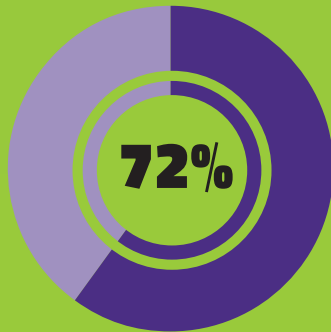




## A FALSE SENSE OF SECURITY IN THE U.K.

A recent survey conducted by Wakefield Research for Webroot looked at the security preparedness of IT decision-makers (ITDMs) at small- to medium-sized companies in the U.K. It found that many companies have a false sense of security, which could lead to lax security policies.

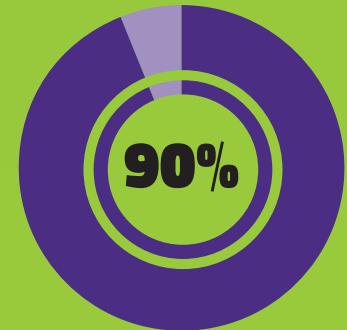


72%  
of U.K. businesses aren't ready to address IT threats.

£737,677



£737,677  
estimated cost of a cyberattack where customer records or critical data was lost in the U.K.



90%  
of U.K. businesses are confident their staff can address external security threats.

## HERE'S WHAT YOU CAN DO:

01



### CROSS THOSE Ts:

Being prepared is crucial. Create a plan of action to respond to any type of breach that includes outside resources, like an MSP, who you can enroll for assistance.

02



### EMPLOYEE EDUCATION:

Workers may not know how to avoid phishing and other types of attacks. Investing in regular security training is a great way to prevent attacks.

03



### DON'T FORGET MOBILE:

Employees' mobile devices are doorways into business networks, and can leave them vulnerable to unseen risks. Reliable mobile security is essential to protect from malicious applications.

04



### SPEND WISELY:

Look to allocate any additional budget you may have where risks are highest. If you're unsure, ask a security expert or your MSP where your vulnerabilities lie.

05



### UPDATE SOFTWARE:

Keep business devices up-to-date with the latest software and security patches.

06



### BEWARE OF RANSOMWARE:

The U.K. is consistently one of the most phished nations, and phishing can lead to ransomware. Create a layered defence by implementing strong back-up and business continuity plans.