BIZCOMMUNITY

5 security and risk management trends you need to pay attention to

By Peter Firstbrook

29 May 2018

Security - once merely a small part of enterprise IT - is now a significant function, crucial for organisational success. This has elevated the role of security and risk management (SRM) leaders, who are currently faced with the difficult task of protecting their organisations from harmful cyberattacks and tougher regulators with increased expectations

Security and risk management leaders have operated in the shadows for a long time. Now it's their opportunity to shine. If they exploit emerging trends and build a strong security program, they can keep their organisation safe and significantly elevate their standing.

Here are five major upcoming security and risk management trends, along with some of their key impacts:

#1: The spotlight is on

Security breaches threaten C-level jobs and cost organisations millions of dollars, as proven by Equifax and Maersk. As a result, business leaders and senior stakeholders now focus much more on what is going on in the security department.

SRM leaders should capitalise on this increased attention and work closely with business stakeholders to link security strategy with business initiatives. This is also a perfect opportunity to address skill shortages and increase professional development of the internal security workforce.

When speaking with senior executives, an important but often neglected aspect is the language barrier. Speak the language of the business and don't lose yourself in technical terms when you deal with the C-suite.

#2: Regulations enforce change

The rise of data breaches forces enterprises to comply with an increasingly complex legal and regulatory environment, including Europe's General Data Protection Regulation (GDPR).

GDPR: ground zero for a more trusted, secure internet

Bill Buchanan 28 May 2018

Data is both an asset and a potential liability. Digital business plans must weigh both and seek innovative solutions to lower costs and potential liabilities.

Leading organisations are focused on how a compliance program can act as a business enabler. The message SRM leaders must communicate to CEOs is that data protection has both costs and risk but can also be used as a business differentiator.

#3: Security moves to the cloud

Enterprise security organisations are getting buried under the maintenance burden of legacy security solutions. Cloud-delivered security products are more agile and can implement new detection methods and services faster than on-site solutions.

#AfricaMonth: The time to become a disruptor is now

Brett St Clair 15 May 2018

But not all cloud security services are created equal. Exploiting the cloud is more than moving legacy management servers to the cloud. SRM leaders should look for solutions that take full advantage of cloud scale, increased data telemetry, staff augmentation, machine learning, API-based access, and other services and products that are disruptive to the status quo.

#4: Machine learning becomes the watchdog

By 2025, machine learning (ML) will be a normal part of security practice and will offset some skills and staffing shortfalls. In its current state, ML is better at addressing narrow and well-defined problem sets, such as classifying executable files.

We can't escape the fact that humans and machines complement each other, and together they can outperform each alone. Machine learning reaches out to humans for assistance to address uncertainty and aids them by presenting relevant information.

Today it is difficult to unpack the difference between marketing and good ML. SRM leaders should focus on how AI makes its product superior in terms of efficacy and administrative requirements. Keep in mind that ML requires human assistance,

but the key question is where that assistance comes from.

#5: Origin beats pricing

The recent US government bans against Russian-based security products and Chinese smartphones are only the latest results of a growing distrust of the influence of competitive world powers in cyberspace.

Organisations that deal with government agencies should be especially sensitive to the geopolitical demands of their upstream and downstream business relationships.

#AfricaMonth: The power of smart technology in Africa

Greg Morris 8 May 2018

All security and product buying decisions are based on trust in the integrity of the supplier.

SRM leaders should start to incorporate geopolitical risk in all business-critical software, hardware and services purchasing decisions and, where necessary, consider local alternatives.

ABOUT THE AUTHOR

Peter Firstbrook is research vice president at Gartner.