IBM Security

Risk Quantification Services

Quantifying security risk in financial terms to help guide cybersecurity decision making.

IBM Security identified vulnerabilities in a client's human resource system. The client was faced with the decision to invest in cybersecurity solutions for a legacy HR system or accept the risk of successful phishing attacks.

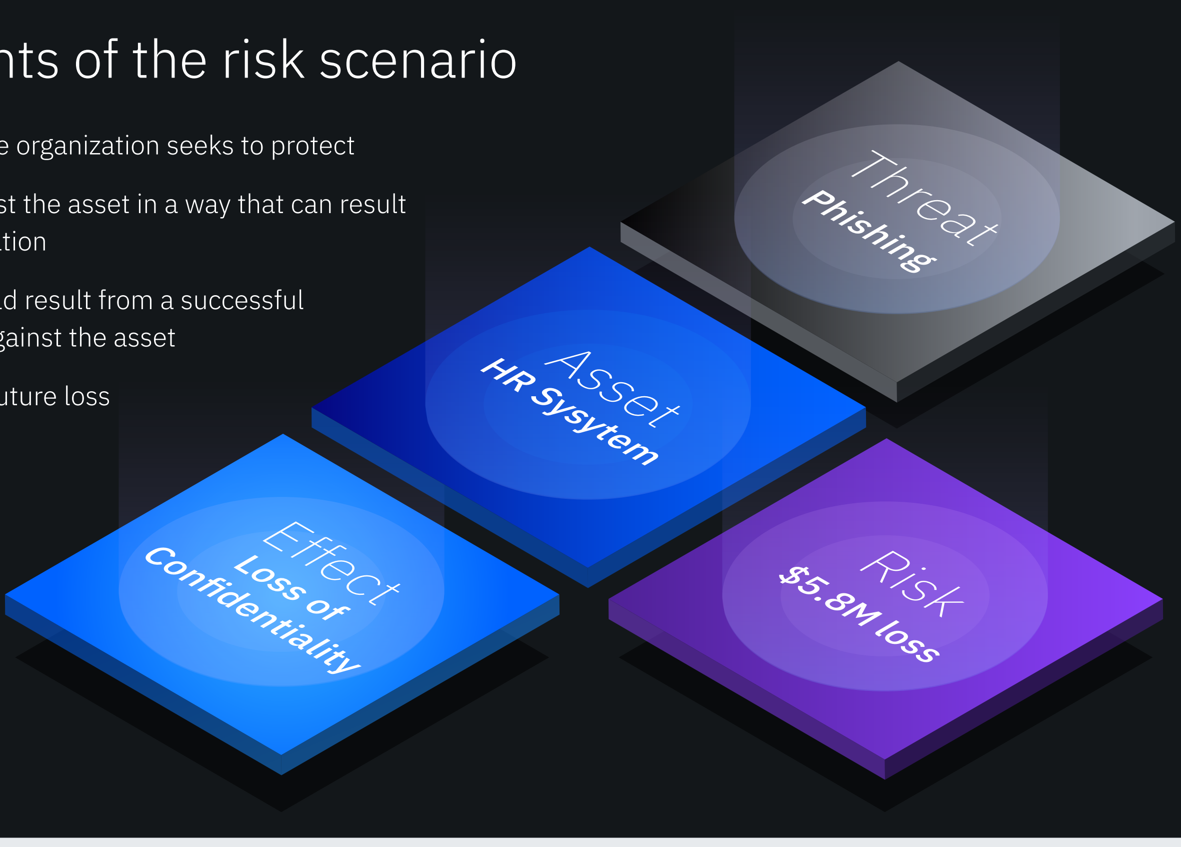
Identify elements of the risk scenario

Asset: Thing of value that the organization seeks to protect

Threat: Agent that acts against the asset in a way that can result in loss to the organization

Effect: Type of loss that would result from a successful action of the threat against the asset

Risk: Financial amount of future loss



Key data inputs

80% maximum chance of vulnerability resulting in a successful attack

30% minimum chance of vulnerability resulting in a successful attack

$150 Average cost per lost or stolen record*

25,230 average loss of records per data breach*

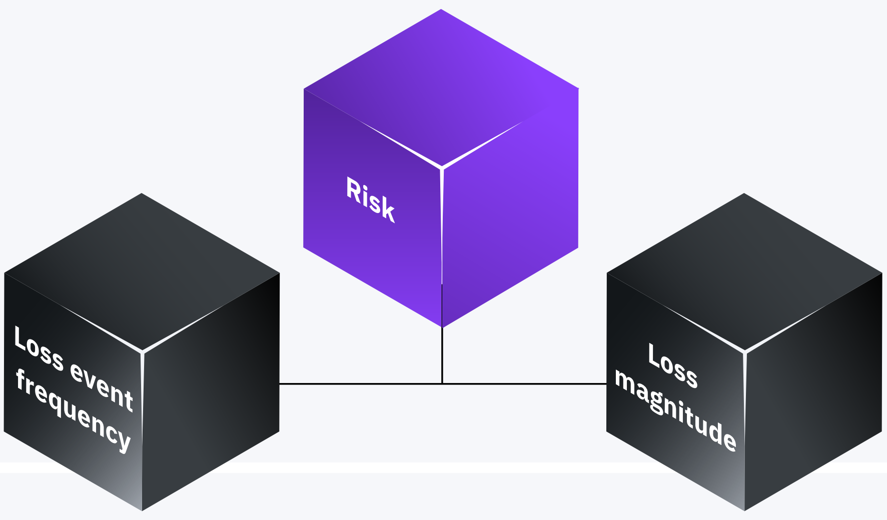
The FAIR model for risk calculation

Inputs

Frequency

Vulnerability

Industry loss data



Output

$2M - $10.7M

Range of possible financial loss

The results

Quantifying risk in financial terms helps provide a clear understanding of the impact to the business.

47% probability of $2M or greater loss – With current state of HR system

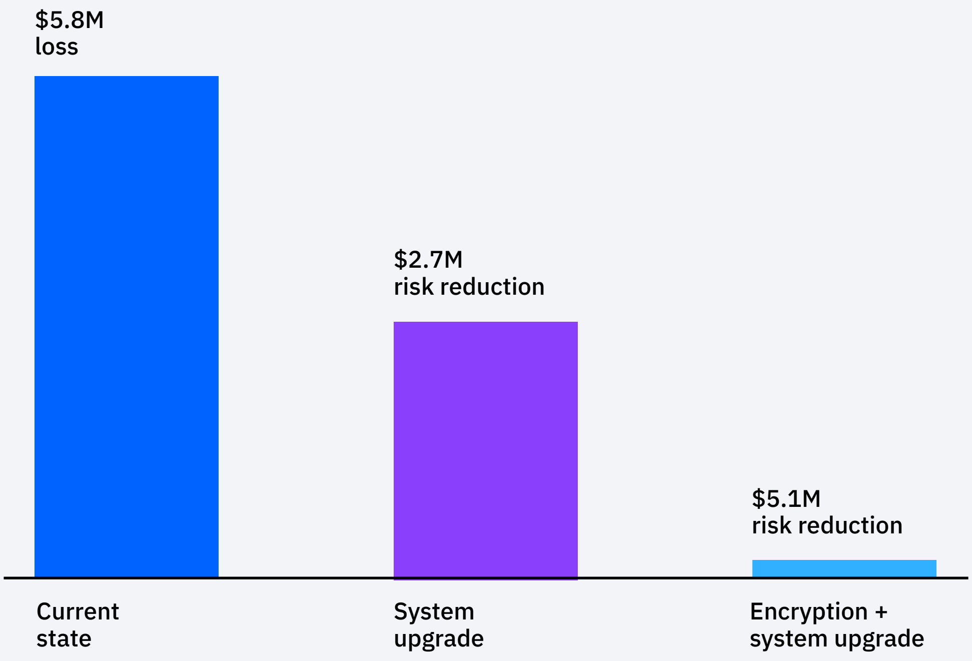
12% probability of $492K or greater loss – With upgrade of HR system

Making an informed decision

The client is equipped with risk analysis measured in financial terms. The client can seek upgrade and encryption solutions that maximize return on investment.

$5.8M financial loss
Possible future financial loss with current state
vs
$400K security investment
Estimated cost of security solutions

Empowered decision making using risk qualification



Get more info to help you quantify risk in financial terms.

Contact IBM Security Services: Contact us

*2020 Cost of a Data Breach Report

IBM