Tips for C-level employees when managing IT security risks

By Charl Ueckermann

2 Feb 2018

Although most companies have invested in IT security solutions focussing on mitigating threats like viruses and malware, many fall short of addressing more sinister risks such as fraud, identity theft and espionage.

Charl Ueckermann

These are damaging threats that can put a company's reputation and business continuity at risk and can have serious financial implications. It is only when IT security-related risks are considered as business risks that the relevance of addressing them with proactive, strategic and appropriate solutions really becomes apparent – and this has to come from the top.

I believe, cyber risks should be treated as business risks and should form part of a company's overall risk management strategy. This has to be a top-down drive; from C-level employees, for whom the cost of a breach or leak is highest, to everyone else in the organisation that has access to information systems.

#BizTrends2018: The developing cyberthreat landscape

Riaan Badenhorst 15 Jan 2018

Cybercrime is burgeoning rapidly, not only in volume but sophistication as well; while 70% of threats faced by enterprises are known, 30% are unknown, advanced threats that traditional signature-based security technologies alone cannot tackle.[1]

Cybercriminals are also becoming far more discerning and are targeting their attacks. Though more targeted, they often employ basic methods to implement their attacks. These methods can include social engineering, stealing of employee credentials, imitating legitimate software or even using malware covered by a stolen certificate to infiltrate systems.

Ransomware, a type of malware that encrypts data and either prevents or limits users from accessing their systems, is typically targeted at C-level employees as well as departments dealing with sensitive information, such as accounts and human resource departments. These types of advanced, targeted cyber incidents are becoming more prevalent – even in South Africa.

How to avoid disaster in the wake of Spectre and Meltdown

Colin Thornton 23 Jan 2018

For me, it becomes quite clear that organisations need a multi-disciplinary approach that is aligned with their specific risk management requirements and includes the implementation of appropriate IT security solutions, ongoing monitoring, analysis of IT security intelligence, and employee education.

Regardless of how expensive or robust the IT security technologies are, they will not be fully effective unless everybody throughout the enterprise, starting at the top, understands the risks and supports the IT security strategy.

Advice to C-level employees

I would like to offer some advice to C-level employees when managing IT security risks in organisations:

1. We must understand that the threat landscape has changed and keeps on changing. With cybersecurity threats and the associated business risks increasing, we should treat IT security risks as business risks. Traditional, signature-based security technologies are not enough to address these risks; don't bring a knife to a gun fight.
2. I also believe that we should be more pro-active and prepared to avoid reactive firefighting after a breach or leak. Consult with IT security experts to help identify potential risks and implement the most appropriate and effective solutions to support your risk management strategy.
3. Having been in the IT industry for over 20 years, I know that if you don't understand that it is impossible to predict exactly how your systems might be attacked or threatened, you will be in trouble. I believe in an adaptive system with machine learning and pattern recognition capabilities, to deal with evolving threats.
4. Aim for machine/man symbiosis; use computers for their strengths, but don't neglect to leverage the intuition of your people. There are things a computer can do that even the smartest person in the world can't, but there are things a child can do that a computer cannot.
5. Get expert advice and support to understand, defend and deal with advanced threats like zero-day attacks.
6. In my opinion, conducting regular vulnerability assessments of your IT infrastructure will help you to uncover the loopholes in your organisation's security architecture and avoid damage that could be caused by cyberattacks.
7. More than 80% of all cyber incidents are caused by human error.[2] Make sure all employees are trained and are informed of risks that can occur. Companies lose money recovering from staff-related incidents, yet education and training programmes intended to prevent these problems are limited, and they usually fail to engender the desired behaviour and motivation. When employees are educated about the potential risks associated with clicking on links in emails, responding to phishing emails, connecting unsecured devices to company IT resources or sharing access

credentials, they are less likely to put systems in danger.

I want to put organisations at ease with the fact there are various computer-based training products available that leverage modern learning techniques and address all levels of the organisational structure.

We must realise that every individual in the organisation using a computer is responsible for IT security, not just the IT department. And that cybersecurity awareness and education are, therefore, fundamental to the effectiveness of your risk management strategy.

References:

1. **Lab, K. (2017, 01 18). the Enterprise. Retrieved from Kaspersky: p.4**
2. **Lab, K. (2017, 01 18). the Enterprise. Retrieved from Kaspersky: p.12**

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...