NSBI Trade Market Intelligence Report:

Cyber Security in the US, and the growing cluster in Nova Scotia

Executive Summary

The Cyber Security industry, including IT security services, is growing strongly, driven by advances in technology and widespread adoption of e-commerce, cloud computing, and online services. The largest markets for this industry are in financial services, the public sector, the information sector, healthcare, insurance, and retail. Distribution of IT security establishments is relatively proportional to the US population distribution, but California, Washington D.C., and New York have been identified as most desirable locations due to the high density of clients in these areas in technology, government services, and financial services respectively.

Cybersecurity is a major challenge in the US, with an increasing amount of attacks affecting organizations of all sizes in both the public and private sectors. This challenge has been identified by the current federal administration and efforts are being made to improve cybersecurity. To see recently passed legislature, or seek information on newly proposed bills that could pass into law, monitor the *Federal Register* and the Cybersecurity Legislation Watch.

This growing market is attracting a growing number of service providers. There are many choices for cybersecurity services including HIPAA compliance services and DDoS threat protection services, though concerns remain that many of the services are too expensive for smaller firms.

No compliance products targeting ITAR were identified, as these requirements are complex and vary depending on what is being exported and where it is going.

With strong academic support, Atlantic Canada is becoming globally recognized for its world-class cyber security talent. In Nova Scotia, the existence of this talent has resulted in the recent birth of a young, but globally connected, cyber security cluster (Described in the Appendix of this report).

With the Canadian market for these services being limited in scale, simply due to the country's population, it is crucial that Atlantic Canadian companies look globally in order to grow.

Nova Scotia Business Inc.

Nova Scotia Business Inc. is the province's private sector-led business development agency. Through trade development, investment attraction, business advisory services, and business financing, we assist local companies and attract international companies to Nova Scotia.

With a team of sector and market specialists, we are dedicated to helping Nova Scotia companies enter and pursue growth in markets around the world.

Disclaimer

All Rights Reserved

The information and facts of this report are believed to be accurate at the time of publication, but because of the rapid changes in the market or other conditions, cannot be guaranteed. Please note that the findings, conclusions and recommendations that NSBI delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. All information is provided "as is" without warranty of any kind, and NSBI makes no representations, and disclaims all express, implied, and statutory warranties of any kind to user and/or any third party, including but not limited to, the accuracy, timeliness, completeness, merchantability, fitness for any particular purpose and freedom from infringement. As such NSBI has no liability in tort, contact, or otherwise, to user or any third party, for actions taken based on any information that may subsequently prove to be incorrect.

Trade Market Intelligence: Cyber Security in the US

Introduction

The recent, and rapid, growth in the number of connected devices globally has drastically increased the importance of the cyber security industry. Estimates of the global Cyber Security market size reach as high as $122 billion (USD) in 2016, with anticipated growth to over $200 billion by 2021.[1] Although Financial Services and the Public Sector are still the predominant purchasers of cyber security services, the consumer market is growing in part due to the sheer number of devices connected to global networks. It is anticipated that by 2020 there will be more than 34 billion devices online.[2] This trend to connect even more devices, commonly referred to as the Internet of Things (IoT), requires significant security increases for two broad reasons: The connected devices themselves must be secured in order to protect their direct owners, and new robust anomaly detection technology is required due to the increased potential of large scale botnets conducting distributed denial of service (DDoS) attacks. To this end, the portion of the Cyber Security market directly related to IoT is anticipated to grow with a compounded annual growth rate (CAGR) of nearly 55% from 2014-2019.[3]

With strong academic support, Atlantic Canada is becoming globally recognized for its world-class cyber security talent. In Nova Scotia, the existence of this talent has resulted in the recent birth of a young, but globally connected, cyber security cluster (Described in the Appendix of this report).

With the Canadian market for these services being limited in scale, simply due to the country's population, it is crucial that Atlantic Canadian companies look globally in order to grow.

[1] Cyber Security Market by Solutions (IAM, Encryption, DLP, UTM, Antivirus/Antimalware, Firewall, IDS/IPS, Disaster Recovery), Services, Security Type, Deployment Mode, Organization Size, Vertical & Region - Global Forecast to 2021

[2] Business Insider. 2016. "How the 'Internet of Things' will impact consumers, business, and governments in 2016 and beyond". Accessed on 22/10/2016

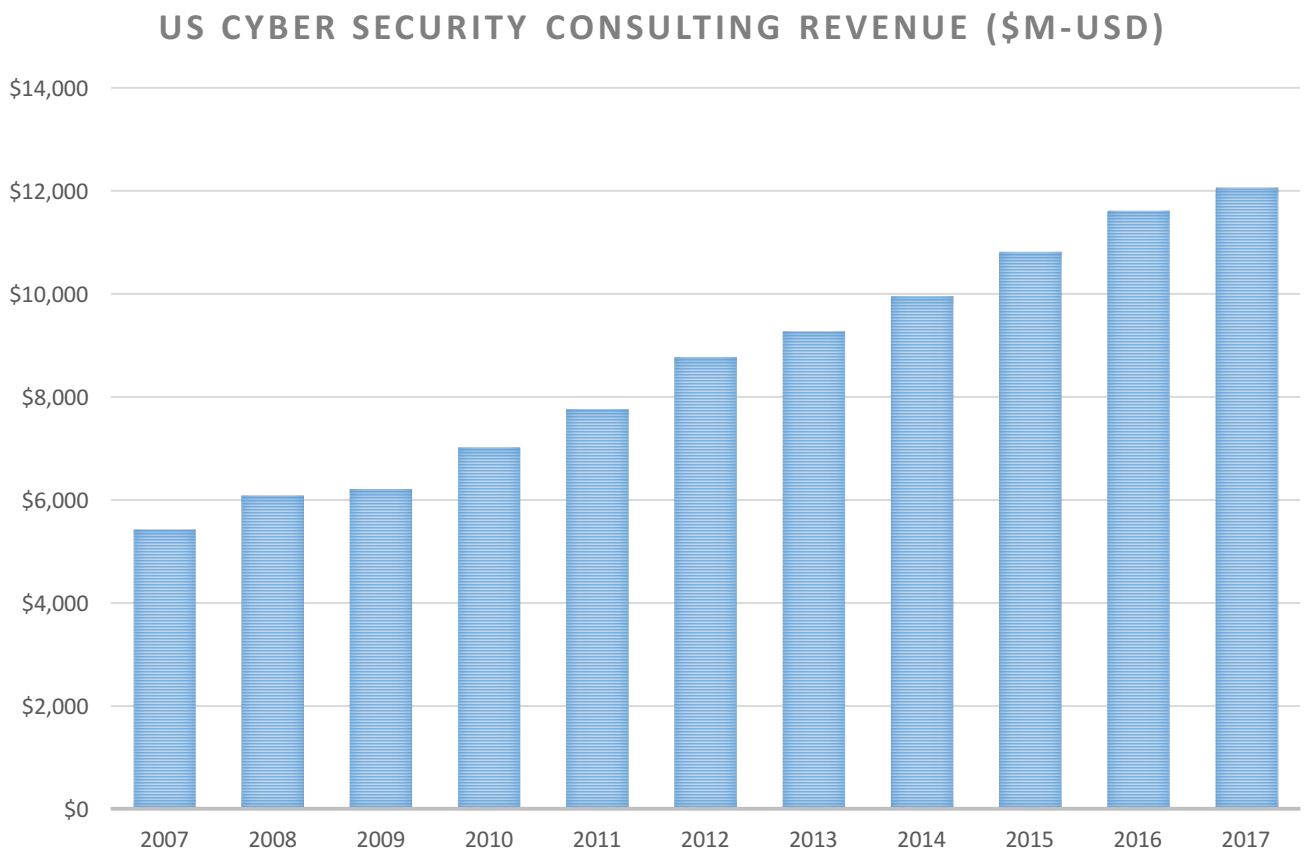
[3] Forbes, 2015. "Cybersecurity Market Reaches $75 Billion In 2015; Expected to Reach $170 Billion by 2020". Accessed on 22/10/2016

Cyber Security in the US[4]

According to an analysis by IBIS World, consulting services within the Cyber Security industry in the US had a revenue of more than $10 billion (USD) in the US in 2015, and employs almost 60,000 people. This industry includes companies that offer managed IT security services such as firewalls, intrusion prevention, security threat analysis, proactive security vulnerability and penetration testing, and incident preparation and response, which includes IT forensics.

This industry saw strong growth over the five years from 2010 to 2015, with an average annual growth rate of 14.1%. This growth can be attributed to the increasing adoption of e-commerce, m-commerce, social networking and cloud computing and a variety of high-profile data breaches. IT security consultants have benefited from these trends as they increase the amount of data stored in cloud servers that require protection. Furthermore, the rise of cloud computing and software as a service (SaaS), a model of software deployment in which a provider licenses an application to customers for use as a service on demand, have caused an increasing percentage of services to be conducted online.

Downstream markets, such as banking and financial services, insurance, health, telecommunications and government agencies, continue to fear high-profile, reputation-threatening breaches, which is expected to drive continued industry revenue growth at an average annual rate of 11.0% to $14.4 billion over the five years to 2020.



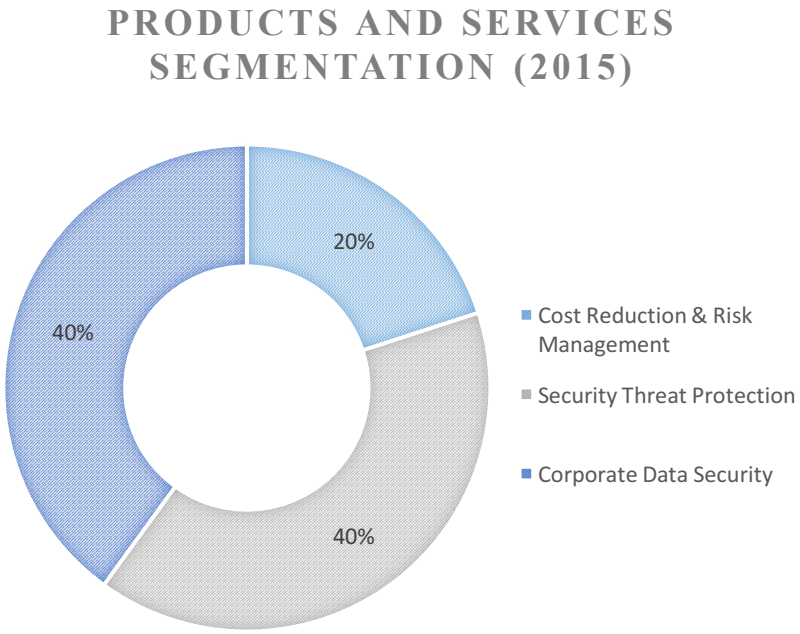
[4] IBIS World. 2015. *IT Security Consulting in the US*. Accessed on 05/10/2016

Security Threat Protection

Security threat protection represents about 40.0% of industry revenue. This segment of the industry is growing as companies manage increasing amounts of data. Firms in this market segment can reduce the cost of cyber-attacks and strategically align a company's security program to manage security threats efficiently. This service is highly sought after by government and technology firms facing increasingly complex network security threats and cyber terrorist threats that can damage business operations and a brand's reputation, consumer trust, intellectual property and other key organizational functions.

Major Markets

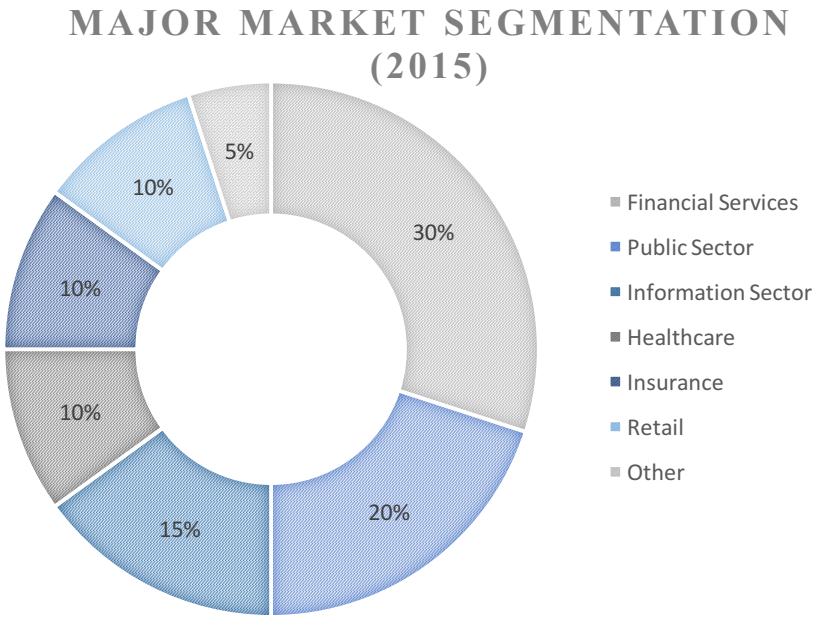
The largest market for Cyber Security in the US is the financial services sector. Accounting for about 30% of the total market, this segment is increasingly reliant on IT security consultants to protect sensitive client information as an increasing proportion of financial transactions are becoming automated.



The public sector is the next most important market for this industry. Federal and state government agencies make up 20% of the Cyber Security market. This segment is significant due to the vast number of government records and information systems that must be maintained and protected. However, public sector clients are often constrained by tighter budgetary restrictions than business consumers, and this sector has decreased Cyber Security expenditure from 2010 to 2015.

Operators in technology, media and telecommunications make up the information sector which generates about 15.0% of the industry's revenue. The technology and online services market has grown quickly over the five years from 2010 to 2015 as online shopping and social media websites gained more users. This growth, paired with the constant evolution of technology, has increased the demand for Cyber Security in this sector.

Next, the insurance and healthcare sectors each represent 10% of the market. The insurance sector represents a small but stable market for Cyber Security, mostly relying on these services to lower the risk of fraudulent claims. Meanwhile, the healthcare sector is expected to grow significantly between now and 2020 as companies continue to integrate big data solutions and predictive analytics throughout their operations.



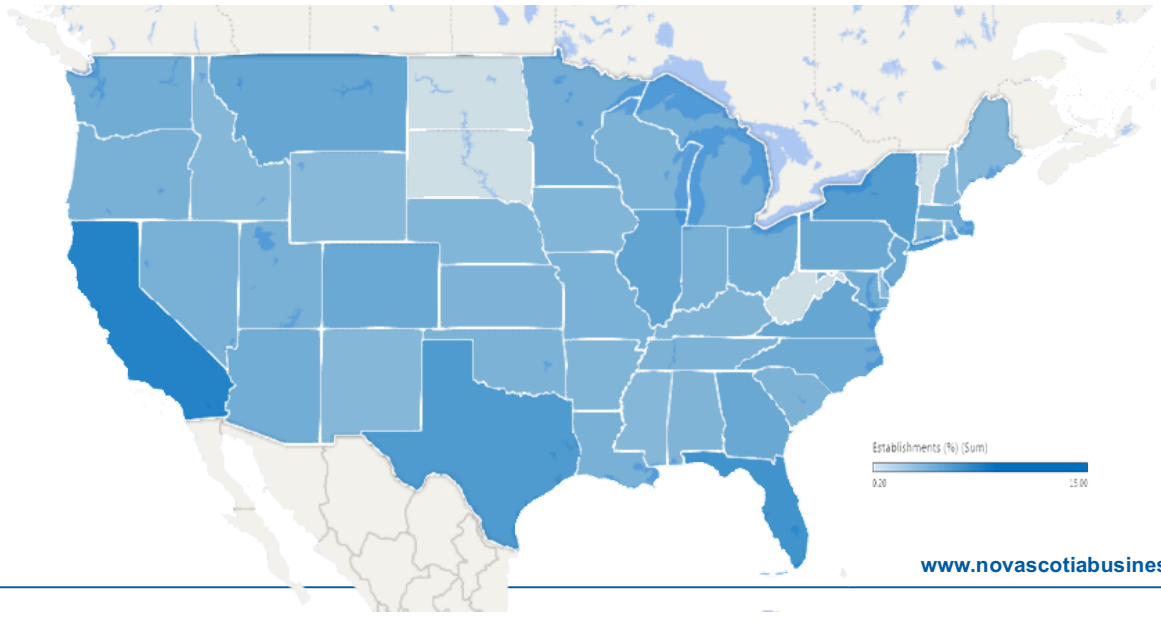
The remaining 15% of the market comes from retail and other segments. Clients in these segments are diverse as IT security consultants service most industries that use electronic information.

Business Locations

The distribution of Cyber Security establishments generally reflects the US population distribution, though there is increased consulting density in areas with technological centers and major markets such as financial service companies, large technology corporations and government clients.

California produces the greatest share of IT consulting revenue, establishments and employment of any state and represents 15% of industry establishments primarily due to the concentration of technology and software firms located in Silicon Valley.

The Southeast region of the US is a popular destination for industry operators due to its proximity to the industry's largest government clients in Washington, DC. New York is also a desirable location as it houses the headquarters of many major firms in the financial services sector.



Cybersecurity Regulations in the US

Major Cybersecurity Deficiencies

With incidents of computer attacks up 1,100 percent since 2006, cybersecurity is a significant challenge in the US.[5] Organizations of all sizes in both the public and private sectors in any industry are vulnerable to cyber-attacks. According to a May 2016 list by Forbes, the top five industries at risk of cyber-attacks are healthcare, manufacturing, financial services, government, and transportation.[6]

A 2016 report by the Congressional Research Service found that attackers are constantly probing complex ICT systems for weaknesses that can occur at many points, of which many can be defended. Three weaknesses were identified as particularly challenging:[4]

- inadvertent or intentional acts by insiders with access to a system;
- supply chain vulnerabilities, which can permit the insertion of malicious software or hardware during the acquisition process; and
- previously unknown, or *zero-day*, vulnerabilities with no established fix.

Furthermore, even in cases where vulnerabilities and their remedies are known, budgetary and operational constraints prohibit organizations from being able to take action to put suitable defenses in place.[7]

Another major concern, is the 'bring your own device' (BYOD) trend that is increasingly popular in many industries. The use of mobile devices, particularly employees' personal devices, increases risk exposure as companies must balance the need to monitor use with personal privacy, and have less power to apply restrictions to what the device may be used for.[8]

Legal Developments

The regulatory environment for cybersecurity in the US evolves as new legislation is proposed and enacted by congress. The most recently enacted federal legislature on cyber security is the Cybersecurity Act of 2015, which came into effect on December 18, 2015, and promotes the responsible exchange of cyber threat information between the private sector and the US government. A recent publication by DLA Piper provides useful analysis of this act among other recent cybersecurity developments.[9]

President Obama's administration has identified cybersecurity as one of the most important challenges facing the United States. The most recent effort by this administration to address this challenge is the launch of the Cybersecurity National Action Plan. This plan includes an increase in government funding for cybersecurity, a focus on modernizing government IT and empowering Americans to secure their online accounts, as well as the establishment of the Commission on Enhancing National Cybersecurity. This commission is expected to report to the President with recommendations for future actions to protect Americans long-term security online before the end

[5] Foreign Policy Association. 2015. *The Systematic Deficiency in the U.S.' Cybersecurity Mindset.* Accessed on 10/19/2016 http://foreignpolicyblogs.com/2015/06/24/the-systemic-deficiency-in-the-u-s-cybersecurity-mindset/
[6] Forbes. 2016. *Top 5 Industries At Risk Of Cyber-Attacks.* Accessed on 10/18/2016 http://www.forbes.com/sites/stevemorgan/2016/05/13/list-of-the-5-most-cyber-attacked-industries/#5c7bfd963954
[7] Congressional Research Service. 2016. *Cybersecurity Issues and Challenges: In Brief.* Accessed on 10/19/2016 https://www.fas.org/sgp/crs/misc/R43831.pdf
[8] CIO. 2015. *6 Biggest Business Security Risks and How You Can Fight Back.* Accessed on 10/20/2016 http://www.cio.com/article/2872517/data-breach/6-biggest-business-security-risks-and-how-you-can-fight-back.html
[9] ISACA. 2016. *Cybersecurity Legislation Watch.* Accessed on 10/18/2016 http://www.isaca.org/cyber/Pages/cybersecuritylegislation.aspx

of 2016. Their recommendations may give some insight into what changes and new regulations can be expected in the coming years. However, the upcoming presidential election must also be considered as the new administration may take a different direction in regulating this industry.[10]

It is difficult to ascertain what changes to regulations will come into effect, as proposed bills must be voted on by congress, and the outcomes of such votes are not predictable. The ISACA's Cybersecurity Legislation Watch is a useful tool for viewing recently passed legislature and monitoring the development of newly proposed bills.

ITAR

The International Traffic in Arms Regulations (ITAR) control the export and import of defense-related articles and services on the United States Munitions List (USML). Any company involved in the manufacture, sale or distribution of goods or services covered under the USML must register with the State Department's Directorate of Defense Trade Controls (DDTC) and must understand and comply with ITAR as is applies to their USML linked good or service.[11]

Any company with a product, software, or service and related technical data which is included in the USML is subject to ITAR and would be impacted by any changes to these regulations. Aside from physical products, the USML also includes technical data, which is defined within ITAR as information that is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of articles listed on the USML. [12]

Under ITAR, different companies will have different requirements for data security, depending on the nature of their product, service or related data, and to whom they are exporting or sharing their ITAR covered information with. Due to these differences in requirements, it is impossible to provide a comprehensive list of requirements for ITAR cybersecurity requirements. Meanwhile, this 2016 list of general best practices for meeting current ITAR compliance from the Digital Guardian can provide a good starting point for most companies:[13]

- Maintain an information security policy
- Build and maintain a secure network by installing and maintaining firewall configuration to protect data and avoiding the use of vendor-supplied passwords and other security defaults
- Assign a unique ID to each person with computer access
- Regularly test security systems and processes
- Protect sensitive data with encryption
- Regularly monitor and test networks
- Implement strong access control measures
- Track and monitor all access to network resources and sensitive data
- Maintain a vulnerability management program
- Implement measures to prevent the loss of ITAR-controlled data

Due to the variance in standards of reasonable security measures for protection of sensitive data, and the complexity of ITAR, it is generally recommended that companies engage an expert such

[10] The White House. 2016. *FACT SHEET: Cybersecurity National Action Plan.*
[11] Digital Guardian. 2016. *What is ITAR Compliance?* Accessed on 10/12/2016 https://digitalguardian.com/blog/what-itar-compliance
[12] Export Virginia. 2012. *Is my Company Subject to ITAR.* Accessed on 10/12/2016 http://exportvirginia.org/wp-content/uploads/2013/06/IS-MY-COMPANY-SUBJECT-TO-ITAR.pdf
[13] Digital Guardian. 2016. *What is ITAR Compliance?* Accessed on 10/12/2016 https://digitalguardian.com/blog/what-itar-compliance

as an ITAR consultant or ITAR lawyer.[14] ITAR compliance seminars and courses are also available through a number of operators to provide companies with the required expertise to ensure that they are operating within the given regulations.

While it is possible that specific ITAR cybersecurity compliance products may be discovered through consultation with an expert in that field, our search did not reveal any current offerings for such a product.

Amendments to ITAR are published in the *Federal Register*, and can also be accessed directly through the Department of State's website. An expert in ITAR should be consulted to determine the exact implications of these amendments in terms of cybersecurity requirements.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for sensitive patient data protection with its Privacy and Security Rules. Any company providing treatment, payment, and operations in healthcare, classified as 'covered entities', and any company which has access to patient information and provides support in the activities of covered entities, classified as 'business associates', must meet HIPAA compliance.[15]

HIPAA's Privacy Rule establishes national standards for the protection of certain health information. Meanwhile, the Security Rule establishes national security standards specific to the protection of health information that is held or transferred in electronic form. The Security Rule, requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting electronic patient health information. Specifically, it requires that companies:[16]

- Ensure the confidentiality, integrity, and availability of all electronic patient health information they create, receive, maintain or transmit
- Identify and protect against reasonably anticipated threats to the security or integrity of the information
- Protect against reasonably anticipated, impermissible uses or disclosures
- Ensure compliance by their workforce

The Security Rule does not dictate exactly what security measures must be taken by companies, but requires that companies consider their size, complexity, and capabilities, their technical, hardware, and software infrastructure, the costs of security measures, and the likelihood and possible impact of potential risks to electronic patient health information when choosing, reviewing, and modifying security measures.[17]

To ensure compliance with HIPAA's rules as new technology allows the increased use, storage, and transmission of electronic patient health information, a supplemental act was passed by the US government. This act, The Health Information Technology for Economic and Clinical Health Act (HITECH), raises penalties for organizations that violate HIPAA.[18]

The HIPAA Omnibus Rule was established in 2013 to revise certain definitions, clarify procedures

[14] Government Relations LLC. 2016. *What is ITAR?* Accessed on 10/13/2016 https://gov-relations.com/itar/
[15] Digital Guardian. 2015. *What is HIPAA Compliance?* Accessed on 10/13/2016 https://digitalguardian.com/blog/what-hipaa-compliance
[16] US Department of Health and Human Services. 2016. *Summary of the HIPAA Security Rule.* Accessed on 10/18/2016 http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
[17] US Department of Health and Human Services. 2016. *Summary of the HIPAA Security Rule.* Accessed on 10/18/2016 http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
[18] Digital Guardian. 2015. *What is HIPAA Compliance?* Accessed on 10/13/2016 https://digitalguardian.com/blog/what-hipaa-compliance

and policies, and include business associates within HIPAA regulations. However, few audits were performed to verify compliance to the 2013 changes until 2016 changes to auditing policies by the Office for Civil Rights. Lack of enforcement resulted in many organizations failing to make changes to meet the new requirements, so Omnibus rule revisions are still in the process of being implemented.[19]

Other Relevant Regulations

CSO Online provides news analysis, and research on a broad range of security and risk management. They published The security laws, regulations and guidelines directory which covers the basics of broadly applicable laws and regulations, industry-specific guidelines and requirements, key state laws, and international laws to which American companies must be compliant. This directory is a useful resource for exploring the range of regulations to which companies in various industries must be compliant.

Another useful resource for identifying cybersecurity compliance requirements is this 2014 report by the Congressional Research Service Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation.

[19] Help Net Security. 2016. *Is your business still HIPAA compliant after the 2016 federal changes?* Accessed on 10/18/2016 https://www.helpnetsecurity.com/2016/07/26/hipaa-complaint-2016-federal-changes/

US Industry Leaders

HIPAA Compliance Business Software

HIPAA compliance is required by any entity which has access to patient information.[20] Many companies have been attracted by this broad market, and have developed HIPAA compliance products.

A search of Capterra, a list of business software solutions, retrieved 85 HIPAA compliant products. The largest, top-rated HIPAA compliance product as identified by this search are:[21]

Qualio QMS for Life Sciences is a quality management solution that helps life sciences companies reduce the risk of FDA and other regulatory non-compliance. Medical device and pharmaceutical companies use Qualio QMS to create policies, procedures and other controlled content; integrate training with document workflows; and reduce the risk of non-compliance with powerful reporting tools.

LogicGate is a governance, risk, and compliance focused workflow engine that automates complex processes unique to legal, regulatory, and compliance pressures. Drag and drop to build complex business process workflows. With LogicGate users can define rules and logic at each step that drive their GRC processes, escalating issues and approvals to the right person, on time.

Field iD is a leading EHS and HSE safety compliance management solution for the web and mobile devices operating on Google Android and Apple iOS. The easy to use, cloud-based software has revolutionized the way companies manage safety compliance and create safer workplaces. Field iD is fully customizable to a client's specific safety needs.

Paradigm 3 Quality and Document Control Software provides users with the systems you need to manage the challenges of their compliance system. These systems include, full document control, a complete competency and training module, risk analysis, audit scheduling and reporting, management of CAPA's, customer complaints, calibrations and asset management and more. Targeted action items are sent to applicable personnel and progress tracked ensuring that all facets of a user's system are under control.

DynamicPolicy is an application to manage corporate policies, procedures, and compliance related documents. Distribute and assign policy documents with ease. Includes version control, reports, read and acknowledge documents, audit trails and more.

PolicyTech by NAVEX Global is an easy and efficient way to create, review, and approve all of your documents for compliance needs.

HIPAA One platform helps anyone who has contact with electronic medical records increase the security and privacy of those records.

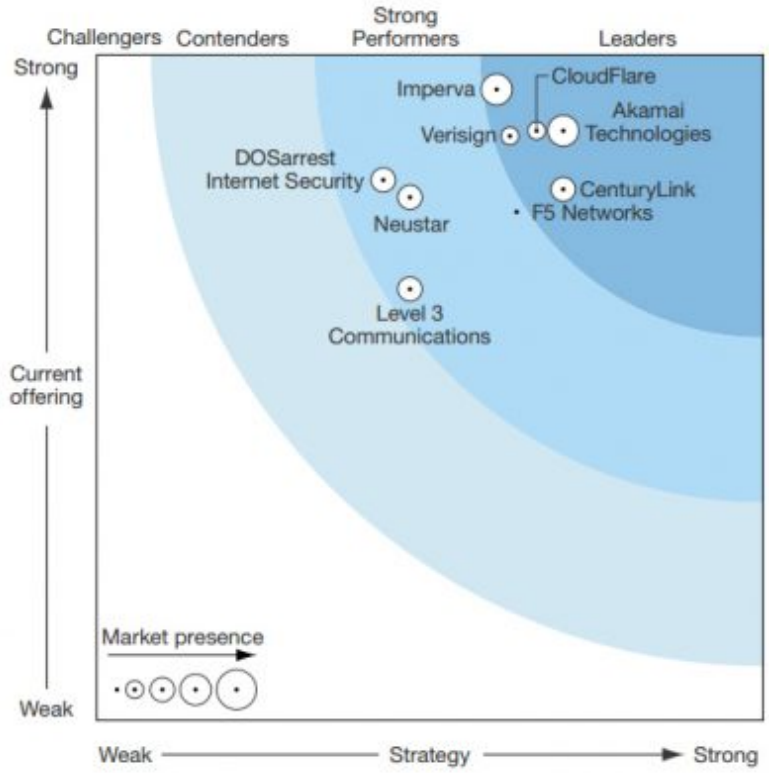
Onspring is a user-friendly, process automation platform puts you in control of your compliance. Easy setup & amp; fully customizable.

[20] Digital Guardian. 2015. *What is HIPAA Compliance?* Accessed on 10/13/2016 https://digitalguardian.com/blog/what-hipaa-compliance
[21] Capterra. 2016. *Top Compliance Software Products.* Accessed on 10/24/2016 http://www.capterra.com/compliance-software/?utf8=%E2%9C%93&review_stars%5B%5D=4&users=64&feature%5B8%5D=18200&commit=Filter+Results

DDoS Protection Service Providers

The number of DDoS protection service providers has risen in response to the increasing number of DDoS attacks. Vendors in this market share core similarities, but differ in response tactics and in types of protected network protocols. Additionally, quality of service varies, based on a number of factors. The following graph by Forrester Wave identifies providers which are best able to protect their customers' businesses based on their 36 criteria evaluation.[22]

FIGURE 6 Forrester Wave™: DDoS Services Providers, Q3 '15



Source: Global Dots. *DDoS – Distributed Denial of Service Explained*. Accessed on 10/20/2016

The names and descriptions of those, and other industry leaders who have operations in the US have been retrieved from Global Dots:

> **Akamai** prides on a global DDoS mitigation network, comprised of six scrubbing centers located strategically around the world to protect Internet-facing infrastructures against all known types of DDoS attacks at the network, transport and application layers. Their DDoS filtering techniques, advanced routing, and anti-DoS hardware devices remove DDoS traffic close to the source of the botnet activity. For non-routed DDoS protection, as well as DNS protection, their 175,000 servers and 1,300 network locations in more than 100 countries claim to maintain website availability and performance during DDoS attacks. Akamai has successfully mitigated some of the world's largest and most sophisticated DDoS attacks and has been active in this field since 2003.

[22] Global Dots. 2016. *DDoS – Distributed Denial of Service Explained.* Accessed on 10/21/2016 http://www.globaldots.com/ddos-distributed-denial-service-explained/

CloudFlare's advanced DDoS protection, a service at the network edge, can be used to mitigate DDoS attacks of all forms and sizes including those that target the UDP and ICMP protocols, as well as SYN/ACK, DNS amplification and Layer 7 (application layer) attacks. CloudFlare offers the documentation that explains the anatomy of each attack method and how their network is designed to protect your web presence from threats. However, not even CloudFlare was always completely immune to attacks. In 2013, they have suffered a hit, while they were defending Spamhaus, an anti-spam organization, against the attack that peaked at 300 Gbps and was one of the largest DDoS attacks recorded at the time. CloudFlare reckons 30,000 unique DNS resolvers have been involved in the attack against Spamhaus.

Imperva Incapsula service delivers a multi-faceted approach to DDoS defense, providing blanket protection from DDoS attacks to shield critical online assets. *The Incapsula Website DDoS Protection* solution is an always-on, cloud-based DDoS defense service that automatically detects and mitigates DDoS attacks launched at websites and Web applications. This DDoS protection service is built on top of the Incapsula Content Delivery Network (CDN) and leverages a PCI DSS compliant Web Application Firewall technology. Imperva also offers *Infrastructure Protection*, an on-demand security service that safeguards critical network infrastructure from volumetric and protocol-based DDoS attacks. Finally, *Imperva Incapsula Name Server DDoS Protection* service safeguards DNS servers from DDoS attacks. Deployed as an always-on service, it automatically identifies and blocks attacks seeking to target DNS servers, while also accelerating DNS responses.

DOSarrest is a cloud based DDoS technology service that since its inception in 2007, has developed, implemented and real world tested a wide range of proprietary methods and techniques to stop DDoS attacks. They do not (as it says on their website) rely on purpose built DDoS mitigation devices to stop all attacks. Their experience has taught them that no single DDoS mitigation device can stop all varieties of DDoS attacks in existence today.

F5 Networks, Inc. is a multinational American company that specializes in application delivery networking (ADN) technology that optimizes the delivery of network-based applications and the security, performance, availability of servers, data storage devices, and other network resources. F5 is headquartered in Seattle, Washington, and has development, manufacturing, and sales/marketing offices worldwide. F5 originally manufactured and sold some of the industry's first load balancing products. In 2010 and 2011, F5 Networks was on Fortune's list of 100 Fastest-Growing Companies worldwide. The company was also rated one of the top ten best-performing stocks by S&P 500 in 2010.

Level 3 Communications is an American multinational telecommunications and Internet service provider company headquartered in Colorado. It operates a Tier 1 network. The company provides core transport, IP, voice, video, and content delivery for medium-to-large Internet carriers in North America, Latin America, Europe, and selected cities in Asia.bLevel 3 is also the largest competitive local exchange carrier (CLEC) and the 3rd largest provider of fiber optic internet access (based on coverage area) in the United States. Currently, Level 3 has over 13500 employees.

Verisign, Inc. is an American company based in Reston, Virginia, United States that operates a diverse array of network infrastructure, including two of the Internet's thirteen root nameservers, the authoritative registry for the .com, .net, and .name generic top-level domains and the .cc and .tv country-code top-level domains, and the back-end systems for the .jobs, .gov, and .edu top-level domains. Verisign also offers a range of security services, including managed DNS, distributed denial-of-service (DDoS) attack mitigation and cyber-threat reporting.

aiScaler Ltd. is a multinational software company founded in 2008. It develops application delivery controllers designed to allow dynamic web pages to scale content by intelligently caching frequently requested content. aiScaler can be implemented at the customers' datacenter, in a hosted environment, or through a CDN. The company maintains offices in the United States, Europe and China. They are currently stationed in Dublin.

Arbor Networks is a software company founded in 2000 and based in Burlington, Massachusetts, United States, which sells network security and network monitoring software, used – according to the company's claims – by over 90% of all Internet service providers. The company's products are used to protect networks from denial-of-service attacks, botnets, computer worms, and efforts to disable network routers.

Nexusguard as a longtime leader in DDoS defense is at the forefront of the fight against malicious Internet attacks, protecting organizations worldwide from threats to their websites, services, and reputations. Continually evolving to face new threats as they emerge, they have the tools, insight, and know-how to protect their clients' vital business systems no matter what comes their way.

Neustar, Inc. is an American technology company that provides real-time information and analytics for the Internet, telecommunications, entertainment, and marketing industries, and a provider of clearinghouse and directory services to the global communications and Internet industries. Neustar is domain name registry for .biz, .us (on behalf of United States Department of Commerce), .co, and .nyc top-level domains.

Radware is an Israeli provider of integrated application delivery / load balancing and application & network security solutions for virtual and cloud data centers. It has regional headquarters in the U.S. in Mahwah, New Jersey, Asia Pacific headquarters in Shanghai, China and its international corporate headquarters are located in Tel Aviv, Israel. Radware has over 10,000 enterprise and carrier customers worldwide. Radware is a member of the Rad Group of companies and its shares are traded on NASDAQ.

Zenedge, unlike other Web Application Security solutions in the market, leverages patent-pending deep machine-learning capabilities to detect anomalies, dynamically alter security postures, and initiate auto-mitigation and automatic routing with minimal to zero human intervention. This allows the company to provide better cybersecurity and faster time to mitigation than traditional Cloud and on-premise cybersecurity vendors.

Staminus, founded in 1998, provides industry-leading DDoS mitigation services to users and companies around the globe, with over 15 million IPs protected. As one of the most experienced DDoS mitigation firms in the industry, Staminus has evolved into the world's most advanced and intuitive DDoS mitigation company.

Appendix: The Cyber Security Cluster in NovaScotia

Nova Scotia has many advantages that attract a growing cluster of companies with strategic interests in cyber security.

AN ESTABLISHED ECO-SYSTEM

A growing number of companies such as **Track Group Analytics**, **Ping Identity**, and **BeyondTrust** are working in this sector to undertake R&D activities, outsourcing services, and offer cyber security as a service. The military's east coast intelligence centre is located in Halifax. A wide range of expertise translates into a full ecosystem.

A NATURAL FIT

Nova Scotia's complementary economic clusters show that Cyber Security has become a natural extension of the expertise being built here.

- **Aerospace & Defence:** Nova Scotia is a hub for aerospace and defence activities.
- With close to 15,000 people employed by the Department of National Defence and another 3,000 in the private sector, the expertise here has attracted globally-recognized companies including **Lockheed Martin**, **General Dynamics**, **IMP Aerospace & Defence**, and **Pratt & Whitney**.
- **ICT & Big Data**: Nova Scotia ranks #1 in Canada for operating costs in software development, which has attracted companies like **Salesforce** to join a growing cluster of Software as a Service firms. Nova Scotia has also been recognized by top companies such as **IBM** as a **Centre of Excellence for Big Data** and **Data Analytics**.
- **Financial Services:** Nova Scotia has among the highest ratios of educational facilities and educated workforce to population in the North America. Close to 70% of the workforce has

  post-secondary certification in Halifax - with many schools offering specialized programming - a factor that helped attract top firms such as **Citco**, **Mitsubishi UFJ,** and **Maitland Fund Services**.

ROBUST WORKFORCE

Nova Scotia has the highest concentration of graduates with ICT degrees in Canada and our ICT cluster actively employs 20,000 people - a growing number.

SUPPORTIVE INDUSTRY

The ICT industry in Nova Scotia is thriving and supported by **Digital Nova Scotia**, the province's industry association for information technology.

Halifax is home to two annual conferences related to Cyber Security - the **Halifax International Security Forum** and the **Atlantic Security Forum**. With the completion of our new Convention Centre -the Nova Centre - Halifax will continue to host internationally recognized conferences, bringing potential customers, suppliers, and partners right to your doorstep.

ACADEMIC SUPPORT

With **10 universities** and **13 community college campuses**, the province has among the highest ratios of educational facilities and workforce to population in North America. Our universities enroll students from over 100 countries around the world.

Cyber security related courses are offered at 6 out of the province's 10 universities, enhancing computer science programs offered across the province.

Examples of Academic Programming

DALHOUSIE UNIVERSITY

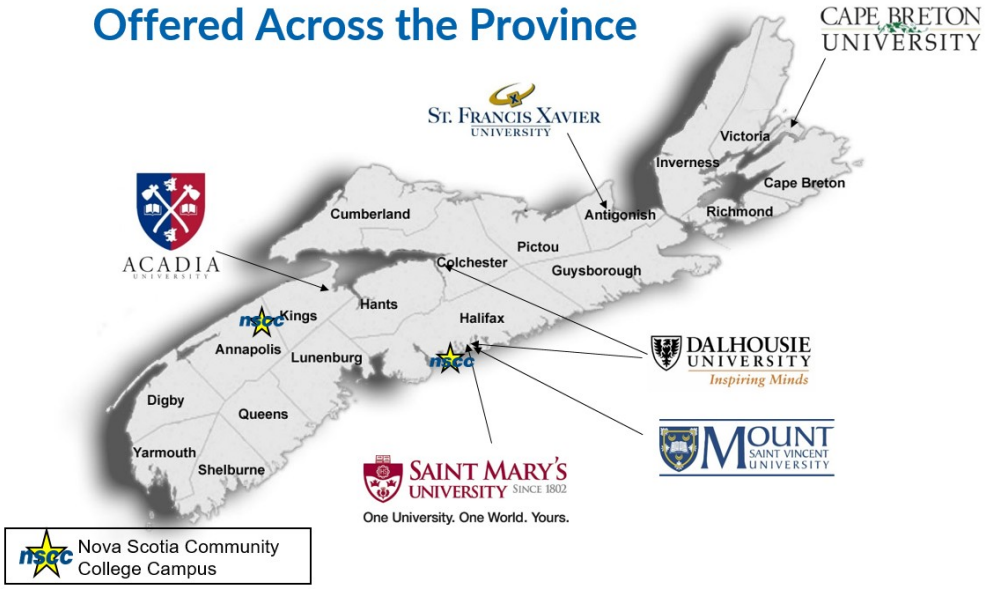
Dalhousie University offers a unique **Communication Technologies and Cyber Security** specialization through its Computer Science program, ensuring top talent is consistently produced.

Dalhousie University is home to the Cisco Network Security Teaching Lab and **Network Information Management and Security Group** and an **Internetworking Faculty of Engineering**, **offering a broad range of expertise and research abilities**, accessible through an Industry Liaison Office.

nscc

Nova Scotia Community College (NSCC) offers an Information Technology Diploma and its programing concentration focuses on network security as a key feature. This program is currently offered at two different campuses in the province, educating students across the province of the opportunities available in cyber security.

Nova Scotia: Cyber Security Education Offered Across the Province



Cyber Security education offered at 6 universities and 2 NSCC campuses across the province.

n | s | b | i
Nova Scotia Business Inc.

1800 Argyle Street, Suite 701
Halifax, Nova Scotia
Canada B3J 3N8

E-mail: info@nsbi.ca
www.novascotiabusiness.com

Tel: 1.902.424.6650
Fax: 1.902.424.5739

Toll-free in Nova Scotia
1.877.297.2124

Toll-free in North America
1.800.260.6682 (NOVA)

Join the conversation: