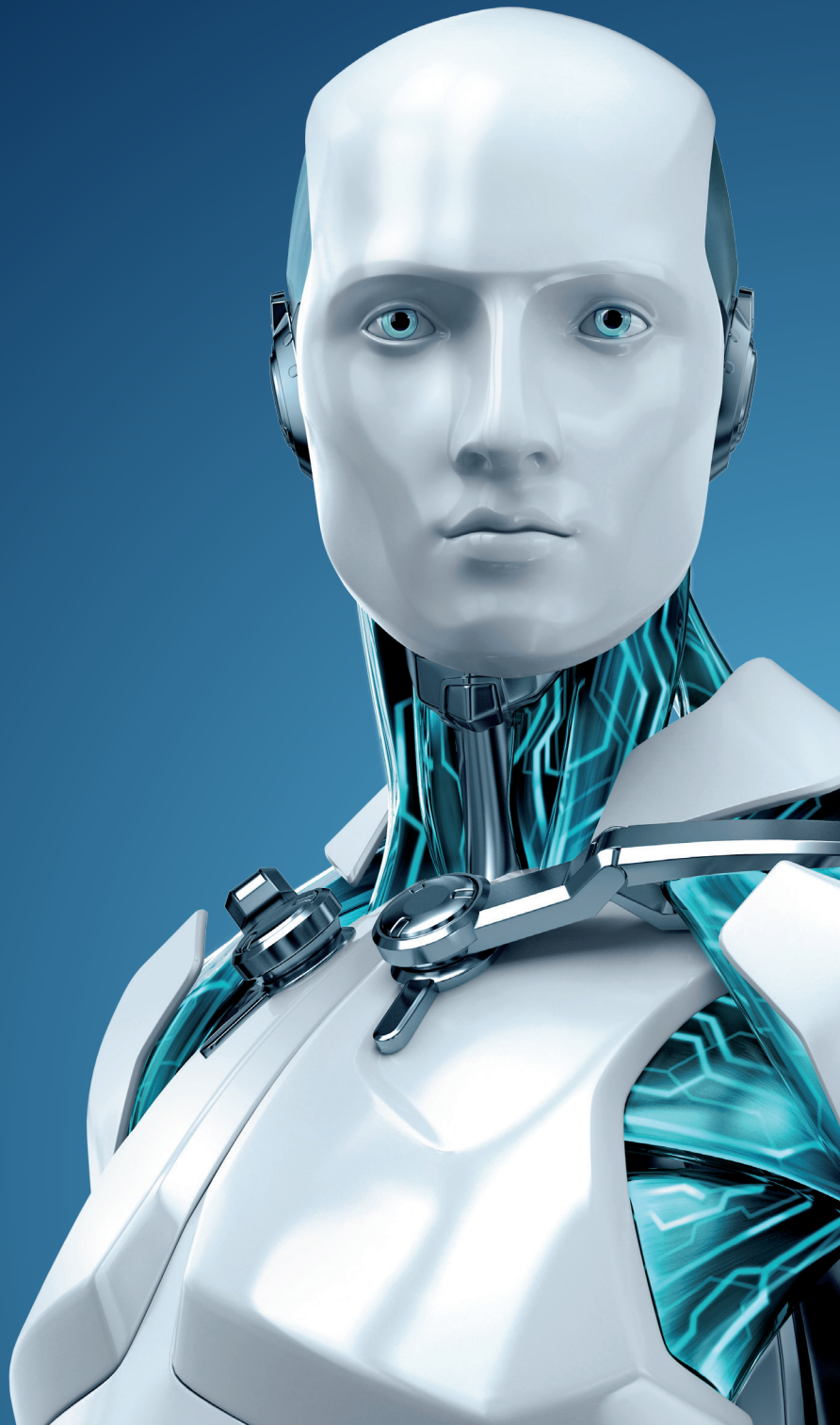
TECH BRIEF

5 ways businesses can save money on Internet security in 2015



ENJOY SAFER TECHNOLOGY®

5 WAYS BUSINESSES CAN SAVE MONEY ON INTERNET SECURITY IN 2015

By Rob Waugh, We Live Security

A recent report from Piper Jaffray found that 75% of companies expected to increase their IT security spending in 2015, following a year of high-profile hacks and data breaches in 2014. But are there ways businesses can save money on their security spend?

Some of the top tips of recent years – particularly the encouragement for businesses to switch to cloud storage and enterprise software – are being received with caution after notable attacks on cloud providers. And while old adages about "getting what you pay for" remain as true as ever, there are ways to reduce company spending on IT – or rather, ensure you don't over-spend.

1. Educate your employees

The number one tip to save money on security is continuing to educate employees. Staff should be trained on: recognizing security threats; the importance of installing updates; using stronger passwords (and changing them more often); and perhaps most of all this year, to recognize that mobile access represents a significant threat.

2. Tighten up security policies

At the same time as trying to instill good practice in employees, companies need to set more stringent top-down security policies. Ask who really needs access to what data, and don't put everything in the control of one single person; even your CIO or IT security manager. Track who accesses sensitive data.

Make sure you have a system that can disable USB ports if necessary, and do not allow employees to change security settings on their devices.

Security policies must be kept up-to-date – if you're using cloud storage and off-premises enterprise software, or if your employees do more and more work on tablet or mobile, your security policy needs to reflect the systems you're using.

Consider implementing two-factor authentication, a simple yet powerful way to strengthen passwords, block unauthorized users and protect lost or stolen mobile devices from breach. ESET Secure Authentication uses a one-time password plus an employee's smartphone to let you implement two-factor authentication quickly and effectively.

3. Assess the real risks – don't panic buy

Save money by engaging security consultants to thoroughly assess which areas of your business need the highest levels of security. While you don't want to introduce weak links, if your data policy is properly laid out and followed, there may be some areas that need top-level protection more than others.

Risk assessment will also help save money in the event of a hack: if you are aware of your potential weak spots you can develop a policy to reduce their vulnerability – again saving money in the long run.

ESET Professional Services include risk assessment and business continuity planning, both designed to complement our powerful business security software solutions. Engage us to tap into the tools and knowledge of our team to diagnose and solve the unique information security challenges of your business.

By understanding the technologies you employ, the resources you manage and how they need to secure and support your business, we can quickly identify issues that require corrective action. Our services range from security implementation and customization to employee training and tech support. These can be completed either onsite or remotely.

4. Consider open-source

Many big brand applications are mirrored by lesser-known open source platforms – and the "own-brand" alternatives are rarely such big targets for hackers. You could save money on software and minimize your exposure to hacks by using open source CRM, CMS, bookkeeping and e-commerce apps. However, open source can be unwieldy and less frequently patched. Make sure your CIO is well versed in the platforms you're using.

5. Spend money to save money

Large-scale IT spending can often seem like a major outlay – whether it's on hardware, services or manpower – but the costs of combating a hack will almost certainly far, far outweigh them.

As the Wall Street Journal's Steven Norton noted recently, large businesses are starting to treat cyber attacks as a case of "not if, but when." With that logic in mind, it makes sense to spend now rather than spend later.

Smaller businesses would do well to follow the same logic; while Sony or Microsoft are always going to be a headline-grabbing target for hackers, cybercriminals know that small businesses are more likely to be "low-hanging fruit." Eighty percent of small businesses that experience a major hack either go bankrupt or suffer severe financial losses in the following two years, according to Price Waterhouse Cooper.

Find out more about how implementing cross-platform, multi-layered security solutions can help keep your business going strong. Visit www.eset.com to learn about our customized solutions for antimalware protection, mobile security, encryption, secure authentication and much more.