DATA SECURITY

Companies & Sectors

Quote

"There are two types of companies: those that have been hacked and those who don't know they have been hacked."

John Chambers

CEO of Cisco

Companies and Sectors

All companies, regardless of size, can suffer a cyber security attack. They have a constant battle to keep data safe, whether it is business data or personal data.

Companies can be divided into three categories:

- **Small**
- **Medium**
- **Large**

Size of companies defined

Company Size	Number of employees	Annual Turnover
Small	Less than 50	Less than £6.5 million
Medium	Less than 250	Less than £12.9 million
Large	Over 250	Over £12.9 million

Cyber Security Challenges

The different sized companies will all face different cyber security challenges depending on the type of data they hold and the sector they operate in, but they all face, to an extent, the same challenges. These are:

- Data can be stolen, and sold or used illegally
- Data can be held to ransom
- Data can be manipulated and changed by hackers
- Computers can be taken over and used to conduct other attacks
- Websites can be taken offline

Small companies

Small companies may not have many expensive or ‘valuable’ data for a hacker to steal, but they do have user accounts that can be vulnerable to a ransomware attack.

In a small company, a hacker may lock all employees out of their accounts until a ransom is paid. This can quickly cost a small company thousands of pounds in lost sales, as staff are unable to access their sales data and customer contacts.

Other attacks that may occur are attacks on the company website.

The website can be taken offline, again costing thousands of pounds in lost revenue, as customers are unable to make purchases from the online store.

Small companies can be quite a soft target and more open to hacking attempts, as they may not have an expensive firewall and security suites to protect their small network or single computer account.

They will also most likely not have a dedicated security team responsible for security of the network and company data.

Small companies

One positive to take from being a small company is that, by having less of a public profile compared to medium and large companies, it may be considered a ‘less valuable’ target to hackers.

A summary of low cost, simple techniques that can improve cyber security within a small company can be found on the National Cyber Security Centre website.

Website: https://www.ncsc.gov.uk/collection/small-business-guide

Size of network and network traffic	Employees	Security resources	Public Profile
Small computer network. Fewer connections, much easier to protect.	Less than 50. Staff can be trained in good cyber practices. Easier to enforce IT policies and implement security.	Limited. Off-the-shelf resources.	Low. Safety in being obscure.

Challenges Summary: small companies

Medium companies

Medium companies are just as open to attacks as small ones.

A medium company may be spread over a larger geographical area, via different sites through a town or country.

The public profile of a medium company would be higher than that of a small, local company.

Therefore, it makes them more of a target.

They have enough employee accounts to make it possible for human error to go unnoticed, and this could leave the company at risk. Without proper cyber awareness training, employees may adopt weak passwords and have poor cyber security practice, leading to a data breach.

Medium companies, however, will have dedicated IT staff in place that would be responsible for maintaining the network and its security. However, they will not have a dedicated team of security professionals responsible for the overall cyber security of the company.

Size of network and network traffic	Employees	Security resources	Public Profile
Relatively large, can be spread out over several geographical areas.	As significant amount of staff. This Increases the risk associated with social engineering and poor cyber practices.	Moderate: Identifies what the most important aspect of the company that needs protected is. Money and resources would be put there, potentially leaving other parts less protected.	Significant to make them a target. Depending on the sector the company operates in, the more valuable a target they may appear.

Challenges Summary: medium companies

Large companies

Large companies such as Facebook, Amazon, Tesco, BT, etc. hold millions of account details for millions for people all over the world.

These companies are global and have a large public profile, so would be of great interest to hackers.

They have many employees and, therefore, many potential weak points in their cyber security.

Like with a medium company, staff must all be trained properly in cyber awareness, but this would be more difficult in a large company due to the number of staff required to be trained.

Large companies would have a dedicated team of cyber security experts to help prevent an attack.

They often employ an external agency that can provide ‘white hat’ hackers to conduct penetration tests on their systems, in order to help them identify weak points in their networks and apply patches once these have been discovered.

Size of network and network traffic	Employees	Security resources	Public Profile
Very large. Many devices connected across many locations. Difficult to protect so many devices, and monitor so many access points to company network.	Many employees. Employees from all over the world, in many different countries. Very difficult to maintain security and to enforce cyber security policy. Employ a dedicated team to look after security.	Very high level of sophisticated technology.	Very high. Makes it a target for hackers.

Challenges Summary: large companies

Watch

Click here to watch: Some of the biggest attacks on companies

Video URL: https://www.youtube.com/watch?v=i1ZyOk4La9Q

Also, try watching this cool video about 10 major cyber attacks:

https://www.youtube.com/watch?v=D2mxKEa2xmA