How to Decide on Your Company's IT Security Budget?

How businesses should go about budgeting for cyber security measures in this day and age?

Cyber security is the foremost concern of Chief Information Security Officers (CISO's) and IT security professionals globally. It is the first and last thought on their minds during their working day when they strive for securing the data and assets of their enterprise.

Budgeting for cyber security must be done like budgeting for any other enterprise expense bucket. Spend on information security measures and advancement has increased exponentially in the last several years to keep up with the ever-evolving cyber threats landscape. Spend in Australia on cyber security was $5.6b in 2020, while globally it was estimated to reach $123b.

Traditionally, information security has been considered as a “necessary evil” investment where organisations have put in the necessary foundational and basic measures, but not done much with the remaining budget. This outlook has changed dramatically to cope with and counter the variety of threats and risks enterprises face today from hackers and cybercriminals.

The Covid-19 pandemic resulting in a global shift to working from home arrangements forced enterprises to rethink their information security strategy, move superfast and adopt enhanced security measures which they would not have budgeted for in their fiscal year 2020 budgets.

As a result, the majority of all enterprises, small and big, needed to put a halt to other IT projects and divert the budgets and resources to enhance cyber security operations for the newly formed remote workforces and the enterprises.

Read Also: Cyber Security Threats and Measures for eCommerce Companies in 2021

BUDGETING FOR CYBER SECURITY – A NECESSITY

Cyber security measures and operations are an absolute must-have for any sized business. They can no longer be considered as secondary or tertiary items for a company's budget. Global damages from cyber attacks in 2020 hit $1 trillion! The high degree of losses has been, in part, due to new hacking avenues that opened due to the Covid-19 pandemic and the changes to the global work environment.

These changes are now the new normal, and cyber criminals will keep at attempting to discover and exploit new threats and vulnerabilities. In such scenario, an enterprise needs to plan and be well prepared with an adequate information security strategy and threat response.

Here you can read the cyber security statistics of 2020 and trends for 2021 which can help with planning for your organisation.

CONSIDERATIONS WHEN BUDGETING FOR CYBER SECURITY

1. RISK-BASED APPROACH

CISO’s should carry out a cyber security risk assessment for their enterprise. It is important to note that with the budget allocated for cyber security, it is not possible, neither is it advisable, to try and solve all the threats faced by the enterprise. An enterprise needs to analyse the critical business risks – for e.g., which threats could lead to downtime, damage to reputation, lost business, monetary losses, or confidential data breach.

Use tools such as likelihood vs. impact matrix to quantify the threats, which can help gain an understanding of areas where the enterprise needs to be prepared to address any unforeseen, sudden threats immediately, and hence, budget accordingly.

2. INDUSTRY AND SIZE ANALYSIS

While cyberattackers do not distinguish amongst enterprises based on the industry and/or size, there are specific types of risks that commonly affect a particular industry and particular sized business. For e.g., with the nature of an eCommerce business where transactions are completely online, they are highly vulnerable to DDoS attacks or credit card fraud.

Healthcare providers, hospitals, medical centers are mostly targeted for stealing of private and confidential consumers' data. Similarly, specific threats exist for banking and financial organisations. In addition to the risk assessment highlighted in the point above, CISO's need to consider potential penalties and fines that an enterprise would be liable to pay should there be a breach within their systems.

3. READINESS OF THE ENTERPRISE

Every enterprise needs to delve into their existing controls of cyber security and how good they are at defending its systems and data. This is a measure of the readiness of the enterprise to manage potential threats and attacks.

If it is not at an acceptable level, the enterprise needs to budget for and invest more in cyber security controls. Paul Proctor, former Chief of Research for Risk and Security at Gartner, explains about the importance of readiness in this article of IT budget planning.

4. CYBER SECURITY OPERATIONS AND ACTIVITIES

An enterprise should plan and budget for the operations and activities they need to undertake as part of its cyber security strategy. Penetration testing, preferably by an external services provider, should be one of the critical activities, as it provides a neutral assessment of the readiness and threat environment.

Penetration testing of the various components of the enterprise's IT landscape should be carried out periodically, for e.g., every quarter, or every six months.

The enterprise should also consider the model with which it operates its cyber security operations – whether it's managed internally or outsourced to an external services provider. In addition, it should include activities like security training and awareness for staff, security tools and upgrades, policies, and procedures, etc.

Find out how the team at Secure Triad can help you plan for and execute penetration testing of your enterprise's IT environment with their suite of services. Contact us now!

Original Source of This Content: https://securetriad.io/how-to-plan-cyber-security-budget-effectively/