Brought to you by Informa Tech
OMDIA

Publication date:
20 Apr 2023
Author:
Maxine Holt, Senior Director, Cybersecurity

Cybersecurity: Maximum attention, minimum budget – the carrot and the stick

Omdia view

Summary

Maximum attention, minimum budget. This is what Omdia is hearing from organizations about cybersecurity when it comes to addressing today's economic headwinds. New attack techniques, attempted breaches, and staffing shortages are a fact of everyday life in cybersecurity, but organizations must maintain digital resilience despite these challenges. Furthermore, these same organizations must be consistently available to their customers and citizens and be able to take advantage of new digital opportunities. There are carrots and sticks in the equation.

The mantra of "doing more with less" applies across most functions of most organizations. How are security functions dealing with compressed security budgets under intense scrutiny? Omdia asserts that the ability to adapt to these changing industry dynamics will be a significant factor in the success – or lack thereof – of enterprise cybersecurity programs.

Maximum attention remains on cybersecurity

Cybersecurity as a requirement has a high profile in most organizations, yet there is little sign of increased budgets to deal with this scrutiny – and indeed, budgets are often being reduced. The security function is not being singled out; organizations are being economically prudent in challenging times.

For many a year, the return on investment (ROI) equation has failed security. Typically, the best result from investing in security technology, services, and controls, is that "nothing happens." This hardly sets the CFO's heart rate going, at least not in the right direction. In today's economic climate, a better case must be made for cybersecurity investment to support and address the internal and external scrutiny that security receives.

Many organizations are today using return on security investment, ROSI, as a way of demonstrating this. The approach is open to interpretation but is typically based on risk, prioritization, and organizational objectives, with two outcomes:

- Investment is focused on the areas of highest priority
- The organization can innovate and use its security posture to its (competitive) advantage

Innovation is the "carrot" side of the balance; making the investment in security could result in the organization being more competitive in the market (or serving its customers better). A strong model is US retailer Walmart. It has invested tens of millions of dollars in cybersecurity over the past decade and has largely avoided major cybersecurity incidents. The company now seeks to differentiate by positioning itself as "the world's most trusted retailer" (see, Further Reading).

Prioritization is more of the "stick" side of the balance; without making this investment, the organization is at greater risk of cyberattacks and other incidents that can affect business success (and draw the ire of regulators). One need only look to the numerous business disruptions faced recently by US carrier Southwest Airlines. Its latest incident, this month, which was blamed on a failed network firewall, resulted in more than 2,200 delayed flights.

The carrot and the stick for cybersecurity budget

Today's world is digital, and organizations must be digitally resilient and, in turn, cyber-resilient. Omdia defines these as:

- Digital resilience: The ability to minimize the impact of disruptions and continuously operate, in order to quickly leverage digital opportunities.
- Cyber-resilience: A core component of digital resilience, ensuring that the organization continuously operates despite inevitable security breaches and other incidents.

The standard risk equation is a good starting point to consider the "stick" side of the balance. The equation is: Identify a threat to the organization, determine the likelihood of that threat happening on a numerical scale (e.g., 1 to 5), determine the impact of that threat happening on a numerical scale (again, it could be 1 to 5), and multiply the two together to give a risk "number". For a series of threats, there will then be a series of risk numbers associated with specific threats (let's call the outcomes "identified risks"), and these identified risks can be ranked highest to lowest. A decision will need to be made about each identified risk – accept, mitigate, or transfer.

The "carrot" side of the balance comes from organizations needing to manage security to the very best of their ability to remain operational and, crucially, take advantage of digital opportunities.

Making the accept/mitigate/transfer decision about each identified risk needs to consider the organization's risk appetite. This is the extent to which the organization is prepared to accept identified risks based on strategy and demands. Highly regulated organizations will generally have a low cybersecurity-risk appetite, whereas those organizations operating in a fast-moving and highly competitive (and lower regulated) market are likely to have a higher risk appetite, to take advantage of opportunities and steal a march on their competitors.

This means that the identified risks will have a nominal "cut-off" point according to cybersecurity-risk appetite. The ROSI will use risk appetite (where formally recognized in the organization) to prove the case for investment, demonstrating the link to business objectives. There are many permutations to the

identified risks, and it isn't as straightforward as stating that a fast-moving organization will always have a higher risk appetite. Such an organization may want to be triply sure that any new business initiative has the best security surrounding it so that there is minimal risk of failure upon launch.

Besides the obvious quantifiable impact of security incidents and breaches, organizations want their customers or citizens to trust them. This is the crux of the "maximum attention, minimum budget" conundrum. Headlines are all too easily made and not so easily forgotten. Thus, the ROSI focuses on the potential positive impact of proactive cybersecurity, addressing the identified risks and demonstrating the opportunity for more customer trust and thus – for private sector organizations – more commercial benefit. This is more difficult to define for public sector organizations, but nevertheless trust is important here too. The ROSI tends to focus more on the stick, although the opportunity to deliver improved services to citizens is also needed in the equation.

The FUD factor is outdated – focus on business outcomes

Pushing fear, uncertainty, and doubt – often referred to as the FUD factor in cybersecurity – will only yield results from the least tech/security savvy executives. Vendors, services providers, and enterprises alike that know this, spend far more time focusing on the business outcomes of various cybersecurity investments. They balance the organization's priorities with those of the cybersecurity function, ensuring that any asked-for security investment is in line with these priorities and can demonstrate business outcomes.

Enter, ROSI. Understanding the benefits and costs of security investments enables budgets to be spent ever more wisely – consideration of risk, compliance, innovation, resilience, commercials, and customer/citizen trust all help demonstrate to the CFO and their peers the value of investment in cybersecurity.

Appendix

Further reading

Omdia Market Radar: Identity Governance & Administration (IGA) (September 2022)

2022 Trends to Watch: Enterprise Security Management (January 2022)

"Cyber-risk highlighted by World Economic Forum Global Risk Report 2022" (January 2022)

Cybersecurity Dive: https://www.cybersecuritydive.com/news/walmart-security-operations-headquarters/641450/ (January 2023)

Author

Maxine Holt, Senior Director, Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com