Trickle Research

Every raging river, every great lake, every
deep blue sea starts … with a trickle

Initiating Research Coverage

SideChannel

SideChannel, Inc.

(OTCQB: SDCH)

www.sidechannel.com

Report Date: 10/10/23

12- 24 month Price Target: $.18

Allocation: 4

Closing Stock Price at Initiation (Closing Px: 10/09/23): $.045

Prepared By:
David L. Lavigne
Senior Analyst, Managing Partner
Trickle Research

Disclosure: Portions of this report are excerpted from SideChannel's website(s), presentations or other public collateral. We have attempted to identify those excerpts by *italicizing* them in the text.

Company Overview

SideChannel ("SDCH" and/or "The Company") is a provider of cybersecurity services and technology to middle market and enterprise companies.

Our mission is to make cybersecurity easy and accessible for mid-market and emerging companies, a market that we believe is currently underserved. We believe that our cybersecurity offerings will reduce risks for our customers through identifying and developing cybersecurity, privacy, and risk management solutions. We anticipate that our target customers will continue to need cost-effective security solutions beginning with but not limited to what we refer to as virtual Chief Information Security Officer services ("vCISO" or "vCISO Services"). We also have also recently commercialized a new software product, Enclave, that we believe offers mid-market and emerging companies the means to simplify several crucial cybersecurity infrastructure procedures, including encryption, microsegmentation and access control.

Our vCISO engagements provide our clients with the C-suite cybersecurity leadership needed to effectively mitigate cybersecurity risks and support ongoing operation of critical business functions. This strategic cybersecurity leadership will often result in additional statements of work for SideChannel to deliver the Cybersecurity Software and Services needed to address gaps in our clients' cybersecurity framework. We now have over 20 C-suite level information security officers, who possess combined experience of over 400 years in the industry. Since inception, SideChannel has created over 50 multi-layered cybersecurity programs for its clients.

We believe that our customers, and prospective customers, in the mid-market will favor our approach, as it provides them with an efficient way to work with a single vendor to manage and oversee their cybersecurity programs. We also believe that our approach will reduce our customers' overall security costs and streamline their ability to increase their sales, reduce regulatory risks and monitor their risk posture.

We believe that we provide a full range of cybersecurity solutions through our employees, and through our network of subcontractors, and our array of partnerships with third party service providers and software companies. We work with our clients to help them select the right cybersecurity tools, products, and solutions. We believe that our use of a combination of employees and subcontractors allows us to cost effectively grow our client base and broaden the subject matter expertise on our bench while maintaining the agility needed to move directly into implementation of projects, which we believe reduces the risk to our customers. Our subcontractors also provide us with sales leads and referrals, and may resell our services to their own client base.

During September 2022, SideChannel announced a proprietary product, Enclave, which simplifies a particularly important cybersecurity task called "microsegmentation". Industry standard cybersecurity and risk management frameworks, such as National Institute of Standards and Technology Cybersecurity Framework ("NIST CSF") and Center for Internet Security Controls ("CIS"), prioritize inventory of assets and access control as top requirements for a sustainable and compliant cybersecurity program.

As a bit of history, SideChannel as it stands today, was formed through the combination of Cipherloc Corporation (the public entity) and SideChannel, Inc. (a private company and the de facto surviving business). That combination was completed in mid-2022, and current SideChannel CEO and Director Brian Haugli is the founder of SideChannel.

We were originally introduced to the story prior to the above combination, and at the time, we had a difficult time getting our arms around the opportunity. Thereafter, we were reintroduced to the story by CFO Ryan Polk. We knew Mr. Polk through prior endeavors, and he subsequently set up an introduction to Mr. Haugli and the new (combined) entity. Needless to say, we found the combined entity much more compelling than the original Cipherloc story.

Briefly, as we are often quick to point out we are generalists, so we are certainly not experts in cybersecurity. On the other hand, we do not feel like we need to be experts in the field to recognize that cybersecurity is a growing concern, and it is not going away. Further, while there are certainly large organizations, enterprises, infrastructures etc. that are obvious targets of ongoing cybersecurity attacks, the reality is that small and midsized companies are becoming increasingly more frequent victims of cyber-attacks. As a recent Forbes article notes: Small Businesses Are More Frequent Targets Of Cyberattacks Than Larger Companies: New Report (forbes.com) :

> *"...When it comes to avoiding cyberattacks, bigger is apparently better. At least that's according to a new report that shows small businesses are three times more likely to be targeted by cybercriminals than larger companies…".*

From another perspective: 30 Surprising Small Business Cyber Security Statistics - Fundera Ledger

> *"According to the US National Cyber Security Alliance, 60% of small businesses that suffer a cyber-attack go out of business within half a year. That's right—if a cyber criminal successfully breaches your small business's data, then odds are that your business will have to shutter within just six months…".*

The above notions underscore a portion of our investment thesis around SDCH, which is that small and even medium sized companies face a growing dilemma around cyber security risks, which is that while those risks are real and potentially catastrophic, they struggle to implement effective cybersecurity programs and protocols in part because of associated costs, but also because of their inability to understand how (and with what technologies) to implement effective solutions. Succinctly, and as we will attempt to demonstrate throughout this report, we think SDCH's products and services are aimed at addressing each of these barriers (cost and efficacy), which will allow them to address businesses that have struggled to effectively address growing cyber security risks.

Industry Overview

Industry estimates suggest that the global cybersecurity market is between $150 billion-$200 billion. We do not suspect that will surprise anyone because we think it is likely that nearly all the people that may read this document have been compromised by a data breach, and some of those more than once. Data breaches have become so pervasive that many of us have become numb to the notion. Not because we do not care about our data, but more so because it seems like there is not much we can do about it. That by the way, is not how enterprises *should* approach security, because the repercussions can be considerable or even catastrophic for smaller organizations.

To illustrate our "repercussions can be considerable" notion, as of this writing, two of the more recent high-profile cyber-attacks occurred at The Clorox Company (NYSE:CLX) and at MGM Resorts International (NYSE:MGM). Reports following the MGM attack suggested that the event cost the company over $50 million. At Clorox, the company noted that the attack would *"hurt its current-quarter financial results* ***materially****"*, as well as compromising the availability of some of its products for an undetermined period of time. As one might surmise, both companies have seen their share prices decline markedly since the respective events.

Table 1.

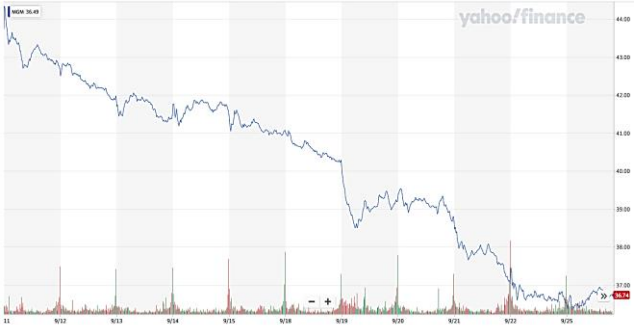


Table 2.

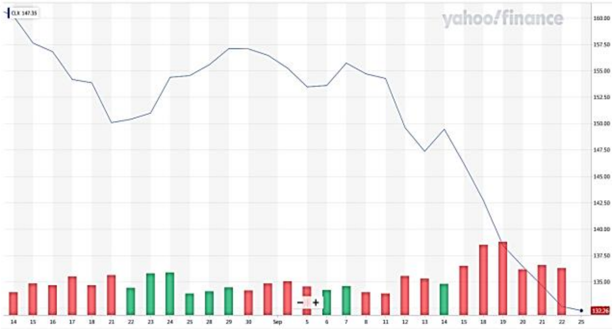


Table 3.

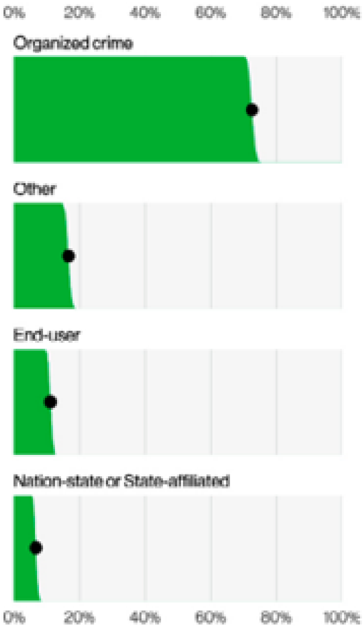


Figure 13. Threat actor Varieties in breaches (n=2,489)
2023 Data Breach Investigations Report | Verizon

As an extension to the above, a recent security threat report from Verizon notes that most security attacks are perpetrated by organized crime. When organizations can effectively build businesses around nefarious activities, it's a good bet that they will, and with greater frequency. With that said, it seems to us that there is little question that cyberattacks are becoming an engrained business risk for enterprises of all sizes, and that includes non-business related organizations as well.

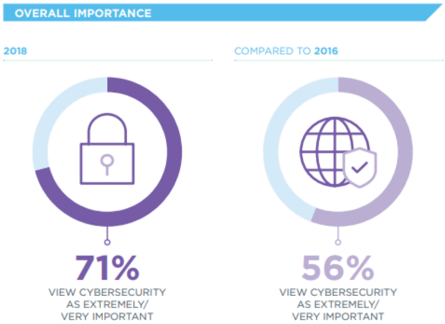
Given the increased risks associated with cyberattacks as well as the considerable costs associated with them, those in charge of protecting the information of their organizations have choices to make with respect to mitigating those risks. In short, they can choose to ignore them and hope they are not attacked, they can purchase insurance specifically for cyberattack claims and/or they can mitigate them through security products, services and protocols like those provided by SDCH. Industry data provide some interesting insights into how middle market players are approaching these choices, but first some definition might be helpful.

Generally middle market companies are defined as those with revenues between $10 million and $1 billion. While there are differing estimates around the number of middle market companies there are in the U.S., according to the Harvard Business Review, Bridging the Gap Between Capital Providers and Midsize Companies (hbr.org) *"There are 350,000 middle-market companies in the United States, accounting for over 33% of U.S. GDP".* We recognize, the revenue thresholds of that definition ($10 million vs. $1 billion) provide some stark contrast between those on each end of the spectrum. To translate, while by definition if SDCH's target market is middle market enterprises, their total addressable market is ostensibly 350,000 businesses. However, some of these (presumably those with higher revenues), may be more viable candidates than others. Regardless, the point is, there are thousands of potential customers for SDCH's products and services, and data suggests a large number of them are likely not adequately addressing cyberattack risks.

National Center for the Middle Market provides a number of reports regarding the status of the "middle market" in the U.S. That's includes specific reports and surveys regarding cybersecurity amongst middle market enterprises. Here are some results from their most recent study, as well as some of our color around that information: National Center for the Middle Market: Leading Middle Market Resource (middlemarketcenter.org) .

Since 2016, the percentage of middle market executives who are focused on cybersecurity issues jumped by 15 points. Leaders of upper middle market firms ($100M-$1B in annual revenue) and those operating in the financial, retail trade, and healthcare industries are the most likely to view cybersecurity as a highly important issue.

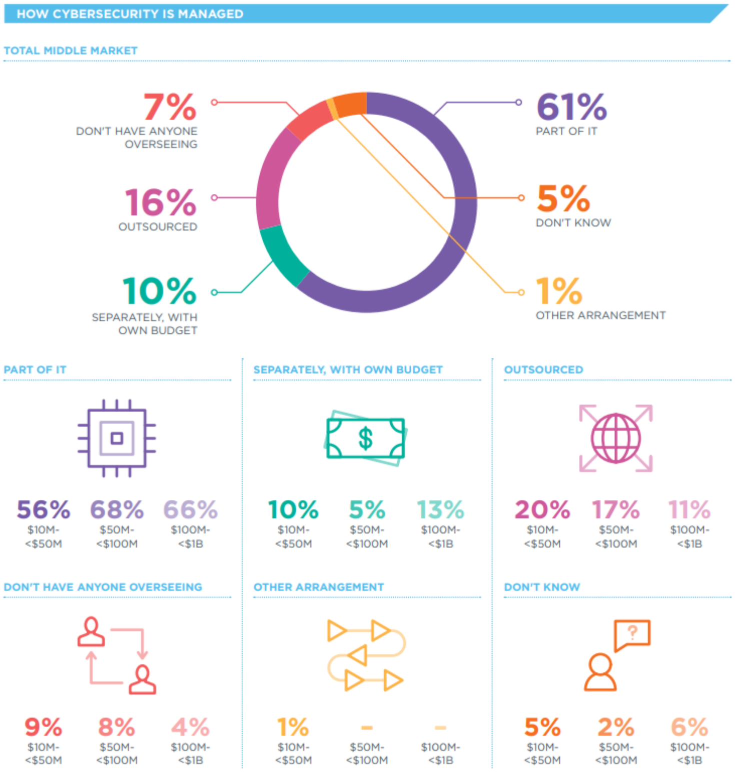
Table 4.



Clearly, cybersecurity is becoming a top-of-mind issue for middle market executives.

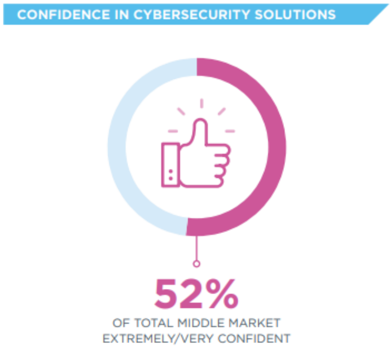
In most middle market businesses, the IT department is responsible for cybersecurity. One out of 10 companies has its own cybersecurity department with a dedicated budget. Lower middle market companies are most likely to outsource cybersecurity, perhaps because they lack the resources or expertise to address it in-house. The lower middle market is also the most likely to leave responsibility for cybersecurity issues unassigned.

Table 5.



We think these graphics/data require some unpacking. First, it is interesting to note that 16% of the respondents outsource their cybersecurity, which is 600 basis points higher than those that deal with cybersecurity solely in-house. Not surprisingly, of those that rely strictly on in-house resources the largest portion is amongst those in the higher end of the middle market (revenues between $100 million and $1 billion). Further, of the outsourced group, the lower end of the market ($10 million to $50 million) was more likely to use a completely outsourced solution than the higher two. We believe that fits our narrative that outsourcing cybersecurity is likely the most cost-effective solution for middle market companies, but that advantage may diminish as enterprises grow.

Table 6.



Some of the other results provide additional insights. For instance, the largest portion of the those surveyed (61%) indicate that they self-manage part of their cybersecurity, and presumably outsource the balance. We assume some of that portion use vCISO services like SDCH's, but we are more inclined to think many of those are still struggling to find the best approach, and or stay ahead of the challenges. That is, we suspect some of these ostensibly 213,500 companies, (61% of 350,000) may yet end up with vCISOs. Table 6. may support that view. As it illustrates, just under half of the respondents have some hesitation regarding their confidence in their cybersecurity efforts.

The most intriguing group is the 7% of respondents that have no one overseeing their cybersecurity, and perhaps worse yet, an additional 5% *who do not know*. To put that into perspective, 12% of 350,000 middle market companies rounds out to about 42,000 companies. For further perspective, and as we will illuminate further in the Operating Overview below, we believe SDCH's breakeven to be around 70 vCISO clients (including additional up sales of Enclave). To translate, in the context of the TAM assumed from the numbers in the survey, SDCH's success does is not predicated on them capturing even a meaningful piece of what we see as the addressable market.

While the above provides a glimpse of the middle market's high-level approaches to addressing cybersecurity today, as we note throughout this report, that endeavor is likely to get more complex and more difficult going forward and for a variety of reasons. As we discuss below, we think emerging technologies are likely to add an increasing number of points of vulnerability for many organizations. Moreover, we also expect various regulatory entities as well as other standards bodies to require additional safeguards that will also add to the complexity. Below are a few brief examples.

As we touched on above, one of the approaches to dealing with cyberattacks is cyber insurance. While it probably goes without saying, there are a few things to note about this approach that bear consideration. First, cyber insurance originated in the 1990's largely as an "add-on" to existing liability coverages. However, since that time, cyber insurance has become, more encompassing, more complex and much more expensive. As a recent Bloomberg article notes: US Cyber Insurance Sharp Price increases, Profit Improvement to Moderate (fitchratings.com) *"US cyber insurance premiums surged 50% in 2022 as increased ransomware attacks and online commerce drove demand for coverage"*. Further, as premiums have increased (along with demand) insurers have markedly increased the security requirements of their insured. Our point here is that cyber insurance is not a substitute for security protocols. In fact, the implementation of ever-increasing cybersecurity standards is becoming paramount to the insurance industry. We would argue that insurance requirements are in turn driving demand for cybersecurity services and products.

Insurance companies are not the only ones weighing in on the need for increased cybersecurity. Recently, the U.S. Department of Defense ("DoD"), upgraded its Cybersecurity Maturity Model Certification (CMMC) program, to what is now referred to as "CMMC 2.0". As the DoD notes, *"CMMC 2.0 will dramatically strengthen the cybersecurity of the defense industrial base. By establishing a more collaborative relationship with industry, these updates will support businesses in adopting the practices they need to thwart cyber threats while minimizing barriers to compliance with DoD requirements. The CMMC program includes cyber protection standards for* *companies in the defense industrial base (DIB). By incorporating cybersecurity standards into acquisition programs, CMMC provides the Department assurance that contractors and subcontractors are meeting DoD's cybersecurity requirements".*

Basically, the DoD requires contractors/vendors handling particular types of data to comply with CMMC 2.0 in order to do business with or other collaborate with the department. In other words, those organizations need to have their own cybersecurity houses in order if they are to deal with the DoD, and the requirements therein are becoming more robust. More specifically, DoD provides the following guidelines for CMMC compliance. Notice, as we will illustrate in the Service/Product Overview below, these coincide with some of the specific functionality of **SDCH's new Enclave platform.** That by the way is not coincidental.

CMMC Implementation (defense.gov)
Five Steps to Make Your Company More Cyber Secure

1. *Educate people on cyber threats. Most cyber incidents start because of user error. Educate people about the importance of setting strong passwords, recognizing malicious links, and installing the latest security patches. Helpful materials and training videos are available through Project Spectrum.*
2. *Implement access controls. Limit information systems access to authorized users and the specific actions that they need to perform.*
3. *Authenticate users. Use multi-factor authentication tools to verify the identities of users, processes and devices.*
4. *Monitor your physical space. Escort visitors and monitor visitor activity, maintain audit logs, and manage physical devices like USB keys.*
5. *Update security protections. Make sure to download the latest security patches when new releases are available. Always double check to make sure they are coming from a trusted source.*

Aside from DoD, the U.S. Security & Exchange Commission ("SEC") also recently adopted new rules around reporting companies' cybersecurity initiatives and associated risk disclosures. Here again, these rules pose added challenges to reporting companies around hardening their data and information assets:

> *The Securities and Exchange Commission ("Commission") is adopting new rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incidents by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934. Specifically, we are adopting amendments to require current disclosure about material cybersecurity incidents. We are also adopting rules requiring periodic disclosures about a registrant's processes to assess, identify, and manage material cybersecurity risks, management's role in assessing and managing material cybersecurity risks, and the board of directors' oversight of cybersecurity risks.*

As one final example, from https://www.nist.gov :

> *The National Institute of Standards and Technology ("NIST") was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical SDCHence laboratories. Congress established the agency to remove a major challenge to U.S. industrial competitiveness at the time — a second-rate measurement infrastructure that lagged behind the capabilities of the United Kingdom, Germany and other economic rivals.*
> *From the smart electric power grid and electronic health records to atomic clocks, advanced nanomaterials and computer chips, innumerable products and services rely in some way on*

> *technology, measurement and standards provided by the National Institute of Standards and Technology.*

Given the above description, it should be no surprise that the NIST has developed a specific standards framework around cybersecurity. The NIST provides the following narrative regarding their activities around cybersecurity:

> *"NIST develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies and the broader public. Our activities range from producing specific information that organizations can put into practice immediately to longer-term research that anticipates advances in technologies and future challenges. Some NIST cybersecurity assignments are defined by federal statutes, executive orders and policies. For example, the Office of Management and Budget (OMB) mandates that all federal agencies implement NIST's cybersecurity standards and guidance for non-national security systems. Our cybersecurity activities also are driven by the needs of U.S. industry and the broader public. We engage vigorously with stakeholders to set priorities and ensure that our resources address the key issues that they face".*
>
> *The NIST Cybersecurity Framework was intended to be a living document that is refined, improved, and evolves over time. These updates help the Framework keep pace with technology and threat trends, integrate lessons learned, and move best practice to common practice. NIST initially produced the Framework in 2014 and updated it in April 2018 with CSF 1.1. Based on stakeholder feedback, in order to reflect the ever-evolving cybersecurity landscape and to help organizations more easily and effectively manage cybersecurity risk, NIST is working on a new, more significant update to the Framework: CSF 2.0.*

In addition to NIST standards, there is another prominent cybersecurity organization that also develops standards, measurement tools and best practice protocols to guide the industry. That organization is called The Center for Internet Security, Inc. ("CIS")

From: http://www.isaca.org/Journal/Past-Issues/2001/Volume-6/Pages/The-Center-for-Internet-Security-Global-Security-Benchmarks-for-Computers-Connected-to-the-Internet.aspx

> *CIS is a not-for-profit organization comprised of large corporations, government agencies, and academic institutions in the U.S as well as internationally. The center's founding partners include ISACA®, The American Institute of Certified Public Accountants (AICPA), The Institute of Internal Auditors (IIA), The International Information Systems Security Certification Consortium (ISC2) and The SANS (System Administration, Networking and Security) Institute.*
>
> *CIS founding partners and members formed the organization in October 2000. Their global consensus process is an effective and cost-efficient method to enumerate user-originated technical security standards and keep them continuously up-to-date.*

As with CMMC Implementation, the Service/Product Overview below also specifically covers some of the ways in which Enclave address new CIS version 8 controls. As a further point to both the CMMC 2.0 and the NIST narrative above, we would refer readers to the Management Overview of this document. Recognize that Company founder and CEO Brian Haugli has "led programs for the DoD, Pentagon, Intelligence Community", which we assume likely included CMMC issues and he is a '*renowned speaker and expert on NIST guidance*".

Service/Product Overview

SDCH offers a handful of services/products that we will cover below. Currently these include:

- vCISO services.
- Other software and integration
- Enclave

- **vCISO**

As we addressed in our opening to this document, the Company's primary business is the provisioning of "virtual" (or "fractional") Chief Information Security Officers, which they refer to as "vCISO". From the 10,000-foot view, outsourcing portions of the C-Suite is not new or novel, and that is especially true amongst middle market and smaller companies. We suspect that most of our readers have encountered a virtual CFO ("vCFO") along the way, so again, the concept of contracting out portions of the C-Suite is not proprietary. Further, we think that is probably most common in roles that are perhaps a bit more technical and perhaps specific in nature (security for instance). That said, we think success with that type of strategy/approach likely hinges on a handful of attributes/advantages that successful players need to bring to the table.

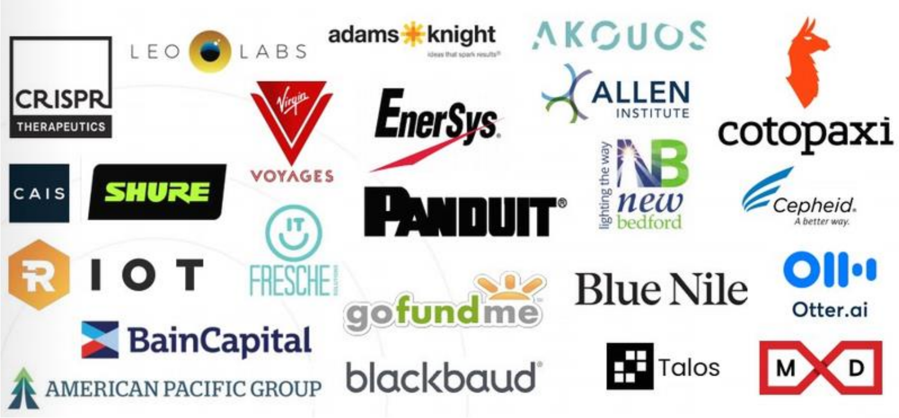
First, from the "10,000-foot view" we think those providing vCISO services must be able to create a platform that is able to attract individuals with the education, experience and credentials necessary to effectively develop and manage the cybersecurity challenges of their customers. We think it is reasonable to suggest *that process* starts with an individual with the same pedigree. Part of our enthusiasm here hinges on our sense that SDCH CEO and founder Brian Haugli fits that profile.

As we illustrate below in the Management Overview, Mr. Haugli is a *"renowned expert on NIST guidance, threat intelligence implementations, and strategic organizational initiatives…".* Succinctly, our sense is that Mr. Haugli's profile within applicable circles in the industry has allowed SDCH to attract 15 to 20 security experts capable of helping multiple clients develop, implement, and maintain effective cyber security protocols. For reference, we would add, most of their current vCISO's have *decades* of cyber security experience. Further, the Company indicates that it has a pipeline of other seasoned security professionals that they believe they can attract either on an employee or a 1099 basis, to address future expansion of their vCISO business. While attracting new customers is an obvious pre-requisite to future growth, having the human capacity to service those clients is also paramount to their success. Again, we view management's collective posture in the industry, as well as the platform it has developed to service clients, as a large part of SDCH's "secret sauce", which we see as a comparative advantage.

To clarify a point we made above (and we reiterated in the Risks & Caveats below), while vCISO services are not proprietary to SDCH, the Company *has* included functionality to the platform that we believe provides some proprietary advantages that are certainly worth pointing out. Over years of development around applicable experiences, the Company's vCISO service is designed around a turnkey platform of policies and technology to assess, track, and push remediations into clients. As a result, they bring to every engagement a standardized methodology that streamlines the evaluation and onboarding process of each client. That alone may provide marked advantages vis-à-vis competitors that may not possess that same standardized approach. Further, SDHC's platform was also built to be scalable to fit both different sized organizations, but also to accommodate the growth of their clients over time. Recognize, the standardization of the platform can provide continuity, collaboration and redundancy amongst and between individual vCISOs. At the same time, the platform was also designed with the flexibility to address the *specific* requisites of particular clients and/or industries, for example HIPAA requirements in the healthcare industry or the NYS DFS ("Part 500") cybersecurity rules in the financial industry.

As a result, while providing vCISOs may not be proprietary on the face, The Company does possess a proprietary system to deliver its vCISO services.

As an extension to the recruitment of qualified vCISOs to deploy into the field, the Company also needs to then identify applicable customers that "fit" their value proposition. As we touched on in the Industry Overview, cybersecurity is an acute risk for many organizations, and that includes both middle market and even smaller enterprises and groups. In fact, those risks are often potentially more catastrophic for smaller enterprises than larger ones. However, inasmuch as many of these entities recognize those risks, they may lack the resources and/or the expertise to implement effective cybersecurity platforms and protocols. As we noted previously around this point, we think SDCH's vCISO solution is focused on both these weaknesses (limited resources and limited cybersecurity aptitudes). By providing, contract/part-time cybersecurity executives, SDCH arms these organizations with the direction and guidance required to implement effective cybersecurity programs, at a fraction of what it might cost them to develop internal organizations to do the same. In that regard, to date the Company has established a base of over 40 customers that include some recognizable names that we think afford them some "reference customer" clout in selling additional customers:



We submit, the Company needs more than 40 vCISO customers to reach profitability (we think that number is closer to 70), however, we also believe that the current customer base provides validation for the business plan. Obviously, their success will depend on their ability to continue to market and attract new customers to the platform. To that end we would add, while we believe the vCISO platform will prove to be quite sticky in terms of retaining clients, we think some churn will be inevitable as certain customers grow into a posture where in-house cyber security processes become more practical. We would add, while we have suggested the Company's target market is the "middle market" ($10 million to $1 billion in revenues), the Company views its market as companies with revenues between $10 *and $5 billion*, and that threshold is reflected in the size of some of their larger clients (closer to $5 billion than to $1 billion). That said, some additional color regarding the on-boarding and maintenance of customers might be helpful.

Recognize, the vCISO revenue model is largely based on the hourly billing of vCISO hours, and we believe that rate blends to something around $350 per hour. However, the required manhours at the front end of an engagement, are typically greater as SDCH assesses the posture of a new client and then develops the required protocols/platform to initiate an effective cybersecurity strategy. As we understand it, the ongoing vCISO requirements for an average costumer beyond the startup phase is approximately 1 day per week. The onboarding/setup portion of the engagement generally includes the acquisition and integration of other 3rd party software and/or systems as well, which brings us to SDCH's second revenue source.

- **Cybersecurity Software and Services**

As we alluded to above, part of the Company's vCISO onboarding process is identifying 3rd party software/services that the client may need to complete their security protocols. In that regard, along with vCISO revenues, SDCH also has value added reseller ("VAR") arrangements with other cybersecurity providers. As a result, the Company recognizes significant revenues through these VAR arrangements. Specifically, for the 9 months ended June 30, 2023, SDCH recognized revenues of $4.9 million of which $1.7 million or 34.3% was for "Cybersecurity Software and Services". From our perspective, the Company's vCISO platform provides synergies through its VAR endeavors that's we think are worth noting. That is, in SDCH's VAR capacity, they recommend mixes of security products and services to their vCISO clients that the believe best fit the clients' needs, which provides them a VAR revenue stream, but in some cases they have reciprocal VAR relationships whereby those cybersecurity vendors provide SDCH with leads for their vCISO platform. That sort of symbiotic approach extends to their vCISO recruiting as well. For instance, as we understand it, one of their better referral sources are job recruiting agencies that have enterprises looking to fill CISO positions. In some cases, those enterprises realize that they may not be ready for full time CISOs in which cases the agencies send those leads to SDCH. In turn, when SDCH clients grow into the in-house cybersecurity model (and out of the vCISO approach), SDCH can in turn steer their clients to those agencies for potential fulltime CISOs. Again, we think the Company is developing (and monetizing) an elegant ecosystem around its vCISO platform.

- **Enclave**

Enclave is the Company's new cybersecurity platform. It is software driven and it is aimed at solving some of the pain points and weaknesses the Company has identified in legacy systems and approaches after years of evaluation and implementation. In addition, it was also developed to address compliance with the NIST and CIS standards we noted in the Industry Overview above. Recognize, that much like cybersecurity threats around us, the NIST compliance/standards framework is always evolving to stay in front of those threats. Enclave was developed in part to address that evolution as well.

As we noted in the opening of this report, we are not experts in cybersecurity, so we certainly do not understand the minutia of the technology and process used to combat it. As a result, we will defer to the Company's description of Enclave, but we will provide some of our own perspectives that may clarify how some of these issues fit together and what Enclave is designed to address.

> *Enclave, is a SideChannel proprietary software product. **It was developed around SDCH's unique insight into mid-market and emerging companies**. Additionally, CIS version 8 controls call for organizations to:*
>
> - *Control 1 - "Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data",*
> - *Control 2 - "Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution."*
> - *Control 3 - "Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications."*
>
> *We built Enclave to address these extremely critical cybersecurity controls along with many others. Enclave seamlessly combines access control, microsegmentation, encryption and other secure*

networking concepts to create and comprehensive solution. It allows Information Technology (IT) to easily segment the enterprise network, place the right staff in those segments and direct traffic. Unlike open, traditional models, Enclave allows for near-limitless micro-segmented networks to operate insulated from one another.

Enclave provides:

- ***Simplified Security Operations** - Simple, fast, no training required. Deploy in minutes and configure in seconds.*
- ***Enhanced Resilience** - Gain confidence that only authorized systems, people and data are interacting at any time.*
- ***Capacity to Scale and Deploy** - Deploy and scale across virtual machines, Kubernetes containers, on premises, or in the cloud.*
- ***Real-time Visibility of Network Flows** - Visualize application dependencies without the need for any knowledge of the underlying architecture.*
- ***Monitoring & Reporting** - Enclave stores flow records with workload context, enabling network and security teams to use this data for compliance reports.*
- ***Stronger Security** - Easily deployable end-to-end encryption protects data in transit.*
- ***Scalable Solution** - As your environment scales, Enclave will adapt automatically – on premises or in the public cloud.*

Here is a bit of color from our perspective regarding the "CIS version 8 controls" referenced above*:*

Control 1 - "Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data".

While this seems straightforward, it is a challenge for many organizations, especially those without a robust cybersecurity strategy. Consider, every new device added to a network (cell phones, computers, laptops, printers etc.) all represent points of vulnerability for threat actors. Clearly, the most basic part of making sure these assets are properly protected, is a protocol/platform that identifies and recognizes them in the first place.

We suspect many investors are familiar with emerging technologies like artificial intelligence ("AI"), 5G, the internet-of-things ("IOT"), edge computing and other applications. While all these technologies and associated products provide their own advantages, they also come with challenges. For instance, edge computing processes data via devices at the "edge" of the network. The advantages of edge computing include reducing the traffic across a network by allowing devices at the edge to store and process applicable data thereby reducing data transfers to/from larger data centers. While that approach may reduce latency and improve data center efficiency it also adds an exponential number of points of network vulnerability. Recognize, edge computing devices include the usual suspects like smart phones, laptops, tablet etc. but also things like sensors, smart cameras, autonomous cars, and a multitude of others. As we see it, the convergence of emerging technologies may considerably increase the number of assets (re: points of vulnerability) that enterprises will need to harden and protect against cyber-attacks.

Control 2 - "Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution."

This is an issue that most consumers have likely encountered. Specifically, the operating systems, software and applications that drive our devices, require periodic updates and/or patches that install improvements (or added cyber security upgrades) to keep them current. For an enterprise, it is paramount that these upgrades be made *across their respective network(s).* For instance, if Microsoft provides a patch that users need to download to counter a new threat, but the enterprise has no means of determining if all the assets on the network have downloaded the patch, that leaves some obvious vulnerabilities.

From another perspective, there may be popular applications across social media that organizations may not want on their networks. Enterprises and organizations forbidding the use of TikTok on their networks over security concerns is just one example. While security concerns may be the primary reason the network administrators need to manage what is allowed on their networks, productivity and inappropriate content are on the list of others. The point is, effective security platforms and protocols need to be able to "actively manage" third party applications. By the way, this approach encompasses the term "zero trust" in cyber security vernacular.

Control 3 - "Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications."

This issue encompasses the "microsegmentation" piece that is referenced throughout this report. In short, microsegmentation involves separating the network into relevant buckets and isolating and/or limiting their access to one another on an ongoing basis. Further, microsegmentation allows administrators to quarantine breaches in particular segments so they cannot spread to others. As a (simple) example, people in marketing may be segmented versus those in accounting, whereby a user in one may be prohibited from accessing data in another. While this is the "10,000 foot view" of microsegmentation, as one might imagine the process is quite complex. Among other things, Enclave provides a turnkey and scalable microsegmentation choice for those trying to protect their networks.

To summarize, the Company has built an impressive (initial) list of vCISO customers, some of which we believe serve as reference customers for their ongoing sales processes. They have demonstrated that they can implement and maintain viable cybersecurity protocols through their vCISO platform. We think they have also laid the appropriate groundwork to scale the platform by adding both vCISO professional and vCISO clients.

As we covered, adding vCISO clients in turn drives their Cybersecurity Software and Services revenues as well, as each client requires combinations of available 3rd party software and services to execute the cybersecurity strategies designed by SDCH and their respective vCISOs. As VARs for many of these products and services, SDCH benefits additionally through the implantation of these offerings.

Lastly, Enclave represents the Company's entry into the software side of the cybersecurity business. The Company has announced that it has closed its first two Enclave customers, and they are actively marketing the platform. We believe, and we think the Company will validate, that the existing vCISO customer base will provide SDCH with a promising upsell opportunity for Enclave. Further, we would expect the Company to continue to try to upsell new vCISO clients as well. In addition, if we understand the opportunity correctly, it appears to us that there may be a considerable market for Enclave amongst customers that may not be in the market for vCISO services. Succinctly, we think the addition of Enclave will at least provide a new revenue segment, but perhaps more importantly, it may create some cross selling or other marketing opportunities to/from the vCISO business as well. In short, we see the recent commercialization of Enclave as milestone for the SDCH.

Operating Overview

As we covered, SDCH currently has two primary revenue streams: vCISO Services and Cybersecurity Software & Services. Further, they recently commercially launched their new cybersecurity platform Enclave, which we expect to ultimately be reflected as a separate line item as well. vCISO revenues are generated largely as an hourly rate for the time each vCISO spends with each client. We believe that rate is in the $350 to $400 per hour range, the typical client will require the equivalent of about 1 workday per week. Ostensibly, that math works out to something considerably less than keeping a full time CISO. (From another angle, that math suggests that SDCH requires one vCISO for every 5 clients, although we would submit that some clients may be more “typical” than others, requiring more or less hours than the average).

Cybersecurity Software & Services revenues represent reseller fees/commissions the Company earns from arrangements they have with the vendors they purchase and deploy products and services from to complete the cybersecurity platforms of their clients.

As we also noted above, Enclave is the Company’s newly released comprehensive cybersecurity software suite/platform. We believe this represents a new valuation leg for the Company, and it is the basis for a meaningful portion of our estimates around the Company’s future growth. SDCH utilizes a SaaS model to monetize Enclave sales. That is, Enclave revenues are predominantly generated via a monthly fee based on each user. While some users may deploy Enclave differently than others, we assume that in most instances, each employee will have a license, as well as perhaps additional assets around the organization and we are currently modeling a fee of $15 per month per license. We submit, the Company is very early in the commercialization of Enclave, and actual license fees will likely vary based on a variety of inputs, number of licenses, the deployment of part versus all the functionality of Enclave and a host of others. As with much of our current SDCH modeling, we expect (currently limited) visibility to improve as the Enclave sales process matures.

We expect vCISO revenues to (continue to) represent approximately 2X those of Cybersecurity Software & Services. However, over the next several years, we project that Enclave sales may ultimately make up 25% of total revenues, in which case we think vCISO sales will make up about 50% of revenues, with Software & Services making up the balance.

We believe that historically, vCISO COGS have approximated 50% while Software & Services have approximated 65% to 70% of sales. Our model assumes similar margins on an ongoing basis. However, we expect Encore gross margins to be around 80%, in line with typical software margins. Obviously, we are in the first inning of Encore, so we will need additional data points to verify that assessment.

Currently, the Company’s operating expenses are approximately $500,000 per month or around $1.5 million per quarter. While we anticipate SG&A increasing with revenues, we believe there is marked operating leverage in the business. We think that will be especially stark if Enclave revenues ramp as we are projecting. As we alluded to above, when we believe the Company can achieve operating breakeven at something around 70 vCISO clients, although that also includes some relatively modest Enclave revenues. We are ultimately modeling a 50% upsell rate (Enclave to vCISO clients). We submit, we have little visibility to that end at this point, however, we do not believe that is within the boundaries of the Company’s expectations. We would add, while we have modeled Enclave sales as a percentage of vCISO clients (the upsell ratio), we actually think they will likely make Enclave sales outside of their vCISO base, so in that case the upsell rate will be less aggressive than our 50% assumption. Again, we have little visibility to that end at this point, but we expect that to improve going forward, which should help us tighten our assumptions.

As we covered above, the SideChannel business was merged into a public vehicle (Cipherloc) in mid-2022. That combination resulted in the SideChannel shareholders being issued approximately 40% of the NewCo, with an additional share earnout (roughly 60 million additional shares) upon the achievement of $5.5 million in revenues. They eclipsed that threshold in the 2QF23 quarter resulting a marked increase in share count. As of 06/30/23 the shares outstanding were 212,765,780. At 06/30/23 the Company had working capital of approximately $1.5 million. Our modeling suggests they will need additional capital to get to cash breakeven and beyond, and if our model proves aggressive that likely dilution could be more acute than we are assuming. On the other hand, we think the current burn rate in the context of our anticipated path forward is manageable, which means that we think they can keep future dilution to a minimum. We have worked that assumption into our model, reflecting that further dilution.

Lastly, as adjunct to the burn rate/profitability narrative, we believe that pre-merger, SideChannel was a comfortably profitable enterprise, and much of the fiscal 2023 burn is (was) related to their (new) public posture, some of the costs associated with the combination as well as some added overhead layers from the combination. Some of these may be eliminated going forward, but it is not clear to us at this point how/if that may unfold. While we think we may be overstating *some* overhead in that regard, we feel like selling and marketing efforts around vCISO and perhaps especially Enclave.

To reiterate, we submit that our operating projections lack visibility, but we expect that to improve as we move forward, and we will assess those new data points as they arise.

Management Overview

Brian Haugli – CEO

Brian has been driving security programs for two decades and brings a true practitioner's approach to the industry. He creates a more realistic way to address information security and data protection issues for organizations. He has led programs for the DoD, Pentagon, Intelligence Community, Fortune 500, and many others. Brian is a renowned speaker and expert on NIST guidance, threat intelligence implementations, and strategic organizational initiatives.

Brian is the contributing author for the latest book from Wiley, "Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework".

Lastly, he is a professor at Boston College, in the Woods College of Advancing Studies, Master's Program in Cybersecurity.

Nick Hnatiw – CTO

Nick has more than 15 years of experience creating technologies spanning network security to artificial intelligence and robotics. He has served as the founder, majority owner and CEO of a network security firm and as a technical director within US Cyber Command. As CTO, Nick is responsible for the creation of repeatable processes and to drive the technical direction of the technologies.

Joe Klein – EVP, Service Delivery

Joe Klein is a cybersecurity executive with 20+ years of experience working to improve the overall security posture of organizations and ensure the confidentiality, integrity, and availability of IT infrastructure. Seasoned at serving as a trusted advisor to senior executives, Mr. Klein is skilled at assessing cybersecurity maturity, long-term strategic planning, security product evaluations, project management, incident response planning (IRP), data protection, identity & access management, and security awareness training.

He has previously served as CISO for the financial technology SasS company, Billtrust, as well as the industrial battery manufacturing firm, EnerSys.

Mr. Klein has earned a Master's Degree in Cybersecurity from the University of Delaware, a Masters Degree in Information Systems from Drexel University and holds both CISSP and PMP certifications.

David Chasteen - EVP, Chief Operating Officer

David has been a leader and communicator in national security and information security for two decades, with a particular focus on NIST framework, critical infrastructure security and advanced threat intelligence. He has built best-in-class, collaborative programs at local, federal and nonprofit institutions and has a passion for community service, change leadership and fostering inclusive organizational cultures.

David was most recently the CISO for the San Francisco Police Department and previously served as the Executive Officer of the CIA's Covert Action Staff, a CTO at L-3 MPRI and a founding member of Iraq and Afghanistan Veterans of America. He was technical consultant for Amazon's Jack Ryan.

Ryan Polk - Chief Financial Officer

Ryan brings over 10 years of responsibility for full p&l ownership and 15+ years of international business experience to SideChannel. He has delivered growth, integration, and turnaround results to founder-owners, private equity firms, and public companies with revenues between $80M to $4B.

He identifies new business insights by analyzing transaction details and motivates his peers and employees to use the insights to deliver greater results. Starting with an analytical and finance platform, Ryan built a well-rounded skill set by adding strategic planning and employee engagement.

Ryan earned his BS from Purdue and commits his spare time to a number of volunteer causes improving the health, intellect and life outcomes of elementary and middle school-aged children.

Risks And Caveats

To reiterate a few points from above, we believe the value proposition of vCISOs, especially among middle market enterprises and perhaps other "midsized" organizations is demonstrable. We also believe that SDCH's notable customer base provides validation for the notion that they have developed a commercial platform to deploy, maintain and monetize their service. However, as we covered, there is nothing acutely proprietary about providing vCISO services, and as such, our research came across what look to us like a variety of competitors. In that regard, we expect them to face marked competitive pressures which could limit their opportunities as well as their pricing power and margin contribution. We submit, we were not able to identify large and/or ostensibly dominant vCISO providers (although there still may be), and we do not discount the Company's notion that they may have some competitive advantages over at least some of those competitors. Moreover, we would add, the Company believes they are the largest vCISO provider in North America. That said, they are certainly not the only ones offering the service.

While the vCISO services may represent a small portion of the multibillion-dollar cybersecurity industry, the software segment of that market is large and loaded with competitors that have far greater resources and a well-established presence in the marketplace. To be clear, it is difficult to ascertain which companies and products actually compete with (as opposed to perhaps compliment) one another, but we are comfortable suggesting that Enclave faces a myriad of competitive challenges. That may be particularly disconcerting in the context of our notion that a meaningful portion of our growth assumptions are based on Enclave success.

The Company is not profitable and as a result has had to rely on the capital markets to fund its deficits. As a result, they will likely have to continue accessing the capital markets and diluting the shares perhaps beyond what we have modeled. Moreover, there is no guarantee that they will be able to continue to access capital with equity in the future. We would add, because revenue visibility is limited, our model and resulting price target assumptions could end up being considerably overstated. Further, we believe this issue is currently the "elephant in the room" with respect to the valuation of SideChannel and here is some much-needed color to that.

In April 2021, (prior to the merger with SideChannel) Cipherloc completed a financing that included 55 million warrants. In short, the warrants are exercisable at $.18 through April 2026. However, those warrants include a ratchet provision whereby if the Company did/does a subsequent equity raise, the warrants reset to a value commensurate with the subsequent offering price (among some other adjustments). Succinctly, those ratchet provisions are considerably onerous. In response, the Company has proposed a warrant tender/exchange to replace these warrants with a combination of stock and new warrants. It remains to be seen if/when they will be able to get ALL of the warrant holders to agree to that exchange. *As we understand it*, there are a few ways this could play out.

1) The warrant holders could agree to the exchange, in which case the Company will issue something around 10 million shares (exact amounts to be determined) and a new batch of $.18 warrants without the ratchet. This would allow the Company to engage additional equity financings without the draconian ratchet provisions blowing up the cap table. Without this concession, we believe the Company will do everything in its power to avoid triggering the ratchet (raising new capital), which could impact their ability to grow the business and that may include growing the existing footprint as well as perhaps funding other accretive acquisitions. To be clear, our initial model, and by extension our price targets are based on this scenario (restructuring of the warrants). **Recognize, if this does not occur, our model and target will likely prove aggressive.**

2) The Company could attempt to get cash burn to neutral as quickly as possible and to avert an equity raise until the warrants expire in April 2026. We believe the Company has and will likely continue to manage expenses to that end, anticipating the potential for them to be unable to reach an agreement with the warrant holders. We have modeled this contingency as well, which we believe will include lower revenue and future earnings projections as they dial back selling efforts and other expenses to match revenues. For reference, if we assume this is the scenario that occurs, our model will reflect a lower price target from $.18 to $.10.

3) The worst-case scenario is that the Company decides to engage in an equity raise and accept considerable dilution from the outstanding ratchet warrants. We have modeled this iteration as well. Again for reference, in this scenario our model reflects a price targets of $.04, or roughly where the stock is trading now.

Currently, the Company relies on a small number of people to operate the business. That posture carries obvious risks with respect to the performance and continued employment of those individuals.

We argued throughout this report that cybersecurity is becoming an increasingly relevant and recognized business risk. As such we expect enterprises and other organizations to continue to seek ways to mitigate those risks. While the urgency of that pursuit may provide some cover from a deteriorating economic backdrop, we do not expect it to insulate it completely. Put another way, we would expect a waning economic environment to have a negative impact on SDCH.

The Company's stock is thinly traded, which generally leads to volatile share prices and illiquidity. That may remain the case into the foreseeable future.

These are just some of the more obvious risks we see in the Company. There are likely others we have overlooked as well as others that may arise in the future.

Summary and Conclusion

To summarize our collective thesis above, from the macro view cyberattack risks have been increasing for some time now, which is why the global cybersecurity market is between $150 billion and $200 billion. Most cyberattacks are perpetrated by organized crime, which probably explains the breadth of the problem and suggests that it will likely get worse before it gets better. Surprisingly, cyberattacks are not limited to large governments, enterprises, organizations or infrastructure operators. On the contrary, industry research suggests that small businesses are three times more likely to be targeted by cybercriminals than larger companies. More acutely, estimates also reflect that cyberattacks of small businesses are fatal more times than they are not.

As a result of the increasing business risks associated with cyberattacks, companies large and small are searching for solutions to protect themselves. Unfortunately, that process requires personnel and protocols that challenge the resources that many of these enterprises can commit to those ends. Succinctly, when it comes to cybersecurity, it is difficult for them to afford it, but they cannot afford to be without it. That is not a good problem to have. To make that problem worse, several organizations, government agencies and others have created cybersecurity standards and thresholds that require those within their purview to adopt. That may mean vendors, members, or for instance, in the case of the Security and Exchange Commission, public filers. Consequently, enterprises under those purviews may not be able to make choices about when and what they adopt to address their own cybersecurity protocols. As an extension, many businesses have historically chosen insurance to address some of these risks. However, as cybersecurity insurance has evolved (and become much more expensive), providers have also required that their insured adopt appropriate measures to mitigate cyberattacks. In short, outside of simply rolling the dice and doing nothing, companies are left with little choice but to commit increasing resources to cybersecurity.

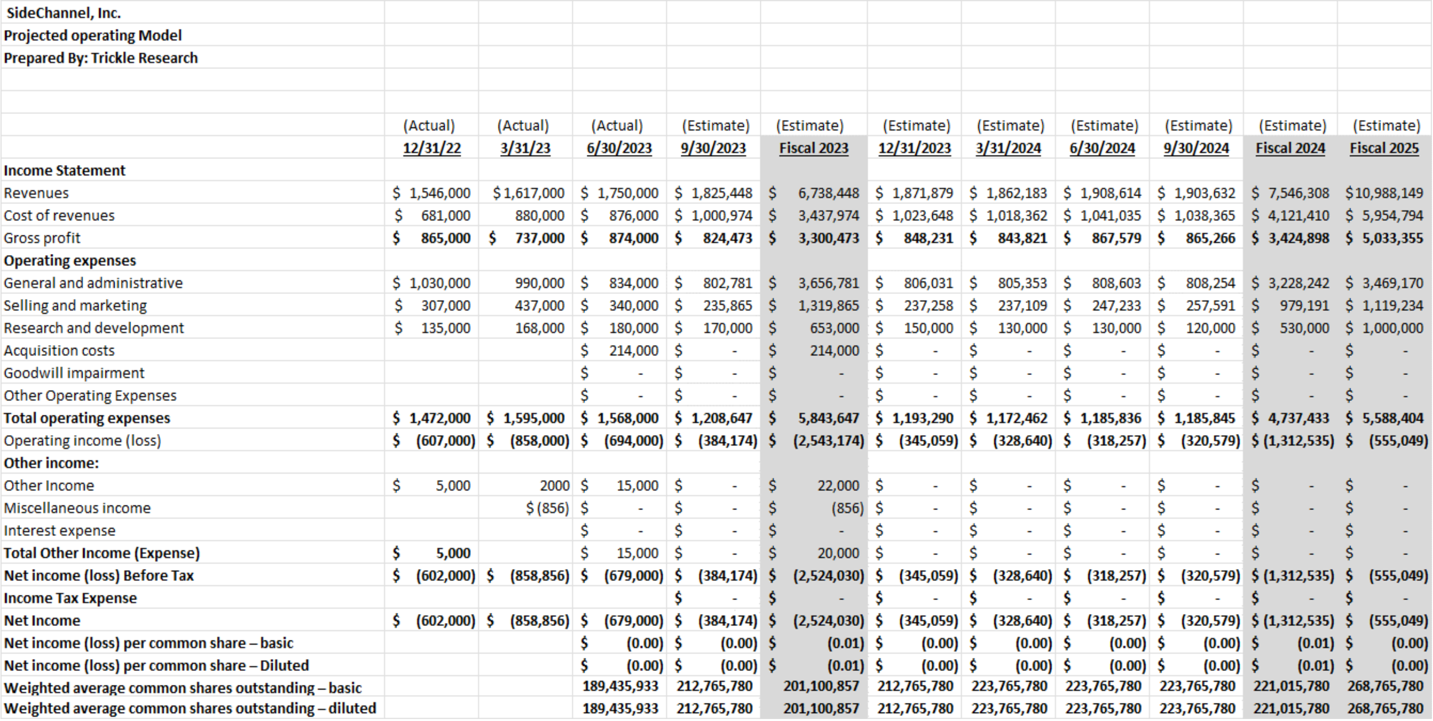
In response to those challenges, SDCH has developed a virtual Chief Information Security Officer platform (vCISO) that at a high level, provides qualified Chief Information Security Officer on a part time and/or as needed ("virtual") basis. This provides their clients with a cost-effective approach to the benefits of a dedicated CISO. However, beyond the personnel, SDCH's vCISO platform also provides a standardized methodology that streamlines the client evaluation and onboarding process and provides continuity, collaboration and redundancy amongst and between individual vCISOs. At the same time, the platform was also designed with the flexibility to address the *specific* requisites of particular clients and/or industries, for example HIPAA requirements in the healthcare industry or the NYS DFS ("Part 500") cybersecurity rules in the financial industry. The vCISO platform affords SDCH clients with the benefits of a vCISO (including the development of applicable cybersecurity protocols) at a fraction of the costs typically associated with employing a fulltime CISO and/or internal cybersecurity team. As a segment (before contributions to public corporate overhead) we believe their vCISO operations are profitable. More granularly, they currently have approximately 40 vCISO clients, and we see them achieving all-in profitability somewhere around 70 clients.

Beyond vCISO billings, the Company also earns reseller fees for the third-party software and services they recommend and implement for their clients. We are modeling these fees to approximate 50% of vCISO revenues on an ongoing basis.

In addition to the two legacy revenue streams, the Company recently released a cybersecurity software platform that they refer to as "Enclave". Enclave provides "*mid-market and emerging companies the means to simplify several crucial cybersecurity infrastructure procedures, including encryption, microsegmentation and access control".* Enclave will be sold via a typical SaaS approach whereby customers will pay a monthly fee based on each user and/or appliance. We believe these fees will garner fourth quartile software margins. Since they just recently commercialized the platform, we submit we do not have good visibility with respect to the sales cycle of the product. However, we believe (and are modeling) that they will have a successful upsell opportunity for Enclave into the existing and future vCISO base, as well as perhaps to other non-vCISO clients. Despite the poor current visibility, we anticipate Enclave will become an increasing contributor to revenue and future growth, and our targets are based in part on that assessment.

While we submit, SDCH has some remaining challenges and will continue to face competitive pressures across the company, we believe they are positioned to grow the business through profitability and ultimately to levels that will support valuations of multiples to the current market capitalization. As a result, we are initiating coverage of SideChannel, Inc. with an allocation of 4 and a 12-24 month target of $.18 per share. However, we would refer readers back to the Risks & Caveats section of this document for potential iterations around this target. Further, we will revisit these as business visibility as well as visibility around their efforts to restructure outstanding warrants unfold.

Projected Operating Model



SideChannel, Inc.											
Projected operating Model											
Prepared By: Trickle Research											
	(Actual)	(Actual)	(Actual)	(Estimate)	(Estimate)	(Estimate)	(Estimate)	(Estimate)	(Estimate)	(Estimate)	(Estimate)
	12/31/22	3/31/23	6/30/2023	9/30/2023	Fiscal 2023	12/31/2023	3/31/2024	6/30/2024	9/30/2024	Fiscal 2024	Fiscal 2025
Income Statement											
Revenues	$ 1,546,000	$ 1,617,000	$ 1,750,000	$ 1,825,448	$ 6,738,448	$ 1,871,879	$ 1,862,183	$ 1,908,614	$ 1,903,632	$ 7,546,308	$10,988,149
Cost of revenues	$ 681,000	880,000	$ 876,000	$ 1,000,974	$ 3,437,974	$ 1,023,648	$ 1,018,362	$ 1,041,035	$ 1,038,365	$ 4,121,410	$ 5,954,794
Gross profit	**$ 865,000**	**$ 737,000**	**$ 874,000**	**$ 824,473**	**$ 3,300,473**	**$ 848,231**	**$ 843,821**	**$ 867,579**	**$ 865,266**	**$ 3,424,898**	**$ 5,033,355**
Operating expenses											
General and administrative	$ 1,030,000	990,000	$ 834,000	$ 802,781	$ 3,656,781	$ 806,031	$ 805,353	$ 808,603	$ 808,254	$ 3,228,242	$ 3,469,170
Selling and marketing	$ 307,000	437,000	$ 340,000	$ 235,865	$ 1,319,865	$ 237,258	$ 237,109	$ 247,233	$ 257,591	$ 979,191	$ 1,119,234
Research and development	$ 135,000	168,000	$ 180,000	$ 170,000	$ 653,000	$ 150,000	$ 130,000	$ 130,000	$ 120,000	$ 530,000	$ 1,000,000
Acquisition costs			$ 214,000	$ -	$ 214,000	$ -	$ -	$ -	$ -	$ -	$ -
Goodwill impairment			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Other Operating Expenses			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total operating expenses	**$ 1,472,000**	**$ 1,595,000**	**$ 1,568,000**	**$ 1,208,647**	**$ 5,843,647**	**$ 1,193,290**	**$ 1,172,462**	**$ 1,185,836**	**$ 1,185,845**	**$ 4,737,433**	**$ 5,588,404**
Operating income (loss)	**$ (607,000)**	**$ (858,000)**	**$ (694,000)**	**$ (384,174)**	**$ (2,543,174)**	**$ (345,059)**	**$ (328,640)**	**$ (318,257)**	**$ (320,579)**	**$ (1,312,535)**	**$ (555,049)**
Other income:											
Other Income	$ 5,000	2000	$ 15,000	$ -	$ 22,000	$ -	$ -	$ -	$ -	$ -	$ -
Miscellaneous income		$ (856)	$ -	$ -	$ (856)	$ -	$ -	$ -	$ -	$ -	$ -
Interest expense			$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total Other Income (Expense)	**$ 5,000**		$ 15,000	$ -	$ 20,000	$ -	$ -	$ -	$ -	$ -	$ -
Net income (loss) Before Tax	**$ (602,000)**	**$ (858,856)**	**$ (679,000)**	**$ (384,174)**	**$ (2,524,030)**	**$ (345,059)**	**$ (328,640)**	**$ (318,257)**	**$ (320,579)**	**$ (1,312,535)**	**$ (555,049)**
Income Tax Expense				**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Net Income	**$ (602,000)**	**$ (858,856)**	**$ (679,000)**	**$ (384,174)**	**$ (2,524,030)**	**$ (345,059)**	**$ (328,640)**	**$ (318,257)**	**$ (320,579)**	**$ (1,312,535)**	**$ (555,049)**
Net income (loss) per common share – basic			**$ (0.00)**	**$ (0.00)**	**$ (0.01)**	**$ (0.00)**	**$ (0.00)**	**$ (0.00)**	**$ (0.00)**	**$ (0.01)**	**$ (0.00)**
Net income (loss) per common share – Diluted			**$ (0.00)**	**$ (0.00)**	**$ (0.01)**	**$ (0.00)**	**$ (0.00)**	**$ (0.00)**	**$ (0.00)**	**$ (0.01)**	**$ (0.00)**
Weighted average common shares outstanding – basic			**189,435,933**	**212,765,780**	**201,100,857**	**212,765,780**	**223,765,780**	**223,765,780**	**223,765,780**	**221,015,780**	**268,765,780**
Weighted average common shares outstanding – diluted			**189,435,933**	**212,765,780**	**201,100,857**	**212,765,780**	**223,765,780**	**223,765,780**	**223,765,780**	**221,015,780**	**268,765,780**

General Disclaimer:

Trickle Research LLC produces and publishes independent research, due diligence and analysis for the benefit of it investor base. Our publications are for information purposes only. Readers should review all available information on any company mentioned in our reports or updates, including, but not limited to, the company's annual report, quarterly report, press releases, as well as other regulatory filings. Trickle Research is not registered as a securities broker-dealer or an investment advisor either with the U.S. Securities and Exchange Commission or with any state securities regulatory authority. Readers should consult with their own independent tax, business and financial advisors with respect to any reported company. Trickle Research and/or its officers, investors and employees, and/or members of their families may have long/short positions in the securities mentioned in our research and analysis and may make purchases and/or sales for their own account of those securities. David Lavigne does not own shares of SideChannel, Inc.

Trickle Research co-sponsors two microcap conferences each year. Trickle Research encourages its coverage companies to present at those conferences and Trickle charges them a fee to do so. Companies are under no obligation to present at these conferences. Sow Good has paid fees to present at past Trickle co-sponsored conferences and we will encourage them to do so in the future.

Portions of this publication excerpted from company filings or other sources are noted in *italics* and referenced throughout the report.

Rating System Overview:

There are no letters in the rating system (Buy, Sell Hold), only numbers. The numbers range from 1 to 10, with 1 representing 1 "investment unit" (for my performance purposes, 1 "investment unit" equals $250) and 10 representing 10 investment units or $2,500. Obviously, a rating of 10 would suggest that I favor the stock (at respective/current levels) more than a stock with a rating of 1. As a guideline, here is a suggestion on how to use the allocation system.

Our belief at Trickle is that the best way to participate in the micro-cap/small cap space is by employing a diversified strategy. In simple terms, that means you are generally best off owning a number of issues rather than just two or three. To that point, our goal is to have at least 20 companies under coverage at any point in time, so let's use that as a guideline. Hypothetically, if you think you would like to commit $25,000 to buying micro-cap stocks, that would assume an investment of $1000 per stock (using the diversification approach we just mentioned, and the 20-stock coverage list we suggested and leaving some room to add to positions around allocation upgrades. We generally start initial coverage stocks with an allocation of 4. Thus, at $1000 invested per stock and a typical starting allocation of 4, your "investment unit" would be the same $250 we used in the example above. Thus, if we initiate a stock at a 4, you might consider putting $1000 into the position ($250 * 4). If we later raise the allocation to 6, you might consider adding two additional units or $500 to the position. If we then reduce the allocation from 6 to 4 you might consider selling whatever number of shares you purchased with 2 of the original 4 investment units. Again, this is just a suggestion as to how you might be able to use the allocation system to manage your portfolio.

For those attached to more traditional rating systems (Buy, Sell, Hold) we would submit the following guidelines.

A Trickle rating of 1 thru 3 would best correspond to a "Hold" although we would caution that a rating in that range should not assume that the stock is necessarily riskier than a stock with a higher rating. It may carry a lower rating because the stock is trading closer to a price target we are unwilling to raise at that point. This by the way applies to all of our ratings.

A Trickle rating of 4 thru 6 might best (although not perfectly) correspond to a standard "Buy" rating.

A Trickle rating of 7 thru 10 would best correspond to a "Strong Buy" however, ratings at the higher end of that range would indicate something that we deem as quite extraordinary..... an "Extreme Buy" if you will. You will not see a lot of these.