Genesis Grant

Bristol Myers Squibb

CTEC 345 Final Project Report

Bristol-Myers Squibb is a global company who focuses on the discovery and research, manufacturing, distribution and sale of biopharmaceutical products. The four main components of the business are pharmaceuticals, consumer products, medical devices, and nutritional products. They were founded in New York, New York in 1887 and currently have over 20,850 employees. They have offices and research centers internationally - including locations in NY, China, WA, NJ, MA, FL, Puerto Rico, Canada, Belgium, Japan, etc. These independently may operate with 1+ of these purposes: research and development, manufacturing or corporate/HQ responsibilities. The company corporate headquarters is located in Lawrenceville, NJ and the European headquarters Uxbridge, UK. Some popular brand names owned by them include Clairol a hair care company, Excedrin a migraine medication and a partnership with Pfizer.

To illustrate the company’s network, a WAN hub and spoke topology is used. The hub will be the core routers (located in NJ to represent US headquarters and UK to represent European headquarters) and spokes (edge routers) in 5 different areas to equally represent each purpose; New Jersey (HQ), UK (HQ), WA (Research and development), China (manufacturing), and Arizona (manufacturing). A WAN would be most beneficial as our company is global spreading over thousands of miles, thus needed multiple LAN’s in varying areas. The hub and spoke would be the best type of WAN because it allows for connection to all the LAN’s through the core routers to each LAN, providing a centralized control, cost efficient and smoother flow of traffic as connections with the simplified network design.

**IDENTIFY:**

ID-AM1 & ID.AM54 : The network devices used within for the company network are 2 clouds to represent ISP internet, 2 edge routers for the US and European networks, 5 edge routers for each LAN (AZ, WA, NJ, UK and China) and switches to each router to connect to end devices including 2 multilayer switches at each of the headquarters. These multilayer switches provide a layer of security, as it allows for segmentation and better traffic performance which works best for the headquarters as they store more information, employees, client and business information as well as will have more internet traffic. Wireless routers as well are available for the tablets used in manufacturing.

The endpoint devices used are:

Computers: To allow for employee day to day work. One computer is stationed in each LAN to represent the population computers.

Servers:

Backup Servers: in case of failure backup servers are available for rebooting an managing any lost data.

Email/Website server: database of employee and partnership emails and website information.

Proxy Server: Supposed to be stationed before switches but configuration would not allow. This will act as a tunnel for internet access in order to hide and allow for seamless and safe internet access and uploading of vital information.

Data Storage Server: Utilized to store pharmaceutical recipes, ingredients, history, and past and ongoing research. This will also store partnership deals and developments and any vital information within those collaborations.

Client Information Server: Utilized to store client information regarding sales to distributors, what companies utilize which products, partnerships, etc.

Inventory Servers: Positioned only in manufacturing locations, used to keep track of day to day products.

IP Phone: Only put in HQ in order to allow communication from important partners, other locations, used primarily for priority uses for corporate purposes.

Tablets: Positioned only in warehouse/manufacturing locations in order to illustrate tablets used by employees to keep work activities going including inventory, manufacturing processes, data tracking, etc.

ID.AM6 : The ISP will provide the internet connection and core routers for the company, other devices including but not limited to end devices (computers, ip phones, servers, etc.), edge routers, switches and multilayer switches the company will provide in order to run their network. Employees will be advised what to do with work stations including limitations and abilities that comes with them.

ID.RA1 & ID.RA2: Based on past instances researched through informational and databases such as the New York Times, UpGuard, Console and Associates P.C., etc. potential vulnerabilities to the network include: insider threats, third party risks, and single point of failure regarding the hub and spoke topology. Insider threats may come from a disgruntled employee with high levels of access to vital information possibly in the research and development locations and/or HQ locations. These threats are easily able to retrieve information like pharmaceutical recipes, network application login and internal sources, data servers, etc and if revealed to public can lead to putting business reputation at risk and public hysteria. Third party risks include the utilization of third party entities and their own vulnerabilities leading to adversaries gaining vital access to company entities, applications and data. This can include third party applications use to upload and organize client information, backups, employee logins, etc. Single point of failure pertains to the ISP. If the ISP goes down then the entire system would go down and a recovery plan would need to be set in place beforehand. Thus a backup server within each HQ in our topology is implemented.

ID.RA4 & ID.RA5:

Insider threats: High Risk - dependent on level of access the employee, visitor, insider, etc. has will determine what information they will be able to expose. It is better to expect worst then to underestimate risk.

Third Party Risks: High Risk – using past instances where client information (SSN, names, address, etc.) has been exposed. This includes third party applications where client information is stored, pharmaceutical components, company and partnership critical information etc. The risk and damage of these being exposed could be detrimental to company.

Single Point of Failure: Significant Risk – single point of failure would lead to network being down but the company currently does not critical work where they would need to be up and running 24/7 in order for clients to do significant day to day tasks. Downtime would hinder employee work but once up tasks will continue. Also if using a reliable ISP then downtime should not be long and if reliable they will be able to assist company in what to do if situation were to arise.

ID.RM2 & ID.RM3: Bristol Myers would deploy a successful risk management strategy by implementing qualitative and quantitative assessments, focusing on areas with higher priorities and risk tolerances and implementing more secure tools for layers that require higher classification. This will help the company as well allocate resources, software, funds, etc. to areas that require more security.

**PROTECT:**

PR.AC1 & PR.AC4: In order to log into work everyday every employee must login via a third party software (Zscalar, Cisco Duo, etc.) or internal database to authenticate who they are. Based on this authentication then employees will be granted access and privileges will be determined. A network ACL will keep track of privileges and network access traffic.

PR.AC2: To protect physical assets, each location will be equipped with video surveillance (cameras) on the outside perimeter of each location as well as indoors in hallways to manage who is seen going into which departments, building rooms, etc. As well, guests will have to sign in with front desk to keep track of who has accessed buildings within each of the 5 locations. In the US HQ and International HQ employees will carry around badges in order to badge allowing only authorized users dependent on level of security clearance to gain access into certain areas to prevent any unauthorized personnel.

PR.AC3: Utilizing a VPN and zero-trust software, remote workers can login to an application (in this instance Zscalar) utilizing their company given laptops, computers, set up, etc. Every 24 hours they will be required to be reauthenticated. In order to login to Zscalar and gain any access into internal sites, they must provide multifactor authentication including but not limited to a unique authorization pin, employee login, employee personal pin, etc. Firewalls embedded into software will prevent authorized users from accessing websites that may be deemed potentially dangerous or unreliable to prevent adversaries from gaining access to internal sources from deep/ dark web sites. Implementing a VPN will allow for safe and secure access of the internet without worrying of any eavesdropping or impersonations.

**DETECT:**

DE.AE1, DE.CM1, DE.CM7, DE.CM8 DE.CM3 & DE.AE2: In order to manage traffic flow, the company would need to utilize a network traffic monitoring software and overtime keep track of data captured and ultimately create a baseline. This can include bandwidth activity, accounts, endpoint device communications, etc. Dependent on level of significance (ie. Server that houses client information or pharmaceutical ingredients versus manufacturing inventory) the amount of information collected will vary to take into account data storage costs and storage availability. Areas where traffic is high and information stored there is significant will be monitored and secured more thoroughly as needed. Utilizing endpoint detection tools individual users with suspicious activity can also be flagged and monitored in order to watch and possibly prevent any anomalies, it will also help the company analyze if there is only an individual issue or if the issue is more widespread and will call for a more robust solution.

DE.DP1,2,3,4,5: In order to maintain robust protection and detection of any adversarial activities Bristol Myers can implement Red team penetration testing. As new vulnerabilities need new defenses, deployment of red teams will allow for any overlooked vulnerabilities to be exposed in testing rather than in real time, and allow the company time to build stronger defenses. This will allow for further protection of critical information like pharmaceutical products being exposed from a possible vulnerability from something as simple as an exploitation in a website or email account. Furthermore, implementing consistent monitoring within budget would help the company keep track of any anomaly. And finally, educating employees, corporate, partnerships and clients of phishing, giving out critical information, inconsistencies in emails, texts, calls, links, etc. and what to do will benefit both the company and those involved as all will be more knowledgeable and prevent any issues due to personal negligence.

**RESPOND:**

RS.RP1: After the event or possibility of an successful adversary attack, the company will analyze the affected devices/ part of the network and back track how the adversary was able to gain access, any tools that had vulnerabilities, etc. From this analysis the company will then be able to come up with a solution. For Bristol Myers, the information they harbor (pharmaceutical ingredients, client information, partnership details) is the most critical layer. Thus they would implement stricter authentication and authorization access within those networks, update malware and antivirus software, and encrypt significant files with only administrative access able to gain access. Security configurations could also be adjusted depending on level of criticality.

**RECOVER:**

RC.IM1 & RC.IM2: Specifically recalling a past instance in which a third party risk exposed the vital information of hundreds of clients, the lessons learned forced Bristol Myers to educate clients in what to do if their information was compromised. Although their core intelligence was not affected, it forced the company to educate both clients and employees, launch an emergency patch to resolve the issue and reflect.

The recovery plan in the instance a failure were to happen would be to launch a patch, analyze the vulnerability and educate those involved further. Backup servers within the network are also available in the event that any vital information were to be lost and network needed vital information up. The company will also further implement security strategies base on past instances in order to provide another layer of protection. This includes updating antivirus and malware software. Then after recovering and the company can run Penetration test in order to thoroughly see if there is any overlooked vulnerabilities within the network. Utilizing someone/ a group outside of the company would be beneficial as it would simulate a real attack and further gain any vital information.

A computer screen shot of a network

Description automatically generated

SOURCES:

*Bristol Myers Squibb Informs Employees of Leaked SSNs Following MOVEit Data Breach*. (n.d.). JD Supra. https://www.jdsupra.com/legalnews/bristol-myers-squibb-informs-employees-7692011/

*Bristol-Myers Squibb Co Locations - Headquarters & Offices - GlobalData*. (n.d.). https://www.globaldata.com/company-profile/bristol-myers-squibb-co/locations/

PricewaterhouseCoopers. (n.d.). *Cybersecurity risks from third party vendors*. PwC. https://www.pwc.com/us/en/services/trust-solutions/digital-assurance-transparency/vendor-cybersecurity-risk.html

SecurityScorecard. (2023, October 5). *Qualitative vs. Quantitative Cybersecurity Risk Assessment | SecurityScorecard*. https://securityscorecard.com/blog/qualitative-vs-quantitative-risk-assessment/#:~:text=Performing%20qualitative%20risk%20analysis%20is,and%20can%20be%20prohibitively%20expensive.

*The Bristol-Myers Squibb-Pfizer Alliance is pleased with the U.S. District Court decision to uphold both the composition of matter (COM) patent (US 6,967,208) and formulation patent (US 9,326,945) covering Eliquis®.* (n.d.). https://news.bms.com/news/details/2020/The-Bristol-Myers-Squibb-Pfizer-Alliance-is-pleased-with-the-U.S.-District-Court-decision-to-uphold-both-the-composition-of-matter-COM-patent-US-6967208-and-formulation-patent-US-9326945-covering-Eliquis/default.aspx

*What is a VPN? Why Should I Use a VPN? | Microsoft Azure*. (n.d.). https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn/#vpnprotection

*What is Zero Trust?  | IBM*. (n.d.). https://www.ibm.com/topics/zero-trust

*Worldwide Locations - Bristol Myers Squibb*. (n.d.). https://www.bms.com/about-us/our-company/worldwide-facilities.html

Zscaler. (n.d.). *7 elements of Highly successful Zero Trust architecture | Video - ZScaler* [Video]. Zscaler. https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust

PricewaterhouseCoopers. (n.d.). *Cybersecurity risks from third party vendors*. PwC. https://www.pwc.com/us/en/services/trust-solutions/digital-assurance-transparency/vendor-cybersecurity-risk.html