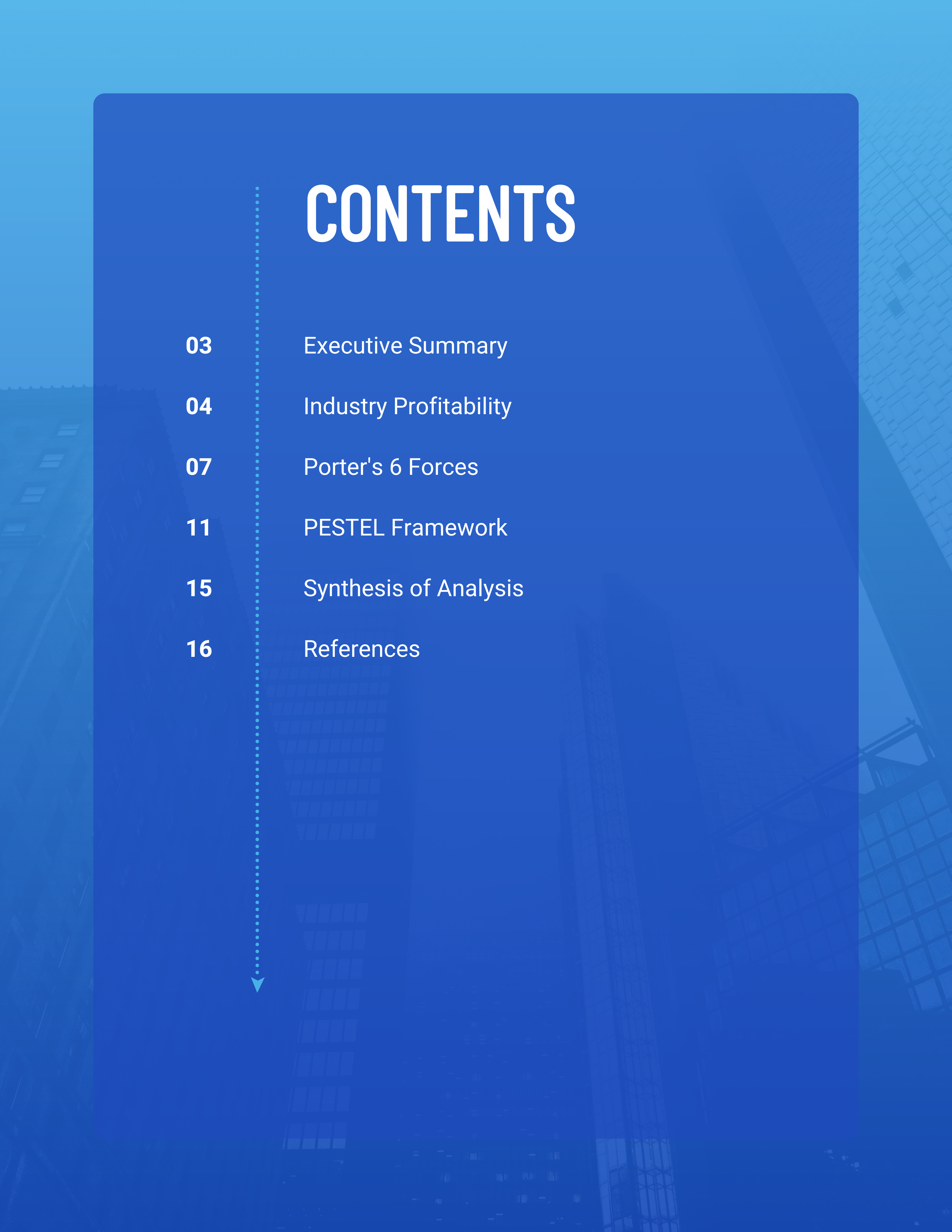
THE FUTURE OF THE CYBERSECURITY INDUSTRY

January 2021

Mand
Consulting
Group



CONTENTS

EXECUTIVE SUMMARY

While cybersecurity is a large field, this paper will specifically be focusing on the future of the service-provider based side of cybersecurity. This includes Advisory Service Providers (ASPs) and Managed Security Service Providers (MSSPs). What are the two? Advisory Service Providers (ASPs) are companies that provide offensive security services such as penetration testing of various applications or devices (i.e. web, mobile, etc.) and other related services such as security awareness training. Managed Security Service Providers (MSSPs), on the other hand, are companies that manage the security of their clients. These clients include small/medium businesses and enterprises alike. According to the NAICS categorizing, both ASPs and MSSPs fall under code 54169. This is the category for ‘Other Scientific and Technical Consulting Services’ and the industry is described as ‘establishments engaged in providing advice to businesses on scientific and technical issues’.

A Clark School study conducted at the University of Maryland quantified that a cyber-attack occurred every 39 seconds in 2019. These cyber attacks, the product of cybercrime, cost the world economy more then one percent of the global GDP (McAfee). With the increasingly unprecedented number of cyber-attacks, it is evident that there is an undeniable need for cyber security services to safeguard sensitive information against hackers. It is not a surprise then, that the global cybersecurity services market size in 2019 reached a value of nearly $88.86 billion. This is alongside a compound annual growth rate (CAGR) of 9.4% since 2015 (Business Research Company). The initial research shows the industry is promising, however, we need to take a deeper dive into the attractiveness of the industry.

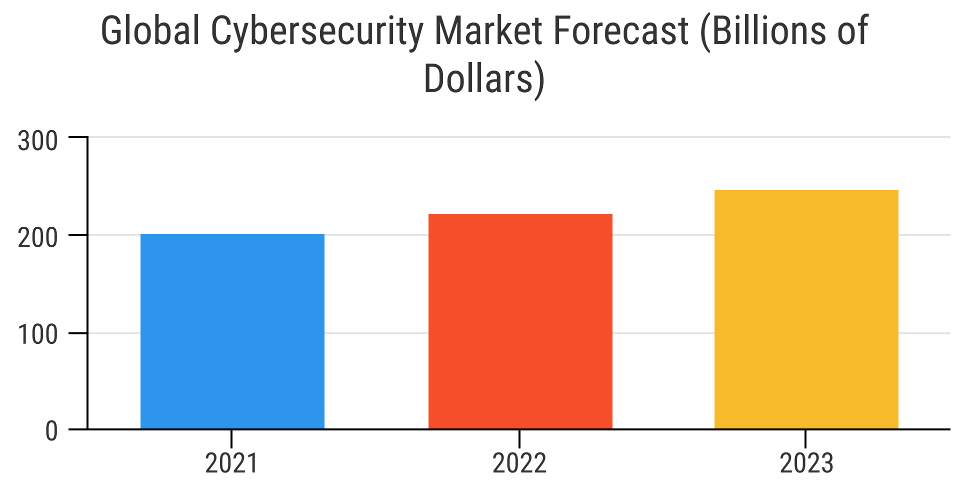
Industry Profitability

When analyzing the industry margins, from an Advisory Service Provider’s standpoint it, it is generally a high margin service. There is not a lot of overhead for small ASPs as the work is completed remotely on an end user’s device (i.e. laptop). For Managed Security Service Providers (MSSPs), there is a degree of cost involved as analysts need to be hired to monitor a client’s network 24/7. The average profit margin on a typical managed service contract in North America is 32% (SolarWinds). The net profit of the global cybersecurity industry in 2019 was USD 112.01 billion and it is projected to reach USD 281.74 billion by 2027 (FortuneBusinessInsights). When analyzing the compound annual growth rate from 2020 to 2027 (CAGR), we arrive at 12.6%. North America is the largest region in the global cybersecurity services market, accounting for 36.1% of the cybersecurity customers in 2019 (Business Research Company).

Taking a look at how the industry will shift, we are going to see a large number of customers transition to the cloud and the increased use of IoT devices. Medium to large sized companies often have large internal networks that are hosted on premises. This makes transitioning an entire organization to the cloud a time intensive process. In these situations, clients will often choose to keep hybrid environments, a mix of on-premises and cloud infrastructure. According to Fortune, cloud adoption rates have risen from 19% in 2015 to 57% in 2016 alone. In the same report, IDC CloudView commented that 73% of their surveyed organizations have a hybrid cloud strategy. When considering applications, there is a large shift of applications from self-hosted to cloud. In a report by Hosting Tribunal, in 2018 the cloud hosted around 45% of a company’s workload, in 2019 it was predicted it would hit 60%. In a report. In an article by Forbes, 66% of IT professionals say security is their most significant concern in cloud strategy. Based on the information gathered, there is a clear pattern that cloud adoption will increase and as a result, the need for cloud security will be in demand. This will create a lot of opportunity from an architecting perspective (migrating infrastructure to the cloud) and an offensive security perspective (cloud security review).

Industry Profitability Cont.

Another major shift anticipated is the widespread adoption, and increase, of IoT devices. IoT devices are embedded devices (such as microcontrollers that can be found in everything from webcams, door locks, light bulbs, speakers or any number of devices) that are connected to the internet. A large number of businesses are leveraging IoT in their business. The adoption of IoT by companies in 2014 was 13%, presently the adoption sits at 25%. By 2023, it is estimated the number of IoT devices will increase to 43 billion, nearly threefold from 2018 (McKinsey). The uptick of IoT adoption stems from a number of factors such as technological advancement that allows for easier adoption. Most homes have a Google Home or Alexa device to automatically connect them to the internet and give them information/music from apps. When analyzing the security side of IoT, to determine if a need exists, there are a number of concerns. In 2018, IoT malware attacks jumped 215.7% to 32.7 million in 2018. In regards to IoT malware attacks, there is a 33% year-over-year increase (SonicWall). Additionally, to make matters more concerning, 55% of companies do not require third-party IoT provider security and privacy compliance (Shared Assessments). Finally, there is an overwhelming number of risk professionals, 76%, that think IoT leaves them at risk of cyber attacks (SharedAssessments). With third party vendors being the cause for catastrophic breaches, IoT presents a significant opportunity for businesses and cybercriminals alike. Interpreting these statistics, it is evident that the IoT segment will continue to grow, and IoT attacks will increase but professionals or companies with the right talent will be able to capitalize on securing devices in this sector.



PORTER'S 6 FORCES

- **Threat of New Entrants**
  There is high potential for profit, however, barriers such as economy of scope and experience make it harder for new entrants.

- **Bargaining Power of Suppliers**
  There is little room for negotiation with most suppliers as these technological suppliers have standardized reseller programs

- **Bargaining Power of Buyers**
  Enterprises and financial institutions have their shortlist of vendors, however, small medium businesses (SMBs) are sensitive to price.

- **Threat of Substitutes**
  Small organizations often employ vulnerability scanners as the relative price performance of the substitute is lower when compared to hiring a consultancy.

- **Intensity of Competitive Rivalry**
  Vendors often exhibit price competition because of low service differentiation and low switching cost.

- **Compliments**
  Advisory Service Providers (ASPs) and Managed Security Providers (MSPs) are complimented by strategic partnerships with consultancies, cyber insurance vendor and certification authorities.

PORTER'S 6 FORCES

Overview

When looking at Porter's Six Forces and applying his model to the industry, we can get a clear picture of the industry players. Porter's Five Forces include the threat of new entrants, bargaining power of suppliers, bargaining power of buyers, the threat of substitutes, and the intensity of competitive rivalry and compliments.

Threat of New Entrants

When considering the threat of new entrants, we need to look at some factors. Due to the potential for profit in cybersecurity there are a number of people trying to enter the industry. However, certain services, such as offensive security services provided by Advisory Service Providers (ASPs) are specialized in nature and the skillset needed is uncommon. There are a small number of established players in the Toronto Offensive Security industry. When considering the supply-side economies of scale, there is an experience barrier to entry. Toronto currently has a shortage of offensive security talent and firms are often competing with each other for talent. While it allows an opening for new entrants, the uncommon skills that are required create a barrier for entry for those same entrants. Enterprises and financial institutions are consistent with the vendors they use, this presents an economy of scope that adds an additional barrier for entry. The sale of offensive security engagements results in multiple projects to the same client over a set period. This could include a giant upfront capital cost that consists of testing a pre-determined number of applications/systems. This is often a preferred option for enterprises and businesses as they usually get a discount and take comfort in knowing the quality of the work being performed. From the service side, there is no cost incurred to companies who switch vendors. This means that despite the fact that enterprises have a select few vendors, it is possible for any service provider to potentially acquire clients from competitors. In respect of costs, a small Advisory Service Provider (ASP) has low capital costs as they often use remote offices and primarily rely on contractors for excess work. From the provider side, there is no cost to switch MSSPs, however there is a much larger initial capital cost.

PORTER'S 6 FORCES

Threat of New Entrants Cont.

Managed Security Service Providers (MSSPs) need a minimum of three employees working 8-hour rotating shifts to be alert of traffic passing through client’s networks. Additionally, MSSPs need to purchase software licenses for relevant software to accommodate their clients.

Bargaining Power of Suppliers

When considering Porter’s force of bargaining power of suppliers, we need to look at it from an MSSP standpoint as Advisory Service Providers (ASPs) often do not have suppliers. Small MSSPs typically rely on reselling cloud subscription services such as Office365, Microsoft Azure, and cloud security solutions such as Palo Alto PrismaCloud and Qualys Cloud Platform. In these situations, the supplier has the bargaining power and the prices are standardized across all clients. The prices typically go down as an MSSP brings a certain number of customers or a certain amount of recurring revenue. In regards to supplier concentration, there are three major cloud providing platforms and only a handful of cloud security solutions. This allows for some competition in the Cloud security space and price differentiation between the different platforms and products. The main industry switching cost, when migrating clients to a different solution, is downtime. If a client was to migrate a company over to new infrastructure, it could potentially cause down time which can affect availability of work-related applications and internal applications.

Bargaining Power of Buyers

Bargaining power of buyers, one of Porter’s Five Forces, refers to the pressure a consumer can place on a business to get higher quality products/services and lower prices. Strong buyers make industries more competitive and often lead to decreased potential profit for the Managed Security Service Providers (MSSPs) and Advisory Service Providers (ASPs). It is not uncommon for repeat clients to try to request out-of-scope work during an engagement nor

PORTER'S 6 FORCES

Bargaining Power of Buyers Cont.

is it uncommon for clients to expect a discount for continued working arrangements. While enterprises and financial intuitions have their short list of vendors, Small Medium Businesses (SMBs) are sensitive to price. If an ASP or MSSP can provide enterprise quality services at a competitive price, it is likely an SMB will switch vendors. Additionally, because there are no customer switching costs, an SMB is even more likely to switch vendors.

Threat of Substitutes

SMBs may often times try to use vulnerability scanners and other solutions which they feel provide adequate security. Vulnerability scanners, like Nessus, have the ability to perform automated tests to flag multiple issues. Due to this, an SMB may be less likely to opt in for a penetration test despite the fact that they are more compressive and pick-up things scanners don’t. These products are often times significantly cheaper then getting an ASP to perform a penetration testing engagement or outsourcing your security to an MSSP. In these situations, the consumer considers the relative price performance of any substitute and the perceived level of product differentiation. An MSSP or ASP trying to tap into this segment should be prepared to demonstrate and explain the differentiation of a security product versus a security service. The substitute products that can replace ASP/MSSP services offer significantly less coverage of security issues but are at a much lower price point when compared to the cost of hiring an ASP or MSSP.

Intensity of Competitive Rivalry

When considering the competition on pricing, ASP and MSSP vendors often exhibit price competition because of low differentiation and low switching costs. Many of the main competitors in Toronto, focusing on ASP and MSSP services, are of equal size and power (outside of the big 4 consulting firms that have created a cybersecurity division of their own). Industry concentration is low which results in a competitive industry. Despite the

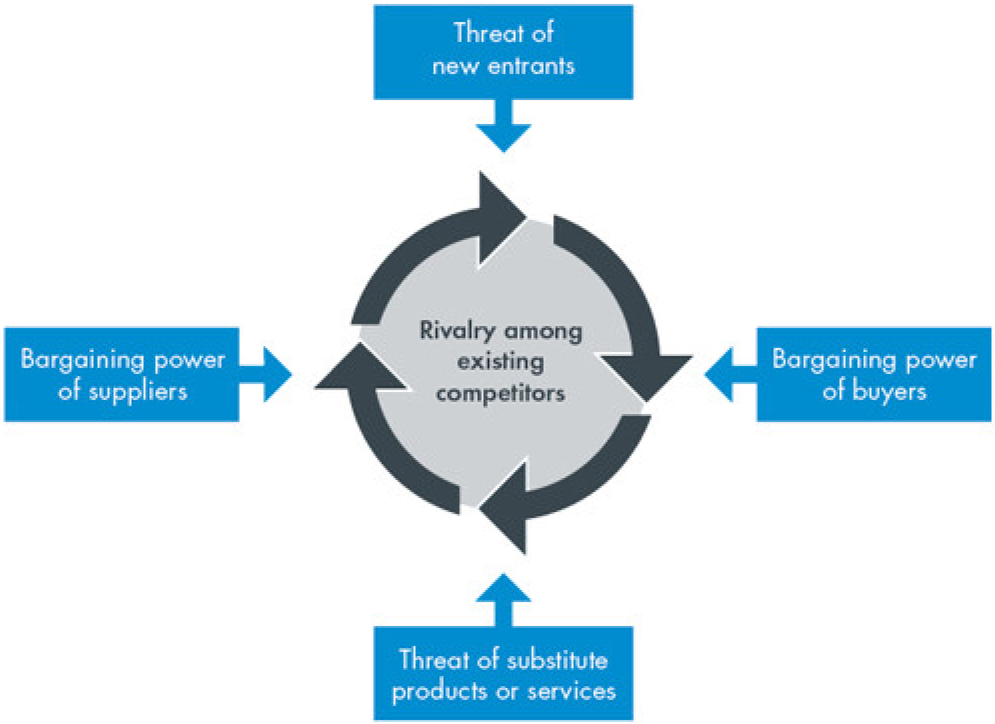
PORTER'S 6 FORCES

Intensity of Competitive Rivalry Cont.

competition, there are a number of compliments to ASPs and MSSPs. Both can form strategic partnerships with existing companies, for subcontracting purposes, and can also resell cyber insurance policies from existing brokers. ASPs and MSSPs that align themselves with secure cloud migration and cloud monitoring, may be able to leverage compliments with cloud related providers. This can include reselling cloud services from Amazon Web Services (AWS), Microsoft Azure or Google Cloud Platform.

Compliments

Despite the competition, there are a number of compliments to ASPs and MSPs. Both can form strategic partnerships with existing companies to be subcontractors as well as reselling cyber insurance policies from existing brokers. ASPs and MSPs that align themselves with secure cloud migration and cloud monitoring, may be able to leverage compliments with cloud related providers.


Threat of new entrants
Bargaining power of suppliers
Rivalry among existing competitors
Bargaining power of buyers
Threat of substitute products or services

PESTEL ANALYSIS

✓ **Political Trends**

Liberal government's budget proposed a $1 billion federal budget for cyber security in 2019. Additionally, programs such as the Cyber Security Cooperation program provide funding for cyber security ventures.

✓ **Economic Trends**

The Canadian dollar, while stable, has plunged over the last few years. Additionally, due to Covid-19 interest rates have never been lower.

✓ **Social Trends**

Population aging acceleration between 2010-2031 will cause all baby boomers to reach age 65. Humans are often the weakest link in the cybersecurity chain and cause a majority of breaches.

✓ **Technological Trends**

Organizations are transitioning towards BYOD (Bring Your Own Device) environments, Cloud infrastructure and IoT (Internet of Things) devices.

✓ **Legal/Regulatory Trends**

Following regulatory frameworks such as PIPEDA and PCI-DSS is expected of relevant industries. Additionally, there is a large adoption of cyber insurance.

✓ **Environmental Trends**

Natural disasters can affect availability and/or data loss. Disaster recovery plans are essential and should be explored by ASPs.

PESTEL ANALYSIS

Political Trends

Political factors deal with government policy, tax policy, labour law and matters of that sort. In the federal 2018 budget, the National Cyber Security Action Plan called for federal budgets totaling close to $1 billion. This funding was to be used to protect critical cyber systems in the finance, telecommunications, energy and transport sectors. The increased budget and spending on cybersecurity would also increase the number of federal government Requests for Proposal (RFPs) related to cybersecurity. ASPs and MSSPs should consider exploring the government sector and bidding on relevant opportunities. The Cyber Security Cooperation Program offers up to $350,000 in grant funding to for-profit and non-profit companies alike. The program was intended to fund organizations that are helping to build a more resilient Canada. If eligible, MSSPs and ASPs should consider applying for the funding.

Economic Trends

Economic factors refer to a number of things such as growth/decline of the economy, interest, inflation, wage rates and cost of living. When applying this element of the PESTEL analysis in the cybersecurity industry, we can observe a weak Canadian dollar (when compared to the US) as well as low interest rates. A weak Canadian dollar results in a higher exchange rate when converting USD to CAD. Canadian-based MSSPs and ASPs should consider setting up remote field offices in relevant parts of the States to try to drive U.S. clients and gain higher profits. In addition to paying more, the conversion rate will result in more profit for the MSSP/ASP that attempts to acquire customers based in the U.S. Due to the Covid-19 pandemic, the Bank of Canada passed a number of actions to support both the Canadian economy and financial system. The most important action taken was the large reduction in interest rates to support economic activity. The low interest rates mean that businesses and consumers can lower payments on existing and new loans. If an ASP was looking to become a hybrid firm and offer MSSP services, a low interest business loan might be what's needed initially to fund it.

PESTEL ANALYSIS

Social Trends

Social factors in the PESTEL analysis deal with demographic characteristics, trends, customs and values. Statistics Canada reports that population aging in Canada will accelerate between 2010 and 2031, a period in which all baby boomers will reach age 65. This would cause a generational shift of power and there would be an increase of millennials and Generation Z'ers in executive roles. As these generations have a deeper understanding of technology, it may present opportunity to sell cybersecurity services to companies that were otherwise run by baby boomers that may not understand the importance of cybersecurity as much. With the current social dynamic, cybersecurity is not a giant priority for businesses. A report by Fundera concluded that 54% of small businesses believe they are too small for a cyber attack. Additionally, 54% of these companies do not have a plan in place for reacting to cyber attacks. Finally, 95% of cybersecurity breaches are due to human error (CybintSolutions) which demonstrates that cybersecurity is not just a technical issue, but a social one as well. MSSPs and ASPs should consider coupling cyber awareness training with their services to address the technical and social challenges of small businesses.

Technological Trends

The technological trends of PESTEL refer to the life cycle of technology, benefits of automation and market awareness and acceptance. There are a number of technological trends that can result in additional opportunities for MSSPs and ASPs alike. The BYOD (Bring Your Own Device) market is on course to hit almost $367 billion by 2022 (Forbes). Additionally, companies favouring BYOD have average annual savings of around $350 per year, per employee (Cisco). With the introduction of employee devices to networks, there exists a number of security concerns. MSSPs and ASPs can introduce various ways to ensure BYOD is as secure as possible. This could include the recommendation of a Mobile Device Management (MDM) system or segmenting the network to ensure that personal devices are not on the primary network. Additionally, as both the Cloud and IoT adoption are increasing dramatically, this creates more opportunity for ASPs that have the skillset to secure cloud environments and IoT products.

PESTEL ANALYSIS

Environmental Trends

The environmental trends of PESTEL consider the impact of natural disasters, which have been pretty consistent and averaging around 300 for the past decade. Environmental disasters can lead to the loss of power or physical damage to infrastructure. Disaster recovery plans are referred to in the event of an environmental emergency and act as a step-by-step guide on how to recover their data. MSSPs and ASPs that can secure the right talent, should consider offering Disaster recovery services in addition to their already offered services.

Legal/Regulatory Trends

When analyzing the legal/regulatory trends of PESTEL, three trends were identified. The first trend was compliance of regulatory frameworks (such as PCI-DSS and PIPEDA). Businesses that process credit card transactions are subject to a regulatory framework (such as PCI-DSS) that ensures a baseline level of security surrounding payment transactions. ASPs should consider partnering with third party compliance experts that can be subcontracted and can assist with any relevant compliance work that may arise. The second trend is criminal charges while performing offensive security engagements. While rare, at the end of 2019, two ethical hackers performing a physical penetration test of an Iowa courthouse were arrested despite being authorized to perform said testing (Coalfire). Caution should be extended by ASPs when performing relevant offensive security engagements as unauthorized testing can potentially lead to criminal action. Finally, the adoption of cyber insurance has been steadily increasing. Cyber insurance is insurance for cyberattacks such as ransomware. According to GlobalNewsWire, the Cyber Insurance Market is to grow with 26.3 Compound Annual Growth Rate (CAGR) between 2020 and 2030. ASPs and MSSPs should consider strategic partnerships with cyber insurance providers so they are able to resell cyber insurance to their respective clients.

SYNTHESIS OF ANALYSIS

Summary

In my overall view, the cybersecurity industry is attractive and should be considered exploring. As of Q1 2021, the macro factors are favorable, the industry factors (such as size and growth) are favorable, and the competitive forces (Porter’s 6 Forces) are unfavorable. The following first level screen summarizes the current conditions.

Problem/ Customer(s) -New trends require niche skillset -Large market for cybersecurity services	**Timing** -Macro factors favorable -Industry factors favorable -Competitive forces unfavorable
Money Making -Multiple revenue streams via strategic partnerships -Big margins (service provider side)	**Team** -Specialized skillsets

When considering the problem and customers, new entrants should target Small Medium Businesses (SMBs) initially as they are sensitive to price. Trends, such as the adoption of Cloud and IoT, will require cybersecurity service providers with niche skillsets. When performing industry attractiveness, we concluded that there is a large market for cybersecurity services, especially in North America.

As a cybersecurity service provider, there are multiple revenue streams that can be tapped into. Forming strategic partnerships, with organizations that can perform services you're not able to, leads to mutual growth. Reselling cloud services results in passive income, which is another revenue stream cybersecurity service providers can leverage.

REFERENCES

There's Nowhere to Hide from the Economics of Cybercrime. (n.d.). Retrieved January 19, 2021, from https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html

Company, T. (2020, November 05). Cybersecurity Industry Overview Shows US To Account For The Largest Share Among Countries, In The Global Cyber Securities Market 2020. Retrieved January 19, 2021, from https://www.globenewswire.com/news-release/2020/11/05/2121251/0/en/Cybersecurity-Industry-Overview-Shows-US-To-Account-For-The-Largest-Share-Among-Countries-In-The-Global-Cyber-Securities-Market-2020.html#:~:text=The%20global%20cybersecurity%20services%20market%20size%202019%20reached%20a%20value,at%20a%20rate%20of%208.0%25.

Cybercrimemag. (2019, June 11). Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021. Retrieved from https://cybersecurityventures.com/cybersecurity-market-report/#:~:text=Worldwide spending on information security,and $170.4 billion in 2022.

Cyber Security Market Size, Share, Growth: Trends Report, 2027. (n.d.). Retrieved from https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

2019 Trends in North American Managed Services. (2019, December). Retrieved January 19, 2021, from https://www.solarwindsmsp.com/sites/solarwindsmsp/files/resources/2019_Trends_In_NAmerican_Managed_Services_Report.pdf

Company, T. B. (2020, November 05). Cybersecurity Industry Overview Shows US To Account For The Largest Share Among Countries, In The Global Cyber Securities Market 2020. Retrieved from https://www.globenewswire.com/news-release/2020/11/05/2121251/0/en/Cybersecurity-Industry-Overview-Shows-US-To-Account-For-The-Largest-Share-Among-Countries-In-The-Global-Cyber-Securities-Market-2020.html#:~:text=The global cybersecurity services market size 2019 reached a value, at a rate of 8.0%.

MSPs' revenue growth decelerated in 1H 2019, but those with key differentiators are still performing well. (2020, March 30). Retrieved from https://www.analysysmason.com/research/content/comments/revenue-growth-msp-ren03/

REFERENCES

Blaine, G. (2019, October 29). Encrypted Attacks, IoT Malware Surge as Global Malware Volume Dips. Retrieved from https://blog.sonicwall.com/en-us/2019/10/sonicwall-encrypted-attacks-iot-malware-surge-as-global-malware-volume-dips/#:~:text=In 2018, SonicWall Capture Labs,year-over-year increase.

The Internet of Things (IoT): A New Era of ThirdParty Risk. (2017, May). Retrieved January 19, 2021, from https://www.ponemon.org/local/upload/file/IoT and Third Party Risk Final1.pdf

Cloud Adoption Statistics - It's Everywhere & Everyone's Using It in 2021! (2021, January 19). Retrieved from https://hostingtribunal.com/blog/cloud-adoption-statistics/

https://www.cisco.com/c/en/us/solutions/cloud/hybrid-cloud/cloud-adoption-rates.html#:~:text=According%20to%20Fortune%2C%20hybrid%20cloud,have%20a%20hybrid%20cloud%20strategy.

Columbus, L. (2018, January 25). 83% Of Enterprise Workloads Will Be In The Cloud By 2020. Retrieved from https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/

Application Information. (2021, January 14). Retrieved from https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/cprtn-prgrm/pplctn-nfrmtn-en.aspx

Canada, E. A. (2020, December 29). Government of Canada. Retrieved from https://www.canada.ca/en/employment-social-development/services/funding/canada-summer-jobs.html

Canadian dollar hits four-year low as fears rise for world economy. (2020, March 12). Retrieved from https://www.theglobeandmail.com/investing/markets/inside-the-market/market-news/article-canadian-dollar-hits-four-year-low-as-fears-rise-for-world-economy/#:~:text=At 9:49 a.m., the,since February 2016 at 1.3854.

Tencer, D. (2021, January 12). Canada's Interest Rates Could Be Headed Even Lower, Markets Signal. Retrieved from https://www.huffingtonpost.ca/entry/bank-of-canada-interest-rate_ca_5ffdf7a5c5b66f3f7961db30

REFERENCES

Highlights. (2015, November 27). Retrieved from https://www150.statcan.gc.ca/n1/pub/91-520-x/2010001/aftertoc-aprestdm1-eng.htm

30 Surprising Small Business Cyber Security Statistics [2021]. (n.d.). Retrieved from https://www.fundera.com/resources/small-business-cyber-security-statistics

15 Alarming Cyber Security Facts and Stats. (2021, January 12). Retrieved from https://www.cybintsolutions.com/cyber-security-facts-stats/

Artificial Intelligence & Machine Learning in Cybersecurity. (2021, January 14). Retrieved from https://cyberstartupobservatory.com/artificial-intelligence-cybersecurity/

https://www.forbes.com/sites/lilachbullock/2019/01/21/the-future-of-byod-statistics-predictions-and-best-practices-to-prep-for-the-future/?sh=2f76278d1f30

PCI Compliance Guide Frequently Asked Questions: PCI DSS FAQs. (2017, September 05). Retrieved from https://www.pcicomplianceguide.org/faq/

Office of the Privacy Commissioner of Canada. (2019, June 07). PIPEDA in brief. Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/#:~:text=All businesses that operate in,provinces with substantially similar legislation).

Global reported natural disasters by type. (n.d.). Retrieved from https://ourworldindata.org/grapher/natural-disasters-by-type

Cyber Security, Data Loss, And Environment Monitoring. (2018, April 18). Retrieved from https://avtech.com/articles/10775/cyber-security-data-loss-environment-monitoring/

Dahlqvist, F., Patel, M., Rajko, A., & Shulman, J. (2020, September 16). Growing opportunities in the Internet of Things. Retrieved from https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things