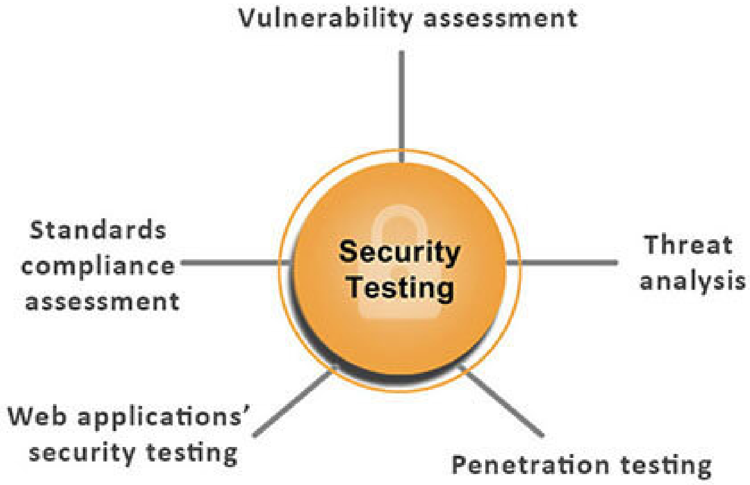
1B. Importance

The importance of security testing cannot be overstated, as **it helps to ensure that software is secure and can protect sensitive data and information from unauthorized access or misuse**.

One crucial benefit of security testing is that it protects against cyber-attacks which are becoming increasingly sophisticated.



Also, security testing helps you stay compliant with regulations. Depending on your industry and region, there may be specific regulations and standards that your software must meet.

Security testing can help ensure that the software meets these requirements, avoiding potential penalties or legal issues.

Security Vulnerabilities: Real Life Case Studies

Case Study 1: Microsoft

	Microsoft disclosed a vulnerability in January 2020, admitting that an internal customer support database that stored the company's anonymized user analytics got exposed online accidentally. This accidental server exposure resulted from misconfigured Azure security rules that Microsoft deployed on December 5, 2019. Microsoft expressed confidence that commercial cloud services were not exposed, and the company's engineers remediated the configuration quickly to prevent unauthorized access to the exposed database. Unfortunately, the 2020 data breach exposed IP addresses, email addresses, and other data stored in the support case analytics database.

Case Study 2: Ring Home

Ring is a home security and smart home company owned by Amazon. In recent years, the company has experienced two security incidents:

- Ring accidentally revealed user data to Google and Facebook via third-party trackers embedded into the company's android application.
- An IoT security breach allowed cybercriminals to successfully hack into several families' connected doorbells and home monitoring systems.

Cybercriminals used weak, default, and recycled credentials during the IoT breach to access live feeds from cameras around Ring customers' homes. They could also use the devices' integrated microphones and speakers to communicate remotely. More than thirty people in fifteen families reported that cybercriminals were verbally harassing them.

Case Study 3: Bangladesh Bank robbery

The Bangladesh Bank robbery, also known colloquially as the **Bangladesh Bank cyber heist**, was a theft that took place in February 2016.

Thirty-five fraudulent instructions were issued by security hackers via the SWIFT network to illegally transfer close to US$1 billion from the Federal Reserve Bank of New York account belonging to Bangladesh Bank, the central bank of Bangladesh.

Five of the thirty-five fraudulent instructions were successful in transferring US$101 million, with US$81 million traced to the Philippines and US$20 million to Sri Lanka.

The Federal Reserve Bank of New York blocked the remaining thirty transactions, [illegible] US$850 million, due to suspicions raised by [illegible] instruction.

As of 2018 only [illegible] illion of the US$81 million transferred to the Ph[illegible] been recovered, and all the money transferred [illegible] as since been recovered.

Most of the money transferred to the Philippines went to four personal accounts, held by single individuals, and not to companies or corporations.

Details: https://en.m.wikipedia.org/wiki/Bangladesh_Bank_robbery

Case Study 4: Bangladesh government takes down exposed citizens' data

The **Bangladeshi government** on July 9, 2023 took down citizens' sensitive data that it had left exposed online on July 7, 2023.

TechCrunch reported that a website belonging to the government of Bangladesh was leaking the personal information of the country's citizens, including full names, phone numbers, email addresses and national ID numbers.

At the time, we didn't disclose which website in particular was leaking because the data was still accessible. We can now report that the issue was with the Office of the Registrar General, Birth & Death Registration website.

Details: https://techcrunch.com/2023/07/10/bangladesh-government-takes-down-exposed-citizens-data/