#Jenny

Finally I get this ebook, thanks for all these I can get now!

#Rio

Cool! I'am really happy

#Markus Jensen

I did not think that this would work, my best friend showed me this website, and it does! I get my most wanted eBook

#Hun Tsu

wtf this great ebook for free?!

#Che Salsa

My friends are so mad that they do not know how I have all the high quality ebook which they do not!

#Diego Butler

so many fake sites. this is the first one which worked! Many thanks

mation erasure. So, why are we classifying at all, if the classification doesn't help to do something as simple as selecting a security measure? Some other examples of incidents that don't fit CIA are operator errors and fraud. To neutralize a threat, a control that regulates the causes of the threat will normally be needed; therefore, for control selection, it would be far more useful to classify by causes than by effects, which is exactly what CIA doesn't do.

CIA doesn't consider the context at all. This is why small and medium size organizations are intimidated by the exigency of Confidentiality, Integrity and Availability, giving up on devoting enough resources to security. Only big organizations aim for Confidentiality, Integrity and Availability.

CIA doesn't consider our expectation about our information systems. You can't demand confidentiality of public information. You can't demand integrity of low-durability information; it is too easy to reproduce. And you can't demand availability of low-priority services.

Many practitioners who use the CIA definition have a stance of "We want to prevent attacks from succeeding." In other words, for us to be safe is equivalent to being invulnerable. The definition of an incident under this light is totally independent of the context, and considers attacks only, neglecting accidents and errors as incidents. Disaster recovery plans show that the need to protect a company from catastrophes is well known, but many accidents are considered a reliability issue and not a security issue, because accidents are not considered a security problem.

So, if no current information security definition or paradigm is satisfactory, what can replace it? An interesting alternative is the use of an operational definition. For example, a meter is defined operationally as the distance traveled by a beam of light in a certain span of time. An example for the need of operational definitions is the collapse of the West Gate Bridge in Melbourne, Australia in 1970, killing 35 construction workers. The subsequent enquiry found that the failure arose because engineers had specified the weight of a quantity of flat steel plate. The word "flat" in this context lacked an operational definition, so there was no test for accepting or rejecting a particular shipment or for controlling quality.

Before detailing the operational definition, some words about probability. Probability has predictive power with the following considerations:

- As long as systems and the environmental conditions don't change, the future is similar to the past.
- You can apply probability to a set of phenomena, not to individual phenomenon.
- A sufficiently big set of historic cases must be available for significant probability calculations.

Probability is often misunderstood. If you drop a coin nine times and get nine crosses, the probability of getting a cross the tenth time is still half, not lower as intuition suggests. Quite the opposite, the more crosses we get, the higher should be our confidence that the next drop will be a cross, too.

An operational definition for information security is: "The absence of threats that can affect our expectations about information systems equivalently protected in equivalent environments."

This operational definition is not only falsifiable, but it is expectations-dependent and deals cleanly with the definition difficulties of context. It is helpful to determine what threats are relevant, to weigh the threats, measure the risk, and to select security measures.

The following definitions of incident and threat follow from the operational definition:

- Incident: "Any failure to meet our expectations about an information system." This definition makes our expectations the pivotal point about what should protected.
- Threat: "Any historical cause of at least one incident." This implies that the probability is not zero, and brings in the context.

The threats relevant to an information system will be the causes of historic incidents in information systems protected equivalently in equivalent environments. Insecurity can be measured by the cost of historic incidents in a span of time for every information system equivalently protected in an equivalent environment.

Many companies have these general expectations about their information systems and the way they are used:

1. Comply with existing legal regulations.
2. Control the access to secrets and information or services protected by law, like private information and copyrights.
3. Identify the authors of information or messages and record of their use of services.
4. Bear the users responsible for their use of services and acceptance of contracts and agreements.
5. Control the physical ownership of information and information systems.
6. Control the existence and destruction of information and services.
7. Control the availability of information and services.
8. Control the reliability and performance of services.
9. Control the precision of information.
10. Reflect the real time and date in all their records.

Every organization will have a different set of expectations, which leads to different sets of incidents to protect from and different sets of threats to worry about, depending on the environment. The more specific the expectations, the easier it becomes to determine the threats and the security measures.

To determine how relevant the threats are, it is necessary to gather historical data for incidents in equivalent systems in equivalent environments. Unfortunately, whereas the insurance industry has been doing this for years, information security practitioners lack this statistical information. It is possible to know the likelihood and cause of having a car accident, but there is not data enough to know how likely you are to suffer an information security incident, nor the cause. Quantitative risk measurement without proper historical data is useless. Some practitioners even mix estimative figures with complex formulae, which is equivalent to mixing magic and physics.

Even if there is no accurate data about risk, it is possible to follow a risk assessment process similar to OCTAVE to identify the expectations about the information systems and the significant threats that can prevent the expectations to materialize.

With the operational definition, every identified threat can be controlled using suitable security measures. If quantitative risk information is available, the most cost-efficient security measures could be selected.

The operational definition of an incident helps to focus on whatever is relevant to our context. If there is no expectation for secrecy, no matter what is revealed, there is no incident. The operational definition of a threat helps focus on threats that are both relevant and likely. It doesn't make much sense to consider meteors as a threat if no information sys-