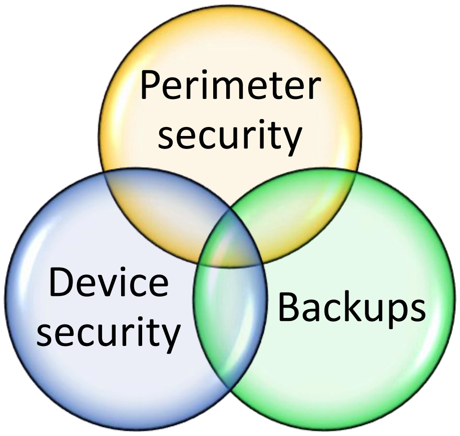
The IT Department
Be more competitive

Securing your business

SME IT security essentials

Do not be lulled into a false sense of security thinking that your small business is too small to be the target of cyber criminals. Cyber-crime is extremely lucrative and low risk for the perpetrators because of their remoteness and hands off tactics. Every business is exposed, from the largest to the smallest. It requires no effort from the cyber-criminal to level an attack against your business. In fact, they don’t even know your name when they are attacking your assets.

For the small business, securing business information assets is as important as for any other size business. However, without the economies of scale that their larger competitors enjoy, information security is often overlooked or under estimated. But it need not be.



The security essentials for the small business could be described as 3 focal areas.

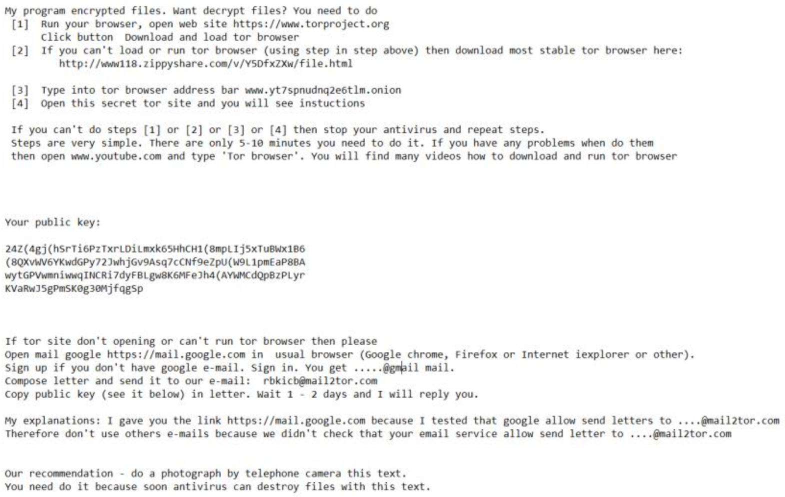
Perimeter security

Perimeter security refers to the bounds of your network. Typically a firewall is used on the network perimeter to protect the information of the business. Firewalls attempt to protect your network from inbound threats, and some advanced firewalls will also protect your business against loss by people transmitting sensitive or restricted documents to external recipients; that is from the inside out.

A decent firewall will allow for the filtering of traffic based on the source of the traffic, as well as the content of the traffic. Restricting browsing and internet usage based on group membership allows the business to optimize its internet bandwidth as well as increasing the productivity of its staff, on top of the obvious security benefits offered.

Keeping threats off the network and away from sensitive business information is critical. Threats posed to the business include the attack on devices resulting in reduced performance and in certain cases, a complete shut-down of services. In other cases threats include the probing of the environment to obtain entry onto the network. Once on the network, files and business information are targeted, either by infecting them, or by stealing copies of the information.

The newest and possible most severe threat faced in 2016 is Ransomware. Ransomware uses encryption technology to encrypt business documents. The encryption technology used is standard encryption technology used in business. The problem is that the documents cannot be decrypted without the matching cypher, or key. The ransomware criminals extort ransoms from businesses to have their documents decrypted. Often the cyphers are not provided even after the ransoms have been paid.



```
My program encrypted files. Want decrypt files? You need to do
 [1]  Run your browser, open web site https://www.torproject.org
      Click button  Download and load tor browser
 [2]  If you can't load or run tor browser (using step in step above) then download most stable tor browser here:
         http://www118.zippyshare.com/v/Y5DfxZXw/file.html

 [3]  Type into tor browser address bar www.yt7spnudnq2e6tlm.onion
 [4]  Open this secret tor site and you will see instuctions

 If you can't do steps [1] or [2] or [3] or [4] then stop your antivirus and repeat steps.
 Steps are very simple. There are only 5-10 minutes you need to do it. If you have any problems when do them
 then open www.youtube.com and type 'Tor browser'. You will find many videos how to download and run tor browser



Your public key:

24Z(4gj(hSrTi6PzTxrLDiLmxk65HhCH1(8mpLIj5xTuBWx1B6
(8QXvWV6YKwdGPy72JwhjGv9Asq7cCNf9eZpU(W9L1pmEaP8BA
wytGPVwmniwwqINCRi7dyFBLgw8K6MFeJh4(AYWMCdQpBzPLyr
KVaRwJ5gPmSK0g30MjfqgSp



If tor site don't opening or can't run tor browser then please
Open mail google https://mail.google.com in  usual browser (Google chrome, Firefox or Internet iexplorer or other).
Sign up if you don't have google e-mail. Sign in. You get .....@gmail mail.
Compose letter and send it to our e-mail:  rbkicb@mail2tor.com
Copy public key (see it below) in letter. Wait 1 - 2 days and I will reply you.

My explanations: I gave you the link https://mail.google.com because I tested that google allow send letters to ....@mail2tor.com
Therefore don't use others e-mails because we didn't check that your email service allow send letter to ....@mail2tor.com


Our recommendation - do a photograph by telephone camera this text.
You need do it because soon antivirus can destroy files with this text.
```

Advanced firewalls offer a degree of protection against Ransomware and are able to inspect inbound traffic in a ‘sandboxed’ environment before allowing traffic onto your business network and assets.

Device security

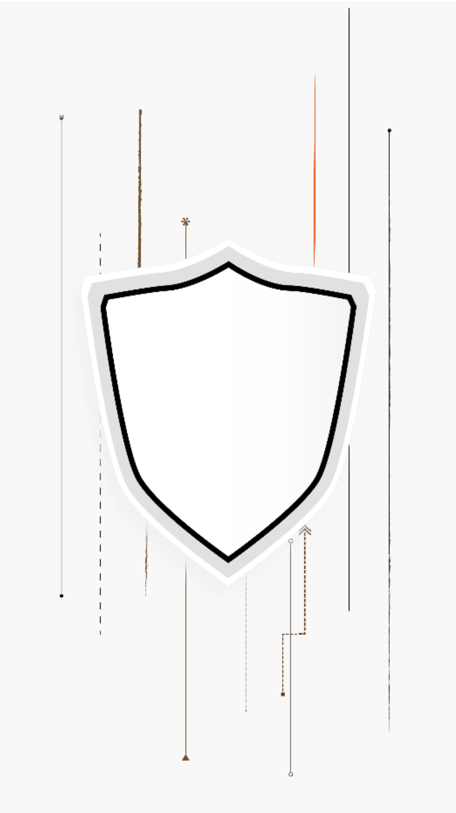
Computer security updates

Microsoft release security updates on the 2nd Tuesday of every month. These updates secure Windows computers by addressing vulnerabilities discovered in the operating system.

Microsoft public security bulletin notifications that help keep your computing environment up to date. These notifications cover:

- basic alerts,
- comprehensive alerts,
- security advisory alerts and
- security response center blog alerts.

Windows machines are able to automatically receive security updates, making keeping machines secure simple. In order to ensure that machines are up to date, and that the updates are being applied, a certain degree of management is required. Issues with the installation of updates may lead to alerts being displayed and corrective action can be undertaken.



Firewall security updates

Modern firewalls need to be protected against threats and attacks in the same way user devices need to be protected. The firewall bears the brunt of the attacks against the organization, and as such, is expected to be as secure as possible. Firmware updates and subscription service updates need to be as current as possible to keep the perimeter as secure as it could be.

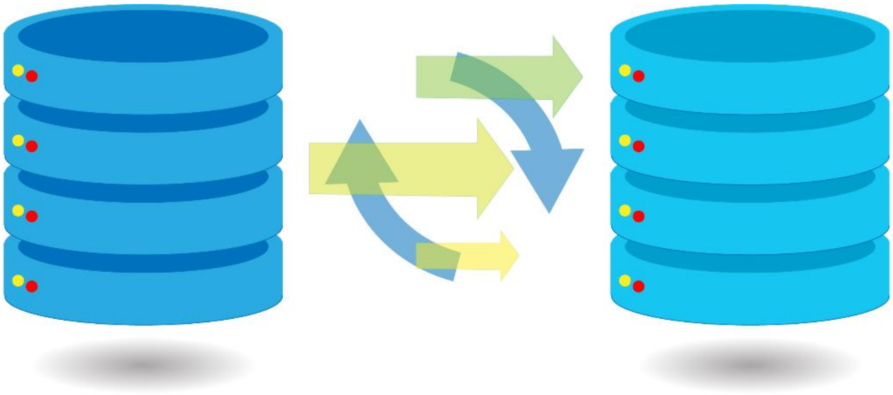
Security suites (antivirus)

Security suites help with keeping user machines safe from viruses and deliberate attacks. They defend against the most common threats and cover a range of use cases. From USB memory sticks, to internet browsing to accessing folders and files on networks, security suites are a fundamental part of the business information security toolkit.

Making sure that everyone is using the same product is important. Most security suites offer comparable degrees of effectiveness. While one person will swear by one product, another will sing the praises of another. Most paid security suites offer the same level of protection so do not be drawn into the security suite holy wars based on claims of effectiveness alone.

Backups

Backups are vital. Without backups your business is at its most vulnerable. Having regular backups will provide an additional layer of protection to your business assets. Backups are probably the first topic that jumps to mind when discussing the essentials for securing a business, yet many businesses today do not have backups of all their information.



With the prevalence of the ‘cloud’, systems management has become considerably more complex than in the on-premises server era. Knowing what information is where, and what is backed up and what is not, is a complex affair which also happens to be an ongoing problem for business. Cloud services T&Cs change frequently and these are often accepted without being read.

Information stored on local hard drives is seldom backed up, even if server volumes are. Business information locations and repositories represent a serious risk to good governance because of the complexities of ensuring that information locations are not created outside the business policy.

Keep track of these locations, ensure that all data is stored centrally as far as possible, and have your backup process run reliably against those stores to ensure effective risk management practices.