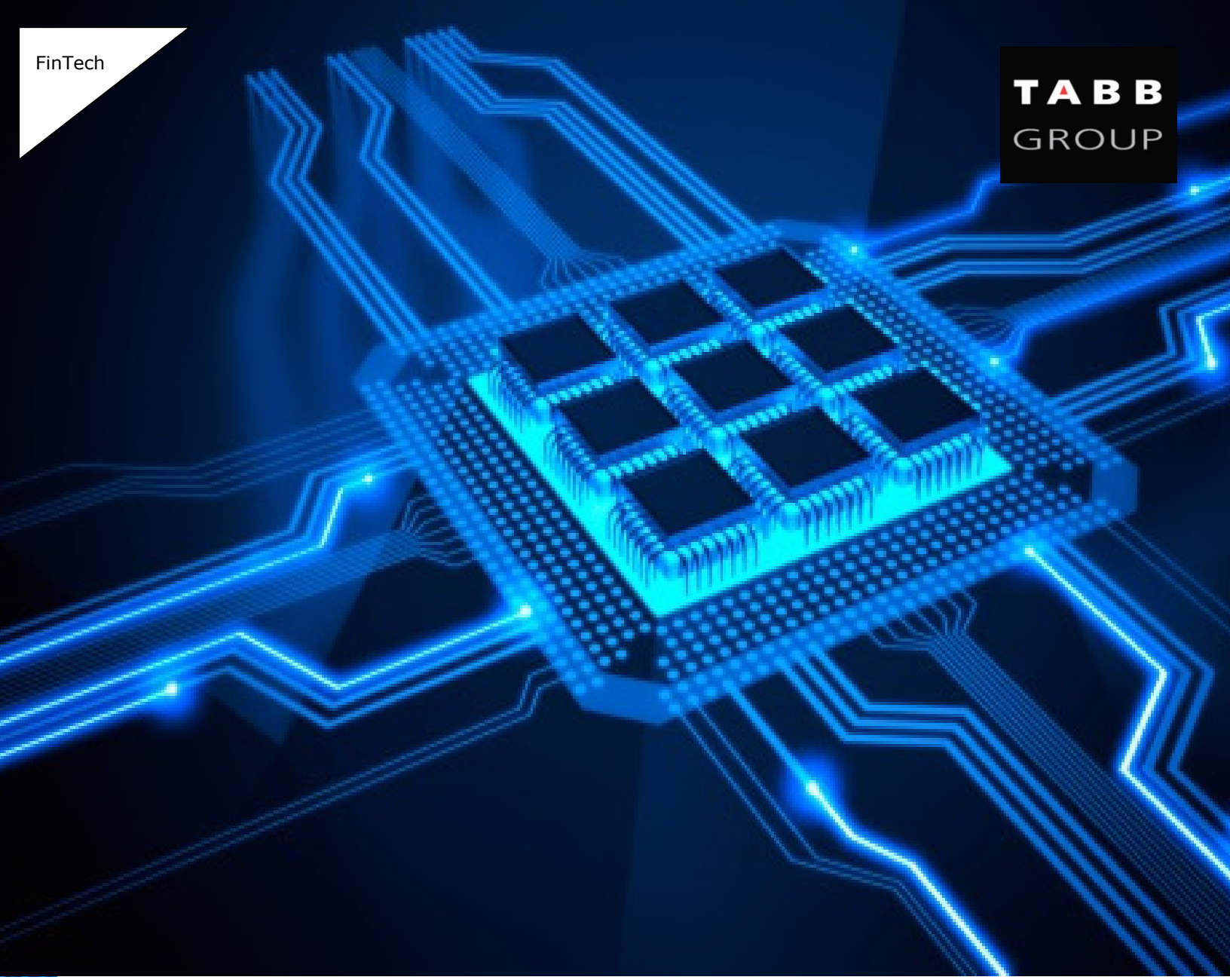
FinTech



Silicon as a Platform:

Empowering the Next Generation of Business

Today's capital markets firms exist in an inter-connected computing world where form and function converge seamlessly in high performance secure environments. When it comes to the computing, it does not matter if you are from the buy-side, sell-side, exchange and/or central clearing space, a vendor or a regulator; your organization is enables by the silicon that empowers and secures your enterprise. Fortunately, today's silicon is not only up to the task at hand, it is supporting unparalleled innovation throughout the sector. Thanks to new technologies developed at the chipset level, firms do not need to sacrifice power, form or security to meet the ever changing demands of the modern markets environment. In this note, we explore what the 'new silicon' can enable; and how your enterprise can harness these innovations to securely execute across an ever increasing set of goals and objectives.

Terry Roche
V14:030
May 2016
www.tabbgroup.com

Introduction

Our lives today are always connected, mobile and data driven for our personal and work experiences. We are constantly on the go, both physically and virtually, and for that reason, we need the devices that propel our lives to be as connected and mobile, while also protecting us from those who would like to use our information against us and/or our firms.

The revolution created by silicon continues to provide significant advancements to capital markets in terms of mobility, ease of use and security. This is made possible by the transistor — a device that is with us all the time and generally taken for granted. The humble transistor is the core building block of our modern technology-driven age; without it, we would be transported back to the 1940s. Developed by Julius Edgar Lilienfeld in 1926, the transistor is the foundation for today's silicon that powers the electronics that drive our world, including your phone, computer, television, the vending machine where you buy snacks or drinks, and virtually everything else that has power. Furthermore, the capability of silicon is continually improving. According to Moore's Law, named after Gordon E. Moore, co-founder of Intel, the number of components on an integrated circuit would double every year. Moore's law — adjusted over the years — now holds that the "…cadence is closer to two and half years than two," according to Brian Krzanich, Intel's current CEO. This constant and unrelenting pace of improvement within silicon is one of the key driving factors in technological progress.

As the power of the transistor has grown and morphed into the power of silicon, silicon's ubiquitous nature has opened up immense possibilities within the capital markets, as well as a host of challenges that we are only just coming to grips with. Specifically, the challenges of security and confidentiality are some of the most critical. In 2001, the Federal Financial Institutions Examination Council (FFIEC) created the following standard for internet banking:

"Financial institutions engaging in any form of Internet banking should have effective and reliable methods to authenticate customers. An effective authentication system is necessary for compliance with requirements to safeguard customer information, to prevent money laundering and terrorist financing, to reduce fraud, to inhibit identity theft, and to promote the legal enforceability of their electronic agreements and transactions. The risks of doing business with unauthorized or incorrectly identified persons in an Internet banking environment can result in financial loss and reputation damage through fraud, disclosure of customer information, corruption of data, or unenforceable agreements."

Over the years, simple security methods such as passwords and tokens have authenticated who is accessing data and systems. Quite often, though, these methods have been defeated. One of the most trusted mechanisms for mitigating the risks identified by the FFIEC is the authentication method that requires multiple layers, known as Multi-Factor Authentication (MFA), for management of access to data and systems.

Silicon is the key to constructing more powerful and sophisticated security methods and ultimately achieving enhanced security.

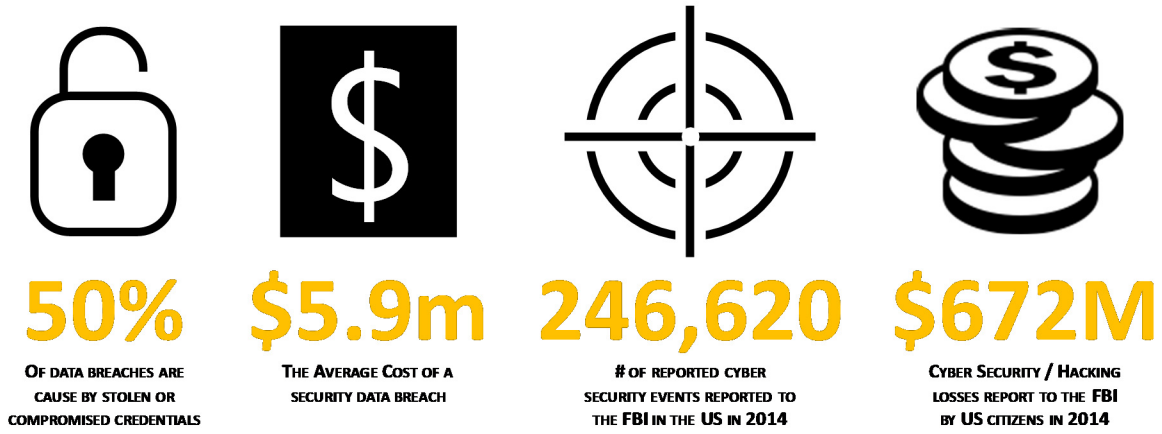
Systems Security at Work

The prime focus of security conversation is often on the cyber aspects of information security, particularly data encryption, as services move to the cloud. Data is unprotected while in transit over networks either private or public, and thus there is attention on the encryption of data while in transit and while residing within infrastructure removed from a client's physical control. A number of cloud services are now using techniques such as hardware security modules to enable encryption key management by the client and not the service provider for end-to-end encryption of data — therefore, protecting the client from the cloud, or the service provider from accessing the client's data. These techniques delivered within a hardware environment are far more difficult to hack than a software-only solution.

The importance of system security cannot be overstated; one massive example of poor systems security was the recent breach at the Office of Personnel Management (OPM) of the United States Government. OPM lost up to 32 billion individual records covering approximately 22 million government employees. An audit done by the US Office of the Inspector General reported in part, *"We believe that the volume and sensitivity of OPM systems that are operating without an active Authorization represents a material weakness in the internal control structure of the agency's IT security program…"*

According to one former intelligence officer, "the OPM breach represents the most damaging loss of US government information since the Rosenbergs and the loss of the atomic bomb." The OPM breach is but one example of poor standards and processes resulting in cataclysmic outcomes (see Exhibit 1).

Exhibit 1: Security Exposure



Source: TABB Group, FBI, Verizon, PWC

One must take into consideration the significant security challenges posed by co-workers. During the working day, everyone has several opportunities to expose, whether intentionally or inadvertently, confidential or sensitive information about their firm, clients or even

themselves. Alternatively, there is opportunity for those physically within the workspace to obtain information for which they are not authorized to access. At best, when confidential information is compromised, it creates an uncomfortable work environment — a place where someone may find out what others are earning or where a confidential personal detail is exposed. At worst, unauthorized access to information leads to information theft, from company secrets to national security breaches. As it pertains to capital markets, unauthorized access to data could compromise personal information of that particular capital market institution's client base and thus conflict with regulations designed to protect the Personal Identifier Information (PII) of clients or reveal highly proprietary trading strategies and positions. Therefore, it is an absolute priority for organizations to ensure that only those authorized to have access to data and systems do so.

Historically, the primary method of authentication to allow a user access to systems and information has been the single-factor authentication process, also known as the password. However, it has become clear that passwords, which are often weak, are no longer sufficient to guarantee the security of your systems and data. Information security standards provide improved password strength through complexity requirements such as minimum character length, password history to ensure non-replication of passwords, special characters and non-dictionary words. Even with these standards, though, malware and phishing are used to obtain passwords and then compromise systems. Moreover, the computational power available within today's systems and field-programmable gate array (FPGA) platforms enable blunt force attacks to break down the files where the passwords are maintained, therefore, exposing even the strongest of passwords.

Military strategy has shown over the centuries that a single point of defense is a flawed concept and often easily overwhelmed. When there is only one thing to assault, the attacker is able to concentrate its resources and overwhelm the opposition. Therefore, it is critical that a series of defenses, also known as "defense in depth," is used to reinforce the protective measures in collaboration with one another.

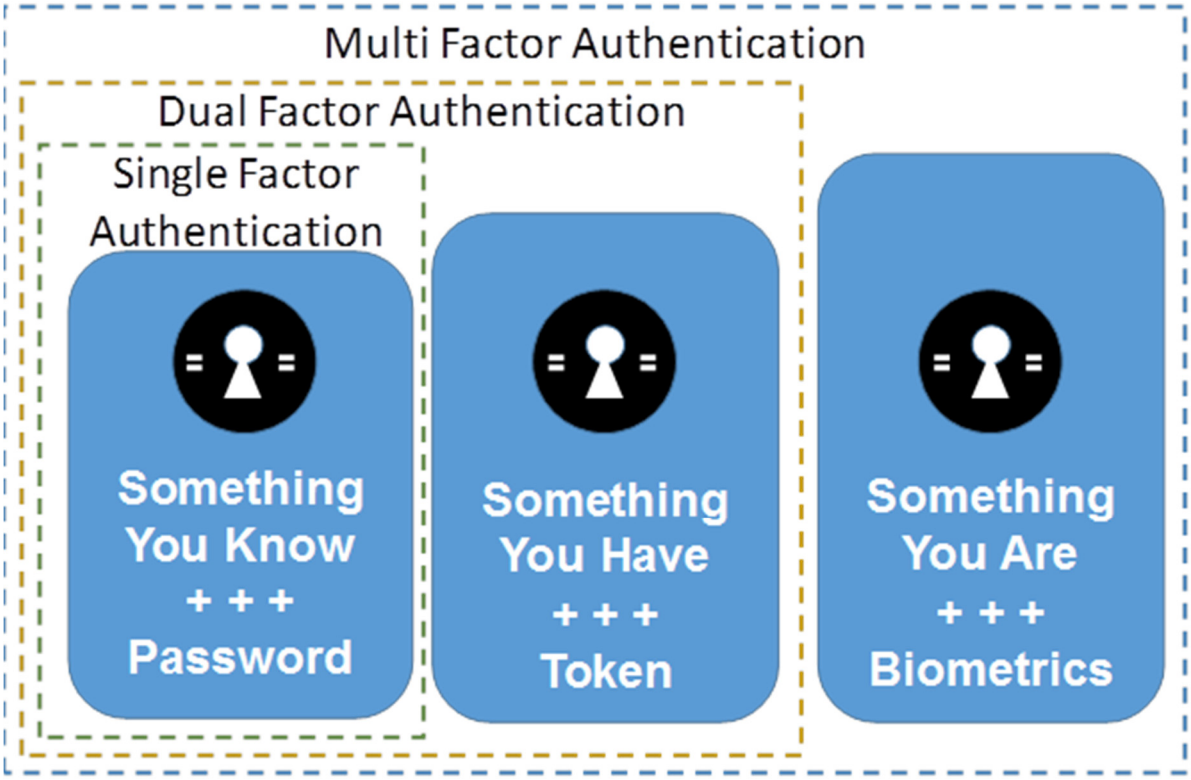
Within a layered "defense in depth" for information security, there are many aspects in play — firewalls, encryption, hardware security modules and more, with passwords being the last line of defense and perhaps the weakest. Therefore, a modern information security regime of authentication must include the use of multi-factor authentication.

Multi-Factor Authentication

In basic terms, multi-factor authentication (MFA) is a mechanism in which more than one validation is required to verify the user's identity. Historically, the financial services industry has been using simple MFA procedures to enable secure access to automated tellers with a bankcard and PIN. Likewise, for more secure operational areas within some institutions, firms have required access cards and biometric validation through the use of hand-geometry readers. These systems, while effective, are expensive to implement and difficult to maintain. They require high-end specialized equipment to enable, and are completely unsuitable in a distributed work environment.

Due to amazing improvements within the distributed compute environment, though, today's MFA is not only cost-effective, it also can be enabled across a global footprint with minimal investment and maximum impact. The improved MFA relies on a combination of logical, knowledge and biometric validation techniques to secure systems or services. Regulations such as the Federal Financial Institutions Examination Council (FFIEC) directive requiring multi-factor authentication for internet banking transactions have amplified the drive toward multi-factor authentication. The SEC and CFTC provide further indication of the regulatory attention focusing on MFA within the Consolidated Audit Trail (CAT) mandate. The goal of the CAT is to collect all data on a daily basis related to the United States equities and commodities markets. The CAT requires the CAT Plan Processor implement multi-factor authentication capability for all logins (including non-PII).

Exhibit 2: Multi-Factor Authentication



Source: TABB Group

MFA combines these credentials to strengthen exponentially identity security for access to systems, applications and data.

Authentication Factors

There are a number of authentication factors for identity validation. Each factor increases the certainty that the person or entity accessing the system is who or perhaps what, they represent themselves to be — a true interlocked "defense in depth", highlighted in Exhibit 2 and below.

- **Knowledge factors** are information that a user must provide to enable login. Yes, password still plays a part in MFA. However, as noted, the use of a password significantly strengthens authentication when used with other forms of validation. Passwords, answers to secret questions, PINs, etc. fall into this category.
- **Possession factors** are things a user would have in their possession such as a security token, an employee ID, a phone's SIM card, etc.
- **Biometric factors** are physical or biological traits of the user that must be verified for login. This includes the full scope of biometric authentication techniques such as facial recognition, fingerprint scans, iris scans, voice recognition, hand geometry and more. Historically biometry authentication has been hampered by the amount of processing power needed to run the scans and thus this method was only available at the server level. With advancements in the latest releases of silicon, sufficient processing power is now available to all devices.
- **Location factors** are also now available for security screening. Since many people are never more than an arm's reach from their smartphones, the Blue Tooth capabilities on the smartphone can signal the location of the user and thus whether or not the user can log into the system they are trying to access. Once again, the power of the newest silicon makes this available to all.

Additionally, location factors are another authentication method now available for security screening. Many people are never more than an arm's reach from their smartphones, and the Blue Tooth capabilities on the smartphone can signal the location of the user and thus whether or not the user can log into the system they are trying to access. Once again, the power of the newest silicon makes this available to all.

Hardened Multi-Factor Authentication Vault

Typically, there is a need for users to install client software to make multi-factor authentication operate. There may be a number of different software packages to deploy to the client machine to make use of a smart card or token, which in turn adds to the support burden and any conflicts with existing client applications.

Even with the methods of multi-factor authentication in place, there still is another step. Traditional user identification and password login methods need a database to hold the information that identifies the user and to store the passwords or other records of authentication of that user. If such a database is penetrated, the game is over. The brute

force attacks that are common today are a real threat to access of the secrets that provide entry to the systems and data.

The lack of technical standards to enable an open, interconnected and straightforward delivery of MFA has created some barriers to deploying a costly and complex MFA environment.

Intel has developed a solution to address this security challenge in the new 6th Generation Core vPro platform. Combined with Windows 10 there is now a seamless and complete level of security that addresses many of the issues in this space. Intel Authenticate is a hardware-based solution for multi-factor authentication within the silicon. What this means is that the secret information, possession, knowledge, and biometric factors and more locked away within the hardware of the silicon, unlike software, cannot be hacked.

So How Will All of This Help?

We have all left our workstations with our systems logged in and displays live. During the course of an active day, physical information security is rarely a priority. Getting to the meeting, running out to lunch or a personal emergency is always at top of mind, not the state of our systems' security. Thus for our systems to be secure, methods must become available that will operate on behalf of the user without the need for the user to be a conscientious security officer.

The built-in camera on every workstation, laptop and two-in-one enables the use of facial recognition. Once registered, the end user will no longer need to remember passwords. Instead, the user will only need to smile at the camera. The passwords are protected in the microprocessor itself.

Likewise, the vast majority of us have our smartphones with us at all times, day or night. A user will mate his smartphone to the desktop, laptop or two-in-one and when the user is physically away from the machine and out of Bluetooth range, the machine will shut down to protect its contents.

The next generation of microprocessors makes all of this easy. Multi-factor methods such as fingerprint biometrics, rotating PIN systems and the strength of your Blue Tooth signal enhance security, and are protected in a safe hardware vault within the silicon itself. These capabilities control information access, application access and machine access.

Formerly, information security had a significant physical dynamic. Identity verification occurred, at least partially, through one's physical presence at a location. Our world has moved on to be mobile, virtual and constantly changing, to deliver significant improvements in worker productivity. This transition to the virtual work experience would not be possible without the layers of protection and authentication that enable our professional lives to be secure and mobile.

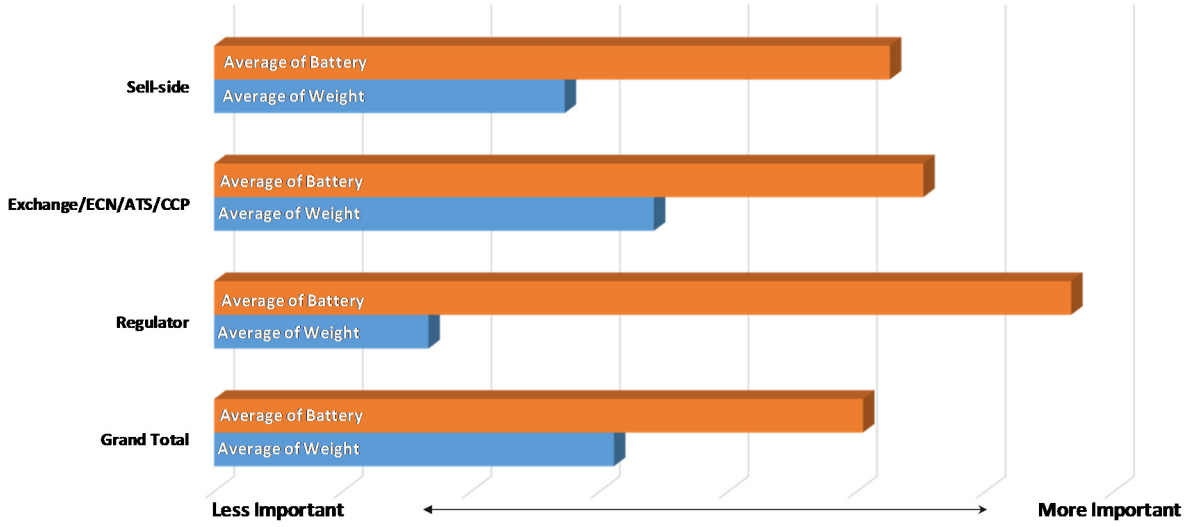
You Are Mobile

A capital markets information worker's technology considerations change once they are mobile. Freed from the desk, you need to carry the office with you. The form factor, weight and battery life of your devices are now of paramount importance. Microprocessor advancements have assisted in driving more extensive capabilities into smaller packages and have materially extended battery life, all while providing powerful computing devices on the go.

Thankfully, new advanced mobile processors allow users to leverage advancements in power consumption with improved form factors. As an example, newer 14-nanometer processors enable fan-less mobile devices, which reduces both size, weight and power consumption capabilities. Engineers were able to achieve this through improved design specifications that lower heat output while improving heat dissipation characteristics. Moreover, they were able to achieve significantly smaller desktop form factors to the order of twenty-five times smaller than previous generations.

In an effort to determine which of these factors were most valuable to capital markets users, Tabb Group asked users to rate which factor was more important to them, battery life or weight. While both factors garnered exceptionally high ratings, the response was unanimous across the board: improved battery life is more important than improved form factor (meaning weight and size) (see Exhibit 3).

Exhibit 3: Mobility Form Factor Preferences



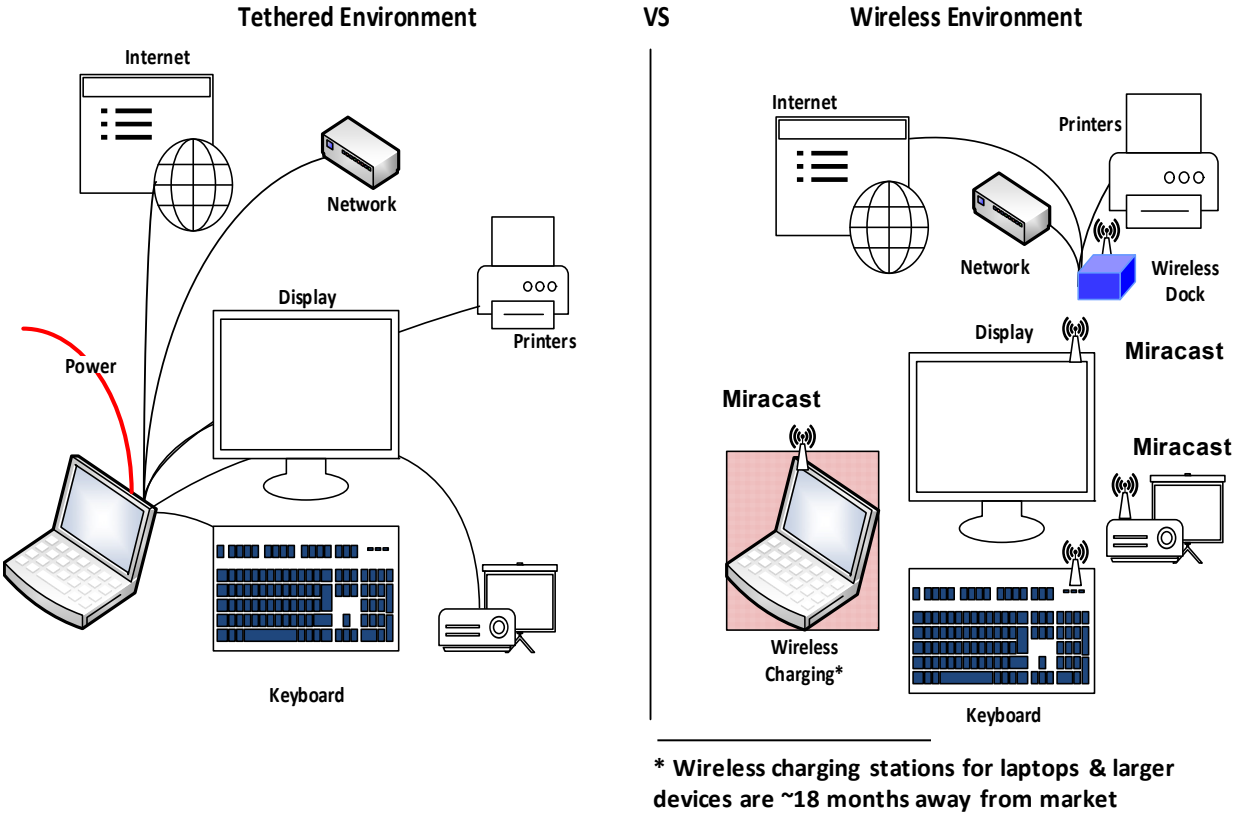
Source: TABB Group

There have been leaps in efficiency in battery life and capability. We see significant reductions, as much as 80%, in silicon power drain from the next-generation chipsets. Additionally, these new products are delivering twenty-five times better graphics performance and low power options for HD-like video conferencing and audio — all adding up to a better experience in terms of usability and sustainability.

When You Are in the Office

Part of being a mobile workforce, however, also requires working in the office; therefore, the office must accommodate the flow of workers from mobile to office located. Hot desking is often cumbersome and slows down work due to the need to connect to the office infrastructure. A wired office has many challenges as it pertains to ease of use and swift collaboration. There are multiple adapters to connect that delay in your sharing of information within a conference room or becoming productive as you find a space to do your work. Moreover, the wired infrastructure has a support cost and burden that is now unnecessary. Innovative technologies are solving some of the nettlesome challenges of being in the office, with new models of wireless; dynamic interaction and productivity now available to the information worker (see Exhibit 4).

Exhibit 4: Tethered vs. Wireless Workspace



Source: TABB Group

Wireless docking provides the same performance as a wired HDMI/DP or USB 3.0 port and is a great assistance to freeing workers. Wireless also extends the ability to power multiple devices without wires — features all made possible by newer, more efficient platforms combined within a Software-Defined Infrastructure (SDI) approach. Additionally, technology such as Miracast, a peer to peer WiFi Direct connection, shown above, allows a user to share a screen to a larger display, which helps to create ease of collaboration and a more natural meeting flow and flexibility since it is done dynamically and does not waste time

physically connecting to the office infrastructure. We are also seeing enhanced collaboration for those in the office as well as mobile via the use of touch-enabled smart whiteboards. Often the best and most collaborative ideas originate during whiteboard sessions, and extending this capability is key to collaboration. Intel Unite is an example of collaboration software that enables wireless integration of existing conferencing equipment or collaboration tools easily, quickly and securely as the data is encrypted. Reduction of the time it takes to start a meeting goes from many minutes to only seconds. The minutes saved results in weeks of productivity recaptured, depending on the size of the firm, over the course of a year.

Conclusion

The pace of activity within our lives is accelerating, not slowing down. This is happening in terms of our mobility and the threats we face by those who would use our information to harm us. While you are on the move, you need access to both your personal and work data. The data demands placed on your business life, however, are more stringent than those within your personal life. You do more for longer hours with your business products than typically your consumer products. Your tools for work historically have been more powerful and far more complex in terms of accessing your business networks, applications, data and peripherals — all requiring information security protections that are even more complex and restrictive, while perhaps still not delivering the protection you and your firm needs.

This no longer needs to be so for the work environment. Advances in silicon combined with advances in operating systems enable the seamless ability to be mobile, connected and secure. You are on the run and need your tablets, two-in-ones, laptops and desktops all the time. The smaller these devices are, the more easily mobile you are. The longer lasting the battery, the more time you can be connected. The easier it is for you to connect to the workplace, collaborate and share ideas, the more productive you ultimately are.

The core enabling capability however is security. Security of our data, applications and personal information should always be of paramount importance for both our personal and professional lives. Ensuring the identity of those accessing our platforms is the first line of a number of important steps toward achieving systems and information security. The more factors one is able to combine to define identity creates an exponentially stronger security blanket.

Our lives, data and systems now virtual, safe, connected and efficient. All made possible by the advancements within silicon.

About

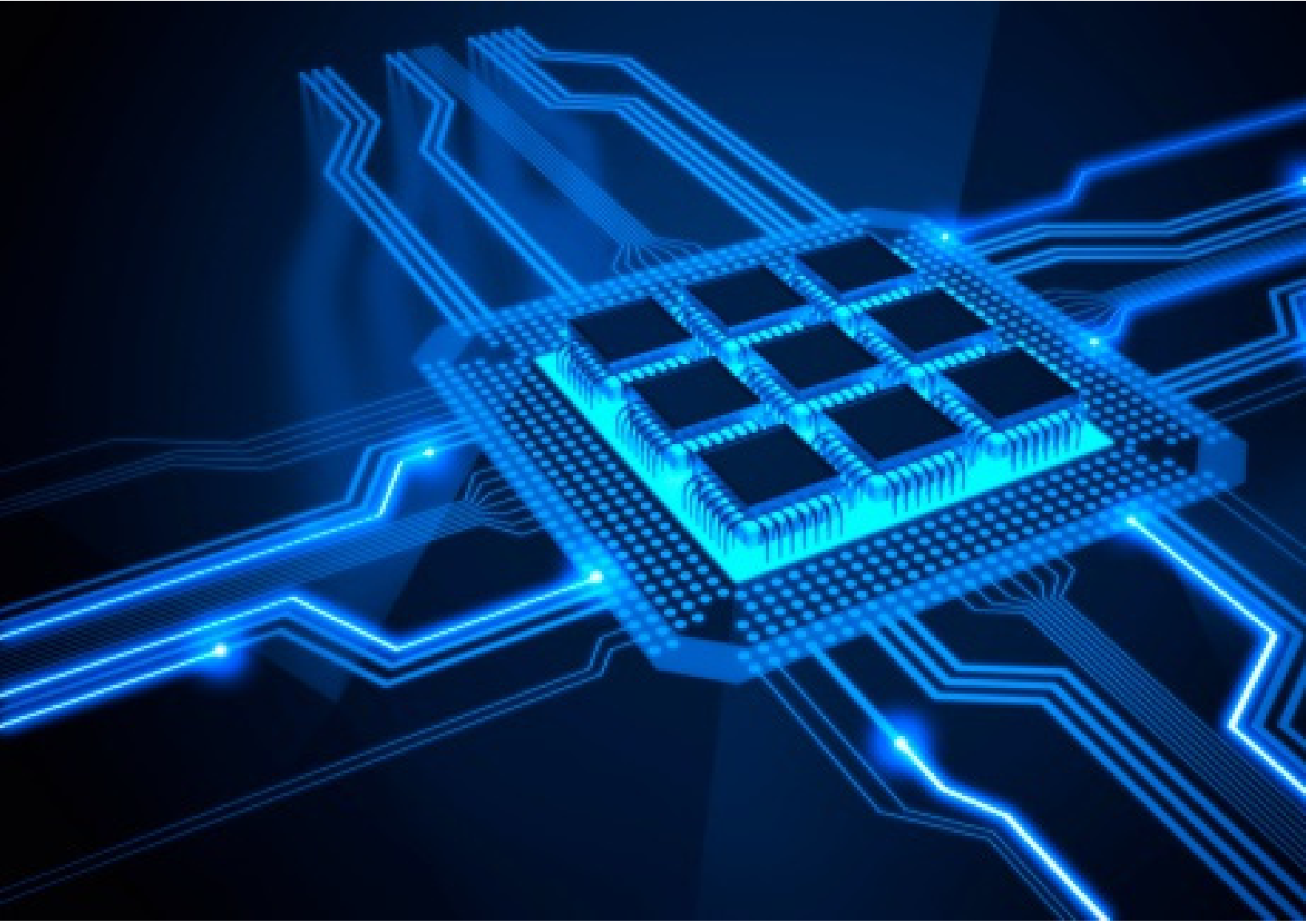
TABB Group

TABB Group is a financial markets research and strategic advisory firm focused exclusively on capital markets. Founded in 2003 and based on the methodology of first-person knowledge, TABB Group analyzes and quantifies the investing value chain from the fiduciary, investment manager, broker, exchange, and custodian. Our goal is to help senior business leaders gain a truer understanding of financial market issues and trends so they can grow their businesses. The press regularly cites TABB Group members, and members routinely speak at industry conferences and gatherings. For more information about TABB Group, go to www.tabbgroup.com.

The Author

Terry Roche

Terry Roche is responsible for the FinTech practice at TABB Group. Prior to his current role Terry was Chief Operating Officer at NYSE Technologies, and previously he held a number of executive positions at Thomson Reuters and Reuters, including Managing Director, Global Head of Elektron Real Time and Platform, along with Global Head of Strategic Business for Focus Group Accounts. Terry also held a number of senior positions at HSBC that included Global Head of Market Data, Head of Global Middleware, and Commercial Director, Fixed Income e-Commerce. Terry is an industry veteran with 30 years' experience. He began his career at Telerate, and his work experience includes Salomon Brothers; Republic National Bank of New York, where he was head of trading infrastructure and data; and WhiteTree Solutions, an advisory firm he founded.



www.tabbgroup.com

New York
+ 1.646.722.7800

Westborough, MA
+ 1.508.836.2031

London
+ 44 (0) 203 207 9477