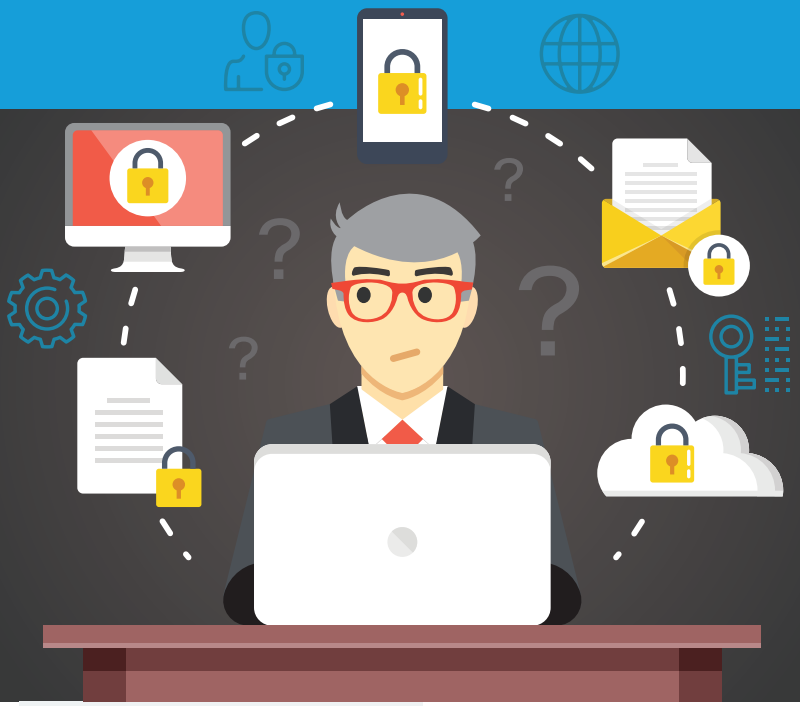
Quantifying Security Incidents

The right process for quantifying the value of security incidents.

Consistent measurement

Visibility to business impact

Support for decision making



But, HOW do you set up a model and get data that you trust?

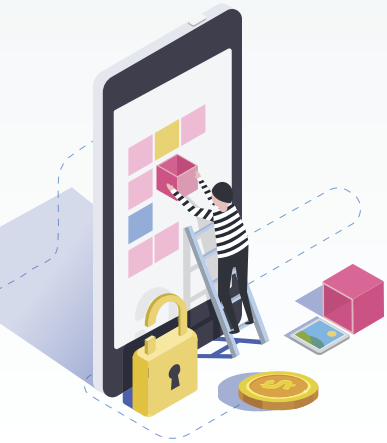
We use a method called Annual Loss Expected (ALE) versus Annual Loss Realized (ALR).

ALE, or the expected losses from security incidents, is influenced by the organization's size, its geographical scope, the nature of its business, and its security posture. ALR captures the actual impact and cost of handling security incidents.

Step 1

FIND THE RIGHT BENCHMARK FOR ALE

We use Ponemon's "Cost of Cyber Crime Study" and their cost framework



Step 2

ESTABLISH EQUIVALENT COMPONENTS FOR ALR

For us, there are 4 broad cost categories that will be impacted during a security incident:

- Operational costs
- Data loss
- Brand impact
- Profit impact

Step 3

COLLECT AND VALIDATE ALR DATA SOURCES

This starts with identifying the teams that own the data and building strong business partnerships with them

Data Gathering
Working with data owners and subject matter experts

Data Preparation
Transforming data into information and formats that work

Data Understanding
Using analytics to move data into 4 cost categories

Step 4

BUILD PROCESS AND TOOLS TO CAPTURE AND COMMUNICATE

Dashboards, discussions and deep dives help us prioritize investments, understand high-impact incidents and prepare for process and tool changes

Find out how we pull it all together, including some use cases, in the "Quantifying Security Incidents" whitepaper.

trust.cisco.com