HOW TO QUANTIFY CYBER THREATS AS A CISO IN 2020

Boardish - IT & Cyber That Speaks The Board's Language

Boardish

Boardish

The Current Landscape

The current threat landscape requires continuous efforts in the identification of main cyber threats to the organization's decision makers. Security posture needs to be maintained and updated for your organization to be truly responsive.

CISOs need to be prepared for 2020 and coordinate their security efforts with the board and their company goals.

Communicating cyber threats in the board's language —exact figures and business impact—requires a way to quantify these threats.

Here's how you do it...

#1 Identify the biggest threats and their financial impact on the company.
#2 Present the impact of technology issues on employees.
#3 Show the financial impact of 'downtime' on the company's salaries.
#4 Consider the role of regulations.
#5 What is the true efficiency of solutions against cyber threats?

Read on to find out more...

#1

Identify the biggest threats and their financial impact on the company.

Identification of the largest cyber threats seems to be the biggest hurdle in presenting cyber risk and exposure, mainly due to the fragmentation of digital solutions in organizations. According to Deloitte's Future of Cyber Survey, 41% of CISOs state that Shadow IT presents the most challenging aspect of cybersecurity management in the organization, followed closely by 37% of CISO stating cyber transformation presents a large challenge.

Shadow IT makes it difficult to quantify cyber risk, as there is no overview of all systems. This makes it next to impossible to get a good snapshot of organizational cyber maturity or security posture.

When the departments integrate digital solutions on their own, there is no alignment of IT with critical business goals.

How This Relates to Quantifying Cyber Threats

Simply saying the largest cyber risk (such as data leakage or breach) will cost the company millions, destroy it, or have far-reaching consequences is not enough anymore.

- How much would the cyber incident cost if left as is?
- How much would your solution cost?
- How much exposure would remain after implementing the solution?
- Would your solution be a sound decision, from a financial standpoint?

Speak in actual numbers, financial impact and exposure, not industry averages or 'educated guesses'.

Boardish

#2

Boardish

Present the impact of technology issues on employees.

To get a clearer picture of how a cybersecurity incident will affect employees, it's best to separate users as high, medium, and low impact.

Technology issues won't affect all users in the company in the same manner.

LOW- IMPACT - Some will experience only mild inconveniences but be able to continue working.

MEDIUM-IMPACT - Some won't be affected at all.

HIGH-IMPACT - Some, however, won't be able to do a single thing until the threat is resolved.

How This Relates to Quantifying Cyber Threats

Quantifying the impact of cyber risk depends heavily on how your operations will take a blow. When you have a clear picture of how dependent your users are on technology, you will be able to calculate the impact.

For example, if users can't do their job at all—high impact users—it means their operations are standing still, which makes the risk and its cost greater.

#3

Show the financial impact of 'downtime' on the company's salaries.

The amount of high, medium, and low impact users determines more than just the extent of the impact. It also shows how much downtime will cost in terms of salaries—how much it will cost the organization that these employees won't be able to work.

How This Relates to Quantifying Cyber Threats

Even if employees can't work because of the security incident that needs to be resolved, they will still get their salary for the day. How much will this add to the total cost of the security incident?

You don't need exact figures for every possible employee you hire, of course, but having an idea of salary averages will help you determine this risk.

To get some idea on salary figures, ask the CFO or somebody in the financial department. You might even want to use external resources that can give you averages for a clearer picture.

Boardish

#4

Consider the role of regulations.

Information and data are top targets of cyberattacks in the current age, and all companies are under strict regulations on how to protect it, no matter what industry you are in.

Take GDPR as an example—the data protection act lists extremely high fines for companies that do not take necessary measures when it comes to personally identifiable information (PII).

How This Relates to Quantifying Cyber Threats

CISOs must quantify the impact of all regulations pertaining to the company in case of worst-case scenarios.

The GDPR, for example, has extremely high fines. Depending on which is greater, the company might face fines of 20 million euros or 4% of its annual revenue in case of a data breach.

Regulations MUST be considered in the potential financial impact of cyber threats! If your organization can't recover from high fines, it increases the risk of threats considerably.

Boardish

#5

Boardish

What is the true efficiency of solutions against cyber threats?

After presenting cyber threats that are most likely to affect the company, CISOs must also present the solution. To sell the solution, you must quantify them too—their immediate and annual costs, in comparison to the costs of the threat they are solving.

In addition, there is also the efficiency factor of the solution—how much of the risk will it mitigate, and how much exposure would remain? The efficiency of the solution depends on the threat type and environment. Is it prem? Is it in the cloud?

How This Relates to Quantifying Cyber Threats

It is likely that you will have more than one solution to mitigating the biggest threats, with each of them having different efficiency depending on the environment. Solution efficiency and cost help you justify investments that will improve the company's resilience and overall security posture.

This is one of the ways Boardish is unique as our TPF (Threat Protection Factor) algorithm quantifies the effectiveness of solutions against threats in two environments!

There are also very few scenarios where a cyber solution will have 100% efficiency so decision-makers need to see the exposure left and weigh up the risk factor themselves.

About Boardish

Boardish is an innovative platform that makes the CISO/CTO/CIO job easier by helping quantify IT threats and solutions into ACTUAL financial impact. Providing decision makers with figures, no guesswork, and no spreadsheets!

The aim is to provide tangible and quantifiable risk analysis to cyber security and bridge the gap between IT and the board in a fast paced and frequently changing area in business.

Boardish is not only revolutionising how technology approach the board by sparking the conversations about risk that we need, it also shows tangible results in explaining how various IT and cyber security solutions combat specific business threats, utimately improving security posture.

Try Boardish for FREE today by visiting:

BOARDISH.IO

Boardish