Middle Market Update

2nd Quarter 2017

Second Quarter Economic Performance and Future Outlook

Aramar Capital Group, LLC

Gross Domestic Product

- The real U.S. GDP increased at an annualized rate of 2.6% in Q2 2017, up from the 1.2% annualized growth rate in Q1 2017, primarily due to[1]:
  - Positive contributions from personal consumption expenditures, nonresidential fixed investment, exports, and federal government spending, which were partially offset by:
  - Negative contributions from private residential fixed investment, private inventory investment, and state and local government spending

Consumer Income and Spending

- Real disposable personal income grew by 3.2% in Q2 2017, a faster pace than the 2.8% growth witnessed in Q1 2017[1]
- Consumer spending rose 2.8% during Q2 2017[1], propelled by a strong stock market, still-improving employment numbers, and wages outpacing inflation

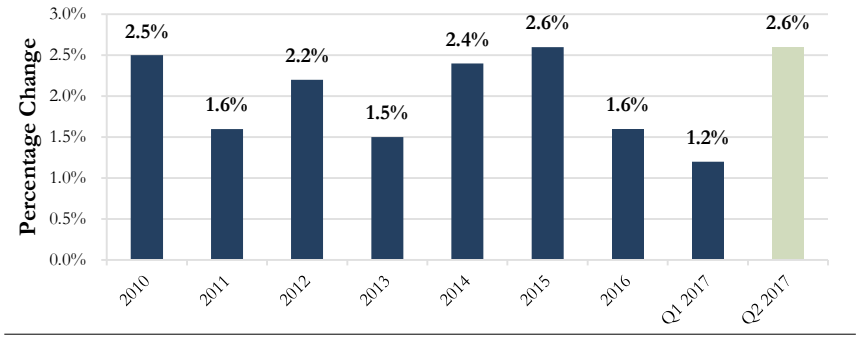
Federal Reserve

- The Federal Open Market Committee (FOMC) views recent economic activity as moderately positive, and expects the GDP to expand, labor markets to further strengthen, and inflation to stabilize at its 2.0% target over the medium term, with support from the Fed's monetary policy[2]
  - During its June meeting, the FOMC increased the federal funds rate's target range by 25 basis points
- The committee expects that economic conditions will evolve in a manner that will justify gradual increases in the federal funds rate, but expects it to remain below anticipated long-term rates for some time[2]

Employment

- The unemployment rate declined slightly to end Q2 2017 at 4.4%, with the total number of unemployed persons at 7.0 million[3]
- U.S. employee wage growth is under 3.0%, despite a 16-year low in unemployment and the third-longest economic expansion on record[4]
  - A key proxy for sustainable wage growth – the sum of business selling price and worker productivity increases – is the lowest in more than 60 years at 2.0%

Real GDP Growth Since 2011 (annualized)



Source: U.S. Bureau of Economic Analysis

U.S. Treasury Securities

- The 10-year Treasury Note yield decreased from 2.40% at the end of Q1 2017 to 2.31% at the end of Q2 2017[5]
  - The yield curve flattened, with only an 89-basis-point spread between the 2- and 10-year securities

	Q3 2016	Q4 2016	Q1 2017	Q2 2017[6]
5-year Treasury Note	1.18%	1.69%	2.01%	1.86%
10-year Treasury Note	1.61%	2.21%	2.52%	2.32%
30-year Treasury Note	2.49%	3.05%	3.27%	3.12%
10-year Treasury Inflation Protected Security	0.08%	0.33%	0.44%	0.44%

Source: U.S. Department of Treasury

Outlook for 2017

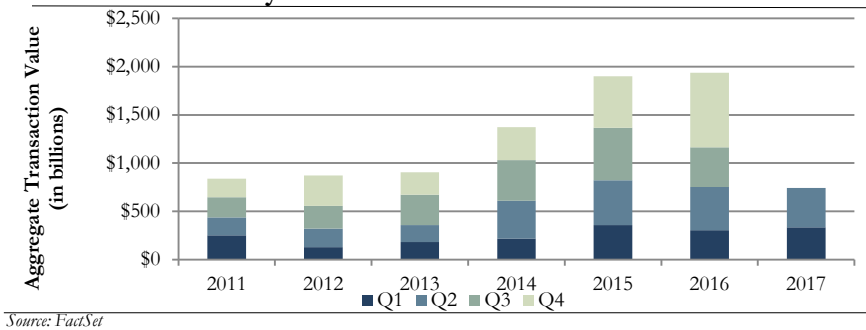
- The World Bank Group projects that the real U.S. GDP will grow by 2.1% in 2017[7]
  - Improving labor market conditions, potential tax cuts, and new infrastructure programs could lead to stronger-than-expected growth in the short term
- PwC's "Economic Uncertainty Index" has reached an all-time high[8]
- Just one-third of surveyed fund managers expect global profits to improve during the next 12 months, the lowest level since the end of 2015 when oil prices were in a freefall[9]

1. *U.S. Bureau of Economic Analysis*
2. *U.S. Federal Reserve*
3. *Bureau of Labor Statistics*
4. *Fox Business*
5. *Baird*
6. *Quarterly yields are three-month averages*
7. *The World Bank*
8. *PricewaterhouseCoopers: The Index is comprised of three components: the first quantifies newspaper coverage of policy-related economic uncertainty, the second reflects the number of federal tax code provisions set to expire in future years, and the third uses disagreement among economic forecasters*
9. *Bank of America Merrill Lynch*

Mergers and Acquisitions and Private Equity

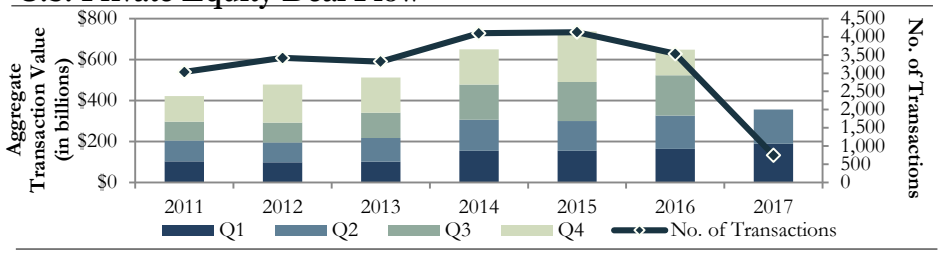
- H1 2017 saw 8,077 global mergers & acquisitions (M&A) worth $1.5T, a drop of 11.9% in deal count, but an increase of 8.4% in total deal value compared with H1 2016[1]
  - Many deal makers sat on the sidelines due to an uncertain economic outlook, pockets of political instability, and currency volatility, but a spate of cross-border megadeals drove global M&A value higher, even as the number of deals fell
  - Energy, mining, and utilities was the most active sector, with 662 deals valued at $267.9B, benefiting from a strong revival in investor sentiment thanks to higher commodity prices
- The North American M&A market had 2,715 transactions worth $656.4B in deal value in H1 2017, a 9.4% decrease in deal count but a 5.7% increase in deal value compared with H1 2016[1]
  - More than 40% of all M&A value in North America came from two sectors: energy, mining, and utilities and consumer, driven in large part by acquirers betting on rising commodity prices and the effects of consumer spending shifting from brick-and-mortar stores to online shopping
  - The median M&A deal size increased to $45.0M in H1 2017, up from $30.9M in 2016, largely due to the effect of certain outsized transactions, the raising of larger PE funds, and relatively easy access to leverage to fund PE-backed M&A transactions, which represent close to one-third of total deal value[2]
- Cross-border activity continued its steady upward trend in H1 2017, as the value of international deals grew 27.7% to $703.4B, while the value of domestic transactions decreased 4.4% to $788.9B, primarily attributable to cross-border mega deals in and out of North America[1]

U.S. M&A Activity



Source: FactSet

U.S. Private Equity Deal Flow



Source: PitchBook

- U.S. PE (private equity) investments recorded 866 completed deals worth $151.1B, an increase from Q1 2017, but a slight decrease from Q2 2016[2]
  - Aided by lower high-yield credit spreads and armed with $545.5B in dry powder, PE firms are continuing to deploy capital, despite historically high multiples
  - Debt usage has scaled right back up, with median debt levels reaching 56.3% of enterprise value in H1 2017, up from 50.0% in 2016
  - After climbing fairly steadily since 2006, add-on acquisitions now represent nearly two-thirds of buyout activity, reaching 64% in H1 2017 from 46% in 2006, as they enable PE firms to be more competitive valuation-wise with strategic buyers due to synergies
- In the middle-market, PE firms invested $236.9B over 1,086 deals in H1 2017, on pace with H1 2016's deal count and a 22.7% increase in value[2]
  - The median PE deal size grew to $208.5M in Q2 2017, up from $129.3M in 2016
  - PE firms consummated larger deals on average, as such buyers sought to deploy larger fund sizes and acquire platforms with greater critical mass in order to facilitate add-on acquisitions
  - IT deals accounted for an impressive $65.0B in deal value over 175 deals, surpassing the amount invested in IT companies during all of 2016
- After reaching a new post-financial crisis high of 10.7x in 2016, the median EV/EBITDA multiple slightly decreased in H1 2017 to 10.5x[2,3]
  - The latest available data for PE-sponsored transactions between $10M and $250M showed an average EV/EBITDA of 6.7x for Q2 2017, down from 6.9x in Q1 2017[4]
- U.S. PE exits continued the downward trend that began in 2015, with $85.8B in exit value over 470 deals in Q2 2017, a 26.0% decrease from Q2 2016 and on track to be down 46.5% for 2017 as compared to 2016[2]
  - The decrease is largely due to a reduction during the past two years in the number of older portfolio companies owned by PE firms, as they exited companies held through the last recession

1. *Mergermarket*
2. *Pitchbook*
3. *These multiples reflect prices paid for mainly public companies and do not account for smaller private company transactions (for which there typically are no publicly available data) that tend to change hands at much lower multiples*
4. *GF Data*

Venture Capital, PIPEs, and Corporate Earnings

Venture Capital Investing

- In Q2 2017, transactions for venture capital (VC)-backed companies in the U.S. totaled 1,152 deals valued at $18.4B, a 27.0% increase in value and 4.0% decrease in volume from Q1 2017[1]
  - VC dollars invested jumped due to a surge of mega-round investments (capital raise rounds of $100.0M or more) to 31, the highest in the U.S. since Q3 2015
  - Nearly 170 private companies are valued at $1.0B or more, up from 60 three years ago and none prior to the most recent financial crisis[2]
  - Strategic companies' interest in VC deals remains strong, as such companies participated in 26.0% of the deals in Q2 2017, often as a means of establishing early alliances with promising startups and technologies
- With $8.7B invested over 505 deals in Q2 2017, the internet sector received the largest amount of funding for the 31st straight quarter [1]
  - Digital health sector funding reached an eight-quarter high, topping $2.7B
- North American venture funds have approximately $96.0B in uninvested capital, the most on record, and SoftBank Group recently launched a $100.0B vehicle to invest in private technology firms, the largest such fund ever[3]
- Globally, while deal activity increased marginally from the previous quarter, dollars invested rose sharply from $28.0B in Q1 2017 to $42.9B in Q2 2017, a 53% increase[1]

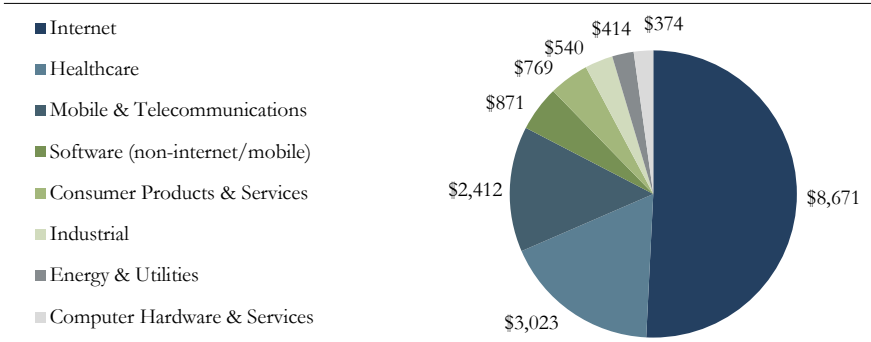
PIPE Investing

- 339 private-investment-in-public-equity (PIPE) deals totaling $19.1B closed in Q2 2017, representing a 7.6% decrease in volume and a 10.3% drop in value from Q1 2017[4]
- Despite the slight decrease in PIPE activity during Q2 2017, the market remains strong, with the quarter representing one of the few quarters to surpass the $19.0B mark during the past 20 years[4]
- PIPE investors continue to invest in small-cap companies requiring significant capital to attain profitability, such as biotechs[4]

Corporate Earnings

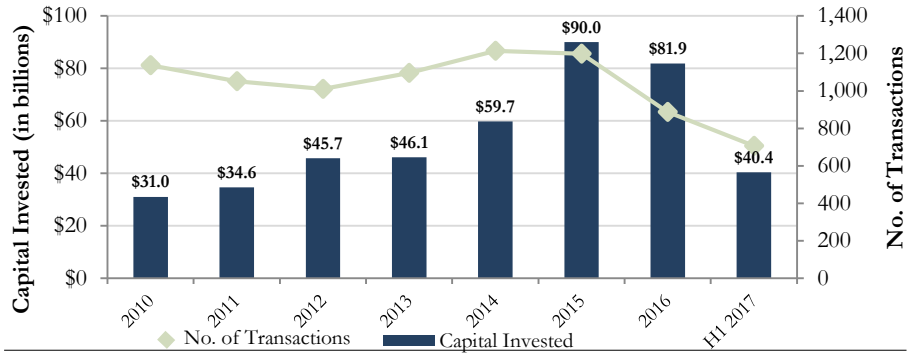
- Corporate earnings for Q2 2017 are on pace to increase 10.2% from the same period last year, marking the second consecutive quarter of double-digit, year-over-year growth since Q4 2011[5]
  - With 91% of S&P 500 companies having reported earnings, 73% of them beat their EPS estimates
  - Portending a slowdown in corporate earnings growth, 63% of the companies that have reported forward-looking EPS guidance have provided negative guidance for Q3 2017
- The forward S&P 500 12-month P/E ratio is 17.7x, above both the 5-year and 10-year averages of 15.4x and 14.0x, respectively[5]

U.S. VC Deal Value Per Industry (in millions) – Q2 2017



Source: MoneyTree Report

U.S. PIPE Activity



Source: DealFlow Report

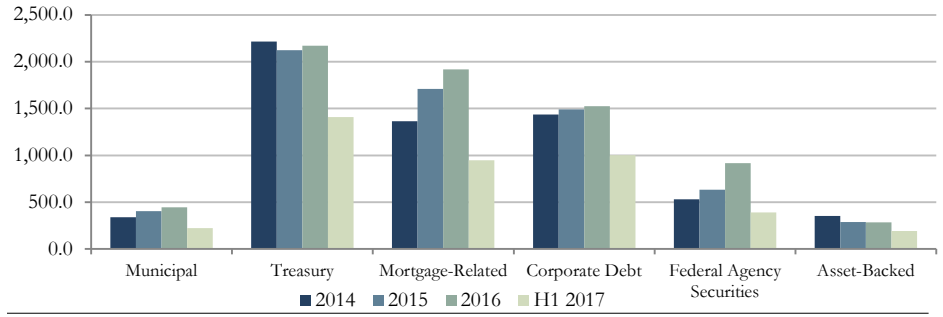
1. *PricewaterhouseCoopers*
2. *Dow Jones VentureSource*
3. *Preqin*
4. *The Deal*
5. *FactSet*

Debt Capital and IPO Markets

Debt Capital

- The Barclays U.S. Aggregate Bond index recorded a 1.5% positive return during Q2 2017, a slight increase from the 1.2% return in Q1 2017[1]
  - U.S. corporate bonds remained an "in-demand" asset in Q2 2017, particularly from foreign investors looking for better yields in light of ultra-low rates and quantitative easing programs in many other developed countries
- The Barclays Investment Grade U.S. Corporate Bond index generated a positive return of 2.5% in Q2 2017, above the return of 1.2% experienced in Q1 2017, but below the 3.6% experienced in Q2 2016[1]
  - Demand from Asian investors and the re-engagement of domestic life insurers in the purchase of long-term corporate bonds have contributed to the tightening of corporate investment grade bond spreads, as demand continues to outpace new supply[3]
- Total U.S. bond issuances reached $1,738.7B in Q2 2017, a 6.8% decrease from the Q2 2017 level of $1,864.5B and a 10.0% drop from the Q2 2016 count of $1,931.0B[2]
  - The largest contributing factor to the decline in U.S. bond issuances in Q2 2017 was the decreases in Treasury and corporate bond issuances, which totaled $570.8B and $393.6B and declined 12.7% and 17.9%, respectively, from Q1 2017
  - The drop in U.S. corporate bond issuances was driven by decreases in both high-yield and investment grade debt issuances, which hit $64.6B and $329.0B in Q2 2017, representing 27.3% and 15.8% slides from the Q1 2017 volumes, respectively
  - Asset-backed debt issuances reached $101.4B in Q2 2017, a 32.1% increase from Q1 2017 and almost two times the volume issued in Q1 2016

Issuances in the U.S. Bond Market ($ billions)



Source: SIFMA

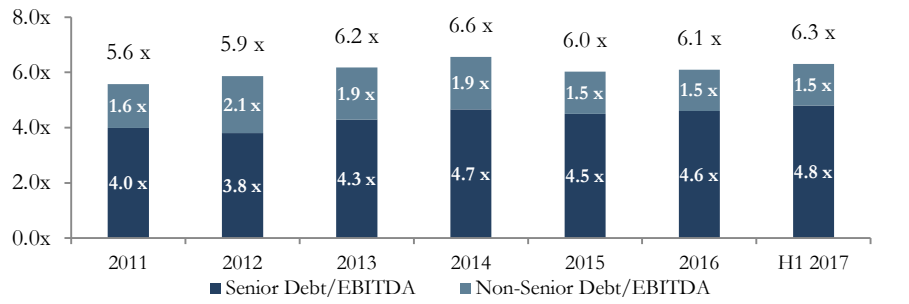
Middle-Market and Household Loan Lending

- Total middle-market lending reached $79B in H1 2017, a significant increase from $53B in H1 2016, as companies raised or refinanced debt facilities in advance of anticipated rate hikes[4]
  - This significant increase was most pronounced in the larger segment of the middle market ($100.0M to $500.0M), which experienced a 61.5% increase, reaching $63B in H1 2017 from $39B in H1 2016
  - Yields on newly issued loans ticked upward, with large corporate credits averaging 4.7% and middle-market loans hitting 6.2%
- Average debt-to-EBITDA levels for broadly syndicated LBO transactions increased to 6.4x in Q2 2017, up from 6.0x in Q1 2017[4]
  - The technology industry continued to have the most leveraged loan issuances in the first half of 2017, representing 13.7% of total loan volume
  - The debt-to-EBITDA ratio was higher for institutional middle-market LBOs, reaching 6.2x in Q2 2017, up from 5.6x in Q1 2017
- U.S. household debt increased in Q2 2017 for the 12th consecutive quarter, peaking at $12.8T, a $114.5B and 0.9% increase from Q1 2017[5]

IPO Market

- In H1 2017, 91 companies went public on U.S. exchanges, raising $27.9B, a 240.2% increase compared to $8.2B for 42 companies in H1 2016[6]
  - Rebounding from a lackluster 2016, H1 2017 U.S. IPO activity surged amidst a backdrop of stable economic indicators, strong job growth, improving corporate earnings, record stock market levels, and low market volatility[7]

Debt Multiples of Middle-Market LBO Loans



Source: Thomson Reuters LPC

1. *Prudential*
2. *SIFMA*
3. *Guggenheim*
4. *Thomson Reuters LPC*
5. *Federal Reserve Bank of New York*
6. *Dealogic*
7. *PricewaterhouseCoopers*

Cybersecurity Risks and Preventative Measures

By Jerri Ravi and Lena Licata, EisnerAmper

Data is at the core of many companies' business operations. However, securing the tremendous amount of data collected on a day-to-day, even second-to-second, basis poses a monumental challenge to companies. Securing this data is critical in maintaining a healthy business operation.

What's at Stake?

Cybersecurity poses threats to all businesses: big and small. Hacking is a game for those doing the hacking: sometimes they do it for fun and other times they do it for financial reward at the cost of their victims. Even Fortune 500 companies can fall victim (*e.g.*, Sony $35 million, Home Depot $28 million, and Target $235 million in expenses).

Even when the costs are relatively small in comparison to total revenues, these events can significantly affect the reputation of a company. To prevent attacks like these a company must develop and maintain an effective, comprehensive cybersecurity program.

Most Common Reasons for Data Breaches

- Insider negligence is the number one internal threat
- Ransomware and phishing attacks are a growing threat
- Employees' jobs require them to access more proprietary data
- Companies aren't tracking employees' access to confidential data
- Many organizations have no searchable records of file system activity
- Companies are slow to detect unauthorized file access
- End users are not deleting files, thus exacerbating vulnerability
- Moving to the cloud is happening much more slowly than expected
- Too many companies aren't taking security seriously enough

Ownership, Access Rights, and Controls

The first decisions a company faces after determining what key data it maintains are who owns the data and who has the ultimate responsibility over the security of said data.

Someone with the requisite IT skills and experience should be charged with establishing governance along with the related cybersecurity roles and responsibilities. While this governance is created through IT, senior management should have a hand in evaluating the success metrics moving forward.

Part of the governance is developing clear procedures for granting data access. The IT personnel responsible for granting this access should obtain authorization from the leadership/data ownership to ensure "least privilege access" to the data. Least privilege means limiting access to only what the user needs. Many data breaches occur when users have more access than necessary and/or when user roles change but access rights stay the same. Unauthorized access to things such as server rooms and data centers also pose a serious threat.

Policies, Procedures, and Incident Response

Once data ownership and accessibility are established, the designated representative should document clear policies and procedures that outline:

- What are key data elements for the company? Does it store personally identifiable information (PII), payment card information (PCI), or protected health information (PHI) data? Does it have and digitally store intellectual property?
- How does the organization store data?
- What are the backup and recovery plans? How often should the company test the reliability of these plans?
- What are the obligations of employees to keep this data secure?
- What proactive mechanisms does the company use to secure this data?
- What actions would be taken in response to a cyber-attack?

Creating this documentation is an often-overlooked or underutilized step by companies, simply performed in a vacuum and then stored away. Why?

It takes time to create, approve, and implement the policies. It may simply be viewed as a regulatory exercise. However, the cost of not establishing standards and consistency baselines could cripple the health and well-being of a business.

Training

Another key to an effective cybersecurity policy is training and socialization. It should go without saying that policies need to be reviewed often to make sure they reflect current business practices. This periodic training creates a consistent top-down message to ensure policies become part of the corporate culture. Data owners should receive training on procedures, but all employees should receive annual training on how to secure data and acceptable use policies.

Audits

Systems should be designed to reconstruct material financial transactions sufficient to support the normal operations and obligations of the entity, and include audit trails designed to detect and respond to cybersecurity events that have a reasonable likelihood of significantly harming any part of the normal operations of the entity. These records should be maintained for a minimum of five years. In addition, entities must develop an effective audit process to monitor that policies and procedures are being followed. Periodic audits will help maintain that the "least privilege access" principles are in effect and only those employees with a business need have data access.

When identity management and group policy objects are used in the network environment, the policy should match granted rights to employees in the system to maintain proper access control. Audits should be performed by either the internal audit department or during the annual financial statement audit. However, it should be noted that a financial statement audit's scope will include only those applications material to the financial statements and may not include all applications with business-critical data.

Data Retention and Loss Prevention

Data retention and loss prevention are critical components of a cybersecurity program. Too often, data retention policies apply to a firm's physical data or paper files and not necessarily its electronic data. The inherent risk in this is tremendous. Network file shares are often jokingly referred to as the "Wild West" of data, but it is no laughing matter.

Before the legal, IT, and risk management teams take the all-important step of developing a comprehensive data retention policy, they must first classify data. Also, in order to ensure data isn't lost, entities must monitor outbound communication and data transferred. This will leave a trail of where data is supposed to go and where it actually went, so nothing is lost in the process.

Governance and Risk Assessment

A risk assessment should be an annual examination of the company's data vulnerabilities, threats, potential impact or losses, and effectiveness of security measures against the assessed risks. The assessment should encompass the key systems, processes, and data flows within the organization. In order to gain the full benefits of a risk assessment, entities should also include:

- Criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the entity.
- Criteria for the assessment of the confidentiality, integrity, security, and availability of the entity's information systems and nonpublic information, including the adequacy of existing controls in the context of identified risks.
- Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the cybersecurity program will address the risks.

Management can then use the risk assessment to plan key IT and data initiatives for the coming year in its annual strategic plan and budgets.

Preventing a Cyber-Attack

In order to prevent a cyber-attack, entities must first start by assessing and improving their cybersecurity strategy. There are five key steps involved:

- **Identify** at-risk data, assess threats and vulnerability of existing infrastructure, and understand all devices connected to the network.
- **Protect** networks by limiting access to only authorized users and devices. Employ services that secure data and be sure to educate users on cybersecurity awareness and risk management.

- **Detect** threats in a timely manner by using continuous network monitoring. Also, look for anomalies in physical environment among users, including the presence of unauthorized users or devices.
- **Respond** by containing and mitigating the event in order to prevent further damage. Once detected, notify proper authorities and coordinate with stakeholders to execute a proper response plan.
- Execute **recovery** systems to restore systems and data. After updating response plans with lessons learned, resume normal business activities and manage public relations.

It's also important to test the effectiveness of an entity's cybersecurity program by using penetration testing. Entities must conduct annual penetration tests based on relevant identified risks from the risk assessment, and bi-annual vulnerability assessments, including any systematic scans or reviews of information systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the entity's information systems.

Conclusion

Securing data for an organization against cybercrime is not a one-step process. It is a holistic program that affects everyone throughout the organization, whether they perform security, own data, use data, or ultimately destroy data. Leadership must make it a priority to establish the program; properly define the program; provide training to those charged with implementing, overseeing, and auditing the program; and mandate an annual review via a risk assessment in order to maintain adherence to the program and keep it current and effective. While no cybersecurity program is 100% effective, not having one (or just going through the motions) is a 100% invitation to disaster.

About the Authors

Jerry Ravi is a Partner in EisnerAmper's Consulting Services Group. Jerry has nearly 20 years of consulting, technology, and audit experience, with a unique ability to bring clarity and forward movement to the decision-making process. Lena Licata is a Senior Manager in the Consulting Services Group, with 10 years of experience that includes public accounting and private industry. Both Jerry and Lena are members of the firm's cybersecurity services team.

EisnerAmper is one of the largest accounting firms in the nation with nearly 1,300 employees, including 180 partners. EisnerAmper's Consulting Services Group provides its clients with one of the most comprehensive families of advisory services in the industry. Solutions include enterprise risk management, internal audits, cybersecurity services, compliance reviews, and IT controls and assessments provided to firms of any size, whether public or private.

Aramar Capital Group, LLC

Differentiation

- Aramar Capital Group, LLC is a boutique investment bank focused on providing merger, acquisition, and strategic private placement services. We are unique among our investment banking peers in that:
  - We focus on middle-market transactions; these transactions are a priority, not a default for when larger deals are dormant;
  - We have significant transactional expertise;
  - We offer senior level attention; and
  - We have a proprietary marketing process that follows a comprehensive approach tailored to each buyer or investor candidate, rather than a typical generic approach utilizing "blast" e-mails, letters, and other contacts.

Clientele

- Aramar focuses on providing a superior level of service to "middle-market" clients. Our M&A transactions range in size from approximately $10 million to $200 million. Our strategic private placements range in size from approximately $10 million to $100 million.
- We provide the high quality of service and substantial transactional experience offered by a major national investment bank, but to a clientele that either is too small for, or cannot receive, the proper level of attention from a larger investment bank, or would receive lesser services and capabilities from a business broker, consultant, or smaller investment bank. This encompasses access to Aramar's senior professionals and proprietary marketing process.

Services

- Aramar offers a highly focused set of corporate finance services to assist our clients in conceiving, defining, executing, and optimizing their objectives:
  - Mergers and Acquisitions
    - Negotiated Sales of Closely-held Companies
    - Corporate and Private Equity Firm Divestitures
    - Leveraged Buyouts
    - Managed Buyouts
    - Buy-side Advisory
  - Private Equity Placements
  - Private Debt Placements
  - Recapitalizations
  - Fairness Opinions
  - Valuations
  - Financial Advisory

Team

- Aramar has assembled a unique team of professionals with a comprehensive and attractive mix of skills and experience. This team has significant investment banking experience, including stints at many other prominent financial services firms.
- Equally important, however, our team has entrepreneurial, managerial, and ownership experience that sets apart Aramar's "principal" perspective from that of most investment banks, where professionals tend to act simply as "agents." As principals, our team members have founded firms, acquired other companies, sold and merged our own companies, and acted as officers and directors of both public and private enterprises. As such, we can relate more closely to our clients and better advise them, at the same time as ensuring senior level investment banking attention.