USF | Muma Case Review
A publication of the Muma College of Business | University of South Florida

Volume 9 Number 2 17 DECEMBER 2025

MARCUS L. GREEN

HAD SOMEONE FINALLY PUSHED HIM ENOUGH TO BECOME A CYBERSECURITY ENTREPRENEUR?[1]

"Business is not about money. It's about making dreams come true for others and for yourself." — Derek Sivers

David Smith sat quietly in his small home office and pondered his next move. The only noises that could be heard were ticking from a clock in the other room and intermittent snoring from his little Shih Tzu dog curled up in his dog bed on top of Smith's desk. Smith, an information security professional, was unsure of his next move as he poured over options for his possible career moves in April 2019. He had just provided help with a friend's computer and heard once again he needed to start his own business and "do this for a living." The friend, an entrepreneur and business owner of 15 years, told Smith he was very helpful and possessed a very positive personable quality when assisting people with their information technology (IT)/information security (InfoSec) problems. She insisted he seriously consider the business owner option this time, even if it meant her providing the "push."

Smith was a retired military IT officer with a pension, over 10 years in the InfoSec vocation, and experience as a cyber incident responder. He was a current student in a Doctor of Business Administration (DBA) program and had a little extra time to reflect on his next move. This current situation was the prime opportunity for him to possibly realize a lifelong dream of becoming a business owner.

His decision hinged on multiple variables, but there were only a few solutions to compare. He had investigated starting the new position and concurrently opening a business offering InfoSec solutions, or he could start a business offering IT and InfoSec solutions and hire a small crew. Smith was also considering hiring a small team and just focusing on InfoSec solutions. Other questions continued to swirl in his conscience as well. Could the market support another IT/InfoSec/Cybersecurity company? What would be the niche? Where would he get the customers? How would he deal with failure if the company wasn't successful?

Smith had positioned himself for a once-in-a-lifetime opportunity. The question was, would he seize it?

Editor: Grandon Gill

The Industry Landscape

David knew he had to conduct research with a broad macro view of the industry he might enter. This data would give him a good picture of the landscape, revealing items such as key competitors, industry outlooks, and forecasts. This current map of the landscape would also provide him with crucial information needed to choose a successful business solution and aid in the development of a plan of action.

The industry landscape he faced involved three main areas: information technology (IT), information security (InfoSec), and cybersecurity. Based on his experiences, formal education, and industry certifications, he felt he could reasonably provide services or products in these areas. He had conducted more specific research to help him further understand market size, competitors who controlled some of the markets, and where these competitors ranked.

Information Technology, Information Security, and Cybersecurity Industries

Information Technology involves a litany of systems, including computers, items connected with computers, and telecommunication devices. These systems create processes and synthesize data into usable information formats for many entities to utilize (Cision, 2019). Transportation of this data and information is included in the technology realm. A quick search in Google for the keywords "information technology sector" returns 1.4 billion results in just under half a second (Google, 2019). The IT sector is a $5 trillion industry with an anticipated growth of 4% expected for 2019 and a $1.6 trillion industry for the United States alone (CompTIA, 2019). These numbers point to the industry being extremely lucrative and could be linked to the increased spending in the information security industry.

Information Security (InfoSec) involves the safeguarding and protection of data and information regardless of the specific form, whether electronic, hard-copy document form, or verbal. The National Institute of Standards and Technology specifically defines information security as:

> "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, in order to ensure confidentiality, integrity, and availability" (Nieles et al., 2017)

The Information Security industry focuses on installing controls and thwarting malicious activities by protecting data confidentiality, integrity, and availability regardless of the state. Specifically, confidentiality of data refers to protecting and hiding data from unauthorized users. Integrity involves protection to ensure data is accurate and retains its original and intended form. Availability ensures that data is available for the intended use of the intended parties (Stewart, Chapple, & Gibson, 2012, p. 3). As shown in Exhibit 1, the IT Security Consulting industry was growing, and factors contributing to this positive life cycle outlook included:

- *The industry is expected to grow faster than the economy over the 10 years to 2024*
- *The number of firms operating in the industry is growing*
- *The industry benefits from a rapid rate of technological change*
- *The potential market for outsourced security solutions remains unsaturated*

Cybersecurity is a subset of information security and involves the protection and security of digital data. The industry consists of companies focusing on processes and functions that secure data. These solutions focus on providing software and hardware that protect the creation, processing, and transmission of this data electronically. The cybersecurity industry was introduced into every conceivable industry based on data breaches on a global scale. Past data breaches and the fear of future ones led some cybersecurity experts to forecast the global cybersecurity industry growth in spending to exceed $1 trillion cumulatively to 2021, according to a 2018 cybersecurity market report provided in Exhibit 2 (Morgan, 2017).

Technologies

Smith knew the market numbers made sense from a growth standpoint, and that it was possible for him to earn revenue by opening a new business. He started to conceptualize and research specific areas of technologies to offer as a service or product to customers. He narrowed these offerings to a few main areas: Information Technology Assistance or "Tech Help," InfoSec, or Incident Response.

The IT assistance or Technology (Tech) help was a type of technology and service meant to help people when encountering issues with any technology-based device or system. This assistance usually involved computers, mobile devices, and small networking infrastructures such as residential wireless (wi-fi) routers. This area focused on those experiencing fundamental computer issues, including mobile devices, issues that a company or individual with essential IT assistance experience and certifications could resolve. Companies provided this service telephonically or through remote desktop support, which involved remotely accessing a customer system via the internet.

InfoSec solutions (to include software and hardware pieces) were meant to provide a more secure environment or monitoring to identify malicious activities. A secure environment included securing data through specific software or hardware. This could be accomplished by implementing or refining more secure infrastructures or architectures. The industry also consisted of consultation services to review processes currently in place and provide recommendations to assist companies in developing and implementing solutions that would provide holistic, secure environments. Some companies provided security awareness training and tools to assist in educating their employees on cybersecurity best business practices, including malicious "social engineering" tactics and ways to combat these attacks.

The incident response arena revolved around processes and actions to prepare and execute in the event an incident was encountered. An incident responder had to be a critical thinker. A successful incident response process is proactive (as opposed to reactive) and attempts to implement tools that provide an incident responder with alerts to highlight possible malicious incidents that might be occurring. The responder would then take positive short-term and long-term steps to ensure the incident was handled. The short-term steps, or mitigation, handle the current specific incident. The long-term actions, or remediation, are steps taken to adjust processes or systems to ensure the malicious event does not occur in the future. Companies provide this service as stand-alone or in conjunction with other cybersecurity solutions.

Customers

From market research, conversations with other entrepreneurs, and interaction with industry leaders in general, Smith decided to focus on three main customers for whom he believed he could offer services.

Government Entities. The government routinely contracted information security and cybersecurity services to outside companies. A significant reason for this involved continuity, as military service

members and government employees usually rotated in and out of security positions every few years, often leaving a void in the experience and knowledge base. Outsourcing or contracting security solutions to companies with this expertise was viewed as more cost-effective and a tried-and-true method successfully used in the past. Former military leaders such as David led a large contingent of these contracted companies. However, he knew this could be an uphill battle because government agencies often preferred to work with established businesses. Also, through research, he knew some businesses had been known to spend between $80,000 to $130,000 on getting a contract and sometimes had to wait over two years to realize a return on investment (SBA.GOV, 2019). Exhibit 3 provides a snapshot of the Federal Procurement Data System website used to research specific government contracts.

Small to Medium Businesses (SMB). There are 30.2 million small businesses in the United States, which account for 99.7% of all business in the United States. The United States Small Business Office of Advocacy defines these businesses "as an independent business having fewer than 500 employees" (SBA.GOV, 2018). These businesses usually have some IT infrastructure, presumably requiring support or IT/InfoSec services to secure data. Smith knew these businesses normally outsourced these services due to a lack of IT/InfoSec expertise, cost-effectiveness, and the inability to reasonably assign the duties to someone within the company because of their small employee numbers.

Residential Technical Assistance. This customer base consisted of individuals who required assistance with personal items such as computers, smartphones, and mobile tablets. Devices might also include home networking devices such as wireless routers, printers, and fax machines. A large majority of this market consisted of customers who lacked a basic understanding of information technology, of which older adults made up a large contingent. The state of Florida considers people in the age range of 60 or older to be elderly (Affairs, 2019).

Key Competitors & Size of Market

Smith knew there were multiple competitors based on his three areas of focus (Government, private sector, and residential support). He decided to focus on two competitors per customer base, as listed in the "Customer" section above. A quick search for services and support in these areas presented him with some active competitors. Exhibit 4 provides a snapshot of the webpage used to compare these companies.

The top government contractor in the area was a company often contracted to work with the government and provided IT solutions and packages that supported national security, government transformation, and cybersecurity support. They provided holistic cybersecurity solutions, including platform and exploitation protection, cyber analytics, and offensive computer and network operations. They held many contracts with government contingents at a military base in the local area. Another successful business was known to offer services to the government on a contract basis. This competitor was a global Fortune 500 company that provided a wide spectrum of services, including data science and engineering, enterprise modernization, mission software systems, and cybersecurity solutions. They held a large presence at local military bases and were often contracted to provide support in cyber areas such as the security operation center, insider threat detection, cyber analytics, information assurance, risk management framework, and accreditation testing and evaluation. These companies were very successful in providing cybersecurity solutions, with Exhibit 5 highlighting the Department of Navy Chief Information Officer security threat statistics.

Multiple cybersecurity companies in the local area were quite successful as well. One of these businesses had grown rather quickly and provided several cybersecurity-focused solutions. This wide range of solutions included incident response, threat management, threat intelligence, health and performance

automation, Security Information and Event Monitoring (SIEM), and security analytics. They strived to assist companies in reducing overall risk, optimizing data, and threat mitigation to prevent data breaches. A second cybersecurity company claimed to offer a full suite of cybersecurity services complete with Governance, Risk and Compliance (GRC) assistance. Threat detection, threat response, data optimization, training & education, and security governance were key areas of services provided to their customers. Continuous monitoring and support were offered in conjunction with around-the-clock Security Information and Event Monitoring (SIEM) and Security Operations Center (SOC) products. Both competitors had the ideal infrastructure to provide InfoSec services to companies with security needs.

Technology Assistance was a service Smith believed he could provide face-to-face to assist customers with IT and InfoSec needs. A leading competitor in the area was a local family-owned business providing support since the early 2000s. They provided support in home technical services, company IT support, monthly IT service agreements, and physical security solutions. The company had a professional, easy-to-navigate website that included real-time communication via chat to provide quick remediation assistance. A similar local competitor did not seem as technologically efficient based on their web page and reviews. Their web page provided basic company information and services offered, and its overall set-up did not seem to elicit any desire to quickly contact the company. More in-depth research showed the company relied heavily on word of mouth, and the owner, who was operating a small one-person company, provided the assistance. Local customers relayed that the owner was swamped with technical assistance requests, not due to great service but due to the lack of choices within the area.

Smith's Landscape

External factors and determining a solution to navigate them weighed on Smith's mind. Internal factors surrounding a possible business venture also swelled in his conscience. His background, current job offer, possible business model, specific core competencies for the new business, and types of services and products to be offered by the startup business were areas he viewed as main internal factors. Smith also had multiple programs available because of his veteran status. His military service allowed him to take advantage of multiple veteran resources to assist service-member entrepreneurs. Exhibit 6 highlights some of these programs, including Boots to Business, Patriot Bootcamp, and Veterans Entrepreneurship Program.

David's specific background

David knew he had the right background to not only start a business but guide a business to success. His background included over 20 years of military service and close to 10 years of experience in the IT and InfoSec vocation. These experiences shaped his understanding of leadership and dealing with people and provided technical understanding and comprehension.

According to a former military colleague and friend, Smith's military service was one of the most impactful pieces of experience he could bring to a business. This friend, a successful business owner for over two years, told David not to overlook the basic things instilled in military service members that translated well into business life.

> "David, the thing that you can't forget is that you have been taught certain things in the military that when you apply them to the entrepreneurship realm in the civilian world you are going to be extremely successful. The values we are taught, the high standards, the way we are forced to learn to get along with people who have differing views. The high standards of honesty and integrity

> when dealing with different organizations and delivering what is promised in a timely manner. Most importantly the leadership attributes learned and how we take care of people and our subordinates." (Smith, 2019)

Smith knew these great qualities were indeed ingrained while serving in the military. He joined the United States Army at a very young age as a Cavalry Scout, where he learned how to seek out the enemy in a combat environment and how to successfully accomplish challenging tasks by working in a team with other service members. Some of the most important things he learned were the basics of physical security and how to holistically develop and implement plans and strategies to secure equipment and areas in multitudes of environments. He also held positions as a U.S. Army recruiter, where he learned the basics of marketing and sales, and as an assistant finance officer, where he learned the basics of budgeting and accounting. Smith's ability to lead was greatly enhanced when he was selected to become an officer and graduated from the prestigious Officer Candidate School.

The military provided a good baseline for dealing with people and accomplishing tasks at hand. However, Smith's IT and InfoSec knowledge and experiences enabled him to give customers products and services to help their companies thrive and prosper. He began his IT experience as an IT Company Commander in charge of 160 rapid deployment technicians who provided services to globally located end users in austere conditions. This position taught him how to think critically on the fly and how to get the most out of people when experiencing tough situations where solutions could rarely be found in a book. He also learned how expansive the IT world was and how a person could quickly fail through hubris by not grasping knowledge limits. His success in this position could be summarized as "knowing what I know and knowing what I don't know." This basic tenet forced him to research areas in which he lacked knowledge. This non-prideful approach kept him in a constant learning mode and ultimately led to him being named one of the top commanders in his unit. He also served as an Information Security officer, requiring him to develop plans to secure digital and physical items, including networks. Because this position was in a small organization, there were many responsibilities, including assisting people with their day-to-day computer and mobile device needs. During this job, while assisting people, Smith learned from his customers that he possessed the right combination of personality, knowledge, and patience to help people remedy their IT/InfoSec issues and should consider beginning a business with that focus.

As a lead security engineer, his next position exposed him to the building of digital security solutions and the validation of these constructs to ensure data was properly secured in its various stages of usage. This knowledge of securing data was further refined when he was hired as an analyst to monitor and respond to real-world cybersecurity issues involving malicious activities and cyber-attacks directed toward exploiting system vulnerabilities. Critical thinking was crucial for success in this position because of the wide range of security answers that had to be decided often in a matter of minutes. Overall, he felt these IT and InfoSec positions had prepared him with a diverse background, a wealth of knowledge, and experiences to be successful as a business owner. Another area that he felt would set him apart was the previously earned InfoSec industry certifications. Just like any specialty job, certifications proved to the industry that he possessed the standards of knowledge needed to operate as a professional in the InfoSec world. He was a Certified Information Systems Security Professional, Certified Information Security Manager, and a CompTIA Advanced Security Practitioner. These certifications set him apart from most IT and InfoSec Chief Executive Officers and Chief Information Security Officers who might have held one of the certifications, but rarely all three.

Current Job Offer

Smith had signed an offer sheet for an employment position with a company contracted to provide security solutions for a government agency. The Senior Enterprise Security Analyst position was 80%–90% remote, paid exceptionally well, and was pretty much guaranteed for five years from the date he began. He was only waiting for a firm start date from the contractor. The position provided a comprehensive medical, dental, and 401K package. The company also offered educational benefits, which included up to several thousand dollars a year in tuition reimbursement and a certain amount of monies, which reimbursed David for annual certification fees and dues required for his position.

Business Model

Before moving forward with any action plan, he had to consider the overall construct of his business model. He had to offer something of value that differentiated the service. Exhibit 7 provides an example of business models used by successful Fortune 500 companies. He understood that some people considered a business model an art rather than a science, and when stripped down to its core, it was nothing more than determining how a business would make money. A famous computer company's business model in the 1990s was to provide software for $120 that cost only fifty cents to produce. Another company's business model was to offer services that cost X dollars at a specific rate, which included the handling of all tasks related to that particular service (Lewis, 1999). Providing IT/InfoSec services was the route that made the most sense. He could start the business with little to no cost by providing hands-on consulting work to remedy issues at a rate of X dollars per hour and set a goal of finding a few customers, assuming the customers' overall working service requirement would not over-extend him. This model had to be adjusted depending on the support and services provided. More services would mean more money, but hiring employees would be required to support the increase in services. This would also require increased infrastructure to support the higher output of services. However, in his favor, the nation was currently experiencing data breaches, which cost, on average, $7.9 million to remedy, as shown in Exhibit 8.

Core Competencies

Smith had a strong military background, which included over 25 years of leadership experience. He understood the importance of core competencies in developing a stable foundation needed to grow a company successfully. He also understood that these competencies would provide a framework for how the company conducted business internally on a day-to-day basis, as well as how the company would interact with customers and business dealings in general. Smith's business would firmly adhere to honesty, character, and common sense.

Honesty was the most critical competency and attribute that underpinned his business. He believed customers should always be treated in an honest matter with integrity, regardless of the situation or circumstance. As a young teenager, he bounced around from restaurant to restaurant and gained experience regularly dealing with customers' wants and needs. During these interactions, there were times when customers were not satisfied with the food or services being offered. He learned that customers treated with honesty were more understanding of volatile situations and returned at a higher rate than those dealt with dishonestly. The secondary effect of being dishonest with customers would be more tragic as those customers would tell family and friends about their bad experiences. This could quickly lead to a death sentence for a business in midwestern towns if the town were connected enough. Honesty had to be the one competency all others would be stacked upon for his business to achieve long-term

success. When dealing with customers, this could be a dilemma in business that could ultimately lead to initial prosperity, but he knew the right thing to do would ultimately be rewarded.

He also believed in *character* and doing the right thing when no one was looking. Smith believed this started from the top, with management setting an example for the subordinates and staff. This competency would be cultivated from the first day and run throughout the organization. More importantly, this competency would extend to the customers as well. Company members who interacted with the customers would also treat customers with dignity and respect while interacting with them, and this would extend behind the scenes when the customers were not present. This competency would ensure that all employees understood that the right "moral" choice would always be made even when management could not oversee a situation. This competency would ensure the consistent return of repeat customers.

Honesty and character were two areas he knew he could use to point his company in the right direction. Using a *commonsense approach* was another area he could use that all staff members would be able to understand. Commonsense would be used for day-to-day operations as well as short-term and long-term planning. Smith had witnessed businesses become too constrained by regulations and procedures as opposed to retaining freedom of maneuver to exercise commonsense if the situation allowed. This would call for open communication to ensure that management was in constant talks with staff, but more importantly, to ensure management was in open two-way communication with the customer. If something made sense, and the financial burden was too outlandish, Smith believed his company owed it to the customer to do the smart thing to keep the customer returning to his business.

What Could Smith Do Differently When Offering Service/Products?

Smith believed he could be successful in the market if he were allowed to showcase the competencies he could offer. He also had to bring something to the table that other competitors were not offering. He had to ensure he was conducting business differently and could find a certain niche. Smith believed that he could offer services and products differently from the competition in a few distinct ways.

Focusing on human beings first and foremost was an aspect that would make the company profitable. This would be beneficial on multiple fronts. The first and major point revolved around establishing a great rapport with customers and getting to know them as people. This distinct approach was consistent with the approach that human beings are the most important piece of any IT infrastructure. This human being's focus would extend to the services provided as well. He believed he could offer services that trained and monitored employees. Custom-modeled packages would train employees to understand security better, which would help create a more secure environment by reducing the number of successful *social engineering* attacks. This constant barrage of social engineering attacks occurs when employees are tricked into giving hackers guarded information such as passwords. Hackers prefer this type of attack because it prevents them from hacking into a company's system to gain access. Focusing on human beings could also lower the number of human mistakes within a company, which would help prevent data breaches. Human error often creates vulnerabilities within a business's infrastructure, creating an open door for hackers to exploit and steal company monies, confidential information such as proprietary data, and, most importantly, customer data.

He knew that placing the human being first would seem old-fashioned, but he also intended to *provide more than what was expected*. Smith knew this way of conducting business would ensure the customer would always be satisfied with their service because the number of services provided would be greater than initially expected. Smith knew he had always wanted to conduct business with this kind of focus. Still, it really hit home a few weeks prior when he was out conducting business meetings and needed to

find a bike shop to remedy a flat tire he had received while riding his road bike a few days earlier. He was not in his neck of the woods and had to randomly call around to find a bike shop that could assist. He found a shop that fixed the flat tire and had it ready 15 minutes quicker than promised. After he provided payment, he thanked the shop for the hard work and for having the tire ready faster than expected. The shop employee said that their goal was to provide more than expected or promised. As a customer, he knew he would choose that bike shop again without reservation and recommend it to someone else if he were ever in the area again. Smith wanted to elicit that same emotional satisfaction from customers who did business with his company.

Another area in which Smith felt he could make a difference was the style of services provided. His unique style would involve providing a deeper comprehension of IT or InfoSec or *enlightenment* while providing services. He knew that most companies offering services did so without concern if the customer really learned anything about what was being done during the process. He felt the time could be taken to explain and show the customer the details of the issue and the steps needed to be taken to fix the issue. This extra time spent with the customers would allow his employees to answer questions and ensure the customer had a good understanding of what steps could be taken if similar issues were experienced in the future. This would also help customers feel more comfortable dealing with IT and InfoSec systems and give them the confidence to help other fellow employees who might experience future issues. Smith had seen this dynamic occur in the past while providing IT tech assistance on a volunteer basis. He noticed customers seemed to learn more and became more comfortable with their computers and mobile devices when he would show them how to fix the issue as opposed to fixing the issue for them. This meant more questions initially but fewer issues later.

Smith's Decision Concerns

Great research had been conducted thus far at a macro view providing a good picture of the industry landscape and at a more focused view giving us an understanding of areas which would affect David more specifically. This clarified the overall decision picture for him. He now needed to process questions and concerns which affected the decision. There were three main areas of concerns which acted as roadblocks to him making a final decision.

- *Money*
- *Lack of Entrepreneurship Experience in Family*
- *Fear of Failure*

Money

Smith had concerns about financing the business regardless of the customers, technologies, or area of focus. He considered three viable options to get the company operational and sustainable. Many options were available, but based on his current situation, he had narrowed it down to just a few.

The best choice was to begin the business with no capital. This would be the best long term option if the business ultimately failed; he would have invested nothing and have lost nothing. This would also take some of the stings out of the overall failed business venture. Securing customers prior to beginning operations would help provide a realistic shot of success. Another option was beginning the business as the only employee and providing hands-on assistance and/or consulting.

The next option he was considering was to speak with a lender and attempt to secure a small business loan. This made sense if he didn't mind taking a financial risk. This option really frightened him based on a lack of savings and horror stories he had read about owners who had failed before him. A loan would allow him to secure these things. IT infrastructure (hardware and software), office space with utilities, and a skeleton crew, legal and accounting assistance would be some of these items or subscriptions. A typical small business loan as shown in Exhibit 9 would fall into three amount categories: $25,000 or less, $25,001 to $50,000, or more than $50,000; interest rates would depend on re-payment time frames of under or over 7 years, with interest rates for the stated amounts of under 7 years being 9.75%, 8.75%, or 7.75%, while taking over 7 years to repay the listed amounts would see a jump in interest rates to 10.25%, 9.25%, and 8.25% (NERDWALLET, 2019).

Smith was considering seeking funds from venture capitalists. He did not want to give up equity or control in his company, so this was an unlikely option. This would, however, provide instant capital, but it would also require Smith to possibly agree to give up a stake in the company or to pay back the invested money within a certain amount of time. This choice would be optimal if he needed to hire a skeleton crew for a certain time frame and purchase infrastructure to become operational without the hassle of dealing with lending institutions.

Lack of Entrepreneurship Experience in Family

Another concern David had was the lack of knowledge and experience of business ventures from his family's inner circle. He had never witnessed anyone in his family start, own, or manage a business. As far back as he could remember, family members had always worked in blue-collar positions, with none having achieved a college degree. Most men in his family held jobs as mechanics or in farming, while women typically toiled at housekeeping or lower-level medical positions. A small number of people he did know had a family member to guide them in making the business decisions that made "business" sense. David had company command experience from the military to understand the processes and financial pieces but lacked mentorship.

Fear of Failure

Fear of failure was a significant concern that weighed heavily on David's mind. He was very proud and could not stand the thought of failing at anything. He had faced challenges in the military and had always been successful. However, this seemed different because small businesses sometimes did fail, which could mean losing everything financially and being saddled with debt for the rest of his life. Exhibit 10 shows that 79.8% of small businesses survived from 2016 to 2017, and an average of 78.6% of small businesses survived one year during a ten-year period from 2005 to 2017. However, only about half of all businesses survive 5 years or longer, and only one-third survive 10 or longer (SBA.GOV, 2018). These numbers provided a short-term calming effect on Smith, knowing that a high percentage of businesses were still in operation a calendar year after inception.

However, the long-term outlook showed storm clouds could be looming as pages on that calendar continued to turn. Smith's fear of failure was often a double-edged sword. The fear often drove him to give extra effort when things were difficult due to the relentless visions of failure. This fear also enabled him to constantly re-assess situations and original solutions, and was a safety mechanism that kept him from making poorly-researched decisions. There were encouraging numbers surrounding the IT Security Consulting industry, which seemed to calm his fears. The security industry was scheduled to grow from 2019 to 2024 at an annualized rate of 5% from $16.7 Billion to $20.3 Billion. Even more encouraging

was the expectancy of the industry to grow faster than the economy over ten years through 2024 (IBISWorld, 2019).

Smith's Decision

With his new employment start date quickly approaching, Smith knew he had to make a choice relatively quickly. The information technology and cybersecurity markets were quickly changing. Current and fledgling companies were seizing market share, which David's new company could take. This was not going to be an easy decision. The decision would have life-long effects that could ultimately bring joy, heartache, or possibly resentment if the wrong choice was selected. Smith would choose from four basic options.

The first route was for Smith to begin working at the company, which had recently presented him with an opportunity to work as a senior security analyst at the management level. This recently accepted job offer would call for him to work remotely 85% of the time. This meant more time with family, more time to focus on doctoral studies, and more time for fitness activities. This "one-job" option would mean less stress worrying about possible business failures and also allow him the opportunity to build capital and enter the market at a later time. There were also negative consequences to consider, as he would constantly be second-guessing whether he made the right decision in foregoing the entrepreneur route. For the rest of his life, he would constantly ask himself what would have happened if he had taken a leap of faith into entrepreneurship.

Another solution involved taking the contracting job as a security analyst *and* beginning a business as the only employee. This business would focus on providing IT and InfoSec solutions to very small businesses and residential customers. There would be no seed money required, allowing him to scale the business at a pace he felt comfortable with. Working in the security analyst role would also provide the financial means to purchase infrastructure as needed. Upscaling would probably not occur quickly, so this choice would likely not be too lucrative financially. This solution would require extra time. However, this choice would allow Smith to break the chains of "what if I had started my own business when given the opportunity" but keep one foot in the safe zone.

Straddling the "danger zone" and "safe zone" lines was appealing. However, he also considered forgoing the security analyst job offer and beginning a startup business offering IT and InfoSec solutions. This would allow him to focus solely on his new business. He would likely be required to hire a small team of employees and purchase a small infrastructure to support providing services. His main target markets would be small to medium businesses and government contracts at the local military base. This would probably require him to secure a small business loan to support initial startup costs, including salaries for newly hired employees. This option would take Smith out of his comfort zone but allow him to give the new business his full attention.

Smith also considered declining the job offer and starting a business focused entirely on InfoSec solutions. He understood that the industry outlook for providing InfoSec services was growing, as shown in Exhibit 11, at an annual rate of $1 billion, and market research showed that the industry was still in the growth stage. Local area research showed it was not overly saturated with InfoSec companies. He would probably have to fund his business with either loans or contributions from venture capitalists. This was a concern because he did not want to worry about someone taking over his company if things faltered.

Smith had a lot of information to consider and had a pretty good idea of the courses of action. Now came the tricky and challenging part: comparing each to determine which choice was the most viable and provided the best vehicle for navigating to the end goal of gratification and prosperity. His choice would not be an easy one.

References

Affairs, F. D. o. E. (2019). 2016 Profile of Older Floridians. Retrieved from http://elderaffairs.state.fl.us/doea/pubs/stats/County_2016_projections/Counties/Florida.pdf

Cision. (2019). Information Technology Global Market Report 2018 Retrieved from https://www.prnewswire.com/news-releases/information-technology-global-market-report-2018-300602988.html

CompTIA. (2019). IT Industry Outlook 2019. Retrieved from https://www.comptia.org/resources/it-industry-trends-analysis

Google. (2019). What is the information technology industry. Retrieved from https://www.google.com/search?ei=HPW8XNPPBrG-ggeN94ywBw&q=what+is+the+information+technology+industry&oq=what+is+the+information+technology+industry&gs_l=psy-ab.3..0j0i8i30l5.11029.12700..14547...0.0..0.179.1506.0j10.....0....1..gws-wiz.....0i71._V0MjMHRzgk

IBISWorld. (2019). IT Security Consulting Industry Outlook. Retrieved from http://clients1.ibisworld.com.ezproxy.lib.usf.edu/reports/us/industry/industryoutlook.aspx?entid=4584

Lewis, M. (1999). *The New New Thing : A Silicon Valley Story* (Vol. 1st ed). New York: W. W. Norton & Company, Inc.

Morgan, S. (2017, May 31, 2017). 2018 Cybersecurity Market Report. Retrieved from https://cybersecurityventures.com/cybersecurity-market-report/

NERDWALLET. (2019, March 13, 2019). SBA Loan Rates 2019 Retrieved from https://www.nerdwallet.com/blog/small-business/sba-loan-rates/

Nieles, M. D., Kelley, L., Pillitteri, Victoria Y. . (2017). *An Introduction to Information Security* (800-12 Rev. 1). Retrieved from https://www.nist.gov/publications/introduction-information-security https://doi.org/10.6028/NIST.SP.800-12r1

SBA.GOV. (2018). 2018 Frequently Asked Questions About Small Businesses. Retrieved from https://www.sba.gov/sites/default/files/advocacy/Frequently-Asked-Questions-Small-Business-2018.pdf

SBA.GOV. (2019). Assess your Business. Retrieved from https://www.sba.gov/federal-contracting/contracting-guide/assess-your-business#section-header-8

Smith, D. (2019) */Interviewer: M. Green*.

Stewart, J. M., Chapple, M., & Gibson, D. (2012). *CISSP. [electronic resource] : Certified Information Systems Security Professional study guide* (6th ed. ed.): Wiley.

Acknowledgments

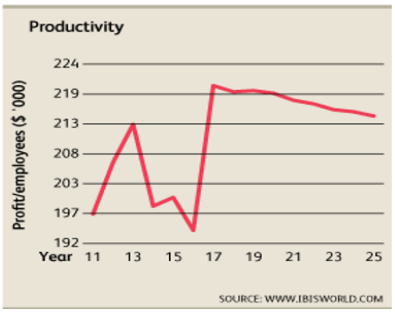
This case study is based upon work supported by the National Science Foundation under Grant No. 1043919, and a substantially similar version is used by the *Journal of Information Technology Education: Discussion Cases*, published by the *Informing Science Institute*.

Biography

Dr. Marcus L. Green is an Assistant Professor in the Department of Computing Sciences at the State University of New York (SUNY) Brockport. Marcus was recently selected as the inaugural Cybersecurity Program Director. His teaching assignment consists mainly of cybersecurity courses, including ethical hacking, information assurance and incident response, and database and web security. He graduated with a Doctorate of Business Administration from the University of South Florida (USF). His primary research interest focuses on human factors related to cyberspace insider threat activities. He holds a Master's in Information Technology Management from Webster University's Walker School of Business and Technology. Green has held many cybersecurity positions, including visiting assistant professor (USF), Incident Responder at the United States Special Operations Command (USSOCOM), Lead Security Engineer (Dept. of Navy), and Information Systems Security Officer (Oregon State University). He is a Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and CompTIA Advanced Security Practitioner (CASP).

Exhibit 1: IT Security Consulting Industry Outlook 2019

Industry Outlook



Over the five years to 2024, IBISWorld estimates that revenue for the IT Security Consulting industry will increase at an annualized rate of 5.0% to $20.3 billion. Industry operators are expected to continue to benefit from trends that have contributed to growth during the current period. These factors include the continued adoption of mobile and broadband internet, coupled with the movement of more information into the cloud. Furthermore, fear caused by the recent spate of high-profile data breaches will encourage companies to invest proactively in IT security solutions, while solid growth in corporate profit levels will provide them with the funds.

The cloud emphasis

Over the next five years, the IT Security Consulting industry will still be in the growth stage of its life cycle. As more services are being conducted online, IBISWorld estimates that private investment in computers and software will increase at an annualized rate of 3.0% over the five years to 2024. The percentage of services conducted online is forecast to increase to 23.2% by 2024, up from 18.5% in 2019. The online provision of services is expected to become more ubiquitous as more companies adopt a software-as-a-service (SaaS) business model. SaaS is a model of software deployment in which a provider licenses an application to customers for use as a service on demand. SaaS offerings tend to be highly integrated with cloud computing and often store large quantities of secure information, which are two primary drivers of industry demand.

Corporate investment in computers and software is not the only factor that will drive industry growth over the next five years. The continued proliferation of mobile and broadband internet connections will also stimulate demand for fraud detection and other services from the technical and financial sectors. Over the five years to 2024, the number of mobile internet connections is expected to rise at an annualized rate of 7.7%. An increasing number of internet connections will ultimately lead to more information being stored online and, therefore, increase the number of potential security breaches. As a result, industry demand for IT security consultants is expected to rise with the continued consumer adoption of mobile technology.

There has been a breach

The industry is also expected to experience an increase in demand from government agencies. The federal government is expected to primarily use industry resources for homeland security reasons and to locate cybercriminals. The Air Force has already proven that remotely piloted aircrafts, including some of the drones it uses, can be hacked. Furthermore, the Stuxnet virus used against Iranian nuclear facilities has demonstrated the vulnerability of high-value targets. Given the increasingly computer-centric nature of weapons and warfare, the federal government is expected to invest heavily in IT security over the next decade.

In addition to rising demand from federal agencies, state governments are also expected to turn to IT security consultants to protect the vast amount of information held in state databases. In 2017, for example, a data breach was announced to have affected almost 200.0 million voter records due to a misconfigured setting in an organization's Amazon cloud-storage service. Additionally, US citizens, encouraged by major online operators, have become increasingly concerned with protecting their private information not from cybercriminals, but from the US government itself. After Edward Snowden leaked highly sensitive National Security Agency (NSA) documents, US citizens became aware of an NSA program that collects millions of Americans' telephone records, claiming that bulk collection had contributed to the prevention of possible terrorist attacks. Concerns of US citizens with the protection of privacy and civil liberties are expected to stimulate change and demand for industry services, including the development of new end-to-end encryption standards.

Industry structure

Rising demand is expected to drive profit growth over the next five years as corporations, consumers and government agencies place more information in the cloud. The emphasis on cybersecurity, coupled with rising demand and profit, is expected to drive enterprise growth in the IT Security Consulting industry over the five years to 2024. During that time, IBISWorld estimates that the number of companies operating in the industry will increase at an annualized rate of 6.1% to 20,649 businesses. In addition, enterprise growth is expected to drive growth in employment opportunities in the industry. As a result, industry wages are expected to increase at an annualized rate of 5.3% to $8.6 billion during the five-year period, accounting for an estimated 42.7% of industry revenue by 2024.

Source: IBISWorld (http://clients1.ibisworld.com.ezproxy.lib.usf.edu/reports/us/industry/industryoutlook.aspx?entid=4584) web site

Exhibit 2: Cybersecurity Market Report 2018

2018 Cybersecurity Market Report

Cybersecurity Ventures predicts global cybersecurity spending will exceed $1 trillion from 2017 to 2021

The Cybersecurity Market Report is published quarterly by Cybersecurity Ventures. We cover the business of cybersecurity, including market sizing and industry forecasts from consolidated research by IT analyst firms, emerging trends, cybercrime, employment, the federal sector, notable M&A, venture capital and corporate investments, IPO activity, and more.

– *Steve Morgan, Editor-in-Chief*

Menlo Park, Calif. – May 31, 2017

Cybersecurity Ventures predicts global spending on cybersecurity products and services will exceed $1 trillion cumulatively over the next five years, from 2017 to 2021.

In 2004, the global cybersecurity market was worth $3.5 billion — and in 2017 we expect it to be worth more than $120 billion. The cybersecurity market grew by roughly 35X over 13 years.

While all other tech sectors are driven by reducing inefficiencies and increasing productivity, cybersecurity spending is driven by cybercrime. The unprecedented cybercriminal activity we are witnessing is generating so much cyber spending, it's become nearly impossible for analysts to accurately track.

We anticipate 12-15 percent year-over-year cybersecurity market growth through 2021, compared to the 8-10 percent projected over the next five years by several industry analysts.

IT analyst forecasts are unable to keep pace with the dramatic rise in cybercrime, the ransomware epidemic, the refocusing of malware from PCs and laptops to smartphones and mobile devices, the deployment of billions of under-protected Internet of Things (IoT) devices, the legions of hackers-for-hire, and the more sophisticated cyber-attacks launching at businesses, governments, educational institutions, and consumers globally.

It is likely that analyst firms will catch up with our projections in 2017 — and update the disproportionately low share of total IT spending which security is expected to account for (over the next 5 years) in their current reports. By 2020, we expect IT analysts covering cybersecurity will be predicting five-year spending forecasts (to 2025) at well over $1 trillion.

Enterprise security budgets are trending up

Many corporations are hesitant to announce breaches they've suffered — and the amounts of their increased security budgets — for fears of reputational damage and of antagonizing cybercriminals.

Rob Owens, Senior Research Analyst for Security and Infrastructure Software at Pacific Crest Securities, recently told Investor's Business Daily that he sees pent-up demand for cybersecurity spending. He says companies still aren't spending enough on security. "I think security has been an under-spend area for decades. You're spending about 3% of your capex (capital expenditures) that's focused on IT on security. That's relatively low."

There are some corporations who have come forward with increased cybersecurity budgets. J.P. Morgan Chase & Co. doubled its annual cybersecurity budget from $250 million to $500 million. Bank of America has gone on the record stating it has an unlimited budget when it comes to combating cybercrime.

Microsoft Corp. will continue to invest over $1 billion annually on cybersecurity research and development in the coming years, according to a senior executive at the tech giant.

The White House states the U.S. Government will invest over $19 billion for cybersecurity as part of the President's Fiscal Year (FY) 2017 Budget. That is up from the $14 billion budgeted in 2016. This represents a more than 35 percent increase from FY 2016 in overall Federal resources for cybersecurity, a necessary investment to secure our Nation in the future.

IT security spending has become more difficult to track

Historic analyst reports are rooted in 'IT security' (servers, networking gear, data centers and IT infrastructure, PCs, laptops, tablets, and smartphones) and not fully evolved to 'cybersecurity' which includes non-computer devices and non-IT centric platforms and environments — which covers entire sub-markets i.e. aviation security, automotive security, IoT security, and IIoT (Industrial Internet of Things) security. All of those market segments combined make up the cybersecurity market.

Even IT security services are difficult to fully size. Tech is a cottage industry which includes tens of thousands of VARs (value-added-resellers), IT solution providers, and SIs (systems integrators) who wrap IT security services around the IT infrastructures they implement and support — but (most of) these firms don't break out and report cybersecurity revenues as a separate bucket.

"A large portion of information security related spending is not accounted for as being information-security related" writes Joseph Steinberg, an Inc. Magazine columnist covering cybersecurity. "Consider, for example, that an organization developing a software package for internal use might spend money from its development budget on technology to scan code for vulnerabilities – the expenditure, however, may never be tracked back to an information-security budget" adds Steinberg.

Big branded tech companies with sizable professional services organizations providing cybersecurity services have yet to set up specific divisions or revenue reporting which analysts need in order to capture accurate market figures.

There's also many new players getting into cybersecurity. CPAs and attorneys who used to answer their clients' what-if and what-now questions around data breaches — are now starting up lucrative cyber consulting divisions.

The IT Security Spending Survey — published by SANS Institute in 2016 — states "Tracking security-related budget and cost line items to justify expenditures or document trends can be difficult because security activities cut across many business areas, including human resources, training and help desk.

SANS states that most organizations fold their security budgets and spending into another cost center, whether IT (48%), general operations (19%) or compliance (4%), where security budget and cost line items are combined with other related factors. Only 23% track security budgets and costs as its own cost center. SANS makes an astute observation which may account for the shortfall in IT spending projections by some researchers and analysts.

Consumer cybersecurity spending is not fully accounted for

Consumer spending on information-security is often impossible to track, according to an Inc. Magazine article. How can analysts possibly know, for example, when, after a malware infection, someone pays a consultant to wipe and restore-to-factory-settings his or her computer or smartphone.

Spending in the consumer category includes personal identity theft protection services, computer and mobile phone repair services specific to malware and virus removal, installation of anti-virus and malware protection software, post-breach services including data recovery and user education on best practices for personal cyber defense.

The consumer cybersecurity market is much bigger than just the anti-virus and malware defense apps that are purchased or come pre-installed. Much like corporations, consumers are spending time and money as a result of cyber-attacks.

Cybercrime damages will cost the world $6 trillion annually by 2021

Cybersecurity Ventures predicts cybercrime will continue rising and cost businesses globally more than $6 trillion annually by 2021. The estimate is based on historical cybercrime figures including recent year-over-year growth, a dramatic increase in hostile nation state sponsored and organized crime gang hacking activities, a cyber attack surface which will be an order of magnitude greater than it is today, and the cyber defenses expected to be pitted against hackers and cybercriminals over that time.

The cybercrime cost prediction includes damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

The worldwide cyber damage estimates do not include unreported cybercrimes, legal and public relations fees, declines in stock and public company valuations directly and indirectly related to security breaches, negative impact on post-hack ability to raise capital for start-ups, interruptions to e-commerce and other digital business transactions, loss of competitive advantage, departure of staff and recruiting replacement employees in connection with cyber-attacks and resulting losses, ongoing investigations to trace stolen data and money, and other.

Market researchers size information security spending

A Gartner report projected global spending on "IT security" products and services would top $81 billion in 2016, an increase of 7.9% over the prior year (this is not a "cybersecurity" projection that would include all aspects of cyber defense i.e. consumers, IoT devices, automobiles, etc.). The largest areas of information security spending are consulting and IT outsourcing, according to the report.

A 2016 report from BI Intelligence — Business Insider's research service — estimated $655 billion will be spent on cybersecurity initiatives to protect PCs, mobile devices, and Internet of Things (IoT) devices between 2015 and 2020. BI breaks down the forecasted spending as follows: $386 billion spent on securing PCs; $172 billion spent on securing IoT devices; and $113 billion spent on securing mobile devices.

A Morgan Stanley Blue Paper published this past summer — "Cybersecurity: Rethinking Security" — examines why and how digital security could evolve in the next several years—and what these changes mean for investors.. and asserts the cybersecurity market could grow by more than four times overall IT spend.

North America and Europe are the leading cybersecurity revenue contributors, according to a report from TechSci Research. Asia-Pacific is rapidly emerging as a potential market for cyber security solution providers, driven by emerging economies such as China, India and South-East Asian countries, wherein, rising cyber espionage by foreign countries is inducing the need for safeguarding cyber space.

India should see huge cybersecurity market growth over the next decade. According to Data Security Council of India (DSCI), India's cybersecurity market is expected to grow nine-fold to $35 billion by 2025, from about $4 billion. This would mainly be driven by an ecosystem to promote the growth of indigenous security product and services start-up companies.

According to IDC, the hot areas for growth are security analytics / SIEM (10 percent); threat intelligence (10 percent +); mobile security (18 percent); and cloud security (50 percent). A Tech Republic story states the cloud security market is expected to be worth $12 billion by 2020, according to a report from Transparency Market Research.

Government spending on cybersecurity has increased at an average annual rate of 14.5% between FY 2006 and FY 2017, outpacing procurement in every other type of major government program, according to Scott Homa, Senior Vice President for Mid-Atlantic Research at Jones Lang LaSalle IP, Inc. (JLL), a financial and professional services firm specializing in commercial real estate services and investment management with 60,000 employees across 280 corporate offices worldwide.

Demand for vendor-furnished information security products and services by the U.S. federal government will increase from $8.6 billion in FY 2015 to $11 billion in 2020 at a compound annual growth rate (CAGR) of 5.2 percent, according to "Deltek's Federal Information Security Market Report". Deltek states that as federal agencies struggle to stay ahead of the cybersecurity threats, more and more of their IT spend is being devoted to cybersecurity, reaching over 10 percent of IT spend by 2020.

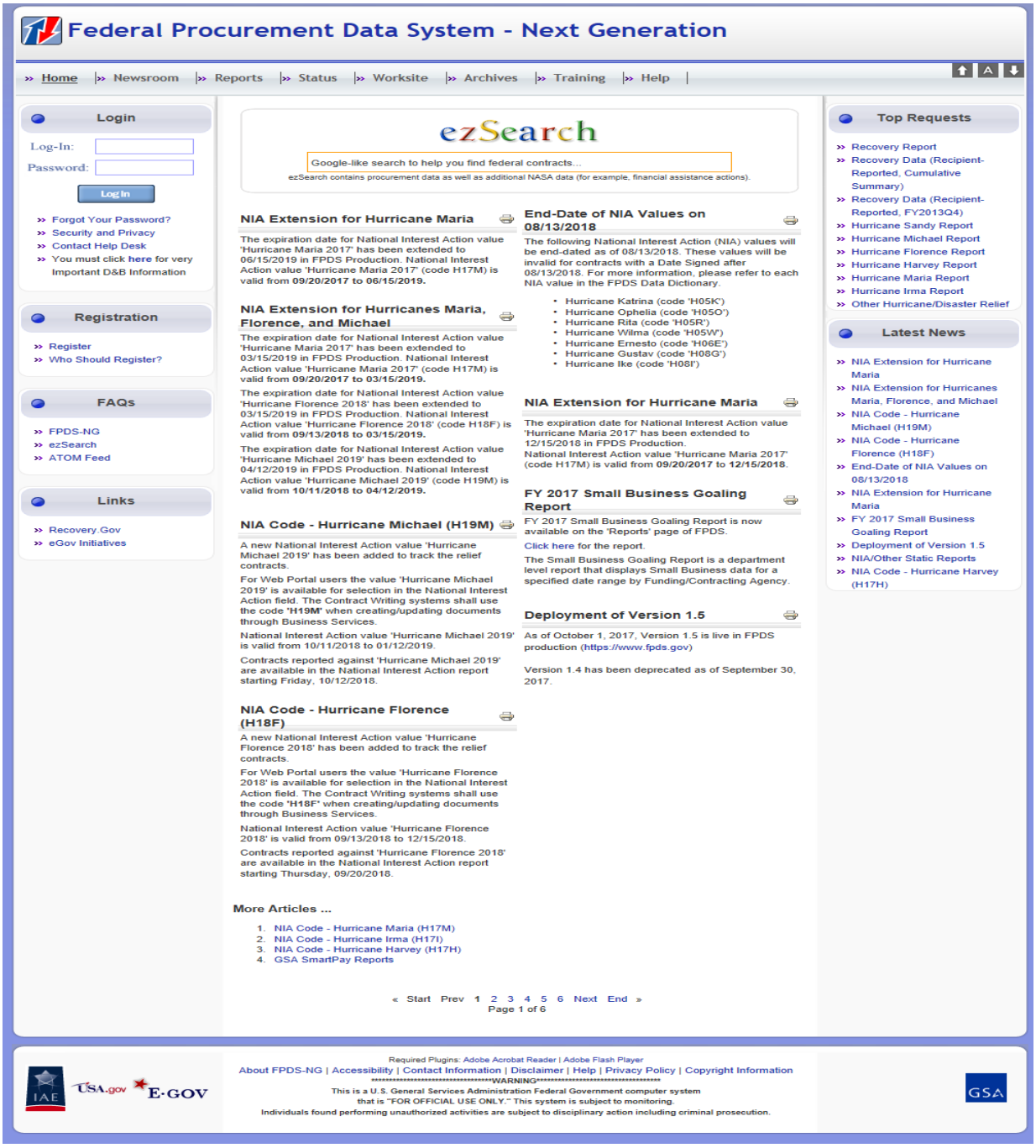
Stay tuned for the 2018 Cybersecurity Market Report coming in Jun. 2018.

– Steve Morgan is founder and Editor-in-Chief at Cybersecurity Ventures.

Go here to read all of my blogs and articles covering cybersecurity. Go here to send me story tips, feedback and suggestions.

Source: Cybersecurity Ventures (https://cybersecurityventures.com/cybersecurity-market-report/) web site

Exhibit 3: Federal Procurement Data System Web Site



.

Source: Acquisition.gov (https://www.fpds.gov/fpdsng_cms/index.php/en/) web site

Exhibit 4: Small Business Market Research Tools

Focus	Goal	Reference
General business statistics	Find statistics on industries, business conditions	NAICS, FedStats, Statistical Abstract of the United States, U.S. Census Bureau
Consumer statistics	Gain info on potential customers, consumer markets	Consumer Credit Data, Consumer Product Safety
Demographics	Segment the population for targeting customers	American FactFinder, Bureau of Labor Statistics
Economic indicators	Know unemployment rates, loans granted and more	Consumer Price Index, Bureau of Economic Analysis
Employment statistics	Dig deeper into employment trends for your market	Employment and Unemployment Statistics
Income statistics	Pay your employees fair rates based on earnings data	Earnings by Occupation and Education, Income Statistics
Money and interest rates	Keep money by mastering exchange and interest rates	Daily Interest Rates, Money Statistics via Federal Reserve
Production and sales statistics	Understand demand, costs and consumer spending	Consumer Spending, Gross Domestic Product (GDP)
Trade statistics	Track indicators of sales and market performance	Balance of Payments, USA Trade Online
Statistics of specific industries	Use a wealth of federal agency data on industries	NAICS, Statistics of U.S. Businesses

Source: U.S. Small Business Administration

Exhibit 5: Department of Navy CIO Cyber Statistics

Source: U.S. Navy Chief Information Officer (doncio.navy.mil)

Exhibit 6: Department of Defense Veteran's Entrepreneur Resources

Veterans Resources

The Department of Defense (DoD) appreciates the sacrifices made by veterans in the service of our country and is committed to making the maximum practicable prime and subcontracting opportunities available to service-disabled, veteran-owned small businesses.

Veterans are 45 percent more likely to be self-employed than non-veterans, according to the Bureau of Labor Statistics. The skills veterans developed in the military—discipline, tenacity and adaptability—make them ideally suited to become entrepreneurs.

Boots to Business

The Small Business Administration's Boots to Business program provides entrepreneurial training within DoD's Transition Assistance Program (TAP). The program has trained more than 50,000 service members and military spouses since its 2013 launch.

Boots to Business Reboot

The Small Business Administration's Boots to Business Reboot program expanded entrepreneurship training to veterans who have already transitioned out of the military as well as members of the National Guard and Reserve. The program includes an eight-week, online Foundations of Entrepreneurship course instructed by a consortium of professors and practitioners led by the Institute for Veterans and Military Families at Syracuse University.

Bunker Labs

Through local chapters in 12 cities, Bunker Labs provides educational programming, mentors and events to help veterans start and grow businesses.

Entrepreneurship Bootcamp for Veterans with Disabilities

The Entrepreneurship Bootcamp for Veterans with Disabilities (EBV) program provides training in entrepreneurship and small business management to post-9/11 veterans with service-connected disabilities as well as military family members who serve in a caregiver role to a veteran with a service-connected disability.

Patriot Bootcamp

Patriot Boot Camp equips service members, veterans and spouses with an entrepreneurial education, access to resources, mentorship and community support to build technology companies.

Procurement Technical Assistance Centers

Procurement Technical Assistance Centers (PTACs) help small businesses navigate the complex federal procurement system to win and execute contracts with the federal government, including DoD.

Veteran Business Outreach Centers

The Small Business Administration's Veterans Business Outreach Centers provide entrepreneurial development services such as business training, counseling and mentoring to veterans.

Veteran Institute for Procurement

The Veteran Institute for Procurement offers five programs to help veteran-owned small businesses and service-disabled, veteran-owned small businesses increase their ability to win government contracts. Training programs vary in length (from 1-3 days) and are held in the Washington, DC, area.

Veteran Women Igniting the Spirit of Entrepreneurship

Veteran Women Igniting the Spirit of Entrepreneurship (V-WISE) provides entrepreneurial training to female veterans.

Veterans Business Development Officers

There is one Veterans Business Development Officer in each of the 68 Small Business District Offices. Veterans Business Development Officers can help veterans get loans and start businesses.

Veterans Entrepreneurship Jumpstart Program

The Veterans Entrepreneurial Jumpstart program provides tools, training and mentorship to enable disabled veterans to start their own businesses.

Veterans Entrepreneurship Program

The Veterans Entrepreneurship Program provides entrepreneurial training to service-disabled veterans interested in starting or growing a small business.

Source: DOD Office of Small Business Programs (http://business.defense.gov) web site

Exhibit 7: New Business Model Idea Examples

CAN'T THINK OF A NEW BUSINESS MODEL?
Try adapting one of these basic forms.

ANALOGY	HOW IT WORKS	EXAMPLE
Affinity club	Pay royalties to some large organization for the right to sell your product exclusively to their customers.	• MBNA
Brokerage	Bring together buyers and sellers, charging a fee per transaction to one or another party.	• Century 21 • Orbitz
Bundling	Package related goods and services together.	• Fast-food value meals • iPod/iTunes
Cell phone	Charge different rates for discrete levels of a service.	• Sprint • Better Place
Crowdsourcing	Get a large group of people to contribute content for free in exchange for access to other people's content.	• Wikipedia • YouTube
Disintermediation	Sell direct, sidestepping traditional middlemen.	• Dell • WebMD
Fractionalization	Sell partial use of something.	• NetJets • Time-shares

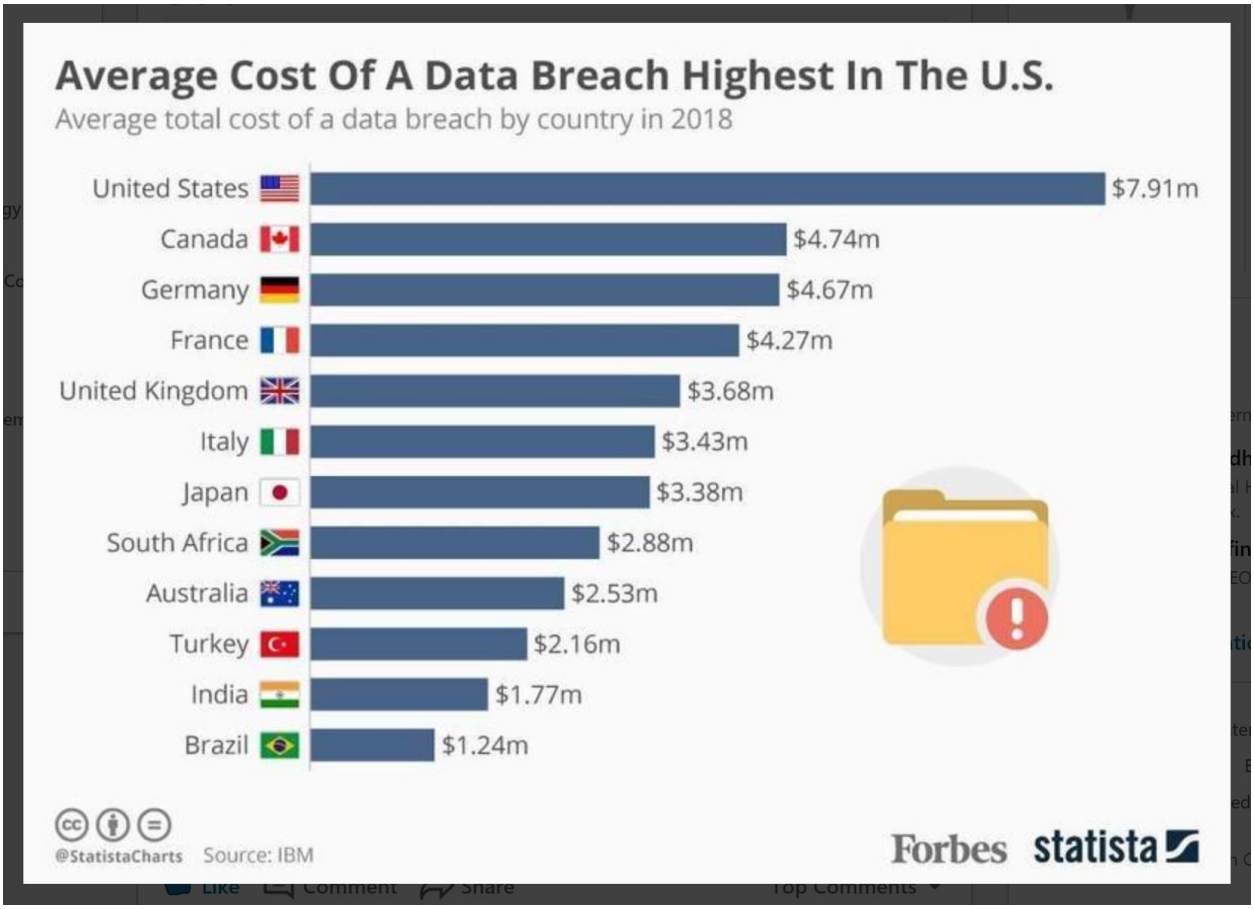
Freemium	Offer basic services for free, charge for premium service.	• LinkedIn
Leasing	Rent, rather than sell, high-margin, high-priced products.	• Cars • MachineryLink
Low-touch	Lower prices by decreasing service.	• Walmart • IKEA
Negative operating cycle	Lower prices by receiving payment before delivering the offering.	• Amazon
Pay as you go	Charge for actual, metered usage.	• Electric companies
Razor/ blades	Offer the high-margin razor below cost to increase volume sales of the low-margin razor blades.	• Printers and ink
Reverse razor/ blades	Offer the low-margin item below cost to encourage sales of the high-margin companion product.	• Kindle • iPod/iTunes
Reverse auction	Set a ceiling price and have participants bid as the price drops.	• Elance.com

Product to service	Rather than sell a product, sell the service the product performs.	• Zipcar
Standardization	Standardize a previously personalized service to lower costs.	• MinuteClinic
Subscription	Charge a subscription fee to gain access to a service.	• Netflix
User communities	Grant members access to a network, charging both membership fees and advertising.	• Angie's List

SOURCE *SEIZING THE WHITE SPACE* BY MARK JOHNSON HBR.ORG

Source: Harvard Business Review (https://hbr.org/2015/01/what-is-a-business-model)

Exhibit 8: Cyber Threat Statistics



Source: The Cybersecurity Hub (https://www.linkedin.com/feed/update/urn:li:activity:6534735999916998656)

Exhibit 9: SBA Loan Rates 2019

SBA Loan Rates 2019

SBA loans offer the lowest rates on the market for small businesses, but rates can change based on the Federal Reserve's actions.

NERDWALLET
March 13, 2019

Small Business, Small Business Loans

At NerdWallet, we strive to help you make financial decisions with confidence. To do this, many or all of the products featured here are from our partners. However, this doesn't influence our evaluations. Our opinions are our own.

For many small-business borrowers, government-backed loans are the holy grail. SBA loan interest rates are some of the most competitive among lenders.

Current SBA 7(a) loan interest rates

SBA loan size	7(a) loan paid off in under 7 years *	7(a) loan paid off in over 7 years *
$25,000 or less	9.75%	10.25%
$25,001 to $50,000	8.75%	9.25%
More than $50,000	7.75%	8.25%
***Rates calculated with the current prime rate of 5.50%**		

Keeping up on the Small Business Administration's terms and rates is part of a smart approach to finding a small business loan. The 7(a) loan is the SBA's most popular product and offers a flexible sum of cash for a variety of uses, including managing daily operations, purchasing new products and refinancing high-interest loans. Business borrowers also find low-cost financing for land and other major purchases with SBA 504 loans.

The SBA sets interest rate guidelines for lenders, which helps keep small-business owners' borrowing costs low.

How SBA loan rates are set: Interest rates for SBA 7(a) loans are the daily prime rate, which changes based on actions taken by the Federal Reserve, plus a lender spread. The spread is negotiated between the borrower and the lender, and can result in either fixed or variable interest rates. However, the SBA caps the maximum spread lenders can charge based on the size and maturity of the loan.

> "Interest rates for SBA 7(a) loans are the daily prime rate, which changes based on actions taken by the Federal Reserve, plus a lender spread."

A lender providing an SBA loan may also calculate interest rates using the one-month London Interbank Offered Rate plus 3% or the SBA's optional peg rate instead of the daily prime rate.

Guaranty fees

7(a) loan guaranty fees are based on the loan amount and maturity date and apply only to the guaranteed portion of the loan. Lenders are required to pay the SBA the guaranty fee, but some pass the expense on to you. However, the SBA limits the maximum amount you will be charged.

> "Lenders are required to pay the SBA the guaranty fee, but some pass the expense on to you."

You'll pay no guaranty fee if your loan is less than $150,000. If it's more than $150,000 and matures in less than a year, you'll see a 0.25% guaranty fee.

If your loan is for more than $150,000 and takes more than a year to mature, you'll be charged based on a three-tier system:

- 3% on loans of between $150,000 and $700,000
- 3.5% on loans of between $701,000 and $1 million
- 3.75% on loans of more than $1 million

Here's a breakdown of SBA business loan terms and rates, including interest and fees:

SBA loan rates

SBA 7(A) LOAN TERMS:

- 7(a) loans do not have a minimum loan amount and max out at $5 million. The average SBA loan was around $374,000 in 2015.
- The SBA guarantees 85% of your loan if it's less than $150,000 and 75% if it's more than $150,000. However, it limits guarantees to $3.75 million.
- SBA loans aren't easy to qualify for. Read up on the qualifications for SBA loans to make sure they're right for you.

SBA 7(A) INTEREST RATES:

7(A) LOANS REPAID IN LESS THAN 7 YEARS

Loan size	$25,000 or less	$25,001 - $50,000	More than $50,000
Maximum interest rate	*Prime + 4.25%	*Prime + 3.25%	*Prime + 2.25%

7(A) LOANS REPAID IN MORE THAN 7 YEARS

Loan size	$25,000 or less	$25,001 - $50,000	More than $50,000
Maximum interest rate	*Prime + 4.75%	*Prime + 3.75%	*Prime + 2.75%

**The prime rate, hiked in December 2018, is 5.50%.*

Remember that interest rates make up only part of your expenses. Your APR reflects your true cost of borrowing, including your interest rate and all fees associated with the loan.

Source: NerdWallet (https://www.nerdwallet.com/blog/small-business/sba-loan-rates/)

Exhibit 10: SBA 2019 Survival Facts

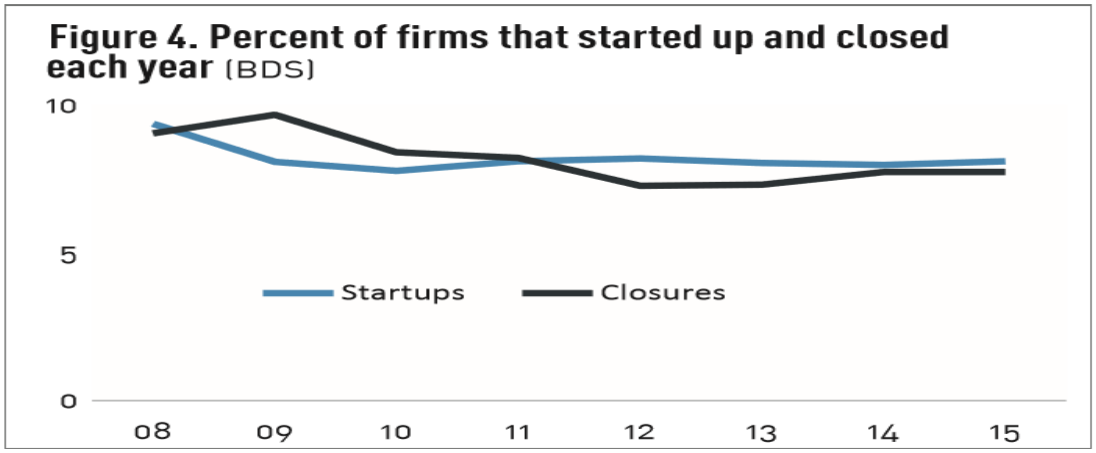


Table 1. Employer firm startups and closures (BDS)

	Startups	Closures
2008	487,673	470,550
2009	406,321	486,491
2010	385,358	416,642
2011	398,364	403,838
2012	408,591	362,398
2013	404,475	367,419
2014	403,902	391,553
2015	414,043	395,602

Four out of five establishments that started in 2016 survived until 2017 (79.8%). From 2005 to 2017, an average of 78.6% of new establishments survived one year.

- About half of all establishments survive five years or longer. In the past decade, this ranged from a low of 45.4% for establishments started in 2006, and a high of 51.0% for those started in 2011.
- About one-third of establishments survive 10 years or longer.

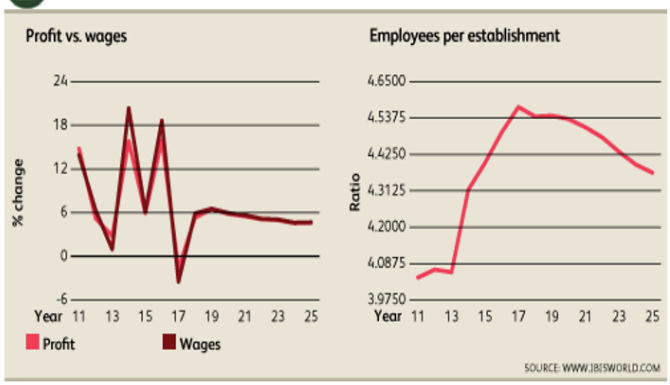
Although data is not available on firm survival rates, other data sources suggest that about two out of three establishment exits are the result of firm closures.

Source: SBA.GOV (https://www.sba.gov/sites/default/files/advocacy/Frequently-Asked-Questions-Small-Business-2018.pdf) and Business Dynamics Statistics, U.S. Census Bureau, U.S. Department of Commerce, (www.census.gov/ces/dataproducts/bds)

Exhibit 11: IT Security Consulting Industry Outlook 2019

Revenue Outlook

Year	Revenue $ million	Growth %
2020	16,787.4	5.8
2021	17,655.3	5.2
2022	18,523.9	4.9
2023	19,387.0	4.7
2024	20,254.4	4.5
2025	21,143.6	4.4



Back to top

Industry Life Cycle

This industry is **Growing**

More Info

The IT Security Consulting industry is in the growth stage of its life cycle. Industry value added (IVA), which measures the industry's contribution to GDP, is projected to grow at an annualized rate of 5.7% over the 10 years to 2024. During the same period, GDP is expected to grow at a much slower annualized rate of 2.2%.

The industry's growth has largely been the result of mainstream adoption of broadband internet, mobile and cloud-based computing solutions and the potential data security issues arising from these technologies. Broadband has caused an increasing proportion of services to be conducted online, which, has caused more consumer information to be put into the vulnerable cloud. The industry has also benefited from several high-profile security breaches, which have drawn the spotlight to the need for IT security. Rapidly changing technologies in software industries and the information sector stimulate the creation of new product segments, another sign of a growing industry. As technologies are introduced, clients hire IT security consultants to make sure they are secure for business and consumer use. The continual and rapid level of technological change will ensure that the industry remains relevant in the near future.

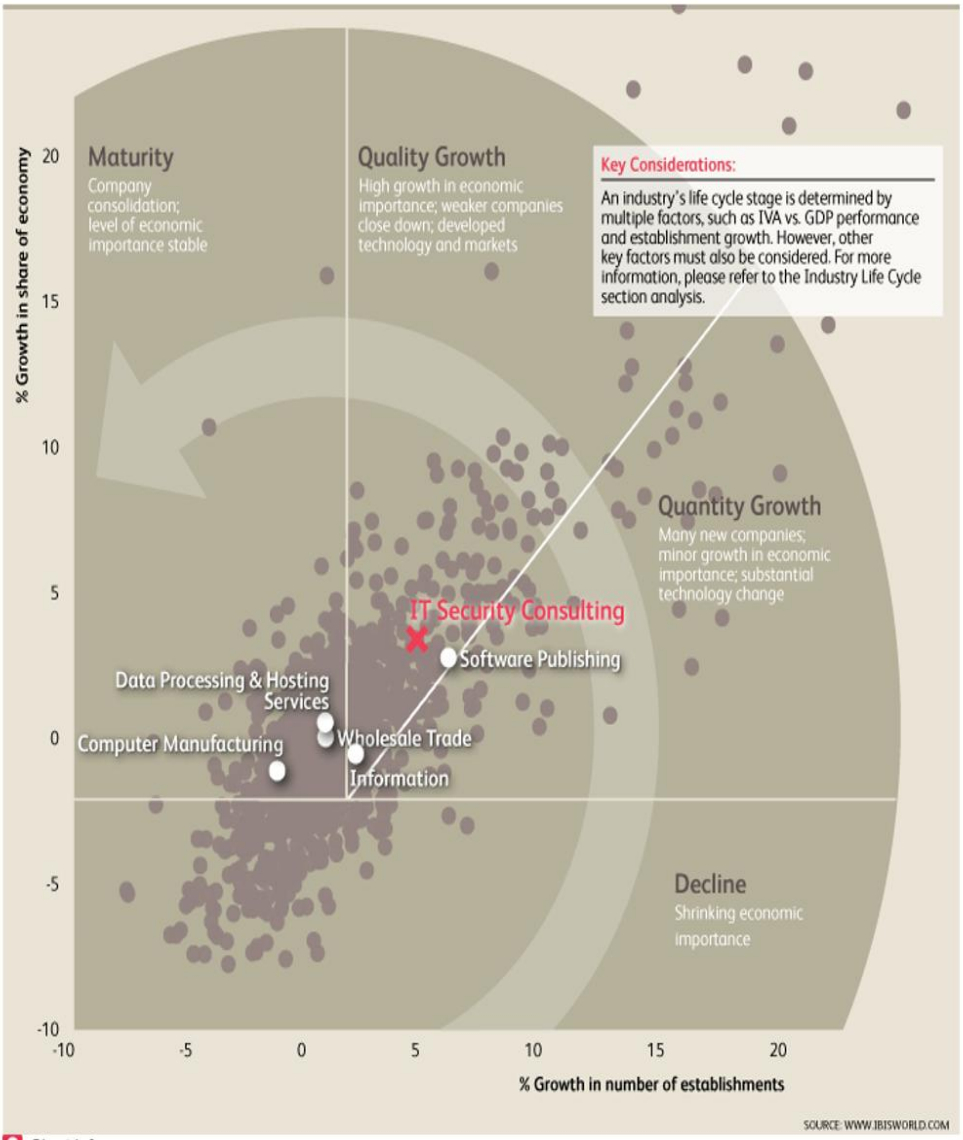
Life Cycle Reasons

The industry is expected to grow faster than the economy over the 10 years to 2024

The number of firms operating in the industry is growing

The industry benefits from a rapid rate of technological change

The potential market for outsourced security solutions remains unsaturated



Source: IBISWorld (http://clients1.ibisworld.com.ezproxy.lib.usf.edu/reports/us/industry/industryoutlook.aspx?entid=4584) web site