The Essentials of a Physical Security Systems Risk Assessment

LCDR Don Davis
6 NOV 2019

The Essentials of a Physical Security Systems Risk Assessment

- The Security Executive Council
- https://www.securityexecutivecouncil.com/spotlight/?sid=30836

What Are Your Security Goals?

- Before you begin an assessment of your security systems, you need to know your security goals.
- All your security activities should support these goals.
- If you don't have a clear understanding of your goals, you will not be able to implement a cost-effective system that meets your needs.

What Are Your Security Goals?

A clear statement of your security goals is usually built on answers to questions like the following:

- Do I want to correct a problem or reduce a potential risk?
- Do my proposed solutions address the needs that I have identified?
- Are my solutions consistent with the business culture?

What Are Your Security Goals?

A clear statement of your security goals is usually built on answers to questions like the following:

- Will the solutions hinder business operations?
- Will the solutions enhance security performance guidelines for the business?
- Is new technology part of the solution?
- Is the new technology consistent with the long-range plans of the business?

Assessing the Needs of Your Business

Physical security must make sense within the context of your business operations.

To build a security system that works for any business, the needs of that business must first be assessed.

Assessing the Needs of Your Business

At the core of this assessment are the following operational issues:

- What is the general level of risk for this business?
- What are the critical events that will stop this business?

Assessing the Needs of Your Business

At the core of this assessment are the following operational issues:

- What are the products, information, and assets at this site?
- What specific risks are associated with each of them?
- How do people and materials enter and leave?
- What are the work schedules?

The Security Assessment

The security assessment as the first step in assessing the needs of your business.

This helps you arrive at an overall assessment of the security issues relating to your business operations—your people, information, property, product, and the corporation's reputation.

The Security Assessment

In order to use a security assessment properly, you first need to understand three fundamental elements of security:

probability, criticality, and vulnerability.

Elements of Security

An effective security assessment applies an understanding of the fundamental elements of security to a particular location or area within the business.

As you look at each area, you must consider the following questions:

Elements of Security

- What is the probability of a security-related incident occurring in this area?
- How critical might the incident be to my business operations?
- How vulnerable is the area to a security incident?

Answers to these questions help you to arrive at an assessment of the level of security risk associated with a particular area of your business.

Element 1: Probability

- Probability is the likelihood that a security incident will occur, independent of any effort you may make to avoid the incident.
- Probability is affected by factors such as your location and environment, your product, the personnel at your site, and other factors that are essentially beyond your control.

Element 1: Probability

- As you perform a security assessment, keep in mind that each area of your business must be evaluated in terms of the probability that security incidents will occur there.
- As you assess each area of your business, make a list of the most frequent incidents that have occurred in your building, at your location, and in the surrounding area or neighborhood.

Element 2: Criticality

The criticality of a security incident is the degree to which it affects your ability to do business.

An incident with high criticality is one that:

- Interrupts your business operations;
- Has significant operational or legal ramifications;
- Impacts or reduces sales;

Element 2: Criticality

- Erodes the quality of your products or services;
- Gives the competition a significant advantage;
- Causes the loss of substantial revenue; and/or
- Damages the corporation's reputation.

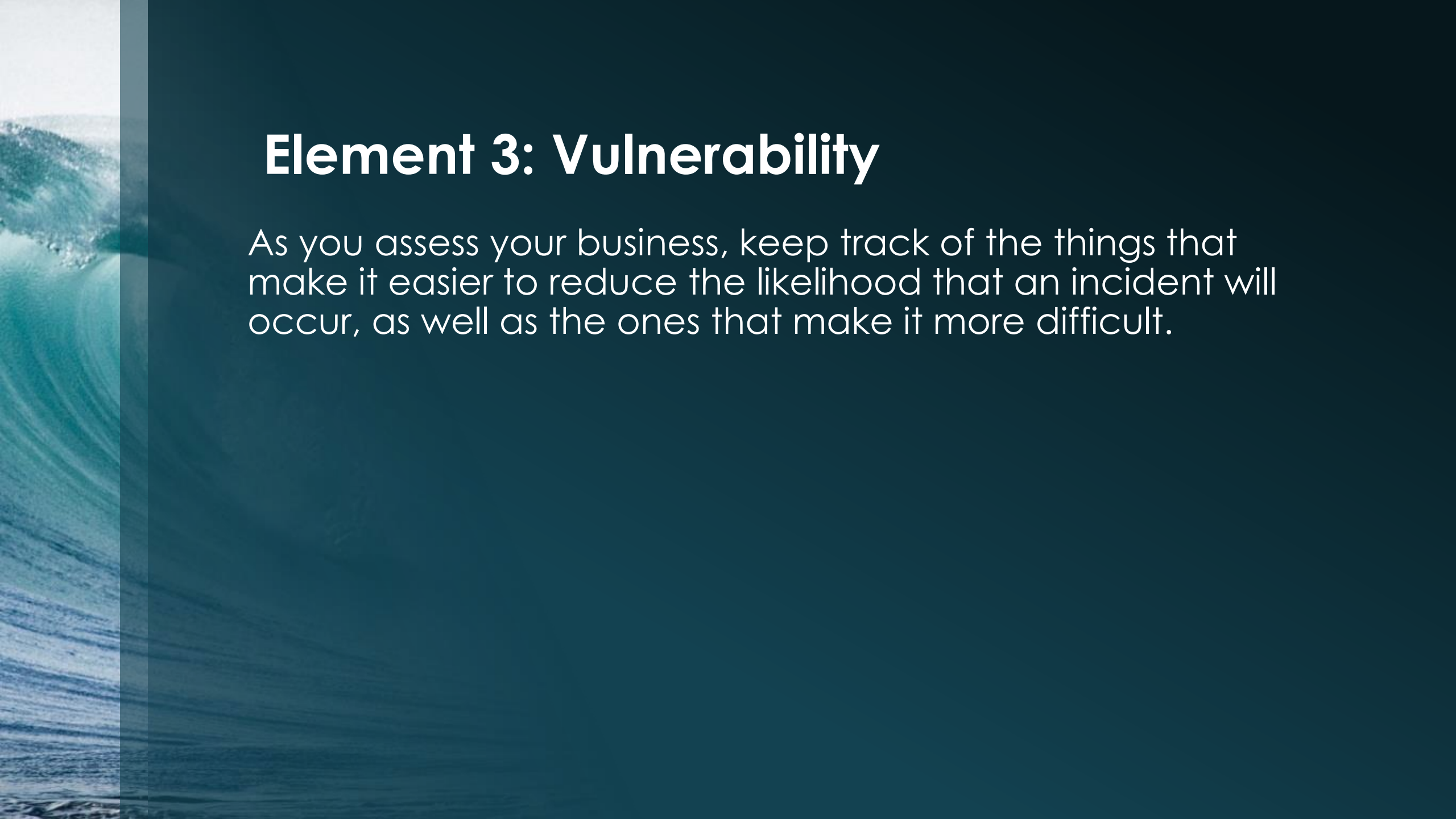
As you assess each area of your business, make a list of the security incidents that could have a high degree of criticality.

Element 3: Vulnerability

- Vulnerability is a measure of your ability to prevent a security incident.
- Your current security system and procedures represent the active steps you've taken to decrease your vulnerability.
- As you assess each area of your business, make a list of the security incidents that could have a high degree of criticality.

Element 3: Vulnerability

- Vulnerability is a dynamic concept.
- It changes whenever your environment, operations, personnel, business and/or systems change.
- Each time a substantive security-related change occurs in an area of your business, you need to reconsider your vulnerability in that area.



Element 3: Vulnerability

As you assess your business, keep track of the things that make it easier to reduce the likelihood that an incident will occur, as well as the ones that make it more difficult.

Combining the Three Elements of Security to Arrive at an Assessment of Risk

The most cost-effective security systems consider all three elements of security simultaneously to arrive at an assessment of the risk associated with a particular area.

You can gauge the overall security risk for an area by determining the degree to which the area has high values for probability, criticality, and vulnerability.

Combining the Three Elements of Security to Arrive at an Assessment of Risk

It makes most sense to concentrate your resources on areas that have the greatest degree of security risk.

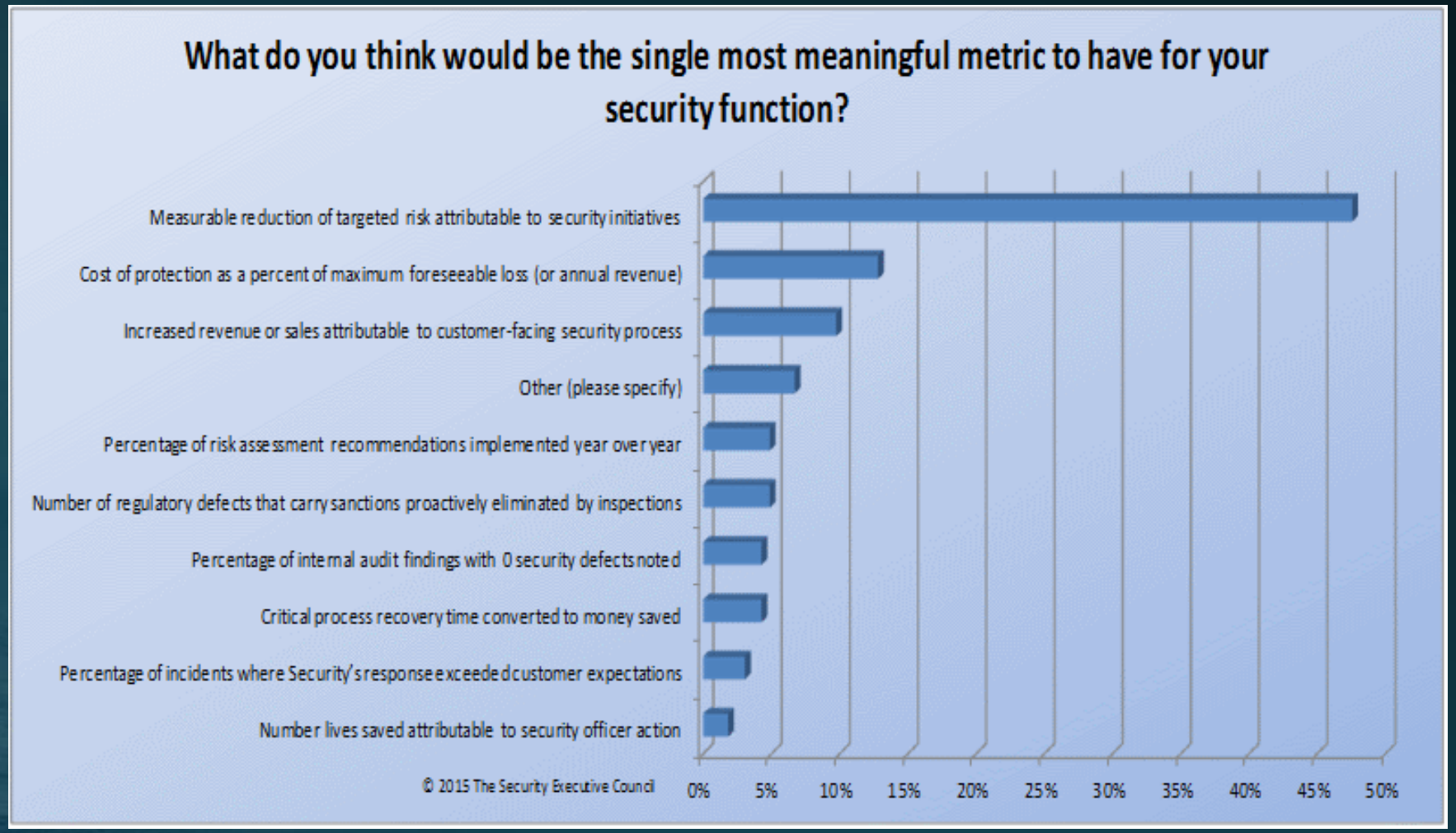
Highest priority should be given to those areas that have high values for probability, criticality, and vulnerability.

Combining the Three Elements of Security to Arrive at an Assessment of Risk

When the values for a particular area add up to an unacceptable level of risk, it is vital that you lower one or more of them by implementing security measures.

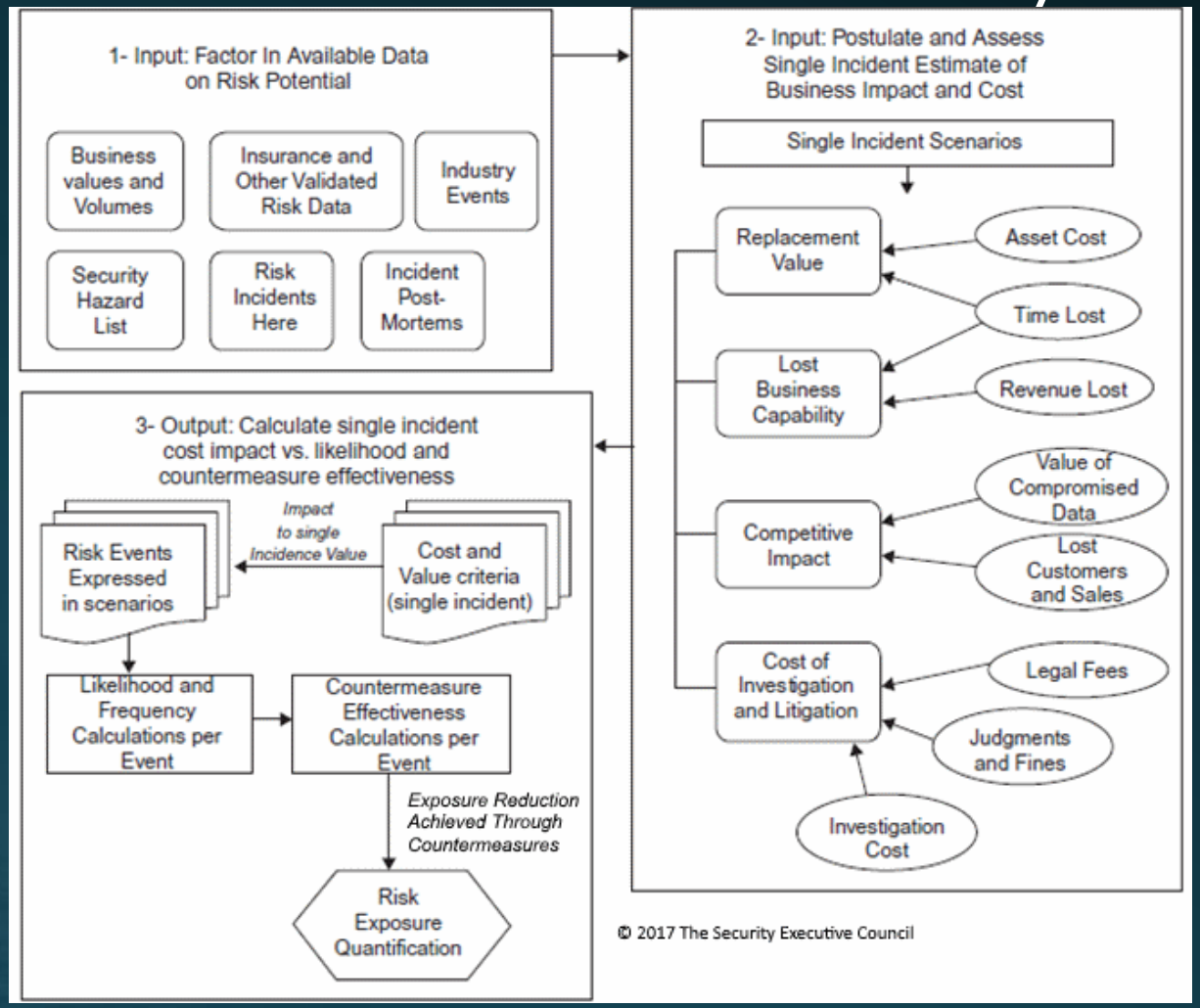
On the other hand, areas that have a uniform set of low values should not be using security resources that could be better spent in other areas of your business.

The Business Case for Security



https://www.securityexecutivecouncil.com/spotlight/?sid=28872

The Business Case for Security



https://www.securityexecutivecouncil.com/spotlight/?sid=30899

Questions