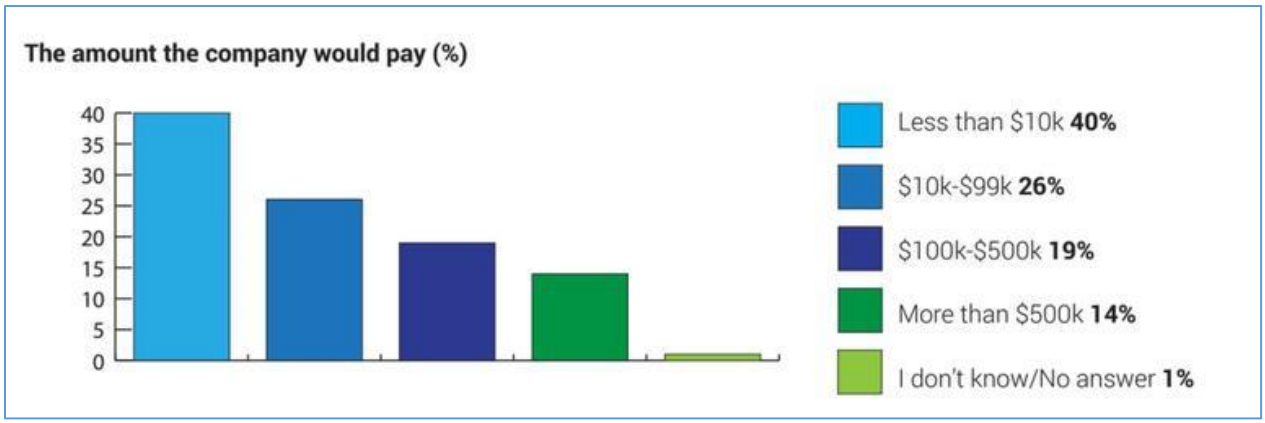
Most US firms would pay to avoid data breach shame going public

Two-thirds admit they would cough up almost $125,000 rather than admit a successful cyberattack has taken place.

By Charlie Osborne for Zero Day | February 14, 2017 | Topic: Security

The majority of US businesses admit they would pay hundreds of thousands of dollars rather than deal with the aftermath of a data breach (hack) going public.

According to new research from Bitdefender, two-thirds of 250 IT decision makers at enterprise firms say their companies would pay $124,000 to avoid public shaming after a data breach, and 14 percent would even go so far as to pay $500,000.



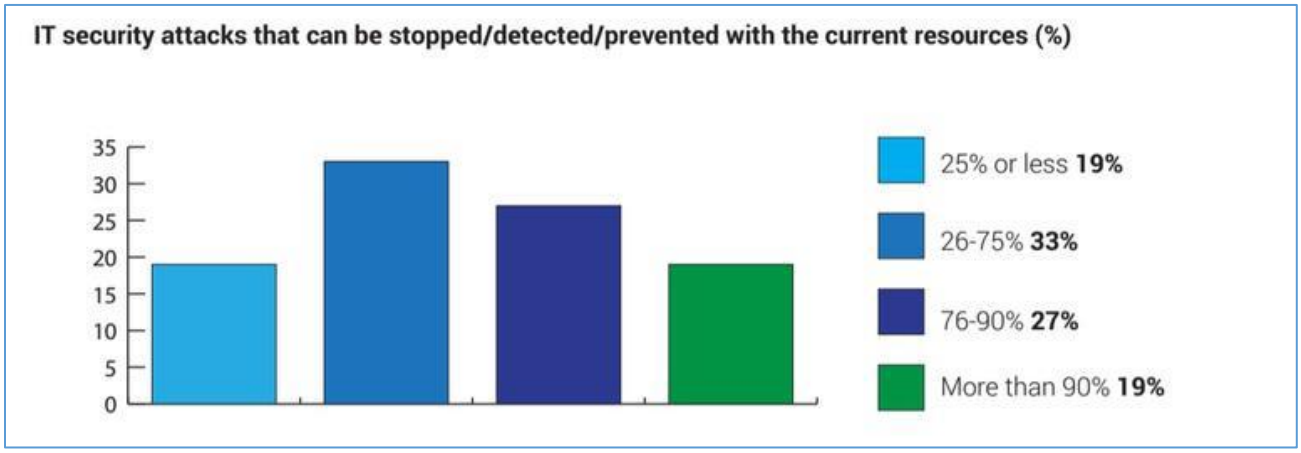
The willingness to pay a vast sum of money highlights just how much devastation a successful cyberattack can cause.

When data breaches occur, this can not only lead to the theft or destruction of customer and corporate information, but companies will take a financial hit to remedy the situation and to compensate customers.

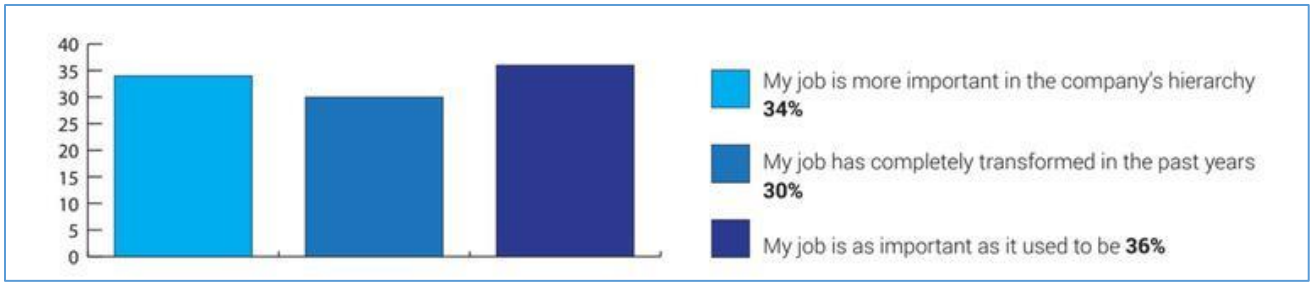
They may also have to pay regulatory fees if they do not have acceptable levels of security in place -- and perhaps most importantly, a hit to reputation in the aftermath can impact future business.

A recent example of just how seriously data breaches can impact a businesses' future is the buyout deal between Yahoo and Verizon. In October last year, Verizon said that plans to buy the tech giant for $4.83 billion could be materially damaged after Yahoo admitted to a data breach which took place in 2014 and exposed 500 million user accounts.

Bitdefender's survey, conducted in October last year by iSense Solutions, also suggests that up to 34 percent of companies in the US may have been breached in the past 12 months -- and the majority, 74 percent, do not know how it happened.



Over 2016, due to a rise in cybersecurity dangers such as Advanced Persistent Threats (APTs), zero-day exploits and the "growing adoption of hybrid environments [which] have significantly increased the attack surface, causing more headaches when securing both physical and virtual infrastructures," Bitdefender says that IT decision makers such as IT managers, security specialists and IT support staff are likely to become more important and rise in corporate hierarchies in years to come.



According to the company, board members are now facing increasing pressure to make sure corporate networks are as safe from cyberattacks and the possibility of data breaches as possible -- and IT-related jobs are transforming as a result.

However, budgets are not adequate for the task. Only two-third of those surveyed said cybersecurity investment levels were enough.

In total, 48 percent of the firms surveyed have increased cloud security spending in the past year, surpassing that now spent on physical security.

This increase makes sense as so many corporate services and systems are now hosted through cloud technologies rather than in-house servers, but according to respondents, security budgets will need to increase by an average of 34 percent in order to keep future corporate networks and strategic DBs safe.