FEBRUARY 2021

WHITE PAPER

THE STATE OF CYBERSECURITY FOR LAW, ACCOUNTING, AND FINANCIAL SERVICES

CONTENT

INTRODUCTION

Since its inception, the internet has proven to be a rich resource for cybercriminals to carry out their nefarious pursuits. Though financial gain continues to be the primary motivator for their exploits, personal consumer information is the invaluable currency used for monetary pursuits.

With more than 1 billion active websites online and 22 billion devices connected on the internet of things (IoT), the sheer size of the world's digital attack surface continues to present such opportunities. From personal cell phones and tablets to laptops and video conferencing platforms, between improperly secured devices and old-fashioned human error, it is not surprising that cyberattacks are on the rise.

Beyond the fold of the internet most people use daily, the access and exploitation of both personal consumer information and business information is an enormous driver of activity on the dark web. As a result, cybercrime-as-a-service has exploded into its own economy, and almost every professional services industry—including law, accounting, and finance—is vulnerable to detrimental cyberattacks.

Attacks against any company within these industries are problematic enough due to the potential exposure and exploitation of client data and reputation damage for the company itself. But uniquely, these industries also face stringent compliance standards such as the Payment Card Industry Data Security Standard (PCI DSS). Ensuring comprehensive security and continuous compliance within the cloud becomes even more important as part of a proactive cloud defense strategy.

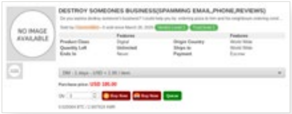
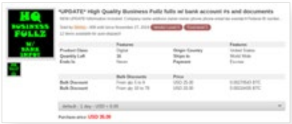
NEW CYBERSECURITY TRENDS

CYBERCRIME-AS-A-SERVICE

In 2018, Information Age[i] reported that the cybercrime industry had an estimated worth of $1.5 trillion. Just two years later, Cybersecurity Ventures estimates cybercrime costs will reach $10.5 trillion annually by 2025.[ii]

While "cybercrime" is a broad term that covers intrusions such as malware, ransomware, and the like, the growth of a new cybercrime category that deviates from these more "traditional" and well-known acts has made it possible for almost anyone to exploit a business by simply hiring an expert to carry out their illegal acts. This "pay-to-play" method, known as cybercrime-as-a-service, is a prevalent cause for the acceleration of cyberattacks.

Conducted by members of Armor's Threat Resistance Unit (TRU) team, the "Armor 2020 Dark Market Report: The New Economy"[iii] identified several new cybercrime-as-a-service offerings.

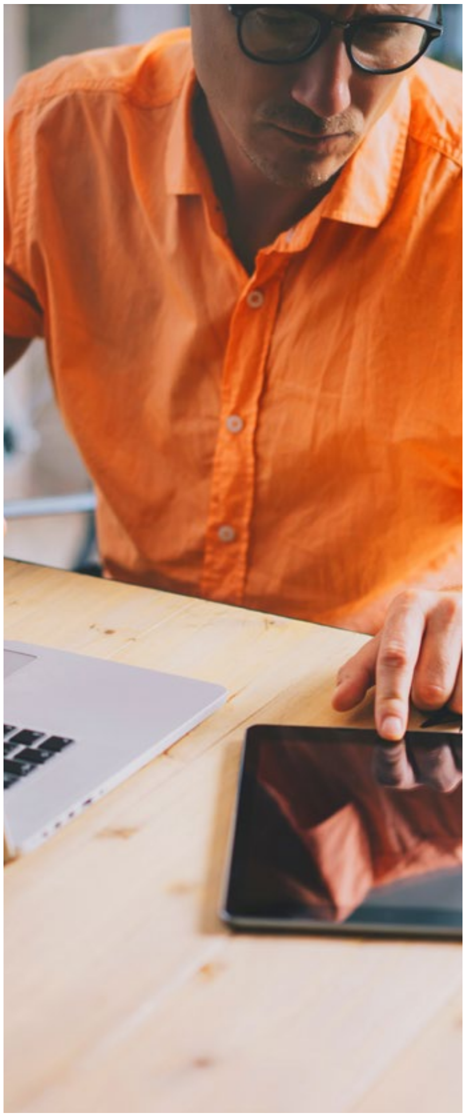
NOTABLE OFFERINGS	
 DESTROY SOMEONES BUSINESS(SPAMMING EMAIL,PHONE,REVIEWS) NO IMAGE AVAILABLE Features Product Class Digital Quantity Left Unlimited Ends In Never Features Origin Country World Wide Ships to World Wide Payment Escrow	One of the most alarming finds was a vendor advertising to "destroy an individual's business" by releasing a slew of spam emails and phone calls to overwhelm communication systems. The vendor advertised that they could also ship unwanted items to the place of business, tying up employee time.
	Dark web vendors offering telephony denial of service (TDoS) attacks remain popular as well. These attacks launch a flood of automated calls to a business—upwards of thousands per day—until a ransom is paid. Attacks of this nature have grown in popularity with financial cybercriminals, who empty a victim's bank account and block notifications from a victim's financial institution alerting them to the fraud.
 *UPDATE* High Quality Business Fullz fullz w/ bank account #s and documents HQ BUSINESS FULLZ W/ BANK INFO Features Product Class Digital Quantity Left Ends In Never Features Origin Country United States Ships to World Wide Payment Escrow Purchase price: USD 35.00	"Business fullz" contain pertinent information that allow criminals to masquerade as if they were an officer of a real business. The information—available for as little as $35—is especially concerning in the wrong hands, as many small businesses have applied for business loans due to the COVID-19 crisis. While financial gain would be the obvious benefit, a greater concern is that these criminals could open accounts and launder money through these stolen identities.

Entering a firm's server, whether by using remote desktop protocol credentials through a brute-force attack or purchasing credentials on the dark web, hackers can access sensitive intellectual property, banking information, client files, intimate emails, key case evidence, and other private information. Once the files are accessed, hackers can easily lock them down and demand payment in exchange for the privileged data or to prevent the deletion of such files. Even with payment, there is no guarantee that law, accounting, or financial firms will get their data back.

AN INCREASING MOBILE WORKFORCE

The ways in which leaders within the law, accounting, and financial firm services integrate digital technology into business operations continue to evolve, reflected in updated processes, altered business models, and enhanced cultures. One of the greatest of these cultural shifts seen in modern work time is the transition from desk-tethered employees to a mobile workforce, empowered to carry out their "9-to-5" duties at almost any time and from almost anywhere through the power of digital transformation. ComputerWorld estimates that just the U.S. mobile workforce alone will increase from 78.5 million to 93.5 million by 2024.[iv] But as the mobile workforce—comprised of fallible humans prone to making errors—continues its growth, so does the cyber risk associated with it.

Clearly, an increase of this nature puts a strain on resources, most notably cloud security, as workers are expected to perform job duties as if they were in the office. In response, technology leaders have granted access to collaborative software, issued company-owned devices, and allowed teams to connect via messaging apps. Though essential for productivity and morale, the security challenges these advancements pose continually challenge C-suite leaders and IT personnel, from training and onboarding to protecting enterprise mobility tools and overcoming scalability obstacles.



While being part of the mobile workforce may not be entirely new for "white collar" employees within law, accounting, and financial service environments, the rise of cybercrime within these fields changes the experience. Attacks are becoming more targeted and focused on infiltration through the services, apps, and work tools professionals use—and now take home with them, outside of a company's in-office network.

Bad actors and malware can only disrupt networks when they are invited in, and humans unintentionally are often the ones extending the invites. Attack surfaces are exponentially expanded with the mobile workforce, and even the most observant employee can fall victim to tried-and-true methods hackers use to gain access to their networks.

Law firms and attorneys, for example, are extremely susceptible to infiltration, especially if there are events cybercriminals can use to their advantage. For example, the ABA Journal recently reported on an increase in scams during the COVID-19 crisis.[v] In a March article, one attorney cited a scam where individuals are falsely hiring attorneys to file a lawsuit, only to trick the attorney into paying them their percentage up front with no payment ever coming from the defendant of the lawsuit. The client is, in fact, in cahoots with the other side.

As safekeepers of privileged financial information that hackers aspire to gain, accounting firms must constantly remain vigilant of their cybersecurity efforts as well.

Corporate phishing scams are a huge culprit, and it only takes one employee to inadvertently wreak security havoc. Tracked by the FBI in what it calls Business Email Compromise (BEC), it is estimated that $3.5 billion was lost by corporations[vi] due to traditional phishing scams in just 2019 alone.

Phishing attacks are simple to design, and one of the easiest ways for cybercriminals to infiltrate an accounting firm's network is "spoofing." This method of mimicking a legitimate email address to request funds or convince the recipient to share network login information or release financial information has been perpetrated against several accounting industry players, including Intuit. Though the two-part attack was deemed unsuccessful, the fact that part of the phishing effort was directed to the company's CEO speaks volumes on the bold attack and nature of the perpetrators.[vii]

Ransomware is another area where the spotlight shines on human error in the corporate arena. Ransomware signatures include "locking up" critical and essential software and threating public release of private company or client information until a usually astronomical fee is paid. It has steadily increased over the years; just in 2019, it is estimated to have cost the U.S. more than $7.5 billion.[viii]

THE STATE OF LAW FIRMS

Digital transformation has greatly helped law firms improve their services or offer those that are more efficient, productive, and accurate. However, due to the sensitive nature of their client data, law firms are especially susceptible to ransomware attacks.

In 2019, ransomware demands topped $12 million,[ix], and the average cost of a ransomware attack on businesses was $133,000.[x] This cost is on the rise, according to Cybercrime Magazine[xi], which estimates that the global costs will reach $20 billion by 2021—an increase from their estimates of $11.5 billion in 2019 and $8 billion in 2018.

According to an American Bar Association 2019 Survey, 26 percent of its respondents overall reported that their law firms had experienced a security breach. An additional 19 percent of respondents reported they do not know whether their firm had ever experienced a security breach.[xii]

Such breaches are especially worrisome, considering attorneys' fundamental ethical responsibilities include "duties of competency, communication, and confidentiality" as the ABA Model Rules of Professional Conduct outlines.

Not to mention, the ABA Formal Opinion 477[xiii] provides that, "[A] lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information..." As threats increased, the ABA introduced Formal Opinion 483[xiv] on Oct. 17, 2018, to specifically address cybersecurity: "Lawyers' Obligations After an Electronic Data Breach or Cyberattack."

The largest ransomware attack on a law firm in the past two years was the May 2020 attack by the REvil gang, also known as Sodin and Sodinokibi, when it hacked the servers of Grubman Shire Meiselas & Sacks (GSMS) and seized more than 750 GB worth of the celebrity firm's client information. The group asked a record $42 million ransom payment for documents it had already gained access to, allegedly including private information on Lady Gaga, Madonna, Nicki Minaj, Bruce Springsteen, Mary J. Blige, Christina Aguilera, and others.[xv]

The hackers had increased their demand from an initial $21 million when the firm failed to respond. The group then threatened to publicly release more data if they were not paid soon and kicked off an auction site with items being sold for $1.5 million for each client. While GSMS refused to pay the ransom so far and recovered some lost data, many of the files are still available to purchase online.

While the GSMS attack made international headlines, it is hardly the only law firm to have fallen victim to a cyberattack, forcing firms to re-evaluate their security stance and ensure cloud security.

NOTABLE LAW FIRM BREACHES

UNITED STATES COURTS	In 2019, at least 250,000 legal documents, some marked "not designated for publication," were left exposed on the public internet without a password for at least two weeks, allowing anyone to access and download sensitive legal materials.[xvi]
	Georgia's Administrative Office of the Courts (AOC) confirmed that its IT team discovered ransomware on the organization's servers. Though no specific ransomware details were provided, the characteristics of the June 2019 incident were consistent with the Ryuk ransomware that had infiltrated multiple companies and government agencies over several months—including at least three Florida cities.
UNITED STATES VETERAN	The hacker group Maze gained access to sensitive data from at least five law firms within two months. Two of those targeted were Texas-based law firm Baker Wotring in November 2019 and Woods and Woods LLC in Indiana in February 2020. Baker Wotring was labeled on Maze's website as a "full dump,"[xvii] while Woods and Woods' files were stolen, including those associated with veterans' personal injury cases for the U.S. Department of Veterans Affairs.
G	According to Law.com, Fragomen, Del Rey, Bernsen & Loewy, an immigration boutique and Am Law 100 firm, experienced a data breach in September 2020, affecting a limited number of people specifically from its client Google.[xvii]

Hundreds of other law firms and court systems have been indirectly affected by hacking of their managed service providers (MSP) such as TrialWorks (October 2019) and Epiq Global (March 2020), according to Law.com. The resulting damage includes lost access to critical trial data, trial postponements, and requests for delays in various court proceedings—all of which can lead to catastrophic results in cases.

As for their response to attacks or data breaches, the ABA 2019 Survey indicates that attorneys are improving in developing incident response plans. In 2018, just 25 percent of overall respondents reported having an incident response plan. For 2020, that number improved to 31 percent.

While progress has been made in some areas of legal security, law firms have further to go in designing and implementing appropriate solutions. Recognizing issues, looking at options, and taking the necessary steps for implementation will determine how firms can improve moving forward.

THE STATE OF ACCOUNTING

Cloud computing has been called "the future" of the accounting and tax services industry for many of the reasons it has revolutionized others. Firms are able to scale their server resources up and down as needed, have real-time access to applications and software, and even gain a competitive edge when clients are reassured that a firm's enhanced cloud framework will protect their data. And it seems firms are embracing the future; 67 percent[xix] of accounting professionals prefer cloud accounting, and 58 percent of large companies[xx] utilize cloud accounting in their operations.

Since the accounting industry has grown to embrace digital transformation to improve productivity and take advantage of the latest software developments, it has long been in hackers' crosshairs with no sign of slowing. Account numbers, social security numbers, tax information—it is a virtual buffet of sensitive information that proves too irresistible for hackers.

NOTABLE BREACHES IN THE ACCOUNTING & TAX SERVICES INDUSTRY

Wolters Kluwer	In 2019, accounting software leader Wolters Kluwer experienced a malware attack, rumored to be ransomware specifically. The Netherlands-based company was unable to access software, and its support website was unreachable.
squarmilner	In March 2020, Square Milner, one of the largest accounting firms in the U.S., experienced a large-scale data breach. It is unknown how many clients were affected, but the exposed data potentially included names, social security numbers, and tax ID numbers.
MNP	In April 2020, Canadian accounting firm MNP LLP was hit with a cyberattack. Later found to be a ransomware attack, the company took the extreme measure of ordering a company-wide computer system shutdown to protect its devices from becoming compromised by malware.

When thinking of accounting firms, the "Big Four"—Deloitte, PricewaterhouseCoopers (PwC), Ernst & Young (EY), and Klynveld Peat Marwick Goerdeler (KPMG)—are often mentioned. Though they have combined revenue that easily totals into the billions annually, there were actually 1.28 million accountants and auditors in the U.S. as of 2019.[xxi] With any number of them working as individual consultants, the risk of malware or ransomware attacks does not decrease. Instead, the risk stands to increase for small business owners, who may not be comfortable entrusting their IT infrastructure to a cloud provider or have the financial means for in-house security teams.

In its "COVID-19's Impact on Cybersecurity"[xxii] article, Deloitte noted spikes in phishing attacks and ransomware attacks. In addition to the weaknesses that remote employees can inadvertently cause, Deloitte's report ventures even further, hinting that terminated employees whose livelihoods have been impacted could begin to explore cybercrime as a potential income source.

Regardless of status—whether individual proprietor or billion-dollar entity—developing and implementing a cybersecurity plan is a must for those in the accounting field. With considerations to the industry's compliance requirements and the need to mitigate risk, leaders should remain steadfast as they protect their data and explore the services needed to do so.

THE STATE OF FINANCIAL SERVICES

More than any other industry, the financial sector holds all that is dear and true to cybercriminals: money.

With digital transformation in full force among financial institutions, they are now more vulnerable than ever before to being exploited by attackers. Yet, to compete in the marketplace, banks, credit unions, and brokerage firms must do all they can digitally to enhance the customer experience. With an estimated 7 billion mobile users worldwide by 2021 and the total value of payments made using mobile devices topping out at $503 billion this year[xxiii], the focus on customer experience is on target.

A 2018 retail banking satisfaction study[xxiv] found that companies providing their customers with a higher-quality service experience than their competitors end up acquiring customers at a faster rate, retaining a larger portion of those customers, and commanding a higher price for their services and products. Digital services have steadily increased within the financial industry, while the need for human-centered interaction is decreasing. Digital payments, blockchain technology, and robotic process automation (RPA) are some of the technological advances that assess credit quality, automate client interaction, and optimize the execution of stock trades.

While digital transformation benefits customers and financial institutions, if not managed correctly it carries several high-stake security risks. Cumulatively, billions of customers have been impacted by attacks on financial institutions—not only regarding lost funds, but also having their personal information compromised. And losses for those in the financial industry have grown to $100 billion, per an International Monetary Fund survey.[xxv]

NOTABLE BREACHES IN THE FINANCIAL SECTOR

Capital One	The 2019 Capital One breach made international headlines after a former Amazon Web Services (AWS) employee hacked the system, compromising personal data of approximately 100 million U.S. customers. Found at fault, Capital One paid $80 million in settlements.
First American	In 2019, First American Financial Corp. suffered a breach that compromised nearly 885 files related to mortgage deeds. The information included bank account numbers, transaction receipts, and tax records.
FINASTRA	Finastra, a global core banking provider, experienced a ransomware attack in March 2020. Though the bank did not give in to the ransomware demand, it did have to take a server offline, disrupting customer service and access.

Financial companies must change with the times, yet they must defend their environments from the multitude of different types of attacks that stem from vulnerabilities arising from the newest services. Even without the impact of a global pandemic, Gartner had predicted that in 2020, 60 percent of digital businesses would suffer major service failures due to the inability of IT security teams to manage digital risk.[xxvi]

While headlines abound about larger corporations that fall victim to cyberattacks, smaller financial institutions are not immune from efforts to breach their networks. Whether it is a belief that they are too small to be a target or there is too much attention paid to large-scale “one-time” attacks versus an ongoing threat such as ransomware, smaller institutions should take heed and understand the risks that can befall them as well.

FINDING THE RIGHT SOLUTION

VENDOR CHOICES

As the threat landscape grows more complex and compliance regulations shift and become more stringent, law firms, accounting firms, and financial institutions should seek out a security-as-a-service (SECaaS) platform with a simplified approach that addresses compliance controls and lessens security burdens. Adopting audit-ready compliance tools that work within the frameworks of industry compliance standards (HIPAA, HITRUST, GDPR, PCI DSS, etc.) can ensure a company’s specific needs are being met for security and that they meet regulatory mandates.

Agility is one of the greatest benefits of utilizing a SECaaS firm. Cloud services allow companies to quickly implement new services, scale services to fit needs, and provide innovative technology. Cloud data center traffic will represent 95 percent of total data center traffic by 2021, compared to 88 percent in 2016, according to research from Cisco.[xxvii] However, as data moves to the cloud, so does the attention of attackers—proving just how invaluable a shared responsibility between companies and their cloud service providers will be. While the security of the underlying infrastructure lies with the public and private cloud providers, companies are responsible for the security of the data itself and any access granted within their systems.

Managed security services remain a viable alternative for law, accounting, and financial service firms either unable to afford or unable to find the in-house expertise needed to protect their applications and data. From underneath the managed security umbrella, SECaaS has emerged with a combination of best-of-breed technologies that leverage the capabilities of the cloud to deliver agility, threat detection and response, remediation, and agility to companies of all sizes.

While there are some similarities between the offerings of traditional MSSPs and MDR vendors, each is missing pieces of the puzzle, and customers are forced to either purchase both types of services or lose out on the capabilities offered by one in favor of the other. The gap between the needs of companies and what many MSSPs are delivering has led to customer turnover and forced many to consider a new approach. For businesses perturbed by the rising cost and complexity of securing an increasingly interconnected, distributed environment in-house, a SECaaS vendor that provides an integrated bundle of services is an effective option. Instead of buying additional security technologies, organizations adopting a SECaaS solution can augment their security efforts and bolster their defenses, optimizing their business outcomes.

For companies bound by compliance requirements, the shift to the cloud and protecting data in their cloud environment—whether public, private, or hybrid—is becoming the norm, and working with a SECaaS partner that can help secure a cloud environment is crucial.

FEATURES	TRADITIONAL MSSP	SECaaS
Ease of implementation (DevOps ready)	Average 45 days	<2 min
Prevention, detection, and response	Alerting only	99.999% threats blocked; response included
Average time to detect and eliminate threats	99 days	1 day
Visibility & threat management across environments (public, private, or hybrid cloud & on-premise)	On-premise ONLY	✓
Audit-ready compliance (HIPAA, PCI, & GDPR)	No	✓
Subscription-and/or consumption-based pricing	Fixed contract	✓
Patching	Client-owned	✓
Vendors	SCWX, IBM, etc.	Armor

EMPLOYEE EDUCATION

Through access management, employees are often the gatekeepers of sensitive data and can be a company's first line of defense against cyberattacks. Because so many breaches can be attributed to human error, compliance and IT leaders should implement a plan focused on educating team members on the role they play in protecting this data.

This education should be communicated across the entire company and, if possible, customized for each department or employee classification. Employees who take work home with them, for example, would need to understand the importance of using VPN to secure data; an intern who is not required or permitted to work from home would not need this, but may need education on how to identify a phishing email.

To convey the seriousness of the role employees play in protecting data, education should also be ongoing, formal, and include real-life examples of breaches. It should also incorporate compliance training—not only to understand the significance of protecting client information, but also to convey how adhering to compliance requirements relates to company reputation, policies, and governing body requirements.

Communicate expectations and employee impact.

Establish proper access management protocols.

Conduct ongoing trainings and encourage reporting.

CONCLUSION

Cyberattackers can be relentless—but they are not always successful. Attacks can be thwarted, and the adoption of new mindsets regarding cybersecurity and compliance for law, accounting, and legal professions can be the first step to protecting data, empowering employee ownership in the fight against cybercriminals, and realizing the importance of compliance. With the addition of a SECaaS platform that provides not only top-notch security and audit-ready compliance but also experience, expertise, and innovation, these industries will be well defended and ready to confidently pursue whatever opportunities await them.

ABOUT ARMOR

Armor is a global cybersecurity software company that simplifies protecting your data and applications in a private, public, or hybrid cloud—or in an on-premises IT environment. Armor Anywhere provides technology to detect and respond to threats and can be activated in minutes. We also assist organizations to achieve compliance with major regulatory frameworks and controls. Armor's cybersecurity experts monitor customer environments 24/7/365 and, if an attack takes place, help customers respond quickly and effectively. Wherever you are on your cloud journey, Armor makes cybersecurity simple.

SOURCES

i. "Global cybercrime economy generates over $1.5 TN, according to new study" – April 24, 2018

ii. "Cybercrime to Cost the World $10.5 Trillion Annually By 2025" – November 13, 2020

iii. "The Dark Market Report: The New Economy" – September 28, 2020

iv. "Mobile Workforce to Reach 93.5M In U.S. by '24" – September 8, 2020

v. "How scams multiply during the COVID-19 crisis and why lawyers are not immune," ABA Journal – March 31, 2020

vi. "2019 Internet Crime Report Released" – February 11, 2020

vii. "Phishing attacks impersonate QuickBooks invoices ahead of July 15 tax deadline"- TechRepublic – June 22, 2020

viii. "Ransomware May Have Cost the US More Than $7.5 Billion in 2019" – MIT Technology Review

ix. "Ransomware: To Pay or Not to Pay Is Not the Question," Law.com – October 19, 2020

x. The State of Ransomware 2020, white paper, Sophos – May 2020

xi. "Global Ransomware Damage Costs Predicted to Reach $20 Billion (USD) By 2021"" Cybercrime Magazine – October 21, 2019

xii. "Technology Basics & Security," Legal Technology Survey Report, The American Bar Association's Legal Technology Resource Center – October 16, 2019

xiii. "American Bar Association Standing Committee on Ethics and Professional Responsibility – Securing Communication of Protected Client Information." – May 22, 2017

xiv. "American Bar Association Standing Committee on Ethics and Professional Responsibility – Lawyers' Obligations After an Electronic Data Breach or Cyberattack." – October 17, 2018

xv. 2020 Dark Market Report, Armor – September 28, 2020

xvi. "Database leaks 250K legal documents, some marked 'not designated for publication,'" Zdnet.com – March 15, 2019

xvii. Hacking group publishes 'full dump' of law firm's data; another responds to cybersecurity incident," ABA Journal – February 12, 2020

xviii. "Fragomen Reports Data Breach Impacting Some Google Employees," Law.com – October 27, 2020

xix. "6 Ways to Make Managing Financial Data Easier for Your Business." - Sage Advice – March 19, 2020

xx. "96 Essential Online Accounting Statistics: 2020/2021 Data and Market Share Analysis." – Finances Online

xxi. "Number of Accountants and Auditors Employed in the United States from 2012 to 2019." - Statista

xxii. "Covid-19's Impact on Cybersecurity." - Deloitte

xxiii. "Mobile Banking Statistics: The Future of Money Is in the Palm of Your Hand." – Data Prot – February 6, 2020

xxiv. "Retail Bank Customer Satisfaction Strained by Growth of Digital-Only Segment, J.D. Power Finds." J.D. Power – April 26, 2018

xxv. "Cyber Attacks Incur $100 Billion Losses to Financial Institutions." – Cybersecurity Insiders

xxvi. "Gartner Says by 2020, 60 Percent of Digital Businesses Will Suffer Major Service Failures Due to The Inability of IT Security Teams to Manage Digital Risk." – Gartner – June 6, 2016

xxvii. "95% of Global Data Center Traffic Will Be from the Cloud by 2021." – TechRepublic – February 5, 2018

ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167