Harbinger Research
Independent Investment Analysis

Research Report

Information Technology
Cybersecurity Advisory and System Management; Value-Added Distribution

October 22, 2018

Brian Connell, CFA
Senior Research Analyst
bconnell@harbingerresearch.com

Cyber Security 1 AB (CYBNY – OTCQX, BoNY ADR)

Buy and Build, Cross-sell and Upsell Make for a Winning Strategy, Allowing CYBNY to Rapidly and Inexpensively Penetrate High-Growth Markets in Africa, the Middle East, and Europe. Opportunity Resulting from Divergent Results and Share Price.

Strong Buy

Balance Sheet Data

Recent Price (ADR):	**$3.64**
Recent Price (Nasdaq First North):	**€0.26** ($.321)
Market Capitalization (mln)*	$96.5
Enterprise Value (mln)*	$99.1
Institutional Ownership	unknown
Insider Ownership	Approx. 42%
Fully Dil. Shares Outstanding (000s)*	262,292
Average Daily Trading Vol (30 day)	862 (ADRs)
Exchange, U.S. (ADRs)	U.S. OTCQX
Exchange, Sweden	Nasdaq First North

***Each U.S. ADR represents a deposit of 10 shares of Cyber 1**, which trades natively on the Nasdaq First North market in Sweden.

Balance Sheet Data

Shareholders' Equity (mln)	5644
Price/Book Value	**12.9x**
Cash (000s)	**437**
Net Working Capital (000s)	**(1,444)**
Long-Term Debt (000s)	**0**
Total Debt to Equity Capital	**1.89**

Company Overview

Cyber Security 1 AB, formerly known as Cognosec AB, is a multinational Value-Added Distributor of software and hardware used in the cybersecurity industry. It's core strategy is to seek out and negotiate the purchase of "not-for-sale" profitable businesses in the VAD or cybersecurity business and acquire them at accretive valuations. Cyber 1 then leverages the acquired company's customer base to sell more hardware and software, or upsell Advisory Services that typically have gross margins that are 2x-3x those typical of VADs. The Company trades on Sweden's Nasdaq First North market as CYB1 and via and ADR that equals 10 shares, as CYBNY.

Company Contact Information

Kobus Paulsen
Non-Executive Chairman

Daniel Holden
Chief Financial Officer

Matthew Glover
VP of Investor Relations
Cyber1@liolios.com,
(949) 324-3860

Cyber Security 1 AB
40 Bank Office
Canary Wharf, London, UK E14 5AB
www.cyber1.com;
+44 (0) 203 903 1071
info@cyber1.com

Summary and Investment Opportunity

- **Cyber Security 1 is an Established Multi-National Vendor with an Innovative Business Model.**

Formerly known as Cognosec AB, the Company's philosophy is focused on squarely on the customer and on providing that customer with the best solution possible. CYBNY usually does this by integrating several best-in-class technologies in the creation of a single solution. We applaud this approach because 1) it allows the Company to consistently put the customers' interests first, with no conflicts of interest. 2) Because the Company doesn't make its own technology, it doesn't suffer from high product development costs nor rapid technological obsolescence. And when a product fails to perform, the Company can simply change the product while keeping the customer. 3) It almost entirely insulates the Company from liability due to breach-related lawsuits. Although this issue hasn't been a huge one in this industry historically speaking, we believe that the passage of GDPR, given its structure and its long-toothed enforcement ability may be a Harbinger of things to come, and a future in which we'll find cybertech vendors to be much more liable if something goes amiss. In any event, Cyber Security 1 has shown to our satisfaction that it can successfully earn a solid margin on value-added distribution and a very nice margin on its Advisory and especially its Managed Service Offerings, all while forgoing product development costs and product risk, and while keeping its customers loyal and happy. If the Company succeeds at executing on its hybrid "Buy and Build" and "Cross-sell and Upsell" strategy, then it should experience even more success in the future than it has to date.

- **We Feel the Company's "Buy and build" Strategy Dovetails Perfectly with Cybersecurity Today.**

The industry today is in our opinion in a period of adolescence that may last longer than is typical in the high-tech world, due to its long-term growth picture and the ever-dynamic influx of new threats and defenses against them. In this type of industry, we see many small to medium sized enterprises that have a well-developed, defensible core expertise and business, and yet have not grown large enough to attract the attention of the larger financial buyers, namely private equity funds. The Company has a solid track record of being about to identify, vet, and successfully negotiate a purchase of several of these companies over the last 12 months, and it has done so with without overpaying for its acquisitions and by using stock and cash in a four-to-one ratio – only – as its acquisition currency. We believe the Company will likely continue its track record of success in this regard, and if that proves correct it will over the next two to three years have expanded its business far more quickly than its 15%ish organic growth rate would have allowed, all done in a manner that is accretive (rather than dilutive) to its earnings per share.

- **Great Strategy + Execution + Financial Discipline = Probable Strong Equity Appreciation**

Cyber Security 1 is in our view extremely well-positioned to maximize the benefit it should derive from the likely long-term secular growth we are currently seeing in cybersecurity, an industry which should remain strong for the foreseeable future. The Company is so well positioned, we believe, because of how its business model fits the governing dynamics of the cybersecurity space, and because of the diligent, experienced, and skillful nature of its leadership team. ***We initiate coverage of Cyber Security 1 with a Strong Buy rating, and set our 12-month price target at $11.39 per U.S. ADR*** (each ADR represents 10 shares of the Company's common stock).

(In €000 except per-share)	FY 2017	H1 '18	Q3 '18	Q4 '18	FY 2018	Q1 '19	Q2 '19	H2 '19	FY 2019	FY 2020	FY 2021
Total revenues	**17,193**	9,786	14,174	15,435	**39,119**	34,633	36.623	58,513	**155,538**	268,745	474,884
Gross margins, VAD	**33.7%**	34.5%	15.9%	17.8%	**16.4%**	20.6%	21.3%	22.3%	**20.7%**	22.4%	22.3%
Gross margins, Advisory/MS	**43.8%**	41.8%	46.4%	50.7%	**47.5%**	55.6%	57.5%	59.8%	**58.5%**	61.4%	61.4%
Gross profits	**6,626**	3,724	3,489	4,280	**13,494**	9,994	11,085	28,460	**95,512**	52,801	176,915
Operating expenses	**9,810**	5,648	5,273	5,271	**16,192**	10,422	10,734	21,156	**44,932**	73,799	126,320
Operating profits	**(3,184)**	(1,924)	(1,783)	(991)	**(4,698)**	(1,294)	(649)	1,942	**317**	21,712	50,595
Operating margin	**-18.5%**	-19.7%	-12.6%	-6.4%	**-8.5%**	-3.9%	-1.9%	3.6%	0.2%	8.1%	10.7%
EBITDA	**(2,918)**	(1,890)	(1,755)	(968)	**(4,612)**	(1,261)	(614)	3,500	**464**	18,742	46,682
Net income	**(3,068)**	(1,385)	(1,308)	(771)	**(3,463)**	(1,023)	(588)	1,624	**12**	12,926	31,975
Earnings per share	**(€0.012)**	(€0.005)	(€0.00)	(€0.00)	**(€0.01)**	(€0.00)	(€0.00)	€0.01	**€0.00**	€0.03	€0.06
Sequential EPS growth	N/A	N/A	N/A	N/A	**N/A**	N/A	N/A	N/A	**N/A**	N/A	93.7%
Net cash before additional financing is secured (future)	**265**	247	437	(843)	**(1,811)**	(3,071)	(3,685)	(1,346)	**(1,346)**	17,396	64,078

Please see analyst certification and required disclosures on page 10 of this report.

Industry Background

An Historical Perspective

Over the last 150 years, civilization has undergone an unprecedented transformation due to the increasingly rapid pace of technological innovation. In the telecom, media, and technology (TMT) sector, this innovation cycle began with the telegraph and telephone in the late 1800s, continued with the invention of wireless communication by radio, and then television. By the late 1940s, the first digital computer had been developed, and during the 1950s, 1960s, and 1970s we saw an ever-accelerating series of developments in telecommunications and computing. This set the stage for the personal computer that became nearly ubiquitous during the 1980s, and then mobile phones, the World Wide Web, and early smart phones beginning in the 1990s. Then in the most recent period of technology history, we have seen the world's computers, telephones, wristwatches, cars, homes, and televisions become interconnected, enabling us to manage much of our lives and businesses more efficiently and effectively than ever before.

Unfortunately, this wondrous technology development cycle has a concomitant dark side, namely the development of hacker technologies that are designed to prevent or alter the function of, or completely commandeer the control of the computing and communications devices upon which we now so heavily rely. In fact, the timeline of key developments in cyberattack technology and the breaches caused thereby has closely paced that of underlying technologies, as shown by the history recounted below:

Key "Milestones" in the Early History of Attacks Against Telecommunications and Computing Infrastructure	
1903	A public demonstration of Marconi's purportedly secure wireless telegraphy system is disrupted by insulting Morse code messages, sent through the auditorium's projector by inventor and magician Nevil Maskelyne.
1949	Computer pioneer John von Neumann authors a paper suggesting that computer programs could reproduce themselves.
1963	MIT's student newspaper mentions MIT telephone hackers had been tying up HarVADd's phone lines to make free calls.
1979	Infamous hacker Kevin Mitnick breaks into his first major computer system at Digital Equipment Corporation (DEC).
1981	Chaos Computer Club formed in Germany. Ian Murphy (Captain Zap) is first hacker tried and convicted as a felon.
1986	U.S. Congress passes the Computer Fraud and Abuse Act, making it a crime to break in to computer systems.
1988	First National Bank of Chicago is the victim of a $70,000,000 computer theft, the first of its kind over $10,000,000.

By the early 1990s, the advent of using the Internet via the World Wide Web changed everything, and quickly. Hackers were now able to share their exploits via webpages and began to collaborate on a global basis, making information security an ever more elusive objective. During the 1990s and 2000s, the number of high profile hacks became too numerous to list, and affected individual users, corporations of all sizes, and various federal, state, and local government agencies. Antivirus and antimalware products continued to evolve and offer users some modicum of protection, but always seemed one step behind the attack technologies. **So, the key question is "What is the state of information security and computer/telecommunications attacks today?"**

Cyber Security in 2018

Unfortunately, we cannot report that the current state of affairs in cybersecurity is any better in 2018 than it has been in previous years, and it could be argued that it is worse. This is due to a variety of factors, the most salient of which is the number and variety of devices that are now connect to the Internet. The average home in the developed world now contains one or two Web-connected televisions, several Web-connected smartphones, one or more computers, and some form of Internet router, typically provided and managed by either the cable TV provider or a major telephone company. In the corporate and government worlds, the scenario is even more complex, as teleworkers routinely use their laptops and/or mobile devices to connect to their "secure" corporate networks, which also are often accessible by key customers, partners, suppliers, and other stakeholders. And because so much of our current economy has become digital, the stakes have never been higher.

Attack methodologies have also continued to evolve and improve, as what used to be a world dominated by rogue "genius hackers" is increasingly dominated by organized groups reminiscent of large crime families. Some have a global presence and a corporate structure – complete with business card carrying sales and marketing teams – such as Italy's famous Hacking Team. These organizations are able to launch ever more complex, multi-vector attacks, which the industry has labeled Advanced Persistent Threats, or APTs. After accomplishing an initial low-level penetration of a target's systems, say the computer of a single user, these threats are known to exist in a dormant, nearly impossible to detect state for weeks or months, just waiting for the opportunity to gain traction. It was just this type of threat that in 2014 compromised Target's computers and stole 40 million credit and debit card records, affecting nearly 110 million Target customers (including this report's author). Another example of such an APT in action was the 2017 Equifax data breach, where cyber criminals were able to access the full names, social security numbers, birth dates, mailing addresses, and in some cases Driver's License numbers of some 145.5 million Americans, including almost all members of the middle and upper income and wealth brackets. Ransomware attacks, while often less high profile, have been at least as damaging, with individuals, corporations, and government entities alike having to pay large ransoms (in untraceable bitcoin, typically) to regain control of their systems and access to their data. So, what does the future hold for the digital economy?

Cyber Security in the 2020s and Beyond

We believe it would not be an overstatement to say that Cyberattacks could be the greatest single risk to the digital economy and the benefits that it promises to bring our world. As grim as the current situation seems to be, the near future is likely to become more so. That is, unless the manufacturers of connected devices become as committed to security as we believe they should be. Historically, at least, attack breaches resulted in data and financial loss only, but in the very near future, cyberattacks could result in casualties very similar to those common in wartime. Consider the following:

In 2015, a pair of former black hat hackers named Charlie Miller and Chris Valasek, now working with an $80,000 DARPA grant, were able to use the Sprint network to compromise the control system of a Jeep Cherokee over the Internet. That's right – with nothing but a laptop and an inexpensive cellphone, working from the comfort of their own home, they developed a way to scan the Sprint network for Jeep Cherokees anywhere in the world, and when they found one they could completely compromise its onboard computer systems. This gave them control over the entertainment system, peripheral systems like the windows, headlights, and windshield wipers, and core systems such as the car's engine, transmission, steering apparatus, braking systems, and accelerator. Essentially, they controlled the vehicle. As scary as this is, imagine a large cybercrime organization (such as the intelligence apparatus of Iran or North Korea) applying scale to this hack, which could in theory allow them to identify and take control of nearly all Jeep Cherokees simultaneously. In 2015 this amounted to 471,000 vehicles in the United States alone. Worse still, Miller and Valasek stated that many cars on the road were nearly as insecure as the one they chose to target, meaning that millions of vehicles might be susceptible to such an attack[1]. And as driverless autonomous vehicles begin to operate early in the next decade – not to mention delivery drones and autonomous robotic workers - this picture becomes even more alarming. So, what does this all mean to the average individual?

Conclusion

Well, one thing is for certain, in our view: we will see exponential growth in the demand for cybersecurity solutions at almost every level of the production and consumption value chains. Whether the currently almost unimaginable cyberattack will in the future kill hundreds or even tens or hundreds of thousands of people, in the process crippling key transportation, electric utility, and other industries, we cannot say. We certainly hope not. But we believe that the software and hardware systems necessary to prevent it will be developed and implemented – either preventing such an attack, or in response to one - as will many shorter-term solutions that prevent the attacks that are so commonplace today. So while the current state of cybersecurity and the cyberattacks it tries to prevent may be somewhat anxiety producing to those in the know, we believe the current state of affairs will produce a long-term bonanza for most significant players in this rapidly growing and changing global industry.

The Rapidly Changing Regulatory Environment of Cybersecurity

Because the cybersecurity industry is and has been so thoroughly characterized by frequent disruptive technology introductions and constant change, it is not surprising that in some cases our and other counties' legislators have been a little slow in passing pertinent legislation, a real problem that has been at least in part caused by the reticence of the very people and organizations such legislation protects, namely technology manufacturers and operators. However, we believe a regulatory sea change has now begun, and that local, state, and federal government agencies in the U.S. (and their European counterparts) have finally gotten serious about creating cybersecurity legislation that is compulsory and enforceable.

Following several rounds of improved / strengthened information security laws that were passed in the last three years, Europe is now setting the tone for the entire globe in terms of protecting individuals' rights from digital exploitation and abuse. The law purported to accomplish this is the General Data Protection and Regulation (GDPR). This law includes compulsory compliance for any and all companies that do business with and keep data pertaining to any EU citizen. Because of the global nature of our highly interconnected digital economy, this effectively means that most large companies with a significant digital component to their business models will be subject to EU fines if they do not comply with GDPR rules, regardless of their jurisdiction of domicile.

The GDPR is a multifaceted piece of cybersecurity and personal privacy legislation, with major functional components in two areas:

1. **Ownership of and control over personal data.** The GDPR stipulates that all entities that collect data from EU citizens will be required to obtain explicit, informed consent regarding the collection, storage, and use of personal data. Furthermore, under GDPR, consumers must have the ability to access their data, and have the right to revoke their previously-granted consent.
2. **Transparency, especially regarding data breaches / successful attacker penetrations.** Over the last few years, many of the announcements pertaining to the largest, most damaging breaches have come as part of a revelation that the breached entity (corporate or government) has known about the breach and kept it secret for some time – in several high profile cases, for a number of years – before coming clean with the general public. Under GDPR, however, **companies have just 72 hours to report a breach once it's been discovered**; compliance with this provision of GDPR will require pronounced shifts in the internal attitudes and ingrained habits of more than a few large corporations. However, it is this provision of the GDPR that

[1] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

gets us the most excited about its potential for positive change, as this will drastically shorten the time from when a new breaching agent or technique is discovered until the IT community at large has "patched" against it.

However, apart from its comprehensive nature and its likely global reach, what is also new with the GDPR is that this law has teeth. Companies found to be out of compliance with GDPR requirements can be fined up to 4% of trailing annual sales or €20,000,000, whichever is greater. Although GDPR enforcement is far more complex that this simple rule would suggest – entailing the operations of supervisory authorities with broad powers of investigation, arbitration, sanctioning, and in some cases issuing legally-enforced cease and desist orders – we believe it is the prospect of being fined up to €20,000,000 or (with no limit) up to 4% of annual sales that will command the most (and most important) Director and C-level Management awareness of and commitment to act on the prevention of cybercrime.

The United States and the National Institute of Standards and Technology (NIST)

Not unlike the Europeans, we Americans have a variety of private and public institutions to help mitigate the damage from cyberattacks, or to regulate certain types of companies such as banks and electric utilities so that they maintain a high level of preparedness with multiple layers of fail-over and protection. One key difference between the United States' strategy and that of the Europeans is that we as of yet have not opted for compulsory compliance. We have, however, made great strides in creating the legislative framework to encourage industry-wide cooperation and information sharing, which are key elements of developing and strengthening cyber resilience. Also, we have recently selected the NIST, a division of the U.S. Commerce Department, to spearhead the creation and promulgation of cybersecurity principles and practices.

Conclusion

In reality, there's very little more that governments and large companies can do than what they are doing. By definition, they are mostly doomed to play defense only, meaning that they must not fail to guard any of the thousands of potential weaknesses in their systems while their adversaries need find only one. Luckily for their constituents, the "game" doesn't end when an attacker successfully breaches an opponent's system and gains a foothold. If the owner of the breached system has been working with a company such as Cyber Security 1, then they will be employing several best-in-class technologies in a layered approach, designed to prevent breaches when possible, and when not possible, to quickly identify them and patch them before the attacker can do any real harm. This type of layered approach to cybersecurity is what, in combination with the help of specialized professionals, is known as "cyber resilience." Cyber Security 1 is a Company 100% focused on delivering maximum cyber resilience to its customers.

Company Analysis

Introduction

Cyber Security 1 is an integrated, multi-national cyber resilience company legally domiciled in Sweden, with its headquarters in London, England, and major offices in South Africa, Turkey, UAE (Dubai), and Austria, with smaller offices throughout Europe. The Company currently has historically derived the slight majority of its sales as a value-added reseller of cybersecurity products, but has generated more of its earnings from its higher margin advisory and ultra-high margin managed services offerings. The Company's overall business strategy is to "buy and build" by executing select and synergistic acquisitions in key developing markets, on which it has so far executed very well. In the two acquisitions recently closed plus one announced just last month, the Company was able to add $57.6 million in 2017 (audited) revenues and $4.4 million in 2017 EBITDA, at a total cash cost of just $7.93 million plus an estimated share grant of just over 56 million shares (or 17.8% of Cyber Security 1 on a pro-forma basis). On a pro-forma basis, these three businesses would have constituted 73.1% of the Company's 2017 revenues, and with their EBITDA contribution, total EBITDA for 2017 would have been EUR €1.2M rather than the reported (€2.6M). Given that two of the three acquired businesses' revenues have been growing at 20% annually – not taking future cost-savings or cross-selling / upselling opportunities into account – we believe these acquisitions will be strongly accretive over time.

Cyber Security 1 trades in the U.S. on the OTCQX market as a Bank of New York ADR under the symbol CYBNY (10 shares of common stock per ADR) and on the Nasdaq First North market in Sweden under the symbol CYB1.

The Problem

As covered in our Industry Background section, cybersecurity now requires protecting against a multitude of attack vectors that include flaws in hardware design, device-level firmware, operating systems, user applications, network infrastructure, and connected non-computing devices such as printers and televisions, as well as flaws in the behaviors and thinking of users. While clever attack code is usually employed to compromise modern computer systems, attacks with a non-technical but human dimension known as social engineering are also responsible for many of the initial breaches of user systems (known as endpoints). Such attacks based on social engineering (e.g. phishing, whereby users are tricked into clicking on a malicious link) are often the most difficult to defend against. And "clever attack code" now typically means polymorphic code that actually rewrites itself to escape the vigil of pattern-matching technology such as antivirus software. To make matters worse, ubiquitous WiFi technologies have recently been declared in impossible to secure, since the most powerful and widely-adopted WiFi encryption technology known as WPA2 has been publicly cracked and is unfixable until a new generation of encryption becomes standardized upon and broadly adopted. The bottom line is this: 100% breach prevention is no longer an attainable goal, so a recent shift in cybersecurity thinking has occurred, from breach prevention (i.e. perimeter security) to breach remediation and minimization. In other words, cyber resilience.

Cyber resilience is attainable, but what exactly does it require? It ideally is comprised of a number of functional components that include hardware and software redundancy and multiple layers of prevention, identification, and remediation. These are comprised of:

- **Firewalls** (which often run on endpoints (e.g. user systems), network access points (e.g. WiFi routers and modems), and network infrastructure devices (e.g. routers and switches) and are geared to identifying and preventing suspicious incoming and outgoing communications (by port numbers 0 to 65,535).
- **Intrusion Detection Systems** (e.g. Snort, Tripwire) that employ sophisticated change monitoring systems that look for alterations in stored files that do not seem to have been altered by authorized users or be the result of typical user behavior. Also, these systems are often the first level of log interpretation that help sysadmins focus on likely problem areas.
- **Intrusion Prevention Systems** which are now based on ever-improving artificial intelligence that proactively prevents what seems to be unauthorized access, all without human intervention.
- **Antivirus software** that screens systems for pattern-based self-replicating code.
- **Antimalware systems** that evaluate program behavior, red flagging programs that seem to have the ability to act maliciously and/or have been installed by users who are unaware of a program's full functionality.
- **Endpoint protection systems** that often include antivirus and antimalware software but also offer more active protection, monitoring (and blocking) well-accepted programs such as those comprising the Microsoft Office suite that may attempt to take unauthorized actions, such as initiating communications with an unknown outside IP address.
- **Anti-keylogging systems** that seek to prevent software that attempts to capture user passwords and other sensitive data for subsequent exfiltration.
- **System level management systems** that give system administrators the ability manage not only their endpoints but all other devices on their local or wide area network. Such systems can be highly complex, and typically offer features such as user management, inventory management and remote administration thereof, and many other valuable IT features.

- **Real-time backup systems** that provide data security, protection against the "unbreakable" encryption used by ransomware attacks; backups are now typically done over the Internet and stored in off-site, secure facilities.
- **Real-time encryption systems** that provide file-level security as well as network communications security, when the encryption is robust enough to survive decryption attacks. This is because intercepted network traffic is useless to a would-be attacker if the captured data cannot be unscrambled and read, and encrypted disk files can only be corrupted, but never infected as long as their encryption remains unbroken.
- **Authentication systems** that use hash functions, passwords, and biometric-based systems such as fingerprint or optical "iris prints" to verify the identity of users, sysadmins, and other computers.
- **User training systems** that are designed to enlighten users regarding what they should and show not do, and to keep these "best practices" of cybersecurity on the forefront of users' minds, which is perhaps the most difficult of all of the challenges cybersecurity entails.

Each of these cybersecurity components is developed by multiple providers and is designed for various levels of integration or interoperation with other components, which may or may not be made by the same vendor. Each requires superior and ever-improving technology, and leadership status in each product category is difficult for each vendor to obtain and easy for them to lose. This makes for a very challenging environment for the cybersecurity purchaser, who at all but the largest and most sophisticated organizations typically lacks the in-house expertise and up-to-date product knowledge required for optimal decision making and implementation.

The Cyber Security 1 Solution

The Company understands the problems facing its customers and prospective customers very well. These customers already want to maximize their level of cyber resilience – in fact, demand it, now at the highest levels of the organization rather than just in the IT department – and yet without very specialized expertise they are unlikely to achieve it. This expertise extends far beyond knowing which provider's solution is "best in class" and requires a deep knowledge of each organization's currently-implemented technology and, if changes need to be made, exactly what change plan will optimally stitch together the new and legacy technologies for a smooth implementation and the best price/value equation. This is where Cyber Security 1 comes in.

Value-Added Distribution (VAD)

The foundation of the Company's buy and build strategy, value-added distribution provides the Company with substantial gross profits and a cost-effective entry point to many attractive, high-growth markets. Value-added distributors such as Cyber 1 make "bulk" purchase orders of hardware and software and then resell it to customers who need both it and the Company's expertise in terms product selection and integration. However, many of these VAD customers need real on-site assistance, not just advice. For these customers, the Company will provide the advice and personnel they need, earning a gross margin of almost 3x standard VAD gross margins in the process (our model has Advisory Services generating almost 60% gross margins at scale). So while value-added distribution is in and of itself a difficult and not particularly attractive business model, in this case it is very attractive to the Company, which has demonstrated expertise in acquiring "not for sale" businesses at very reasonable prices using a 20% cash and 80% stock with which to purchase them.

Advisory Services

This is currently, in our opinion, the most important line of business for the Company. The Company has historically earned gross margins of nearly 70% in this segment, although we believe a sustainable gross margin is approximately 60%. The Company offers its customers a wide range of advisory services, which can help ensure legal compliance, assist with the actual installation and integration of various cybersecurity system components, and in general serve as outsourced staff that can be employed as needed, on demand.

Managed Services

As cyber threats become more advanced and complex, and defense against them (cyber resilience) becomes more challenging and demanding of an ever-widening skillset, many organizations are deciding to simply outsource everything their cybersecurity requires. Although nascent at this time, taking over the management of all cybersecurity tasks and responsibilities is the Company's highest-margin business opportunity, and a natural upsell for its VAD and Advisory customers. Although Managed Services had gross margins of under 60% in 2017, management believes that it will soon attain gross margins of 80% As a result, management is highly motivated grow this segment of its business as aggressively as possible

Conclusion

Unlike product vendors that have a vested interest in recommending the use of their own products regardless of whether they are best for the customer or not, the Company is truly product agnostic and thus is solely focused only on each customer's best interests. As a value-added distributor it helps customers choose and implement solutions, and as an advisor it goes one step further and assists the customer with longer-term, more important decisions such as resource planning and regulatory compliance. But the Company's highest-level value proposition (and by its highest margin line of business, at approximately 80%) is its managed service offering, which entails Cyber Security 1 entirely taking over and managing the entire cyber resilience function for the customer. In our view this is an especially compelling value proposition for the SME (small and medium sized enterprise) market, as companies comprising this market typically have the budget for cybersecurity, but not the resources necessary to hire the Company's level of insight and expertise in-house.

Growth Strategy

Cross-selling and Up-selling

To date, the Company has largely allowed its acquired subsidiaries to be run autonomously as they were before Cyber Security 1 acquired them. However, their previous and newly-acquired value added reseller businesses now constitute excellent platforms for the Company to sell higher margin advisory services and its 80% gross margin managed services. Given that managed services are widely recognized as the highest growth segment of the cybersecurity market, we believe the Company is likely to do very well in this area. Given the margins associated with managed services, we believe their success in this segment will have a disproportionately positive effect on overall EBITDA and net earnings.

Accretive acquisitions

The Company has demonstrated excellence in making key acquisitions in key growth markets – and at a reasonable price and structure. As its last few acquisitions clearly show, this strategy is working, and the Company is committed to continue making it work. We believe it is very likely to continue its track record of strengthening its geographic and customer presence via acquisition, and expect this aspect of its business to enhance per-share growth in sales and EBITDA by 10% per year or more going forward. If this proves to be correct, the Companies acquisitiveness should prove to be a major driver of shareholder value expansion. Our current model calls for the Company to make 13 acquisitions over the next three and a quarter years, including four more VADs and ten more Advisory/Managed Services firms.

Expanding geographic footprint

The Company now has major market share in Turkey, Greece, and South Africa, all of which are growing much faster than the larger European and American markets. The Company also has a significant presence in the UAE, Kenya, and the Ukraine, and plans to continue to penetrate additional developing markets via acquisitions while it simultaneously grows sales in all markets through organic expansion.

While the Company's historical organic growth rate is likely to remain in the 15% range – perhaps trending towards 20% or more – we believe its per-share growth in sales and EBITDA is likely to remain well above 25% CAGR, as long as its current successes continue into the future. This should eventually cause the equity markets to award CYBNY shares with a premium sales and EBITDA multiple, which we do not believe is yet reflected in the valuation of the Company's shares.

Leadership Team

Kobus Paulsen, *Chairman of the Board*

The Company's largest shareholder with just over 90 million shares, M&A specialist, Mr. Paulsen is actively involved as Non-Executive Chairman, a role he has held since 2015. As the Company's majority shareholder, Mr. Paulsen is effectively in control of the Company, although he is a non-Executive Chairman who focuses his time on M&A activities, the Company's strategy and business model to key stakeholders and prospective stakeholders. Mr. Paulsen is a Payments and Cyber Security Entrepreneur and has been a digital revolutionary for many years. Mr. Paulsen is a large shareholder in UC Group, owner of SecureTrading Group, a leading payments company based in Europe.

Robert Brown, *Chief Executive Officer*

Mr. Brown has been the Company's CEO since 2016. In addition to this role, he serves as a Director of Two Robs Property Investments (PTY) Ltd., Awake Investments (PTY) Ltd, Energy and Densification Systems (PTY), Ltd and Professional Technologies (PTY) Ltd. He was educated at the King Edward VII School in Johannesburg, South Africa.

Vivian Gevers, *Group Managing Director*

Recently promoted to this post, Ms. Gevers previously served as the Managing Director of Credence Security Dubai, which is one of the Company's wholly-owned subsidiaries. She holds a BCom in Management from the University of South Africa.

Daniel Holden, *Chief Financial Officer*

Mr. Holden has been the Company's CFO since 2015; and presently a Director of SecureTrading - a leading independent payments service business, licenses in Europe and North America. Other assignments: previously CFO of SecureTrading (www.securetrading.com), the largest independent UK payment gateway SecureTrading Financial Services, now Acquiring.com (www.acquiring.com), an MFSA regulated merchant acquirer with Visa and Mastercard principal membership.
Founding director of regulated Financial Institution. Planning and delivery of original business plan to payment schemes, operational assistance in the establishment of the merchant acquirer and financial co-ordination and reporting.

Daniel holds a LLB, Law and a Chartered Accountant, ACA (Member of the Institute of Chartered Accountants in England and Wales).

Competition

The Company faces robust competition in all of its key markets, and yet has been succeeding despite this. We do not expect competitive pressures to ease any time soon, but due to the underlying strength in the cybersecurity demand picture, we believe that the Company should continue to thrive despite this high level of competitive pressure. Note that the Company does not suffer the same competitive threat as product vendors, who are at constant risk of technological obsolesce, and which must plow a large percentage of revenues back into research and development.

Other Risks

In our opinion, the greatest risk facing the Company (and all companies in this market) is the cost and difficulty of attracting and retaining highly qualified technical personnel. At this point in time, the demand in this space is outstripping the overall market's ability to supply qualified professionals, as cybersecurity requires "the best and brightest" to combat the high degree of talent and expertise found in the many cyberattack individuals and organizations.

Other risks are to a lesser degree currency risk and financing risk. The currency risk facing the Company exists because most of its business is denominated in the local currencies of South Africa, Turkey, and other developing economies, whereas the Company's business largely operates on Euros. However, there is a degree of natural diversification in the Company's various geographical segments that mitigates currency risk to a significant extent; it is also worthy of note that currency fluctuations go both directions, and consequently in the short-term are as likely to help the Company as they are to harm it. Financing risk exists because the Company has historically been cash-constrained, even to the extent that it this has limited its ability to maximize organic growth in its existing businesses. Although its recent acquisitions and their incremental EBITDA should help reduce the limitations imposed by limited working capital, this could be more than offset by the cash required to close on additional acquisitions, for which it typically pays 20% of the value in cash. This is evident in our financial models, which show the Company hitting a low point in terms of available cash sometime in mid-2019. We believe, however, that the larger and growing business that the Company will represent going forward will be easier to finance, providing it both with adequate working capital as well as the cash it requires to make acquisitions.

Financial and Pro-forma Analysis

If one considers only the Company's historical numbers as reported, Cyber Security 1 might seem fairly valued or even overvalued, hemorrhaging cash and just trying to survive until its organic growth and the underlying strength of its markets get it to the point of breaking even or earning a slight profit. But just this year, the Company has completed two acquisitions and announced a third; if we consider all three acquisitions on a pro-forma basis, the picture looks very, very different. Furthermore, over the next 13 calendar quarters the Company intends to continue and in fact intensify its acquisitiveness, seeking to purchase two Advisory and one VAD business in 2019, three Advisory and one VAD business in 2020, and five Advisory and two VAD businesses om 2021. See acquisition models after the text of this report.

Valuation Analysis

Cyber Security 1 is someone of a challenge in terms of valuation. It is essentially two businesses that are highly interrelated in the marketplace, but which have very different fundamental characteristics from a valuation perspective. The VAD businesses that comprise Cyber Security 1 (there are now three of them, and counting) have gross margins ranging from under 10% on the low side (ITWAY) to well over 20% on the high side (Credence Security), and typically have compound annual growth rates in the 10% - 20% range. While we expect the Company's cross-selling and upselling initiatives to accelerate growth in these businesses to some degree, they nevertheless are low-margin, relatively unattractive businesses that lack pricing power. Therefore they are best valued on a price to sales or other revenues-based valuation metric. Note that these are typically very low multiples – our reference group as an average P/S multiple of 0.25x.

The Advisory and Managed Services businesses, on the other hand, have quite different fundamental characteristics that make them far more attractive from a valuation perspective. These businesses are growing at an average of 30% per year, and carry gross margins typically in the 60% range. These businesses are valued by some of the same metrics as are VADs, but measures that look at earnings power and future free cash flows tend to be the best in this area. In this exercise, we consider Managed Services to be special category of Advisory Services, although this is technically not accurate, as the organizational requirement of scaling Managed Services are quite distinct and almost entirely different from those of scaling an Advisory business. Nevertheless, the recurring nature of revenues and high margins (up to 80% in the case of managed services) make this a similar business from a valuation perspective.

The chief challenge with applying the various valuation methodologies to Cyber Security 1 is that it is almost impossible to synthesize two complete companies by deconstructing the Company's expenses. This is because the Company does not report its operating expenses by segment, which is standard. However, this prevents us from conducting a real sum-of-the-parts valuation exercise, at least unless we made some expense allocation assumptions that may not even approximate what either line of business would really look like as a standalone entity. Furthermore, there is another issue: because the Company's sales personnel often serve (or will serve) both business segments in the context of a single customer, it would be impossible to fairly divide the whole company's operating expenses fairly between the two main lines of business.

In the case of the Company, we opted to employ a hybrid approach to valuing the Company, approaching that we might use in a true sum-of-the-parts exercise, but with one important assumption: because we could not adequately justify any arbitrary allocation of the operating costs between the VAD and Advisory/Managed Services business, we opted to value the VAD business on a price to sales multiple, and despite its currently much smaller revenue and geographic footprint, we are valuing the other side of the Company on a multiple of Pre-tax earnings based on its gross margins +60% of the company's forecast operating expenses.

(In €000s, except for per share data)	2020	Q1 '21	Q2 '21	Q3 '21	Q4 '21	2021E
Total revenues, VAD Businesses	**179,361**	**62,191**	**64,924**	**81,382**	**84,997**	**293,493**
Estimated organic CAGR*	*10.00%*	*3.85%*	*3.85%*	*3.85%*	*3.85%*	*10.00%*
Gross profits	40,264	13,891	14,500	18,129	18,933	65,453
Gross margin, if reported	*22.4%*	*22.3%*	*22.3%*	*22.3%*	*22.3%*	*22.3%*
Price to sales multiple, Harbinger VAD reference group		*0.25*				
VAD Businesse, valuation at ref. P/S multiple		€73,373.2				
Total revenues, Advisory and MSvcs	**89,384**	**37,400**	**40,017**	**48,841**	**55,133**	**181,391**
Estimated organic CAGR *	*30.00%*	*10.78%*	*10.78%*	*10.78%*	*10.78%*	*30.00%*
Gross profits	55,248	22,968	24,623	30,003	33,868	111,461
Gross margin, if reported	*61.8%*	*61.4%*	*61.5%*	*61.4%*	*61.4%*	*61.4%*
Operating and other costs, 60% of total	44,280	15,895	16,749	20,784	22,365	75,792
Pre-tax profits**	**10,968**	**7,073**	**7,874**	**9,219**	**11,504**	**35,669**
Pre-Tax Earnings Multiple:	**15**	**Advisory and Managed Servces group valuation:**				**€535,040.7**
*As strange as it may seem - and did to us - 3.85% is the correct compound quarterly growth rate given a one-year CAGR of 10%						
** *as modeled, gross costs less 60% of corporate operating costs*						

Based on our reference group after P/S ratio of 0.25, we value CYBNY's VAD business at €73,373200 – from a late 2020 perspective – based on our model. In the case of the Advisory business, based on a 30% growth rate and 60%+ blended gross margins (Advisory and Managed Services) we feel that a multiple of 15x forward pre-tax earnings is well warranted. Based on our forecast 2021 pre-tax earnings, again from a late 2020 perspective, this gives us an Enterprise Value of 15 x €35,669 = €535,040,700.

When we combine these values, arriving at €608,413,900, we then apply our 2-year discount formula:

$$PV = FV/(1+10\%)^2 = €502,821,428$$

Giving us our target price for the Company and its shares (€0.99 for common stock, and $11.39 for the ADR).

Investment Thesis and Conclusion

In short, we believe in the leadership of this Company, and have so far found no reason not to assume that their demonstrated success in making key acquisitions at reasonable prices will continue, per their plan as reflected in our models. The Company is extremely well-positioned in a rapidly growing industry, and we believe that its growth will likely exceed that currently forecast by most cybersecurity pundits. **We therefore believe that at current prices levels, the shares and ADRs of Cyber Security 1 are rather dramatically undervalued, and set our 12-month price target at €0.99 per share, or $11.39 for the U.S. ADR. We rate the shares of Cyber Security 1 (OTCQX – CYBNY) a Strong Buy.**

Our Rating System

We rate enrolled companies based on the appreciation potential we believe their shares represent. The performance of those companies rated "Speculative Buy" or "Strong Speculative Buy" are often highly dependent on some future event, such as FDA drug approval or the development of a new key technology.

Explanation of Ratings Issued by Harbinger Research

STRONG BUY	We believe the enrolled company will appreciate more than 50% relative to the general market for U.S. equities during the next 12 to 24 months.
BUY	We believe the enrolled company will appreciate more than 30% relative to the general market for U.S. equities during the next 12 to 24 months.
STRONG SPECULATIVE BUY	We believe the enrolled company could appreciate more than 50% relative to the general market for U.S. equities during the next 12 to 24 months, if certain assumptions about the future prove to be correct.
SPECULATIVE BUY	We believe the enrolled company could appreciate more than 30% relative to the general market for U.S. equities during the next 12 to 24 months, if certain assumptions about the future prove to be correct.
NEUTRAL	We expect the enrolled company to trade between -10% and +10% relative to the general market for U.S. equities during the following 12 to 24 months.
SELL	We expect the enrolled company to underperform the general market for U.S. equities by more than 10% during the following 12 to 24 months.

Analyst Certification

I, Brian R. Connell, CFA, hereby certify that the views expressed in this research report accurately reflect my personal views about the subject securities and issuers. I also certify that no part of my compensation was, is, or will be, directly or indirectly, related to the recommendations or views expressed in this research report.

Disclaimer

This report was prepared for informational purposes only. Harbinger Research, LLC ("Harbinger") was paid $10,000 by a third party for the preparation and distribution of this research report. All information contained in this report was provided by the Company. To ensure complete independence and editorial control over its research, Harbinger has developed various compliance procedures and business practices including but not limited to the following: (1) Fees from covered companies are due and payable prior to the commencement of research; (2) Harbinger, as a contractual right, retains complete editorial control over the research; (3) Analysts are compensated on a per-company basis and not on the basis of his/her recommendations; (4) Analysts are not permitted to accept fees or other consideration from the companies they cover for Harbinger except for the payments they receive from Harbinger; (5) Harbinger will not conduct investment banking or other financial advisory, consulting or merchant banking services for the covered companies.

Harbinger did not make an independent investigation or inquiry as to the accuracy of any information provided by the Company and is relying solely upon information provided by the Company for the accuracy and completeness of all such information. The information provided in the Report may become inaccurate upon the occurrence of material changes, which affect the Company and its business. Neither the Company nor Harbinger is under any obligation to update this report or ensure the ongoing accuracy of the information contained herein. This report does not constitute a recommendation or a solicitation to purchase or sell any security, nor does it constitute investment advice. This report does not take into account the investment objectives, financial situation or particular needs of any particular person. This report does not provide all information material to an investor's decision about whether or not to make any investment. Any discussion of risks in this presentation is not a disclosure of all risks or a complete discussion of the risks mentioned. Information about past performance of an investment is not necessarily a guide to, indicator of, or assurance of, future performance. Harbinger cannot and does not assess, verify or guarantee the adequacy, accuracy, or completeness of any information, the suitability or profitability of any particular investment, or the potential value of any investment or informational source. Harbinger and its clients, affiliates and employees, may, from time to time, have long or short positions in, buy or sell, and provide investment advice with respect to, the securities and derivatives (including options) thereof, of companies mentioned in this report and may increase or decrease those positions or change such investment advice at any time. Harbinger is not registered as a securities broker-dealer or an investment adviser either with the U.S. Securities and Exchange Commission or with any state securities regulatory authority.

ALL INFORMATION IN THIS REPORT IS PROVIDED "AS IS" WITHOUT WARRANTIES, EXPRESSED OR IMPLIED, OR REPRESENTATIONS OF ANY KIND. TO THE FULLEST EXTENT PERMISSIBLE UNDER APPLICABLE LAW, HARBINGER EQUITY RESEARCH, LLC WILL NOT BE LIABLE FOR THE QUALITY, ACCURACY, COMPLETENESS, RELIABILITY OR TIMELINESS OF THIS INFORMATION, OR FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL OR PUNITIVE DAMAGES THAT MAY ARISE OUT OF THE USE OF THIS INFORMATION BY YOU OR ANYONE ELSE (INCLUDING, BUT NOT LIMITED TO, LOST PROFITS, LOSS OF OPPORTUNITIES, TRADING LOSSES, AND DAMAGES THAT MAY RESULT FROM ANY INACCURACY OR INCOMPLETENESS OF THIS INFORMATION). TO THE FULLEST EXTENT PERMITTED BY LAW, HARBINGER EQUITY RESEARCH, LLC WILL NOT BE LIABLE TO YOU OR ANYONE ELSE UNDER ANY TORT, CONTRACT, NEGLIGENCE, STRICT LIABILITY, PRODUCTS LIABILITY, OR OTHER THEORY WITH RESPECT TO THIS PRESENTATION OF INFORMATION.

Harbinger Research is an independent equity research firm with a focus on providing coverage to small-cap companies. Our mission is to help our clients achieve fairer market valuations, an expanded shareholder base, improved liquidity, and easier access to capital markets. We do this by providing insightful, in-depth research reports and by making sure those reports are widely distributed and made available to both institutional and individual investors. We strive to deliver superior research coverage and the result is compelling – consistent coverage from industry-expert analysts that is well written and consists of insightful analysis, cogent arguments, and in-depth financial models. To learn more about Harbinger Research and view our research reports, we invite you to visit our website located at www.harbingerresearch.com.

Analyst Highlight

Brian Connell, CFA **Senior Research Analyst**

Mr. Connell has over 20 years' experience in the securities industry, as an equity analyst and portfolio manager, and as the founder and CEO of StreetFusion (acquired by CCBN/StreetEvents), a software company serving the institutional investment community. On the sell-side, Mr. Connell served as the technology analyst for Neovest, an Atlanta-based boutique, and as a Senior Analyst - Internet for Preferred Capital Markets, an investment bank based in San Francisco. Mr. Connell has also held the position of Executive Director of Marquis Capital Management, a technology-focused investment management organization.

Mr. Connell holds degrees in Economics and Psychology from Duke University, and is a CFA Charterholder.