bizcommunity

Industry-specific approaches to cyber risks

Companies of all natures, shapes, and sizes are at risk of cyber threats and crime. No organisation is immune to cyber-attacks, which are increasing in frequency and sophistication a the time. However, the risks to which companies in different industries are vulnerable can vary, and a specialised, industry-specific risk management approach will always trump a generic one when it comes to efficacy and efficiency.

By Evan-Lee Courie 10 Feb 2020

Charl Ueckermann, CEO at AVeS Cyber Security.

“Certain sectors are particularly vulnerable to cyber-attacks. The level of risk to which a business is expose is directly related to the potential returns that cybercriminals can reap with a tolerable amount of effort. The won’t apply the same effort to attacking a restaurant as they would to a financial institution that keeps sensitive information and money. A company’s risk management approach must not only be industry-specific but also curated according to the specific risks the business faces, as well as its risk appetite.

“Similarly, while the principles of IT governance are largely generic, the interpretation and focus will differ

between verticals because the operating landscapes, which include market dynamics and legislation amor other things, are different," says Charl Ueckermann, CEO at AVeS Cyber Security.

Ueckermann has been in cybersecurity for over 22-years and provides insight into the rise of industry-specific approaches to cyber risk management.

Why are industry-specific cyber risk management solutions becoming vital in cybersecurity strategies?

The deep knowledge, speed and efficiency of execution is critical in the fast-moving pace of cybersecurit threat landscape in 2020.

We find that a growing number of companies are seeking the advice of specialist partners and not IT generalist to handle their Cyber Security requirements. Specialist partners furthermore "talk the language" and know how to articulate client needs much faster than generalists.

How can companies make that transition to industry-specific cybersecurity?

Companies need to do a bit of introspection in their capabilities and where their core skills reside. To be everything to everyone is neither efficient and neither sustainable. The days of "box-dropping" IT compani are reaching their "close-by-date" very quickly as they will not be able to compete efficiently in a specialise industry market.

Why are specific sectors more vulnerable to cyber-attacks than others?

Cybercriminals will also go where the money is – attacking say a small florist business will not be as lucrati as attacking a small legal firm. A legal firm may deal with larger clients such as a bank or enterprise clients and have thus a much larger to infiltration motive.

It simply is all about risk and return.

What are these specific industries?

Healthcare, financial services, manufacturing and legal

How can organisations in specific sectors lower their risk profiles?

Always start with a risk assessment such as an ISO 27001 assessment by a qualified lead auditor – then move forward with a structured and pragmatic plan that will address biggest wins first. It is often a case of using the technology in place just much better, if technology is well configured there is more than often les risk.

ABOUT EVAN-LEE COURIE

Group Editor: Retail and Lifestyle
View my profile and articles...