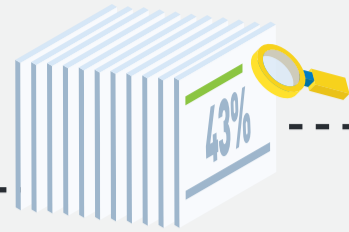


# Safeguard your critical information against data breaches



**One in three** SMEs experienced a ransomware attack in 2016<sup>i</sup>, and the reported cases spiked by almost 10 times from the previous year.



**43%** of security incidents reported to SingCERT by individuals and SMEs occurred through phishing attacks. Cyber criminals may attack SMEs as a means of getting to larger corporations, to which SMEs are suppliers.



Of the **1,750** website defacements reported, majority of the affected websites belonged to SMEs from a range of businesses, including interior design, logistics, manufacturing and construction.



About **21%** of those who had been hit by ransomware **had to cease all business operations immediately**, while **11% lost revenue** as a direct result of the attack.

## PDPA Amendments

### Mandatory Breach Notification Regime

Businesses to inform the affected customers and the Personal Data Protection Commission (PDPC) of a data breach that poses any risk of impact or harm, no later than 72 hours from the time it is aware of the data breach.

## Top 5 security best practices for SMEs

1

### Tighten password security

Best practices for password management include multi-factor authentication (e.g. Username and password with one-time PINs), log-in abuse detection system and regular audits to ensure that inactive accounts are denied access.

3

### Conduct regular tests and audits

With regular vulnerability assessments and penetration tests, you can identify and mitigate weaknesses in your systems and deploy the necessary solutions to remove the risk of data theft.

5

### Evaluate your security policies continually

Regularly review and refine your protection methods to ensure they stay relevant to your changing IT infrastructure, challenges and employee dynamics.

2

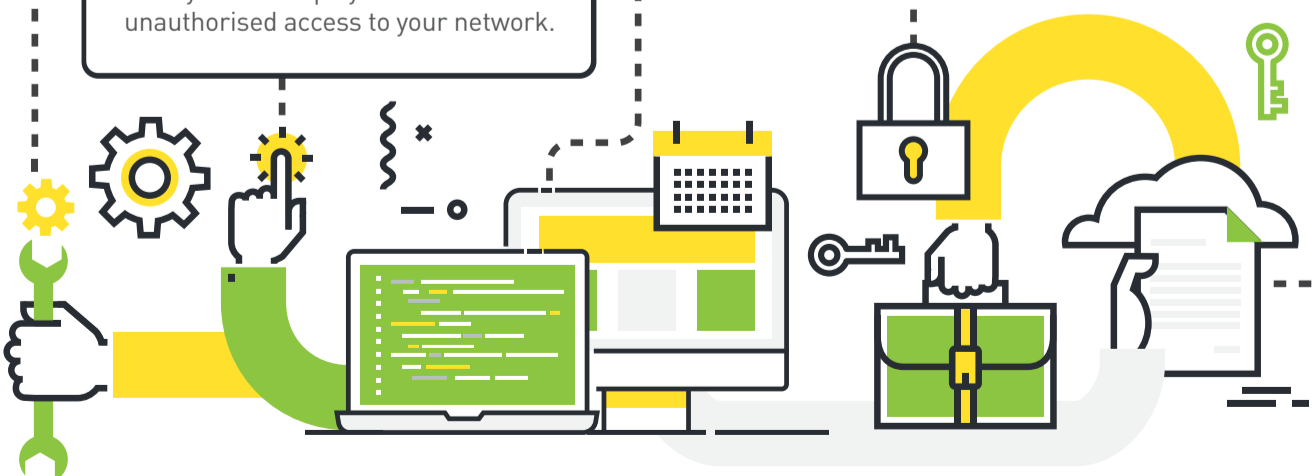
### Deploy the necessary security software

Regular updating of antivirus and anti-malware software in your servers and systems. Deploy firewalls to block unauthorised access to your network.

4

### Limit access to sensitive data

Control and restrict the access of your data only to those who need it and always monitor users with extended privileges.



<sup>i</sup> <http://www.businesstimes.com.sg/technology/a-third-of-singapore-smes-hit-by-ransomware-last-year-study>



1800 888 8888



[starhub.com/cybersecurity](http://starhub.com/cybersecurity)



[enterprise@starhub.com](mailto:enterprise@starhub.com)

StarHub