NAME : AARON MASCARENHAS

HND UNIT 5 - SECURITY

**RISK APPLICATIONS**

**Assess risks to IT Security**

****

horizontal line

# 

# Introduction

The report discusses about the types of security risks to organisations and also describes the organizational security procedures. It identify the potential impact to IT security of incorrect configuration of firewall policies and third-party VPNs and also shows examples for each, how implementing a DMZ, static IP and NAT in network can improve Network Security.

## Purpose

The purpose of this report is to discuss the risks involved in IT security and the precautions taken with evaluated technical notes to support specific statements and a guide to understand the security solutions t enhance the current security instructure.

## What is IT security risks -

## They are risks which can be affected by cyber attacks which mainly target systems, hardware , laptops, PC’s and personal data property. These are usually at risk by hackers as well as government organisations whose data are confidential to the public and are at security risk.

*IT security is a set of cyber security strategies that prevents unauthorized access to organizational assets such as computers, networks, and data. It maintains the integrity and confidentiality of sensitive information, blocking the access of sophisticated hackers.*

Cisco. (2018). *What Is IT Security? - Information Technology Security*. [online] Available at: https://www.cisco.com/c/en/us/products/security/what-is-it-security.html [Accessed 1 Dec. 2018].

## IT security risks involved with Saint Albans pharmaceutical -

* **Unauthorised access/use of a system (inc hacking) -**
* With unauthorised access of systems through which laptops with full disc encryption, firewall, antivirus, VPN and two factor authentication as well as Microsoft Active Directory which stores their credentials which can’t be bypassed. This is where hackers/scammers tend to go towards social engineering, people tend to fail into tras involving money and other offers which include rewards which require filling in important details. In the given scenario, it had not mentioned any contract involving the release of data by the employees, they might not even be apprehended for the incident. They may gain access by fake IDs badges to steal any valuable data from systems within the facility. **✓**
* **Unauthorised removal or copying of data or code from a system -**
* This is usually stealing private data from a system this includes files, social security numbers, personal staff data, organization expenses, profits and losses of the company can be at risk as well. Saint Albans security and privacy are well protected with advanced and excellent forces that can’t be bypassed by anyone. Phishing can be used to get along with the members of staff and collect data to gain access to the facility. They can have identical looking IDs and masking it to match the facilities description. It could also use this information as hostage against the member of the facility to hand in crucial data regarding the facility. This can be used to manipulate the R&D data, which could bring down the facility into losses, or they could sell the information on the blackmarket for their gain. **✓**
* **Damage to or destruction of physical system assets and environment -**
* These can be caused by terrorist attacks, Robbers, heists, intruders, who are against the organization or just want to bring down the company, these can be rivals companies, protestors, uprising groups. As the members of the facility work on laptops, it makes it much easier to steal and destroy the data if they are not backed-up online as Saint Albans clearly have implemented an infrastructure which is 100% in-house due to security and privacy concerns which can be destroyed once hijacked. The infiltrator must me well equipped with gadgets to get around the tight security in place which are designed to protect the facility from these types of attacks.**✓**
* **Damage to or destruction of data or code inside or outside the system -**
* Saint Albans have also used such techniques to keep their system secure the have full disc encryption, firewall, advanced antivirus, VPN and two factor authentication and Microsoft Active Directory to store their credentials but this is not always the case as, the system can be bypassed the server is by launching a DDoS attack, which is a Distributed Denial of Service attack which can overload the servers using small multiple hosts, which makes them unable to be operated and can’t be stopped at all measures and this causes delays in the facilities to further progress on their research and may corrupt their data if not backed up or saved online.**✓**
* **Naturally disasters/occurring risks -**
* The facility has only one data centre for their website and their R&D data, if there is unpredictable natural disasters such earthquakes, storms, cyclones, forest fires, heavy rainfalls, which can lead to destructions. Saint Albans company website is also housed in their data Centre which are protected with reinforces structures. This can lead to lost of data, if it is not backed up and will be destroyed permanently. They should split up their data centres so that there would be lesser loss, as there data centres would be backed up in different locations.**✓**

**Potential Treatments -**

* By increasing the security of the passwords by making the limit word limit larger with special symbols and characters. To decrease the possibility of brute force attacks for guessing the password we can also 128 bit encryption.
* As most members of the facility use portable laptops which may get stolen easily as compared to desktop PC as they are stationary and not easily portable.
* By using third party services like SAP the servers can be spread out, which can make it easier to be secure and easy to to work as well. If there is a natural occurrence in an area, where the servers might be located, not all the data servers might get harmed during a natural occurrence.
* Simple errors made by humans can be eliminated by making sure to log out after you’re done using the computer to avoid data leaks on an open network, which can be avoided. Not logging out in public areas can also be avoided where potential “Shoulder Surfing” can be take place with anyone noticing.
* The research data can also be backed up regularly in a completely off-grid location as to avoid and loss or damage of data during any disaster or theft.
* Trying to setup a fixed password system can increase security of the facility immensely, as it won’t cause any careless mistakes to occur.
* They company data centre is in-housed they can be easily attacked as they are located in a particular location. To avoid any attacker or disasters, relocating the servers into different areas and housing them separately can help them stay protected.

**✓**

**The Importance of organisational security procedures-**

* **Business continuance -**

“Make ‘business continuity’ ‘business as usual’ and imbed it into your management routines as decisions are made, instead of an afterthought check off the box exercise later.”  
Bobbie Garrett

No matter what the size of the business, similar principles will apply:

A senior person in the business should take ownership of the business continuity plan. The plan should be allocated the same importance in business planning as, for example quality management, cash flow or health and safety. The responsibility of managing the business continuity plan must be clearly established within the business and everyone should know the importance of the plan and who has overall responsibility. A small team of suitably qualified and/or experienced people should be assembled to review the business operations and itemise the key features and areas of operation. The scope of the work must be established. An organisation may already have, for example, adequate recovery plan for its IT system. Such a plan would however need to be included in the completed Business Continuity Plan. It is imperative that a business is able to respond to any type of emergency. A disaster or emergency situation is, by definition, unexpected. The business continuity plan should be prepared along the following principles:

* The plan should have a broad scope if it is to effectively address the many disaster scenarios that  
  could affect the company.
* It should not distinguish between a partial loss of service and a complete loss of services and  
  facilities. A “worst case scenario” should be the basis for developing the plan - destruction of the main or primary facility.
* Because the business continuity plan will be written based on the above assumptions, less critical  
  situations can be handled by using only the needed portions of the plan, with minor (if any) alterations required.

The following steps can be taken for business continuance:

**1. Risk Assessment -**

* **Risk Evaluation -**
* Identify critical business functions essential for continued service  
  or production.
* Determine the events that can adversely affect your company,  
  the damage that such events can cause and the controls needed  
  to prevent or minimise the effects of a loss potential.

**Business Impact Analysis -**

* Identify the impacts that result from disruption that can affect the company and the techniques that can be used to quantify and qualify such impacts.
* Prioritise critical business functions.

**2. Develop and Document Business Continuity Plan -**

* **Develop Recovery Strategy -**
* Determine and guide the selection of alternative recovery  
  operating strategies to be used to maintain the critical functions.
* **Document Plan -**
* Organise and document a written plan. Senior management  
  should review and approve the proposed plan.

**3. Test, Approve and Implement Business Continuity Plan -**

* **Test Plan -**
* Develop testing criteria and procedures. Coordinate, test, and evaluate the plan. Document all results.
* **Approve and Implement Plan -**
* Obtain senior management endorsement of plan.
* **Maintain Plan -**
* Develop processes to keep the plan up-to-date with reviews and tests completed at a maximum of 12-month intervals.
* Ensure the plan is in-line with the strategic direction of the company.

**✓**

* **Backup/restoration of data -**
* Always keeping backups is a vital step in every organization’s operation. In an unfortunate event where all the main servers are attacked by an external organization or are destroyed due to some natural occurrence, it is always wise to keep a backup so that all the vital lost data can be restored later.   
    
  The size of the backup depends a lot on the size of the organization. If the organization operate on really large-scale all its data has to be backed up, but it would exponentially increase the cost of operation. For the most part, only the most important is supposed to be backed up in most organization. In our scenario, as they only have one data centre and everything is home-based it is not really economical to backup everything. The most vital part would be their R&D data.

The different types of backups are:

1.Full normal backups: This is the kind of process backs up everything in the database to a server. It is also called mirror backup. In most cases, it is not feasible to carry out this kind of backup as it takes a lot of time and money.

2.Copy: In this only selected files and folders are backed up and archive attribute is not changed to allow other types of backup to be performed on the same data.

3.Incremental: In this only files that have changed since the last backup whether the backup was partly or fully.

4.Daily Occurrence: In this the files that changed since the last daily backup will be backed up accordingly.  
**✓**

* **Regular Security Audits -**
* A security audit is when the organization conducts systematic regular security checks and records all the flows to work on them. It includes diagnostics of all the IT services both hardware and software.
* “According to Ira Winkler, president of the Internet Security Advisor Group, security audits, vulnerability assessments, and penetration testing are the three main types of security diagnostics. Each of the three takes a different approach and may be best suited for a particular purpose.” (SearchCIO, 2005)
* Regular Security audits will help the company to look out for loopholes in their systems. It will always keep an eye on the IT services of the organization. In our scenario, as this is a home-based organization, they have to be on the lookout for potential security issues all the time. As they didn’t hire third-party companies to look after their security and firewall policies, they must conduct frequent audits.  
  **✓**

**Testing procedures on data, network and systems:**

The most basic type of security measure would be set passwords in place. Every step has to have authorization and authentication. As of network, there are various protocols set in every step of a network. There are a lot of firewalls that check for the authenticity of a packet in each step. In a firewall policy, we can control the ports of a network which are accessible by the internet. So we can essentially block unwanted traffic to the server. This can potentially block malicious content coming into the server.   
  
Data can also be protected if the user of the system is careful enough and has various anti-viruses and anti-malware installed on their laptop. This can prevent most of the junk from entering the system.   
  
Security measures can also be set in place of the databases so that unauthorised access can be prevented inside the organisation. For example, the marketing department shouldn’t need access to the R&D data, so they will be stripped from accessing that database.  
  
The most common type of security testing in every situation is penetration testing. This is when individuals or groups of hackers or crackers intentionally try to get into the system to find the loopholes in it for the intention of fixing it.  
  
There are also various methods of testing the softwares used by them. The developers can use unit testing scripts to test out any bugs in the software. There is also integration testing which, as the name suggests, tests out the integrity of the software.  
**✓**

**Types of organisational security testing procedures -**

* During security breaches, the firewall policies should be made more strict to reduce the traffic. All the ports should be closed and the ones that are open should be highly controlled. There can also be reduction in human errors by checking all the systems for vulnerabilities and disabling the systems which are a potential threats.
* We can carry out security audits to make sure nothing worse happens. These are just documentation of any potential threats and their potential solutions. It is used to inspect any internal threats that could happen in the near future.
* Penetration testing is also an option here as well. As mentioned before it is an individual or a group of professionals trying to break through the security of a system.
* The company can also seek help from various third party companies to test out their network and firewalls to keep them intact. They can also use network monitoring systems to make the communication more strict.  
  **✓**

**Impact to IT security for incorrect configurations of firewall policies -**

An example of an incorrect firewall configuration would be to open all the ports. This leads to injection of various kinds of packets into a server that is not meant to treat all that traffic and might end up getting a malicious software through the ports. Moreover, if all those ports are open, it is highly likely that someone might end up doing a DDoS attack as all kinds of traffic is allowed into the network. In our case, this might result in the stop of the functioning of the research that has been going on as all the data has been held on halt. This can only be stopped if the system is reset.

* **VPN security -**

A user may change an encryption algorithm to a valid security protocol which in turn may lead to a catastrophic decreation in the whole security system as this may be a lower encryption capacity which can easily be compromised. Therefore, some of the controls at there from the gateway which not only ensures security protocols which do not compare to VPN security.**✓**

There are two components of a corporate VPN: the remote access server (RAS) and the third party VPN client software. The off-site worker would first connect to the RAS over the internet, then the VPN client software establishes a connection between the RAS and the intranet of the corporation. It also ensures privacy across the whole session. This is how the workers using laptops connect to the intranet while on the road to access information on the go.**✓**

* **Security Breach -**

Potential security breach can take place if the user changes the VPN randomly using pre-shared key. Values are not usually unknown to the user, and in turn the client will not be able to gain access to the VPN connection. This will make the user to try and obtain a valid VPN configuration parameter to try and make the client work again. When and during this process security breaches may take place. For example, the key can be sent through email, or through any social media accounts, or through a phone conversation the key value could be heard. If the VPN client has different security relevant functions which include client firewall, then the situation can become even more worse. It can be critical by changing client firewall rules which are there to protect the access of the device which can lead to significant vulnerabilities.**✓**

* **Pre-configured VPN -**

This can usually be avoided by making available pre-configured VPN client which already comes with a locked down configuration. The VPN configuration lock will prevent any changes made by an unknown source. Fully controlling VPN clients ensures network administrator to make changes on the go or go back to default settings. The system will also make sure that there are identical and there are valid configurations assigned and transferred to the VPN clients, that can avoid mis-configuring VPN clients from the start.**✓**

Nowadays many companies use VPN to connect to the companies network and also gain access to the services and applications. Third party VPN can create a huge problems for companies as hackers can eavesdrop and gain access to the sensitive data of the company. By using VPNs, the hackers can gain easy access to the the routers and data as using VPNs for accessing data can open spots which the hackers can use for accessing the sensitive data of the company. As the Third party VPNs are managed an outside company and not the company’s VPN so there are mainly the case of the outside company managing the VPN rather that the company.**✓**

A Firewall setup is a great way of security for the company’s system. The Firewalls are called safe only if the Firewall policies are configured and correct and have to be checked twice before applying them to the systems of the company. If there are any mistake in the Firewall policy then there will be a chance that the important and sensitive data can be accessed by hackers and also the employees of the company can be in trouble as their data also can be accessed. Blocking the wrong port number from being accessed can cause a lot of trouble in the company as the employees may stop receiving emails and may disconnect from the internet. **✓**

* **Common Firewall Configuration Mistakes -**

Security threats increases as more as it becomes more and more advanced, as managing your firewall configurations has been considered very important, according to Gartner research, 95% of all firewall breaches are caused by misconfiguration, not flaws.**✓**

Firewalls are an essential part of your network security, and a misconfiguration firewall can damage your organisation and give easy access to an attacker. Yet misconfigurations are alarmingly common. Below are five of the most common types that misconfigurations, along with advice on how you can avoid them.**✓**

1. **Broad policy configurations -**

Firewalls are often set up with an open policy of allowing traffic from any source to any destination. This is because IT temas don’t know exactly what they need at the outset, and therefore start with broad rules and work backwards. However, the really is that due to time pressures or simply not regarding it as a priority, they never get round to defining firewall policies. This leaves the network in a perpetually exposed state. **✓**

Organizations should follow the principle of least privilege, that is giving the minimum level of privilege that the user or services needs to function normally, thereby limiting the potential damage caused by a breach. It’s also a good idea to regularly revisit your firewall policies to look at application usage trends and identify new applications being used trends and identify new applications being used on the network and what connectivity they require.**✓**

**2. Risky rouge services and management services -**

Services that are left running on the firewall that don’t need to be is another mistake i often find. Two of the main culprits are dynamic routing, which typically should not be enabled on security devices as best practice, and “rogue” DHCP servers on the network distributing IPs, which can potentially lead to available issues as a result of IP conflicts. I’m also surprised to see the number of devices that are still managed using unencrypted protocols like telnet, despite the protocol being over 20 years old.**✓**

The answer to this problem is hardening devices and ensuring that configurations are complaint before the device is put into a production setting. This is configuring your devices based on the function that you actually want them to fulfill and following the principle of least privileged access, you will improve security and reduce the chances of accidentally leaving a risky service running on your firewall.**✓**

**3. Non-standard authentication mechanisms -**

During my work, i often organisations that use routers that don’t follow the enterprise standard for authentication. For example, a large bank i worked with had all the devices in its primary data center controlled by a central authentication mechanism, but did not use the same mechanism at its remote office. By not enforcing corporate authentication standards, staff in the remote branch could access local accounts with weak passwords, and had a different limit on login failures before account lockout. **✓**

This scenario reduces security and creates more vectors for attackers, as it’s easier for them to access the corporate network via the remote office follow the same central authentication mechanism as the rest of the company.**✓**

**4. Test systems using production data -**

Companies tend to have good governance policies requiring that test systems should not connect to production systems and collect production data. But in practice, this is often not enforced because the people who are working in testing see production data as the most accurate way to test. The problem occurs because when you allow test systems to collect data from production, you’re likely to bring that data into an environment with a lower level of security. The data could be highly sensitive, So if you do use production data in a test environment, make sure that you use the correct security controls according to the classification of the data.**✓**

**5. Log outputs from security devices -**

The issue more often organizations not analyzing log outputs from their security devices or without enough granularity. This is one of the biggest mistakes you can make in terms of network security, not only will you not be altered when you’re under attack, but you’ll have little or no traceability when you’re investigating post-breach.**✓**

The excuse i often hear for not logging properly is that logging instructure is expensive, and hard to deploy, analyze, and maintain. However, the costs of being breach alerted or being able to trace the attack are surely far higher.

Enterprises need to look at the state of their firewall security and identify where holes might exist. By addressing these misconfiguration issues, organisations can quickly improve their overall security posture and dramatically reduce their risk of a breach.**✓**

**Implementing a Demilitarised Zone(DMZ), static IP and NAT in a network -**

* **Demilitarised Zones (DMZ) -**

By implementing DMZ the computers networked together with sensitive information. You don’t want someone hacking into them. They also do not need to be exposed directly to the internet. You also have computers that must be exposed to the internet to function. You essentially split. You essentially split your network up using one or more firewalls. So, requests from outside computers for web pages would be allowed in the DMZ, but not in the rest of the network. The same traffic would be partially or fully blocked elsewhere in the network.**✓**

* **Static IP -**

The benefits of using a static IP address is that computers can host servers using this type of address containing data which other computers can gain access to using the internet. It makes it easier to locate servers anywhere in the world.

The uses of static IP are :

* Access your PC from anywhere - A static IP makes it easier for you to remotely access your computer, so you can get hold of files, use programs, adjust your settings, and so on.
* Host a website - You'll need a static IP if you want to host your own website, rather than have someone else's server host it.  
  Run a server - Any kind of server needs a static IP, not just one that hosts a website. You may also want a server for gaming, a domain name, or FTP to send and receive files more reliably.
* Get direct emails - A static IP also lets you set up an email server, so you'll have more direct control over your email.
* Run CCTV - Want CCTV for your business? You'll need a static IP for that too.
* Make better VoIP calls - VoIP, or Voice over IP, is a way of making phone calls over the internet rather than through a phone line - Skype and Facetime are good examples. It's much more reliable when your IP is static. Read more about VoIP.  
  Enjoy less downtime - Whenever a dynamic IP refreshes, you run the risk of downtime. It's usually for a very short time, but if you're relying on a stable connection it can be havoc all the same.**✓**
* **NAT -**

It helps to reuse private IP addresses which are no longer needed. It also enhances the security of the private networks by keeping all the internal addresses private from the external network. It can also connect large numbers of hosts to a global internet using the same amount of public IP addresses, which saves IP address space.**✓**

Docs.microfocus.com. (2018). *What are the Benefits of NAT?*. [online] Available at: https://docs.microfocus.com/NNMi/10.30/Content/Administer/NNMi\_Deployment/Advanced\_Configurations/What\_are\_the\_Benefits\_of.htm [Accessed 2 Dec. 2018].

**Benefits to implementing network monitoring systems-**

* **Protecting your network against attackers.**
* Network monitoring systems are able to identify suspicious traffic, thereby empowering owners to act fast. A network monitoring service is able to provide a broad overview of an SMB's entire IT infrastructure, so that nothing is missed. Today, exploits are more sophisticated and advanced, and are able to target a system in a variety of ways. Monitoring antivirus and firewall solutions separately may leave security gaps.**✓**
* **Keeping informed without in-house staff.**
* A network monitoring service will send alerts and information to an SMB owner as issues arise. Otherwise, an SMB may need to either attempt to monitor their network security themselves or hire a full-time IT employee -- which could be very costly. Data breaches can be more damaging and more expensive the longer they go without being detected.**✓**
* **Optimizing and monitoring your network.**
* Many small business owners are aimed towards rapid growth. This growth cannot be possible if parts of their IT infrastructure are over-burdened or slowed. Network monitoring services will map out the infrastructure of a small business, showing an SMB owner areas of improvement and any issues that currently need to be addressed.**✓**
* **Remotely connecting to your infrastructure.**
* Network monitoring services are able to be accessed from anywhere in the world, allowing an SMB owner to still conduct business whether they are at home, at the office, or traveling abroad. This can be absolutely essential when you are working with a small amount of staff members or when you simply need to complete tasks on your own.
* A network monitoring service will be able to alert small business owners to any threats or data breaches, so that they can act swiftly to secure their own digital assets and to protect themselves and their customers. Small business owners are often the most vulnerable because they cannot dedicate the time or the resources to managing their own IT infrastructure; a network monitoring service will fill that gap and more.**✓**

**Forming IT security solutions by “trusted network” for Saint Albans Pharmaceuticals PLC -**

* **Questions that recognize security resources and obligations -**

Who is protected ?

* Employees, clients/customers, other facility occupants of Saint Alban Pharmaceuticals

What is protected ?

* Inventory, equipments, intellectual property/intelligence of Saint Alban Pharmaceuticals

What is the ultimate goal and what is the milestones towards reaching it ?

* Their ultimate goal is to sell and develop cutting edge medicines for Parkinson’s disease in a global market where few companies research and develop such conditions. Milestones towards reaching it is by having advanced high level security labs which tests new medicines on controlled environments and if successful then on humans under government approval and schemes.

When do they hope to reach to reach that goal and the respective milestones along the way ?

* At the moment the company is fairly small it has just a office in Saint Albans and factory within Wales, with 1000 staff and a turnover of £750m. Based on this situation it won’t take long enough to reach their goal and their milestone is to stay ahead of their competition.
* **Questions that Evaluate Present Security Realities -**

Where is the vulnerabilities ?

* According to my research and the given situation there are not many vulnerabilities found in their system. Everything is taken care of as to protect from rival companies and government which are after their R&D. These vulnerabilities can be taken care of by adding face detections before entering the vicinity, Keeping track of all the members who are within the company, implementing security checks and scanning before entering the company

How to address those vulnerabilities before they become serious security risks ?

* The vulnerabilities can be addressed by setting up network monitoring systems which help track and data or security breaches and automatically resolves them or specifically detected them so that the IT can focus more on critical problems related to the system.

What resources are there in terms of security equipment, staff training and security procedures - and how can it be improved upon those resources ?

* In terms of security equipments such as cameras, Swipe cards, biometrics. Staffs and many guards are ferried in on busses and in security procedures there are full data encryption, firewall, antivirus, VPN. These can be improved upon investing more on security and privacy by taking into consideration what needs to be protect and what is important to the company.

Which standards and compliance obligations are needed to be met and maintain where security is concerned ? What about installation, equipment and integration?

* Privacy, resources, confidentiality and security compliance obligations are needed to be met and maintained. Security is the number one priority taken care of by Saint Albans Pharmaceuticals hackers may bypass the system to steal data, this must be prevented data all costs by enhancing the strength of the system. Equipments have been installed and advanced high level security have been implemented and integrated into the system.

What happens if there is a failure to execute a security plan and maintain it over time ?

* These should also be a backup plan in case of an emergency where everything is camly taken care of in an orderly fashion without causing any confusion and delay and everything is done efficiently.There should be an emergency protocol that should be followed to ensure that things go smoothly and any problems occured should be resolved immediately without causing any damage to the property.

**An Adaptable Security Plan -**

To create a security plan, these answers to these questions need assessment must be followed in order to form a security plan. These questions must be re-visited by the company in the future as the business evolves and its assets increase. In the future there will be expansion and growth and which will impact all parts of the company and new vulnerabilities will begin to appear. This can be prevented by letting the professional security provider, which the company can acquire some knowledge about the assessment questions and how to make use of them to form a reliable security plan.

**Simmons, J. (2018). *Forming a Security Plan: Critical Business Questions to Ask*. [online] FE Moran Security. Available at: https://www.femoransecurity.com/forming-a-security-plan-critical-questions-to-ask/ [Accessed 4 Dec. 2018].**

### 

### Conclusion

A company is required to implement tools and techniques associated with identifying and assessing IT security risks together with the Organisational policies to protect business critical data and equipment. It also discusses about the issues of security risks as well as evaluation of new and proposed security solution to enhance the current security infrastructure. By ensuring that there is security and protection to the network and as the business booms and new threats may come into sight, technologies getting more and more advanced and complex to keep up, maintaining and regularly checking vulnerabilities to keep the security to its optimum performance so that there is no harm to the company.