercial gain, ensuring that they deploy a variety of ransomware and other malware. Many businesses are reporting an increase in attackers masquerading as legitimate agencies trying to trick people into sharing their account access credentials or opening malicious email attachments.

With many employees working from home and students learning virtually, enterprise Virtual Private Network (VPN) servers have now become a lifeline to companies, and their security and availability are a major focus going forward. In their haste to achieve this, there is a possibility that unpreparedness or inexperience will lead to security misconfiguration in VPNs thereby exposing sensitive information on the Internet and also exposing the devices to DDoS attacks. Additionally, some users may utilize personal computers to perform official duties which could also pose a great amount of risk to organizations.

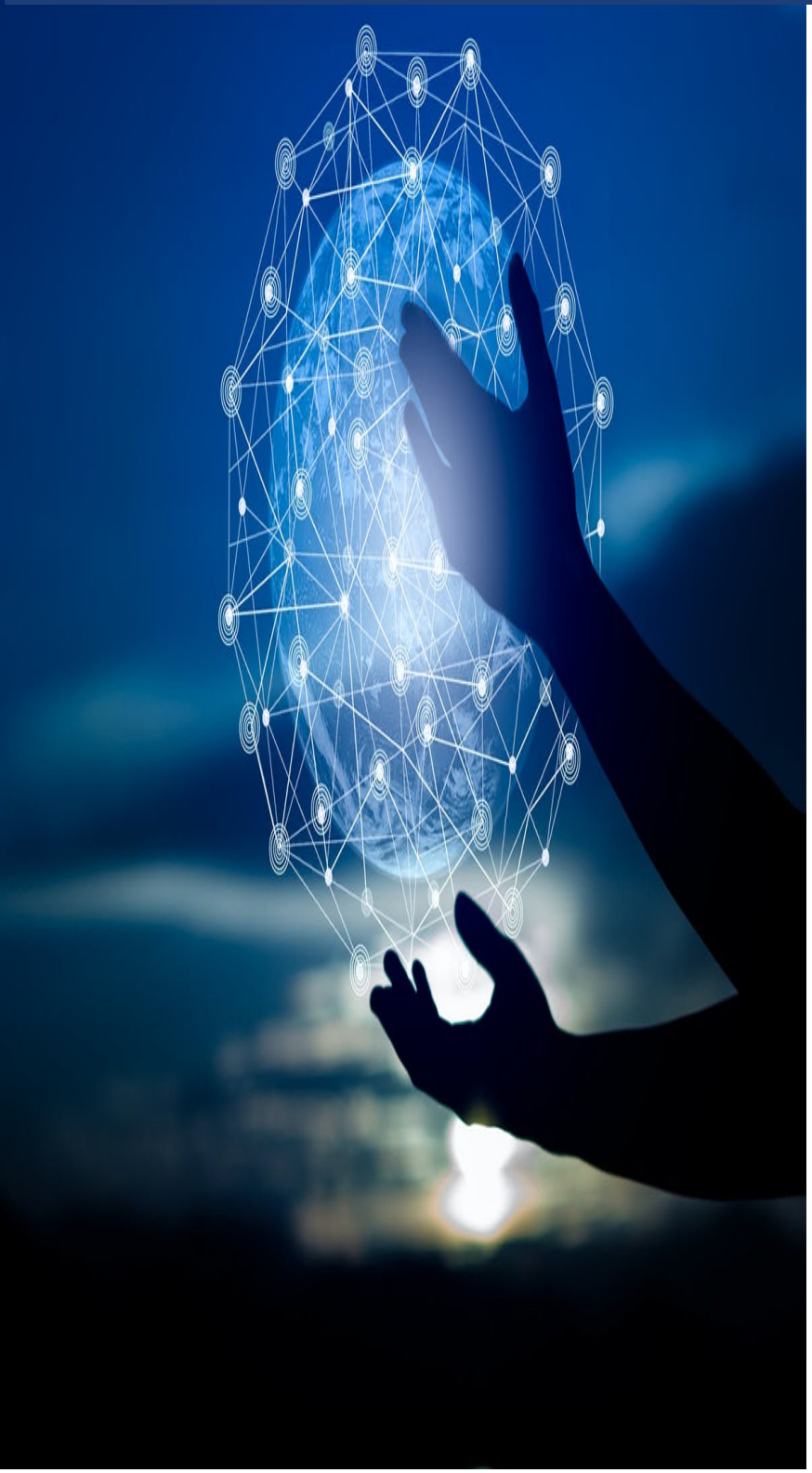
Understandably, the functioning of many security teams is being impaired due to the Covid-19 pandemic thereby making detection of malicious activities difficult and responding to these activities even more so. Keeping up with security patches on systems may also be a challenge if security teams are not fully operational.

Globally, companies are downsizing their workforce to cope with the effects of Covid-19. Some people have also lost their means of livelihood due to the various restrictions of movement by governments across the world. This move would likely encourage the growth of cyber criminals as idle people with Internet access who have lost their jobs from the effects of Covid-19 may see an opportunity to make a living out of this pandemic.



©2020 Black Dragon Capital, LLC

# Digital Transformation Acceleration



Anecdotes abound that the Covid-19-related shutdowns and slowdowns in business and consumer activity, along with closures of physical workplaces have given many companies a jolt they desperately needed to fast track their digital transformation. For the most part, digital transformation has been spurred by competition from digital disruptors. Covid-19 may just be the mega-event that pushes every business to seriously implement digital transformation plans.



©2020 Black Dragon Capital, LLC

# CONCLUSION

The continuous evolution of consumer facing technologies demands new strategies to deal with evolving cybersecurity threats. Companies should not be looking at cybersecurity as a secondary function to what they do, but as a critical component to our safety and well-being.

Many organizations have spent huge sums to acquire the latest cybersecurity solutions to shore up their defenses to protect themselves from cyber-criminal activity. Managing insider threats and investing in a team of cyber professionals are the two areas that often do not get enough focus but are the most critical actions for organizations to confront cybersecurity risks.



©2020 Black Dragon Capital, LLC