BIZCOMMUNITY

Don't spend another cent on cybersecurity until real risks have been assessed

By Charl Ueckermann

6 Apr 2018

IT security has become a business necessity against the backdrop of proliferating threats from the web, malware and cyber extortion.

Companies are also obliged by legislation to protect sensitive business and customer information. But, the cost of protecting systems and data against cyber threats can rocket when investments in security technologies aren't planned and don't consider the company's specific risks.

> ***At the crux of keeping IT security costs as low as possible is choosing the right tools for the job.***

I believe, as threats evolve and as regulations obligate organisations to take stricter precaution, companies often get caught in a cycle of adding new point systems to deal with different threats. That results in a not-so-effective patchwork of technologies addressing different issues.
This is also an expensive approach and investing more in cyber security tools does not necessarily mean equal or higher protection. By making savvy choices that actually address their priority risks first, companies can get better value and more appropriate protection for what they spend.

Conduct a risk assessment

Before spending another rand on a new tool to address a particular threat, companies should first conduct a risk assessment of their IT environment. This will help to identify which risks affect the business most, what the potential impact would be and where there are vulnerabilities in existing IT infrastructure.

In my opinion, from there, companies can make more informed decisions to prioritise their investment in technologies to adequately address the risks affecting their business. This will help to avoid spending too much on expensive tools to address issues that aren't critical to the business.

With a plethora of security technologies available, choosing the right tools and systems can be hit and miss.

> ***Companies should properly evaluate the tool in terms of what it is designed to do, how this aligns with the business's risk profile, if it can integrate with existing systems at play in the business, the opportunities for customisation, and the ease of monitoring and management.***

Cost is always a factor to consider, especially in light of the changes to the National Budget released in February. Companies will need to look at initial acquisition costs, the cost of IT resources to manage the systems on an ongoing basis, software licensing, and system maintenance costs.
For me, systems also need to be adaptable to changing IT security needs as their ability to cost-effectively integrate with future projects and the associated risks can have a huge impact on future IT project spend.

Even once the technology is in place it is not something which can be forgotten. Cyber threats are constantly changing and no system, regardless of how good it is, can be expected to work optimally and effectively without monitoring and management.

This is where cybersecurity can become a black hole and time-intensive, especially for organisations that do not have the skills and resources in-house.

> ***It is also at this point that security technologies stop delivering adequate return on investment and become a drain on the cybersecurity budget if not managed effectively.***

There are several standards and frameworks to guide organisations with the management and protection of enterprise IT. COBIT 5, for instance, provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems. Information security management systems, like the ISO/IEC 27000 family of standards, offer a systematic approach to managing sensitive company information and encompass people, processes and IT systems by applying a risk management process.

I would like to conclude that these frameworks provide an excellent checklist against which companies can tick off what they need to do to keep their information safe.

However, cybersecurity is a specialised field that is rapidly changing.

Choosing a credible partner to help navigate the shifting threat landscape, and evaluate and implement the most effective security tools, will stand companies in good stead for self-sufficiently managing their cybersecurity risks, as well as compliance, in the most cost-effective way.

ABOUT CHARL UECKERMANN

Charl Ueckermann currently serves as chief executive officer at AVeS Cyber Security and assists organisations with strategic IT solutions. He has more than 25 years' in-depth experience in the IT industry, specialising in banking, government, automotive, manufacturing and telecom industry verticals. He has a proven track record in IT and business strategy in the SMB and enterprise markets.

- #BizTrends2020: 6 cybersecurity trends to watch in 2020 - 15 Jan 2020
- Don't spend another cent on cybersecurity until real risks have been assessed - 6 Apr 2018
- Tips for C-level employees when managing IT security risks - 2 Feb 2018

View my profile and articles...