BIZCOMMUNITY

Ineffective security the result of ineffective allocation of resources

The increase in cyber crime and threats evolving to evade even the most advanced security measures are the most important reasons why companies should not cut on their IT security budget.

Simon Campbell-Young, CEO of Phoenix Distribution

When a particular organisation had a weak or ineffective security programme, it usually boiled down to an ineffective allocation of resources. "Sadly, when IT budgets are cut, all too often it's the security budget that suffers," says Simon Campbell-Young, CEO of Phoenix Distribution.

He says particularly in times of economic stringency, finance heads become obsessed with cutting cost, and are more likely than not to refuse the go-ahead to new projects. "They don't realise that cutting costs on security increases the risk to the company exponentially. However, if your finance chief can be made to understand the cyber risks, and fund security appropriately, untold hassles can be avoided.

"When proposing new security programmes and initiatives, the technological and human resources required must be clearly communicated, and analysed as part of the company's yearly budget review as a whole."

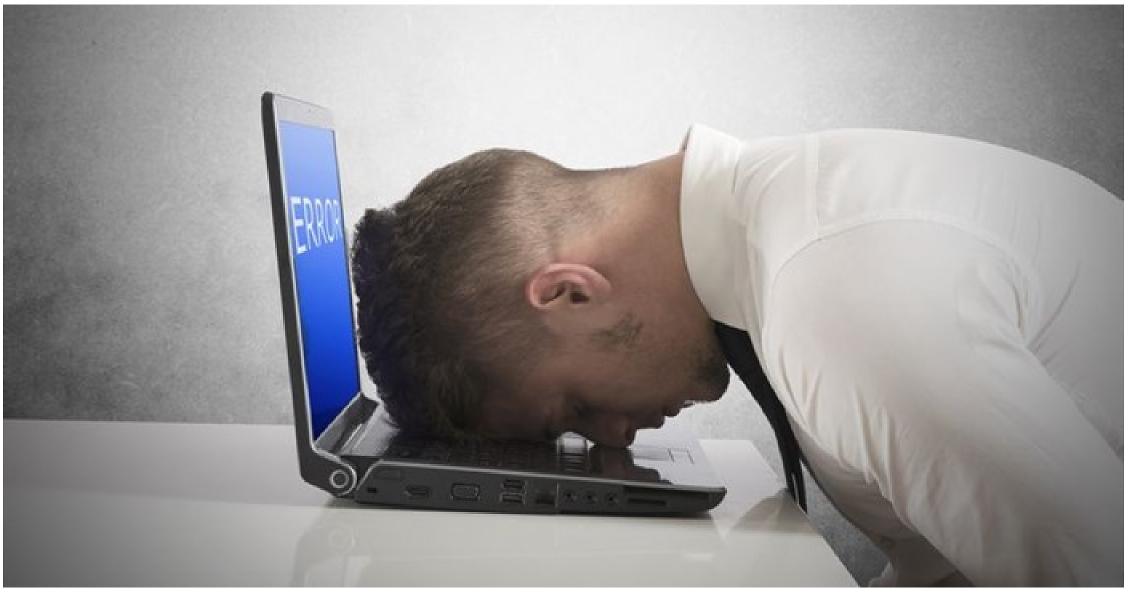
First in line of fire

Chief financial officers need to understand they will be first in the line of fire should a major security incident occur, as has happened with the slew of breaches that have stolen the headlines in the past few year, Campbell-Young adds.

"The recent surge in legal risks related to cyber attacks has undoubtedly helped drive a surge in involvement of the board in terms of managing risk and exposure. We are seeing senior executives, particularly finance heads, becoming actively involved in addressing information security and governance issues, instead of letting the IT department handle these alone."

Ultimately, governance, risk and compliance need to be recognised and understood in terms of the business functions as a whole, and needs to be filtered from the top down. "It's no good having policies and procedures in place without buy-in from C-level executives. In addition, all employees need to be able to access the policies in place, and should be mandated to review them regularly."

Moreover, the finance heads need to be in synch with the security team and consult them right up front, before implementing any new business initiatives. "Security is most effective when built in from the ground up, as this ensures that any security issues are addressed early on, sparing any future nasty surprises."



©alphaspirit via 123RF

Raise security awareness

Too often security is tacked on as an afterthought, but this is often way too late, and has seen many companies falling foul to hackers and other cyber criminals. "Addressing all security challenges and concerns in the initial phases of any initiative, saves time consuming, expensive, and often catastrophic events later on."

Finally, finance heads need to help raise security awareness, and help make the financial team understand how critical solid security is to the company's fiscal health.

"Ensuring the most valuable, confidential data is secure, and all projects have security built in from the word go, will ensure the finance chief's head isn't the first to roll should a security incident occur. Added to that, a cyber risk insurance policy will cover the last base and offer financial security should the worst case scenario occur," Campbell-Young concludes.