



INVESTMENT SUMMARY

Viscount Systems (VSYs) provides a suite of new IP-based products that are changing the game in the physical security business, particularly building access control and management. This is one of those large but stagnant industries where expensive, proprietary “stove-piped” solutions are being displaced by modern technology. Customers want an integrated approach with IT-based security tools and methods that work with systems like Microsoft Active Directory. The situation is reminiscent of what happened with proprietary phone systems (remember those?) during the past 20 years.

Viscount is the only public investment vehicle in this space that we know of and has the potential to reward investors with substantial returns from current levels given our base case intrinsic value (IV)¹ estimate of \$0.27. 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.
- Viscount has also forged a strong working relationship with Microsoft which gives them credibility with large enterprises and government agencies while also enhancing lead generation and ultimately will help the company grow without high customer acquisition costs.
- The “Freedom” product line is 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. They also launched a lower-end “Liberty” version for the channel.
- Viscount has substantially upgraded their company capability over the last 18 months – expanding their board of directors and advisors and upgrading their sales, support and development staff. Most notably a new CEO, Dennis Raefield was put in place earlier this year.
- Combined with some much-needed additional financing we have high confidence that the management team is absolutely focused on the right things – accelerating revenue growth and expanding operating margins.
- Our IV model suggests a value of \$0.27 with upside from there if management can exceed what we feel are very achievable estimates.

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.

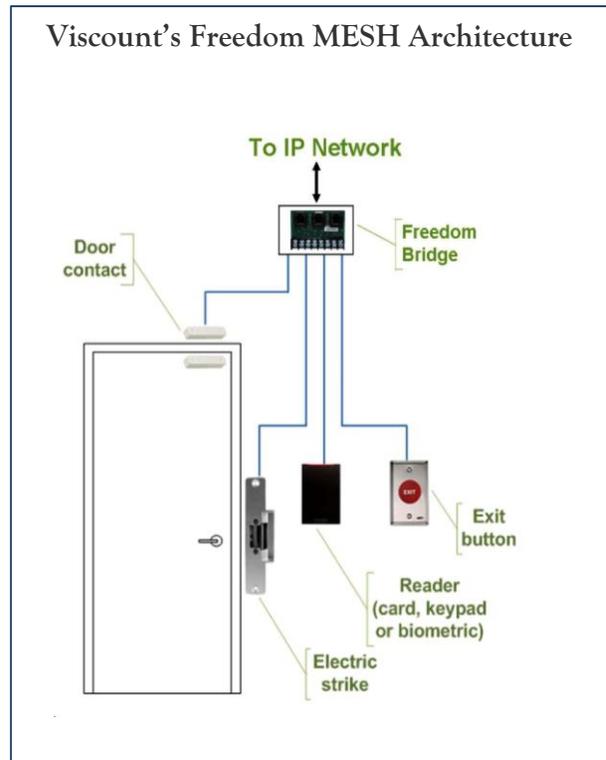
VISCOUNT SYSTEMS “FREEDOM”

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.



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.

INDUSTRY RECOGNITION

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 typically

not technology driven, most of the existing players in IT security have been preoccupied with computerized video platforms.

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 Gyr 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.

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 are well positioned to participate in the unification of physical and information security in the enterprise and government markets.

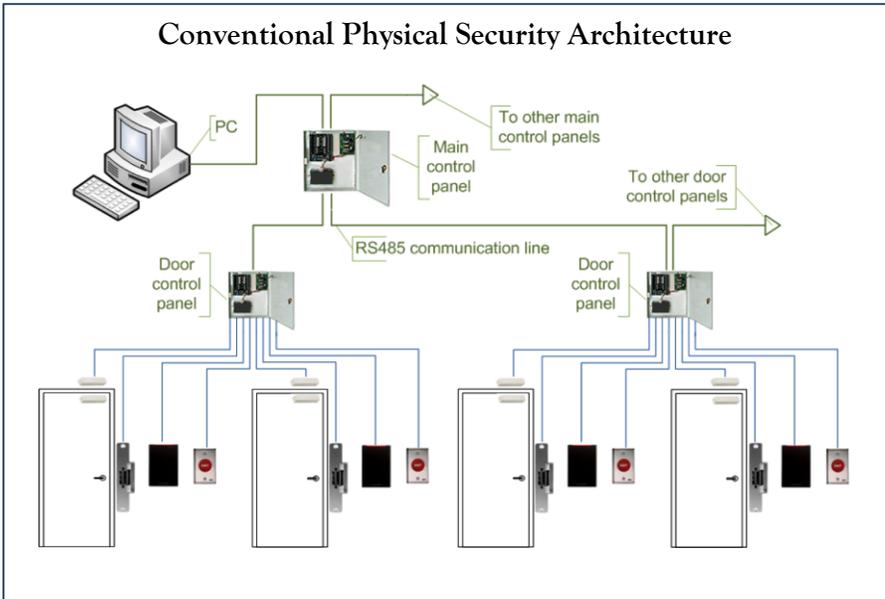
THE PROBLEM

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.



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 infra-**

structure 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 just now demonstrating real growth. 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.

Dennis Raefield joined Viscount’s board in October 2011 and took over the CEO role from the technical founder of the company early in 2014. Dennis brings a wealth operating experience and industry expertise 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.)

Several key additions to the Board of Directors and advisory team has enabled the company to attract additional capital and prepare the company for expansion.

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.

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.

Ned Siegel served as the U.S. Ambassador to the Commonwealth of the Bahamas and also as the Senior Advisor to the U.S. Mission and as the United States representative to the 61st Session of the United Nations General Assembly. In addition to his public service, Ambassador Siegel has over 30 years of entrepreneurial successes. Presently, he is Chairman of the Board of The Siegel Group, a multi-disciplined international business management advisory firm specializing in infrastructure, real estate, ports, energy, utilities, technology and financial services.

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.

As part of the advisory services provided by SSG they supplement company resources with powerful advisors who lend their specific expertise and capabilities as needed. In the case of Viscount these include:

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) Roadmap².

Shayne Bates 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.³

²

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

³ This 47-page document is recommended reading and can be found at:

<http://www.asisonline.org/councils/documents/CloudComputingFinal.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 manufacturer. 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-Grinnell.

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. The 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

Revenue growth has been accelerating from declines in 2011 to flat in 2012 to growth of 15% for 2013. We expect this to continue in 2014 with a growth estimate of 21%. From there we expect the company can grow sustainably at 30% to 40% per year.

Gross margins have fluctuated but at attractive levels of between 52% and 64%. As Viscount further rationalizes their product business these may move around some more but our steady-state estimate now is 58%.

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. Overall the combination of direct sales and channel business should help operating margins reach break-even late in 2014.

A recent financing went better than the company expected which gives them better financial flexibility than they have had in the past. We've had to adjust share count upwards to account for this but now company management believes they can get to positive cash flow without further external investment.

INTRINSIC VALUATION

Since we started covering the company in 2012 revenues have stabilized and started to ramp up, giving us a better handle on the

growth of the business over the longer term. We are still in the early stages of acceleration.

We're modeling the company based on two lines of business - the existing products and the new "Freedom" and "Liberty" lines. Freedom is now a material contributor to the business and will be the driver of accelerating growth as it matures.

The legacy intercom business has been rolled in with the Liberty product line and sold together. This will help both businesses run smoothly and grow together.

Right now we have operating margins ramping to just over 15%. They could be higher depending on how revenues grow and the mix of business between direct and channel. We also think the company has an excellent opportunity to license their technology to other firms which would tend to boost margins.

Because Viscount is still in early stages of commercialization and maturity we've applied a valuation multiple of 16x, much lower than the expected 30% growth the company should achieve. As their track record grows we would be able to revise that multiple upwards in 2015 or 2016 - that would have a big impact on IV.

Factoring it all together, we believe the shares should be trading closer to \$0.15 in the near term and at or above \$0.27 in the next 12 months. We've got a quarterly model for 2014 that will be a way to keep score in the short-term, we will revise our overall IV model again later this year after two or three more quarters are on the books.

VSYS IV Model BASE Case

Viscount Systems Inc. Price \$0.10
 VSYS IV \$0.27
 23-May-14 Delta 182%

	2011	2012	2013	2014	2015	2016	2017	2018	2019	VSYS	Ticker
Top Line Revenue	\$3.47	\$3.60	\$4.13	\$4.99	\$7.00	\$11.00	\$16.00	\$22.00	\$30.00	Nasdaq	Exchange
YoY Growth	-11.4%	3.8%	14.8%	20.6%	40.4%	57.1%	45.5%	37.5%	36.4%		
COGS	\$1.47	\$1.45	\$1.47	\$2.38	\$2.94	\$4.62	\$6.72	\$9.24	\$12.60	27%	LT Rev GR
Gross Margin%	57.6%	58.0%	64.4%	52.3%	58.0%	58.0%	58.0%	58.0%	58.0%	\$0.10	Current Price
Gross Profits	\$2.00	\$2.15	\$2.66	\$2.61	\$4.06	\$6.38	\$9.28	\$12.76	\$17.40	122	Shares Out
R&D%	13.3%	9.4%	6.7%	10.0%	10.0%	10.0%	9.5%	9.0%	8.5%	1%	Avg. Dilution
R&D Expense	\$0.46	\$0.34	\$0.28	\$0.50	\$0.70	\$1.10	\$1.52	\$1.98	\$2.55	\$12	Cap (M)
SG&A%	97.4%	87.9%	80.6%	64.2%	46.0%	42.0%	40.0%	38.0%	34.0%	\$2	Cash
SG&A Expense	\$3.38	\$3.17	\$3.33	\$3.20	\$3.22	\$4.62	\$6.40	\$8.36	\$10.20	\$0	Debt
Net Operating Margin	-53.1%	-37.6%	-23.0%	-21.9%	2.0%	6.0%	8.5%	11.0%	15.5%	35%	Tax Rate
Operating Income	-\$1.84	-\$1.35	-\$0.95	-\$1.09	\$0.14	\$0.66	\$1.36	\$2.42	\$4.65	16	P/E Multiple
Taxed Operating Income	-\$1.20	-\$0.88	-\$0.62	-\$0.71	\$0.09	\$0.43	\$0.88	\$1.57	\$3.02	15%	Discount Rate
Market Value Using P/E	-\$19.16	-\$14.08	-\$9.89	-\$11.36	\$1.46	\$6.86	\$14.14	\$25.17	\$48.36		
Cash Position			\$1.87	\$0.78	\$0.92	\$1.58	\$2.94	\$5.36	\$10.01		
Shares (M)	122	122	122	123	124	126	127	128	130		
Period Share Price					\$0.01	\$0.05	\$0.11	\$0.20	\$0.37		
PV of MV 4 Years Out	\$0.83	\$3.92	\$8.09	\$14.39	\$27.65					\$0.27	Intrinsic Value
PV of Cash 4 Years Out	\$0.53	\$0.90	\$1.68	\$3.06	\$5.72					182%	Up/Downside
PV MV + Cash	\$1.36	\$4.83	\$9.77	\$17.45	\$33.37						
PV Value Per Share	\$0.01	\$0.04	\$0.08	\$0.14	\$0.27						

CONCLUSION

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

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 expanding margins. Our model quantifies this upside based on what we see now but as the market shifts we expect both growth and investor enthusiasm to expand.

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.

Investors should feel comfortable owning shares at \$0.14 right now with expectations of \$0.27 in the next 12 months.

ABOUT SOUNDVIEW RESEARCH

SoundView conducts **independent research** in emerging technologies. Our approach is to combine **major thematic forces** where technology is involved and use analysis to identify the **most promising companies and investment opportunities**.

Our business model is combination of advisory fees, subscriptions and shared revenue agreements. We measure our success by the quality of our analysis, accuracy of the conclusions and the size and influence of our audience. We apply our own proven approach to valuation that we call intrinsic value (IV) for informing investment decisions and optimizing portfolio management.

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. Except where otherwise noted, 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. 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.
4. SoundView is neither a securities broker/dealer/investment bank nor registered investment advisor.
5. SoundView Technology Group does receive advisory fees, has vested interests and/or may have embedded biases in our work. However our aim is on “fact-based research” and providing a balanced and informed analysis to advance thinking and reach better conclusions.
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 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 platforms¹ and via the internet and social networks. We embrace the online community and social and professional networks to engage with colleagues, clients and investors.

SoundView maintains additional online brands for specialty research products including IPO Candy, Technoplasm and Pactum Cogito. We also collaborate and share with research partners like GigaOM.

CONTACT INFORMATION

Main Address: SoundView Technology Group, 1313 Washington St., 326, Boston MA 02118

Phone: 617-828-6462 **Website:** <http://www.soundview.co>

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