SOUNDVIEW RESEARCH

VISCOUNT SYSTEMS (VSYS - $0.06)

THE IT BRIDGE TO PHYSICAL SECURITY

KRIS TUTTLE & STEPHEN WAITE – OCTOBER 11, 2012

INVESTMENT SUMMARY

Viscount Systems has launched a suite of new IP-based products that are changing the game in the physical security business, particularly building access control and management. The existing expensive, proprietary "stove-piped" industry is flipping over to modern technology. These systems are being merged with IT-based security tools and methods that leverage existing databases like Microsoft Active Directory. Investors have seen this before with telephony and more recently with video.

Viscount is the only public investment vehicle in this space and has the potential to reward investors with more than 4x returns from current levels given our base case intrinsic value (IV)[1] estimate of $0.26. If the company ramps the business as planned our IV for 2012/2013 increases to $0.84. There are some additional key factors to consider:

- A combination of acute need to comply with regulations **and** intense pressure on costs is forcing enterprises to upgrade their existing access control approach and embrace open, modern technologies to lower costs and improve effectiveness.
- Organizations have invested billions in IT-based identity management and logical access security. It's dawning on everyone that physical access control should be managed in the same way as an extension of these systems to eliminate the duplication of cost and effort.
- Viscount Systems has developed their "Freedom" product line into a unique and effective software solution that allows enterprises to manage identity and access management in one place and eliminate the need for expensive proprietary infrastructure.
- Viscount has substantially upgraded their company capability over the last 18 months – expanding their board of directors and advisors, opening their first field office in Washington D.C., and putting the required sales and marketing team in place.
- In the next few quarters Viscount will continue to add new revenues from the Freedom line to their existing core of business in advanced intercom systems. This will enable the company to demonstrate accelerating revenue growth and expanding operating margins.
- Our IV models suggest a current share price of $0.10, an early 2013 value of $0.26 and values as high as $0.84 based on a more optimistic case. Both models are included in the report.

This report goes into greater detail regarding the problems, market, solutions, and competition.

[1] Intrinsic Value is our own proprietary and proven method for valuing companies with profitable high-growth opportunities that stretch over several years. Our IV allows investors to "see through" routine variations in business results and market sentiment.

VISCOUNT SYSTEMS "FREEDOM"

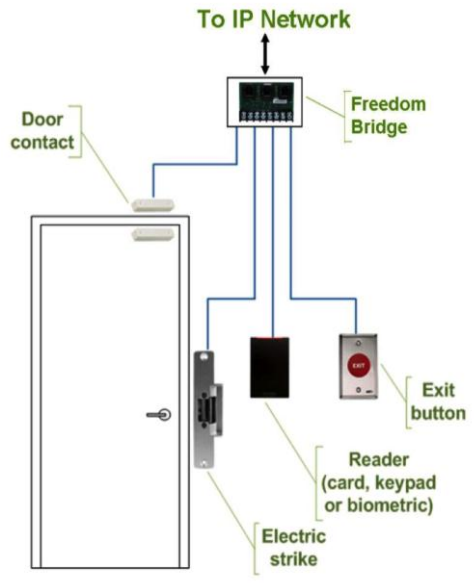
Viscount has organized the company around three main lines of business: 1. An established intercom business, 2. The Freedom line of products and 3. Cloud based services that includes Freedom as well as two products called ABC and Facility Friend. The existing Intercom business has been stable and is poised to remain steady or even grow due to improvements in real estate development. There have been some interesting advances in enabling intercom systems to more effectively handle "edge" cases in physical access control.

Viscount's Freedom product represents a new opportunity in the market – one that could be very disruptive as the company has created a powerful, low-cost technology that unifies physical access control within the IT infrastructure. This line of business has not yet been a material contributor to the top or bottom lines yet, but our research suggests we will begin to see accelerating penetration in the market in the months ahead.

Freedom is essentially a physical security system that eliminates expensive control panel hardware by performing traditional security functions in software. Logical security systems such as Microsoft Active Directory are designed to manage user access to computer networks. Traditional users are assigned to groups and given permissions to files or IP addresses (PC's, printers, copiers). With the Active Directory Freedom platform, these functions are extended to building security; rather than an IP address permission for a printer, a user is given an IP address for a security device – the Freedom IP encryption bridge.

The foundation of the Freedom product is an IP "bridge" that connects the physical access control elements (door sensor, reader, lock and interior release button) to the IP network for all control functions. The decision to control doors using a computer allows Viscount to manage door control on a low cost business card-sized IP bridge and eliminate the expensive laptop-sized circuit boards, boxes, and wiring traditionally used for control panels. This is the key difference between this and all other systems that require the use of proprietary control panels. Those expensive panels have been needed in the past, even if they ultimately support some connection to IP networks.

Viscount's Freedom MESH Architecture



There are several elements in the line of products that come together to form the total solution. The ones Viscount is focused on are:

Freedom Hardware/Bridges – These are small units offered in a few varieties to support both wired (Ethernet) and wireless (WiFi) connectivity. Each IP bridge is wired but can also be directly connected to wireless networks, unlike most panels. Wireless IP bridge versions are also anticipated for remote locations. Also included in this line are more specialized bridges to connect additional sensors, elevators, inputs and outputs, and other physical elements.

Freedom Nanoservers/Cube – The Viscount Freedom Nanoserver is a small standard Linux-based server that is about the size of a pack of cigarettes. Despite their small size, current specifications include 4GB to 16GB of storage and a SQL database. Nanoservers provide localized intelligence, backup, and control for many doors and an essentially unlimited numbers of users, schedules, notification rules and software-defined functions like time and attendance.

Unlike most access control systems that have a target market (small, medium, or enterprise), Nanoservers allow Viscount to competitively scale from very small facilities to large enterprises.

The other important role of Nanoservers is to provide localized backup for Enterprise and Cloud systems. If a primary server fails, the Nanoserver can provide local control so door control and security continue to operate. This provides a significant advantage over traditional control panels because if a panel fails, door control is automatically lost until the panel is repaired.

Freedom Software – The Freedom software suite is what ties all the system elements together and enables distributed administration, management and control. The software layer is really the strategic component, similar to the management and control software that Cisco used in the early days of IP networking. Hardware components like bridges, servers and intercoms can be made by anyone, but as we have all witnessed many times the proprietary software is what makes the system work. Software (and design) explains the difference between the market values of "hardware" companies like Apple at $637B and Dell at only $18B.

These are the core elements of the Freedom system. Although Viscount also offers the reception and access products described below, the Freedom system is most often deployed with access cards, readers and other components from different suppliers. Using COTS (or Commercial, Off the Shelf) products is very appealing to IT and Security Managers.

The Viscount system provides the key IP functions, servers and infrastructure but doesn't try to lock the customer into any specific sensors or edge devices. Although the software is built to work with Microsoft Active Directory there is also a version that works with any system the customer desires. Active Directory is by far the most commonly packaged solution for user management, but many companies have built their own or use other software.

Recent industry Attention

This September at ASIS 2012 (a national security industry conference) Viscount released its first patent-pending applications for physical security using mobile devices. Security Info Watch magazine, in a story titled "Access Control Innovations Abound at ASIS", began their article:

"When you think of what might be the greatest access control innovations from the show floor at ASIS this year, your first thought was probably a neat way to open doors with an iPhone…. Viscount used a mobile phone to open a door using only a QR code. The code is mounted above the door, and the user need only scan the QR code to be granted access."

The three main components of a traditional system are the card, the reader and the control panel. With this mobile platform Viscount demonstrated the ability to eliminate all three components in favor of a Freedom IP encryption bridge and a mobile software application.

Viscount's Freedom Mobile strategy is based on continuing to lower the capital cost of system deployment while developing new opportunities to sell software as a service (SaaS). Other mobile apps on display by Viscount included the ability to track people and property using mobile devices without the need to install any electronic hardware onsite.

Industry press attention for Viscount is helping to build a substantial pipeline of opportunities that gives us confidence that the current financial projections in our IV model are conservative.

Market Overview

1) The combination of new information security regulations, ongoing pressure on costs, aged physical access infrastructure and new technologies that enable unification of logical and physical security has pushed the $100B+ physical security industry to a tipping point.

2) Directionally, the IT-based approach governing logical security will be asserting itself into physical security and facilities management. Most of the established vendors in the physical security industry do not yet have deep IT product development and engineering skills, nor access and relationships with the "IT-side" of enterprise and government organizations.

3) Most legacy systems are based on expensive 40-year-old control panel technology. This severely limits their ability to be upgraded, and to take advantage of advancements in IT and the Cloud.

4) These major challenges for incumbents have opened up opportunities for new entrants. Because access control panels are typi-

A Path Well Travelled

We've witnessed analogous technology-driven industry shifts many times. Two notable examples are telephony and video surveillance. In the past, organizations maintained large separate departments, systems and budgets for their phone systems. Today these have been integrated onto IP networks and rely on IT-based systems to administer them. The result has been reduced costs, better functionality and effectiveness. The old leaders of the market, Northern Telecom and Rolm, are just names from the past now. Cisco and Microsoft have taken over.

Video surveillance has more recently flipped over to an IP base and it has been a big transition. Here again companies like Cisco and a bevy of other specialists are emerging as key suppliers, while prior leaders like Gyrr have disappeared.

The same thing is beginning to happen now in the 40-year-old hardware based access control market. We know the IP-based approach, based on standard IT infrastructure like ? Active Directory, will win.

cally not technology driven, most of the existing players in IT security have been preoccupied with computerized video platforms. Only Cisco has entered the access control space, but with a traditional type panel platform that has not had great buy-in from IT channels. Now with Viscount's Freedom, physical security becomes a software extension.

5) Microsoft Active Directory. In effect, Microsoft software is now poised to disrupt an industry that was previously totally unrelated to logical security. This is a profound threat to the incumbent multi-national suppliers.

With this approach, Microsoft's Active Directory can become a standard in provisioning and managing physical security with Viscount's Freedom as the link between physical and logical security as well as the core infrastructure for cloud-based deployments.

From our vantage point, Microsoft and Viscount Systems appear to be well positioned to become a driving force in the unification of physical and information security in the enterprise and government markets.

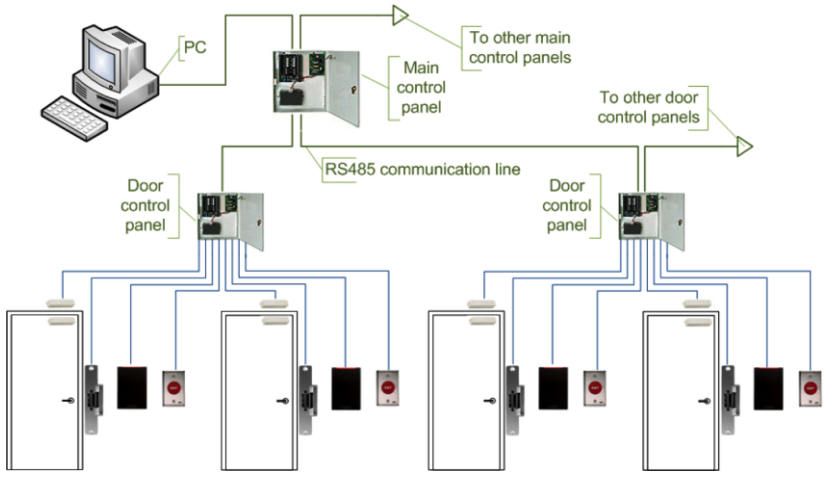
The Problem

Physical access control has remained an isolated system while growing complex, expensive, opaque and increasingly out of step with mainstream IT infrastructure management. Many commercial and government enterprises have already moved from cutting keys to issuing programmable access cards that can be individually configured and handle multiple doors. Unfortunately, the shift to cards and "smart doors" was accomplished by creating a separate (and now massive) proprietary infrastructure. Metal boxes full of wires, control panels, control processors with "firmware" and cryptic instructions have sprouted everywhere.

On top of their increasingly dysfunctional nature, these types of access control systems only give the appearance of security. They have become famously easy to hack. The main reason is that as soon as new systems are introduced and installed they are attacked. It doesn't take long for weak points to be discovered and shared with the online hacker community. By the time many systems are installed they are no longer secure.

Companies requiring high security have been forced to spend more for new systems that include advanced capabilities like biometrics and multi-factor authentication. In short, most existing low and mid-range systems are not secure and high-end systems are expensive and require frequent upgrades to keep hackers out.

Conventional Physical Security Architecture



The isolation of these systems makes simple tasks like automatically revoking access to company facilities for a terminated employee harder than it should be. It also makes it difficult or impossible to correlate real-time information about access and physical presence with information access and events.
While IT systems continue to strive for interoperability and "plug and play" with panels, there is no such thing as open architecture for security. Upgrading a system is often "rip and replace"; everything goes, from the electronics to the cards to the readers. This is an incredibly expensive proposition that has left users stuck with systems they don't want - for those with multiple systems, it's an even bigger mess because systems don't communicate with each other.

A combination of several technologies have reached maturity that provide a catalyst for the market to finally hit a tipping point to shift over to an IT foundation:

More powerful networks – The only reason control panels exist is because early computers lacked the power to control multiple security devices. Now computers far outstrip the power of panels. While the most powerful panel can hold thousands of users, any computer can hold millions.

Wireless communication – Wireless is now ubiquitous. The technologies cover long range (3G, 4G), medium range (WiFi) and short range (Bluetooth, NFC). While the bandwidth demands of access control are modest, panels and readers are typically not IP connected, so incumbent suppliers have a very limited ability to take advantage of new and emerging wireless technologies.

One wire/POE – IP video cameras and other security technologies have already evolved to run on existing IT networks and to take advantage of Power Over Ethernet (POE). POE has the added benefit of eliminating separate field power supplies and power cabling. However, Access Control panels are normally wired using RS485 or other non-IT cable networks, which puts them out of touch with industry trends and end user requirements.

The Cloud – Today every organization is looking at Cloud architecture to save money and improve efficiency, whether through public, private or hybrid cloud models. The Cloud is all about eliminating Capital Expenses (CAPEX) in favor of improved ROI using Operating Expenses (OPEX) – or pay as you go. However, access control systems have large fixed CAPEX pieces, including control panel hardware and cabling, and software that is panel-based and cannot be Cloud-based. In effect, they simply cannot take advantage of the scalability of Cloud platforms.

Smartphones – Most access control systems involve costly RFID, biometric or "multi-factor" combinations of devices. New NFC enabled smartphones can be especially useful for new security and access control applications. Firstly, since they can hold the same information as an RFID credential, they can eliminate the need for a separate card. Secondly, because they are connected to computers, they can authenticate RFID, PIN, and biometric security data wirelessly. These developments severely threaten the control panel model since IT based systems can now perform security functions without the needs for panels, readers, or cards.

What's more, the smartphone is equipped with multiple ways to communicate with doors and readers – NFC, Bluetooth, WiFi, and 3G/4G. New entrants can develop applications that continue to lower costs while increasing security. Smartphone cameras can be used for biometric facial recognition while touchscreens create an opportunity for smartphone fingerprint biometrics. Cards and readers may continue to exist for a long time but the smartphone will be used for many access control applications.

Coincident with these technologies reaching maturity, several economic and regulatory forces are putting extreme pressure on companies to upgrade and improve their security and access control:

Regulations – After 9-11 the US Department of Homeland Security was created. An evaluation concluded that control panels, cards were not secure. With it came FIPS 201, an expansion of processes and regulations designed to update security. An expanded standard, "FIPS-201-2," is now in active drafting for future implementation. These regulations state that the vast majority of the existing access control infrastructure needs to be replaced or upgraded. This presents an enormous opportunity for new lower cost and more conformant technologies.

Cost – Physical access control is expensive. System costs vary widely but the average costs obtained from multiple sources put the per-door installed price in the $2,000 to $4,000 range. While hardware prices may decrease, total installed prices have been increasing over time due mostly to expanding installation fees for complex systems. An IP bridge-based system **reduces typical hardware AND installation costs by 50% or more.**

Customers will save more over time due to lower ongoing costs. The components are less expensive but the real savings come from reduced installation costs, and reduced management costs for proprietary systems. With enterprises having hundreds or thousands of access-controlled doors, the cost advantages of an IP-based approach are impossible to ignore.

Transparency – Modern governance and risk management requires greater integration and complete transparency. Proprietary access control systems are a classic "blind spot" in enterprise systems. These opaque proprietary access control systems (often referred to as "stove-piped"), are untenable. Data and events need to flow in both directions in real time.

Compliance

In order to comply with Sarbanes-Oxley and other rules and regulations, every large public corporate entity is required to have adequate security measures in place for the purpose of protecting IT data from tampering by unauthorized personnel. A component of this includes properly securing physical facilities as well as IT networks. Unfortunately, since control panels typically use a separate security database from IT, it is very difficult to relate usage of the systems for the purposes of audit and compliance. With a unified platform using Microsoft Active Directory, audits and compliance issues are simplified using a single set of IT logs.

This time the nature of the solution is easy to define and design, and the building blocks are more numerous, readily available

and much more capable than those that existed to start the shift to IP telephony. In fact, we have **already built out the infrastructure to handle access control for IT assets**. Companies have already deployed products like Microsoft Active Directory to manage employee access to IT systems and applications. These applications have become sophisticated and offer both individual and role-based access control and privileges. Enterprises are also already using these systems to control physical assets like laptop computers and mobile phones. For example, most companies can "remote wipe" a smartphone of all applications and data and disable it in the case that an employee is terminated or simply loses their company phone.

Management & Board of Directors

Experienced investors know that advanced technology, strong products and a large market opportunity are not enough. The outcome of emerging investment opportunities like this one depends almost entirely on the quality and execution of the management team.

Management execution determines 1) the amount of the available market opportunity the company will capture, 2) the gross margin on the products and services delivered, and 3) the net operating margin and returns on all capital invested.

Behind each one of these there are at least a half-dozen management strategies, programs and processes to make them work – from product engineering to manufacturing; from software design and development to testing and maintenance; from marketing and sales to delivery and support; and finally from customer acquisition, retention, and profitability.

We are keenly aware of the fact that Viscount has been around a long time and is not yet demonstrating the kind of growth and expanding profitability that excites investors. It takes more than new technology to change the DNA of operations. Fortunately, Viscount has reorganized the company and dramatically expanded their board and operational advisory team. In short, we are convinced that the current management team is prepared to deliver a level of execution that will build meaningful intrinsic value over the next few years.

Let's take a deeper look at the recent changes and the current team of executives, starting with CEO **Steve Pineau**. He's been with the company since 1997 and thoroughly understands the technology and the operational and financial aspects of the business. As the CEO since 2001, he has watched the industry evolve from the inside and clearly seen the massive paradigm shift coming. Steve Pineau is a visionary with innate strengths and abilities in terms of innovation and new products. Investors wanting to get better acquainted with the CEO can visit the website where he appears in a number of short videos talking about Viscount's products, the Cloud and some of the dynamics in the market.

During the previous 18 months, several key additions to the Board of Directors and advisory team set the stage for attracting additional capital and preparing the company for an expansion phase.

Shayne Bates is the latest addition to the advisory team. Shayne has a long and documented history as a thought leader in the

unification of physical and logical access control. He has emphasized Active Directory in his approach and has worked closely with Microsoft developing cloud strategy. His 2010 paper "Cloud Computing and Software-as-a-Service for Security Professionals" has played a role in defining the entire space.[2]

Ron Martin is also a member of Viscount's advisory board and is known throughout the security industry as a thought leader in Identity management and Physical Access Control systems. Ron regularly contributes to standards publications published the National Institute of Standards and Technology, ASIS International and the Security Industry Association. Ron was a major contributor to the U.S. Government's Federal Identity, Credentialing and Access Management (ICAM) Roadmap[3].

Paul Brisgone joined Viscount's Board of Directors in December 2011 after 34 years at ADT, most recently as the VP of the Federal Systems Division, which grew dramatically from a small beachhead to over $150M in revenue with a technical and support staff of 200. What's notable here is that Paul has exactly the right experience, in the right market, with the right customers, and against the right competitors, to be extremely valuable to the company in today's market.

Dennis Raefield joined Viscount's board in October 2011 and brings operating experience as the past President of the Honeywell Access Systems division, which operates at a $100M annual revenue scale. Prior experience is rooted in the integration of large security systems, including being president of Pinkerton Systems Integration (now Securitas.)

Robert Liscouski joined Viscount's board in September 2011 and brings expertise in security and IT. He was the first Assistant Secretary for the US Department of Homeland Security, running the $500M Infrastructure Protection initiative for DHS. He's been a homicide detective, a diplomat with the US State Department and Head of Information Assurance for the Coca-Cola company. He is a partner in Secure Strategy Group.

Paul Goldenberg joined the board in October 2011 and brings considerable experience, knowledge and rapport with governments and agencies. He has a long and distinguished career in the criminal justice system and was recognized with an appointment to the Homeland Security Advisory Council by Janet Napolitano in 2010.

Viscount retained the **Secure Strategy Group** (SSG) in June 2011 to help accelerate the company's development. SSG has been instrumental in building out the Board of Directors and advisors as well as raising much-needed expansion capital. They add a strategic advisory and business development capability that the company can leverage as they continue to grow.

---

[2] This 47-page document is recommended reading and can be found at: http://www.asisonline.org/councils/documents/CloudComputingFinal.pdf

[3] http://www.idmanagement.gov/documents/FICAM_Roadmap_and_Implementation_Guidance_v2%200_20111202.pdf

INDUSTRY DYNAMICS & COMPETITION

Physical security is a big, messy industry that was once highly fragmented but has gone through a consolidation process dominated by multi-nationals. We're going to break it down into segments and also touch on related areas like building automation.

Physical access control typically involves two groups – the electronic reader suppliers (RFID readers, Biometrics) and the control suppliers. The control suppliers are typically the top of the food chain and resell electronic reader devices as part of the control platform. This is the core segment in which Viscount competes.

The electronic reader part of this industry grew out of old-fashioned door locks. It's not surprising that at this level the most common companies are **ASSA ABLOY** and Stanley. ASSA ABLOY has been the most aggressive over the years and is now fairly dominant in the area of door control and "entrance systems." Key acquisitions included **HID** (in 2000), which is a leading provider of access control cards and electronic readers. ASSA ABLOY has made over 20 acquisitions in the space and has almost 40,000 employees worldwide. We would say they own the door control segment of the market.

Stanley is in the process of selling off their hardware and home improvement business, which includes major lock brands like Kwikset and Baldwin. The company is running an auction process and so far the most likely serious bidders will be private equity firms. The non-strategic nature of the business to Stanley Black and Decker helps explain why they have been out-executed by ASSA ABLOY.

Behind the door itself is access management and control. There are specialized companies in this segment but most are now part of massive conglomerates that provide a broad range of related industrial products. Major players include Lenel, which is part of United Technologies Corporation (NYSE: UTX), Software House, which is part of Tyco International (NYSE: TYC), Honeywell (NYSE: HON), Schneider Electric (SU:EN Paris), Johnson Controls (NYSE: JCI) and Cisco (NASDAQ: CSCO).

UTC has largely entered the security market through acquisition. Lenel, a Viscount competitor, is one of the key benchmarks for valuing access control suppliers, having been purchased for over $400M by UTC in 2005. Lenel continues to be a leader in providing security control systems. Lenel has advanced the state of their systems to allow more electronic control and web access and make them more "IT friendly," but they are fundamentally a proprietary system manufcaturer. UTC also owns a number of related access control brands, including Chubb Security and Guardall. In 2009 UTC completed another benchmark deal, acquiring GE Security for $1.8B.

Tyco International has also acquired a wide array of security brands. Their flagship access control brand is Software House. Other access control brands include CEM Systems and Kantech. Like UTC, Tyco has several integrator divisions that install advanced technology including ADT and Simplex-Grinell.

The range of Tyco products and services is so broad that there are many overlapping brands and companies even in their own portfolio. Having a captive product/solution

integrator like Software House helps them put together coherent large systems.

Johnson Controls (NYSE: JCI) is another massive conglomerate with broad industrial businesses. Their primary access control brand is the P2000. They have a concentration in "building efficiency" which includes security and fire safety as one of the business lines. JCI is more of a total solution provider and integrator than a product company. Their strength is as a prime contractor to projects like the US Capital Building and the Pentagon.

Another of the massive conglomerates serving the overall market is **Honeywell (NYSE: HON)**, which has their own security line of products and services inside a range that includes power management, building construction management, and process control. Honeywell also has many industry specific product and solution divisions. Their primary access control brands include the Pro2200 and NetAXS.

Schneider Electric is a French based conglomerate competing with Honeywell and Johnson Controls in a range of segments, including building automation and energy management. The company acquired Pelco, one of the largest video camera suppliers, for $1.2B in 2007. The company's primary access control brand is Andover Controls.

Cisco Systems entered the physical security market several years ago, releasing both video and access control platforms. The company appears to have struggled with its access control system because, like other traditional providers, it is not an IP-based product but uses a cable network called CANBUS that has not received buy-in from their own IT channel.

THE IT PLAYERS

The IT security space is an industry of its own with dozens of companies, including Check Point Software (CHKP), Symantec (SYMC), Fortinet (FTNT), Palo Alto Networks (PANW), Imperva (IMPV), Splunk (SPLK), and SourceFire (FIRE) to name some that are public. These companies are "pure" IT-specific technology providers and don't address the physical security challenge. (The one exception might be Splunk in the longer term but that's another story.)

But for many large global IT players like **Microsoft, Oracle, Cisco, Juniper Networks, RSA Security, Unisys, and IBM,** Viscount's ability through Freedom to unify the management of physical and logical security may simply change everything.

Not only does a Freedom type unified system represent a viable adjacent market opportunity that is large enough to be of interest, it may in fact become critical that these companies move in the direction of Freedom. The logic is simple; if Freedom can apply logical security rules to physical access it can also apply physical security rules to logical access. If unified platforms become the trend, any of the large identity management companies will be at a severe disadvantage if they don't enter the market.

The most obvious and clearly focused player so far is Microsoft, which is now in a position to combine the most popular enterprise user-management tool, Active Directory, with the Cloud (Azure in their terminology) to provide a solution for both logical and physical access control with one infrastructure using Freedom.

Microsoft also happens to fit well with the existing business model of the security industry given their historical affinity with resellers and integrators. At a company level, Viscount offers a convenient "bridge" for Microsoft to roll in their solutions to this new market.

Cisco is in a favorable position as more and more systems shift to an IP-base. However, so far Cisco has been far more focused on the video segment, which represents much more revenue than access control and management. Cisco does offer a number of products in the physical access control segment, but has not put the resources into making them really viable in the enterprise market. All indications suggest that Cisco will continue to deliver as many IP-based elements into security as they can with a heavy emphasis on video and core networking. In this regard, router providers such as Cisco may play a major role as devices switch to IP and Cisco provides the backbone.

IBM has fairly substantive security business consisting largely of services and software. However, they are aimed mostly at IT security. Their physical security play is a set of tools to improve video analysis from surveillance cameras. They may have their own identity management system (à la Active Directory) that could also be used as a basis for combining physical and logical access control, should they choose to make that investment.

Apple – The smartphone is quickly becoming the preferred security "credential" for access control. These devices are already capable of strong security but will get even better. Apple is acquiring AuthenTec to increase the security features of future iPhones. It's not clear yet what Apple will be incorporating into the iPhone but it will likely include some biometric security like fingerprint reading and a secure "Passbook" application for things requiring authentication. We can expect similar identity capabilities to emerge from Google, Microsoft, Nokia and Samsung.

VISCOUNT BUSINESS MODEL

Viscount distributes products through a network of value added resellers and integrators. Most end-user customers want a single or small group of companies to handle the myriad systems and technologies needed for physical security and building management. In some cases the access management and control portion is either requested separately or subcontracted out by a large prime contractor who may not have that expertise in-house.

From a marketing perspective Viscount (and IT-based companies like Microsoft) are doing some "direct messaging" to end customers so that they are more aware of the IT-based approach and the benefits it can bring. The combination results in a "push-pull" dynamic for the company in terms of sales and marketing.

Because Viscount has been selling their intercom and older access products for many years they do have an in-place network of integrators and resellers that can be used for the new Freedom products as well. Part of the ongoing Viscount strategy will be to add IT integrators to the customer mix.

The vast majority of the physical security and access control market is addressed by value added resellers, solution providers and system integrators. Customers have little

desire or expertise to handle the complex integration needed for physical access control along with other systems, from video monitoring to fire suppression and building management. However, many end users standardly purchase their own IT network equipment, so there are some sophisticated clients who perceive a reduced role for integrators when deploying Freedom.

Being able to leverage the prevailing network of consultants, integrators and solution resellers confers a massive advantage both in terms of scaling the business **and** profitability. We've witnessed disruptive new technology that required the ramping of a dedicated sales force and customer support network (BEA Systems and Data Domain are good examples.) This strategy takes hundreds of millions to $1B in revenue for operating margins to become attractive. Fortunately, Viscount only needs to make a small number of enabling and market development-focused investments to capture meaningful market share, based on their extreme cost advantage and simplicity.

Tapping into the existing network requires a handful of senior hires initially. The company is already experiencing an acceleration of demand for their Freedom technology from end-users who, in many cases, are asking their existing suppliers about it. Right now senior management and existing Viscount partners are fielding these inbound leads and sales. We expect a handful of senior sales executive hires to be completed in 2012. The initial regional targets are clear enough – Washington DC (government sector), New York (East Coast) and Los Angeles (West Coast.) Their Our first field office in DC was put in place and we expect to see at least two more open in 12 to 18 months.

The company will be addressing international market opportunities using their standard approach with global resellers and integrators. It's too early to know what requirements there might be for any investments in supporting international markets.

Intellectual Property

The company has understood the importance of intellectual property and patent protection. Viscount has over 43 patent claims filed.

Of key importance, though, is the "what" rather than the "how many" in terms of patents. They key patents pending surround the specific application identity management and access control in a unified approach. Viscount has also filed a number of blanket patents that deal with mobile tokens. These patents deal with a range of applications including people tracking, asset tracking, point of sale and printer security. Some of these patents may have an asset value outside Viscount's core business model.

This is one of those ideas that seems obvious in retrospect but appears radical and unlikely when it is first introduced. Today most industry insiders would agree that "ultimately you want to have one common infrastructure for management" and this is an essential area of patent claims for Viscount.

The strategy for Viscount isn't to rely on their patents or use them as a primary business model but to ensure that their innovations will result in commercial success and investment returns for them. In an industry of giants Viscount is a very small company, one that needs the coverage afforded by intellectual property protection.

Ultimately, the success of the company and returns for shareholders will depend on the ongoing software products and services that Viscount delivers. Patents will certainly help.

Income Statement & Balance Sheet

For the past few years Viscount has generated consistent and slightly declining revenues of about $3.5M per year from the base access and intercom business previously mentioned. Our base assumption is for this pattern to continue and improve due to an internal reorganization, allowing specific employees to focus on improving the existing base business. This recent reorganization, combined with a more flexible IT-based intercom system, provides a basis for improvement. For now, however, we are modeling this business as flat. When the company begins to generate growth and improved momentum we will update our view.

Gross margins have been very stable at 56-60% with a slightly increasing trend. After operating expenses for sales, marketing, R&D and G&A are added up, the company is generating a quarterly operating loss of between $300K and $600K.

Viscount can ramp operating margins rapidly by growing revenue, because gross margins are healthy and existing supplier channels can be leveraged.

There will be some increased costs going forward, particularly for sales and marketing, but it's important to note that the use of channels means there is leverage in the model. In other words, when the company begins to deliver more revenue and growth we will see operating margins expand quickly. This is due to the fact that the company does not have to make massive investments in direct sales.

The balance sheet of the company is small but recent current assets of $1.4M are adequate to cover current liabilities of just $964K. We have factored in higher-than-average share count growth due to the recent financing, which has interest and warrants associated with it.

Intrinsic Valuation

Right now Viscount is very near an inflection point in their total business and financial model. As such this makes it very difficult to forecast with confidence and accuracy. In these situations we have found that putting together both a "base" and "optimistic" case is helpful in determining a reliable IV estimate.

The "base" case is a model in which we are already highly confident the company can meet or exceed. By "optimistic" we don't mean "a stretch" but rather what we forecast if the company executes well and there are not material disruptions or differences in terms of market adoption from what our current research work suggests.

We're modeling the company based on two lines of business – the existing products and the new "Freedom" line. Freedom has not *yet* been a material contributor to the business but our checks suggest we will begin to see measurable revenue by the end of this calendar year, with substantial revenues coming in 2013.

The existing line of business has been stable and is poised to remain steady or even begin to grow due to a recent reorganization and some interesting advances in enabling inter-

com systems to more effectively handle "edge" cases in physical access control.

The Freedom line of business will begin to form a very small base at the end of this year but ramp quickly beginning in 2013. This optimism is based on over $12M in quoted projects outstanding, with a 2013 forecasted revenue of over $4M for Freedom alone. For the purposes of our IV model we have put the revenue inflection point in 2014.

We've kept gross margins flat over the forecast period and allowed for continuing investments in R&D and SG&A for the company to scale. Viscount can generate 15-22% operating margins in the next few years with room to move above that depending on how their business develops.

Even though revenue growth will be closer to 35-40% on average, we are using a conservative 15x multiple in our IV model.

Factoring it all together, we would expect Viscount to be trading at $0.26/share by the end of 2013 using our base case. If business momentum builds into the early part of 2013 we can start to consider our "optimistic" forecast an IV of $0.84.

VSYS IV Model BASE Case

Viscount Systems Inc. **Price** **$0.06**
VSYS **IV** **$0.26**
6-Oct-12 **Delta** **340%**

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Intercom	$4,157	$4,671	$3,938	$3,414	$3,400	$4,000	$4,500	$5,000	$5,500	$6,000
Freedom	$0	$0	$0	$0	$125	$750	$3,000	$5,500	$8,250	$11,500
Change in Revenue		$514	-$733	-$524	$111	$1,225	$2,750	$3,000	$3,250	$3,750
Revenue	$4,157	$4,671	$3,938	$3,414	$3,525	$4,750	$7,500	$10,500	$13,750	$17,500
YoY Growth		12.4%	-15.7%	-13.3%	3.3%	34.8%	57.9%	40.0%	31.0%	27.3%
COGS	$1,768	$1,834	$1,788	$1,449	$1,481	$1,995	$3,150	$4,410	$5,775	$7,350
Gross Margin%	57.5%	60.7%	54.6%	57.6%	58.0%	58.0%	58.0%	58.0%	58.0%	58.0%
Gross Profits	$2,389	$2,837	$2,150	$1,965	$2,045	$2,755	$4,350	$6,090	$7,975	$10,150
R&D%	6.5%	5.0%	9.3%	13.3%	14.2%	11.6%	8.0%	6.2%	5.6%	5.4%
R&D Expense	$270	$233	$366	$453	$500	$550	$600	$650	$775	$950
SG&A%	51.4%	46.0%	67.1%	97.4%	99.3%	86.0%	60.0%	50.0%	40.0%	31.0%
SG&A Expense	$2,137	$2,147	$2,643	$3,324	$3,500	$4,085	$4,500	$5,250	$5,500	$5,425
Net Operating Margin	-0.4%	9.8%	-21.8%	-53.1%	-55.5%	-39.6%	-10.0%	1.8%	12.4%	21.6%
Operating Income	-$18	$457	-$859	-$1,812	-$1,956	-$1,880	-$750	$190	$1,700	$3,775
Taxed Operating Income	-$12	$297	-$558	-$1,178	-$1,271	-$1,222	-$488	$124	$1,105	$2,454
Market Value Using P/E	-$176	$4,456	-$8,375	-$17,667	-$19,066	-$18,330	-$7,313	$1,853	$16,575	$36,806
Cash Position			$0	$0	-$1,955	-$3,835	-$4,585	-$4,395	-$2,695	$1,080
Shares (M)	77000	77000	77000	77000	80850	84893	89137	93594	98274	103187
Period Share Price	$0	$0	$0	$0	$0	$0	$0	$0.02	$0.17	$0.36
PV of MV 4 Years Out	-$10,901	-$10,480	-$4,181	$1,059	$9,477	$21,044				
PV of Cash 4 Years Out	-$1,118	-$2,193	-$2,622	-$2,513	-$1,541	$617				
PV MV + Cash	-$12,019	-$12,673	-$6,802	-$1,454	$7,936	$21,662				
PV Value Per Share	-$0.16	-$0.16	-$0.09	-$0.02	$0.10	$0.26				

VSYS	Ticker
Nasdaq	Exchange
13%	Rev Growth
$0.06	Current Price
77000	Shares Out
5%	Avg. Dilution
$4,466	Cap (M)
$1	Cash
$0	Debt
35%	Tax Rate
15	P/E Multiple
15%	Discount Rate
$0.26	Intrinsic Value
340%	Up/Downside

VSYS IV Model Optimistic Case

Viscount Systems Inc. **Price** **$0.07**
VSYS **IV** **$0.84**
8-Oct-12 **Delta** **1196%**

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Intercom	$4,157	$4,671	$3,938	$3,414	$3,500	$4,000	$4,500	$5,000	$5,500	$6,000
Freedom	$0	$0	$0	$0	$125	$2,750	$6,500	$13,000	$22,000	$35,000
Change in Revenue		$514	-$733	-$524	$211	$3,125	$4,250	$7,000	$9,500	$13,500
Revenue	$4,157	$4,671	$3,938	$3,414	$3,625	$6,750	$11,000	$18,000	$27,500	$41,000
YoY Growth		12.4%	-15.7%	-13.3%	6.2%	86.2%	63.0%	63.6%	52.8%	49.1%
COGS	$1,768	$1,834	$1,788	$1,449	$1,523	$2,835	$4,620	$7,560	$11,550	$17,220
Gross Margin%	57.5%	60.7%	54.6%	57.6%	58.0%	58.0%	58.0%	58.0%	58.0%	58.0%
Gross Profits	$2,389	$2,837	$2,150	$1,965	$2,103	$3,915	$6,380	$10,440	$15,950	$23,780
R&D%	6.5%	5.0%	9.3%	13.3%	13.8%	8.1%	5.5%	3.6%	2.8%	2.3%
R&D Expense	$270	$233	$366	$453	$500	$550	$600	$650	$775	$950
SG&A%	51.4%	46.0%	67.1%	97.4%	96.6%	86.0%	60.0%	50.0%	40.0%	31.0%
SG&A Expense	$2,137	$2,147	$2,643	$3,324	$3,500	$5,805	$6,600	$9,000	$11,000	$12,710
Net Operating Margin	-0.4%	9.8%	-21.8%	-53.1%	-52.3%	-36.1%	-7.5%	4.4%	15.2%	24.7%
Operating Income	-$18	$457	-$859	-$1,812	-$1,898	-$2,440	-$820	$790	$4,175	$10,120
Taxed Operating Income	-$12	$297	-$558	-$1,178	-$1,233	-$1,586	-$533	$514	$2,714	$6,578
Market Value Using P/E	-$205	$5,198	-$9,771	-$20,612	-$21,584	-$27,755	-$9,328	$8,986	$47,491	$115,115
Cash Position			$0	$0	-$1,897	-$4,337	-$5,157	-$4,367	-$192	$9,928
Shares (M)	77000	77000	77000	77000	80850	84893	89137	93594	98274	103187
Period Share Price	$0	$0	$0	$0	$0	$0	$0	$0.10	$0.48	$1.12
PV of MV 4 Years Out	-$12,341	-$15,869	-$5,333	$5,138	$27,153	$65,817				
PV of Cash 4 Years Out	-$1,085	-$2,480	-$2,949	-$2,497	-$110	$5,676				
PV MV + Cash	-$13,425	-$18,349	-$8,282	$2,641	$27,043	$71,494				
PV Value Per Share	-$0.17	-$0.24	-$0.11	$0.03	$0.33	$0.84				

VSYS	Ticker
Nasdaq	Exchange
23%	Rev Growth
$0.07	Current Price
77000	Shares Out
5%	Avg. Dilution
$5,005	Cap (M)
$1	Cash
$0	Debt
35%	Tax Rate
17.5	P/E Multiple
15%	Discount Rate
$0.84	Intrinsic Value
1196%	Up/Downside

Conclusion

We believe investors should be looking at this space to add to their exposure to security technology.

Thus far, too many companies have continued to deliver "stove-piped" rather than integrated solutions. These companies are now at a disadvantage in this market. We like what we see in private company VidSys but they are not an option for public investors. All the other public companies are massive and offer little direct investment leverage to this opportunity.

Viscount Systems offers one of the very few public investment vehicles in this space and has the potential to generate multiple years of rapidly expanding revenue growth and high margins. Our models quantify this upside based on what we know but it should be realized that at the early stages of a disruptive market shift investors generally do well by simply owning the disruptor and not being overly concerned with valuation.

The next few quarters will be important as the company captures an increasing share of the access management infrastructure space and builds out their sales and execution team.

Based on the current share price and what could ultimately be an $0.84 IV or better over time we think VSYS is a strong candidate for growth investors.

APPENDIX A – WHAT IS PSIM?

Years ago the physical security industry recognized that over time they would have to provide a more connected and interoperable set of solutions. An industry standard of sorts called "Physical Security Information Management," or PSIM, was developed and has been popularized as a path to a more converged infrastructure.

An entire report can be written about PSIM but it's not clear that even that would be conclusive. In the words of one very experienced industry insider, "you can ask 12 people about how PSIM works and you'll get 12 different answers." In short, PSIM is relevant to the industry but the reality of that quote is that PSIM has failed as a true unifying standard. Another quote that helps underscore our conclusion comes from a PSIM pioneer and one of the more technologically advanced players in physical security: "For VidSys, the increasingly popular label of PSIM fails to capture the full scope of our rapidly-evolving integration platform."

Fortunately, we can simplify the story. PSIM is similar to the "application integration" stack that emerged in the late 1990's as a response to new demands for a more internet-based approach to software. There were several years of robust adoption and a number of successful public companies created in the process, but in the end enterprises went "native" with solutions from companies like Salesforce.com. In other words, if you shift to a unified infrastructure you only need PSIM and "converged infrastructure" for legacy devices and systems.

Where PSIM falls short is in preserving an existing but unnecessary and expensive layer of proprietary infrastructure. It's basically a "wrapper" that existing vendors can put on their products to make them compliant and broadcast their data to other applications for aggregation. Being able to aggregate data from multiple systems is a good thing but doesn't compare to the functional opportunities that come from having everything on one technology platform.

There may be some out there who insist, "PSIM can work!" Here is why it can't – when software is designed and developed for a particular platform yet relies on an external set of definitions, interfaces and implementations to make those features and functions accessible, there will *always* be gaps and mismatches. It's as close to a "law of physics" in the software industry as you will find.

A large, fragmented industry like physical security does not turn on a dime. Over the next several years many "converged" solutions will be installed. But at the same time more and more of the market will shift to a unified solution that is actually based on the same IT platform as virtual security is today. The good news is that converged solutions based on PSIM will still be a step in the right direction. Such systems will be a few steps closer to a unified solution but much more expensive and functionally limited.

VidSys is a key player in the development and adoption of a more integrated software-based approach to security systems. They champion PSIM while acknowledging that it's not a panacea. They are private but have a complete and top-flight management team. Their software is a key

element in integrating disparate systems so that data can be shared and new security applications delivered. In essence, VidSys is a key provider of software middleware for physical security and related areas.

Nice Systems has an array of security products aimed at surveillance and situation management applications using audio, video, sensors and specialized systems to gather information and monitor activity. They are an important provider of what we'd call security-focused applications but don't provide access management and control. Like VidSys, Nice would view access systems as a "feed" for their applications.

APPENDIX B – SECURITY TECHNOLOGY COMPANIES

For illustration we are including a few of the smaller IT-focused enterprise security companies for comparison purposes. As Viscount grows their profile will fit more squarely into this group as a security software and appliance technology provider. With an average multiple of 6.8x TEV/sales these companies are enjoying premium valuations due to the multi-year IT security investment cycle going on now.

Smaller Public Security Companies

11-Oct-12

COMPANY	Segment	Ticker	Price	1 yr chg	3 mo chg	TEV	LTM Rev	LTM Growth	Gross Margin	Oper Margin	TEV / Revenu
CheckPoint	Network Security	CHKP	$45.61	-19%	-1%	7,969	1,307	11.4%	88.4%	45.0%	6.1
Fortinet	Threat Management	FTNT	$23.66	33%	10%	3,341	483	29.0%	73.8%	12.9%	6.9
Websense	Web Security SW	WBSN	$15.40	-14%	-13%	569	364	3.9%	83.6%	6.7%	1.6
Palo Alto NW	Network Security	PANW	$61.44	na	na	3,849	255	115.1%	72.3%	0.3%	15.1
KEYW Holding	Security Services	KEYW	$13.11	45%	18%	484	216	49.1%	29.7%	0.4%	2.2
Sourcefire	Threat Management	FIRE	$45.90	66%	5%	1,199	195	38.2%	77.5%	3.7%	6.1
Splunk	Logfile Data Analysis	SPLK	$31.07	na	10%	2,738	156	0.0%	90.4%	-19.1%	17.5
LogMeIn	Remote Access Control	LOGM	$20.88	-41%	-33%	318	130	15.5%	91.1%	2.9%	2.5
Proofpoint	Email Security	PFPT	$12.98	na	-16%	337	94	0.0%	63.7%	-22.4%	3.6
Imperva	Database Security	IMPV	$36.03	na	27%	748	89	35.3%	79.3%	-10.7%	8.4
Qualys	Threat Management	QLYS	$13.51	na	na	381	83	0.0%	82.6%	-0.9%	4.6
Average				***11.7%***	***0.8%***			***27.0%***	***75.7%***	***1.7%***	***6.8***

ABOUT SOUNDVIEW

SoundView Research conducts **independent research** in emerging technologies. We work and write for the benefit of our advisory clients and investment professionals. Our approach is to combine **major thematic forces** where technology is involved and use analysis to identify the **most promising companies and investment opportunities**.

Companies tend to be late stage private to early stage public. As part of the SoundView Technology Group our business is driven by subscriptions, advisory work and service fees. We measure our success by the quality of analysis, accuracy of the conclusions and overall satisfaction of our clients.

Along with facts, figures and fundamentals we apply a rigorous approach to valuation that we call intrinsic value (IV) which provides a basis for good investment decisions and effective portfolio management.

We reach tens of thousands of qualified professionals using the broadest array of delivery platforms (described below.)

CONTACT INFORMATION

Address: SoundView Technology Group, 1313 Washington St., #326, Boston MA 02118
Phone: 800-979-0280, FAX 888-415-8919 | **Website**: http://www.soundview.co

IMPORTANT DISCLOSURES

1. The analysts who prepared this report certify that the content expresses accurately their personal views and opinions about the subject companies and securities. The analysts have not been and will not be receiving direct or indirect compensation for expressing the specific views or conclusions in this report.

2. Clients or affiliates of SoundView Research may own positions in the securities mentioned and/or provide, have provided or may provide advisory services to some of the companies mentioned.

3. Neither SoundView Research nor SoundView Technology group is a registered securities broker/dealer, investment bank or investment advisory.

4. SoundView Technology Group receives advisory fees, has vested interests and/or may have embedded biases in our work. However our process centers on "fact-based research" and strives to illuminate information and draw out relevant insights to educate and inform any investment process.

5. SoundView Research does not provide investment advice in the form of "buy," "sell," or "hold" ratings. This report is intended strictly for informational purposes. We make no claims as to the completeness or accuracy of this report although we have done our best. We do not undertake to advise you of any changes in our opinion or information contained herein.

6. SoundView Research is solely responsible for all content – whether it is created for a third party, part of an advisory engagement or simply an expression of our ongoing research and analysis. We exercise 100% final editorial control over all content produced and any mistakes, omissions or errors are our own.

Our research is distributed to institutions, investors, company managers and individuals via proprietary platforms[1] and via the internet and social networks.

We embrace the online community and use email, blogs, syndication, social and professional networks. Institutions are now getting their information via iPhone or iPad rather than proprietary access and desktop computers.

SoundView maintains additional online brands for specialty research products including IPO Candy, Dealipedia and Research 2.0. We also collaborate and share with partners including GigaOM and Sharespost.

[1] Bloomberg, Thomson/Reuters/FirstCall, S&P Capital IQ and FactSet.