Humans Are Notoriously Bad at Assessing Risk

Risk assessment should be a rational and objective undertaking. We as humans, with our emotions, can sometimes be irrational and subjective. As security professionals, this would seem to put us at odds with our duty to objectively assess, manage, and mitigate risk.

Unfortunately, subjectivity introduces bias, which skews risk assessment. When too much subjectivity is mixed into risk assessment, it can produce a risk picture that is not an accurate representation of reality. This, in turn, results in a poorer overall security posture.

Given this, how can security professionals remove as much subjectivity as possible from risk assessment? There are likely many different approaches that can be taken. I'd like to offer seven steps that security teams can use to ensure that their risk assessment, management, and mitigation is as objective as possible.

1. **Critical resources and data:** When we begin to think about risk objectively, we quickly realize that we need to focus on where there is the potential for damage and loss to the business. Damage most often materializes due to monetary loss caused by compromised data, compromised resources (systems), and/or compromised accounts. This monetary loss can be in the form of lost revenue (due to app unavailability, brand reputation damage, etc.), regulatory fines, disclosure costs, breach remediation costs, fraud, and others. Thus, the first step towards objective risk assessment is enumerating critical resources and data that are likely

to have a monetary impact on the business if affected in a security incident.

2. **Potential impact:** Once critical resources and data are enumerated, the potential impact of each must be understood. By potential impact, we mean financial. In some cases, this may be easier to determine than in others. Regardless, this impact will need to be determined as an important next step in this process.
3. **Threat landscape:** There is no shortage of security threats out there. Some of these are more relevant and applicable to the business than others. Those that are relevant will need to be enumerated to keep the risk assessment process moving forward.
4. **Mapping:** Risks and threats to a business do not exist within a vacuum. As mentioned above, some are more relevant and applicable to the business than others. Further, not all risks and threats are relevant and applicable to all of the critical resources and data that have been enumerated. Therefore, it becomes important to accurately map the appropriate risks and threats to the resources and data that have the potential to be impacted. This is an important exercise that is necessary before true risk exposure can be measured.
5. **Exposure:** Damage to a business after a security incident results from risk exposure rather than risk in absolute terms. Risk exposure is defined as the probability that a risk will materialize * the impact if the risk materializes. If the potential for impact is large but the probability the risk will materialize is low (or vice versa), the risk exposure will be far lower than the risk in absolute terms. It may take a moment to get comfortable with, but risk exposure is a far more objective and rational way to manage risk. If you need a bit more help getting there, think about the impact of winning the lottery. Huge, right? Nonetheless, the probability of winning the lottery is so low that I know

of no one who quit their job immediately after purchasing a lottery ticket.

6. **Translate:** Our executives and boards understand risk through the lens of monetary damage and loss to the business. This is true across all risks to the business, including security risks. If we have done a good job throughout steps 1-5, we should be able to calculate the potential monetary impact of the risks and threats we've enumerated. To do so, we will need to use all of the data points above, and in particular, the financial impact we assessed in step 2.
7. **Aggregate:** While executives and boards have a good understanding of risk, we cannot expect them to be able to make sense of the detailed work we've done in steps 1-6. Thus, we must identify groupings into which we can aggregate risks and the potential for loss. For example, we must aggregate up into business units, product lines, applications, etc. Once we do that, we can present risk exposure to our executives and boards in the language they are expecting to see it in.

Taking as much subjectivity as possible out of the risk assessment process requires a significant investment in time, money, and resources. It is a worthy investment, however. Beyond the initial work, risk assessment is a continual process that will need to be done iteratively in order to maintain the security posture of a business and work to improve it. As an added bonus, once risk assessment is done objectively and in terms that executives and boards can relate to, it becomes a platform for showing the value of the security team and security investments for necessary people, process, and technology.

https://www.securityweek.com/humans-are-notoriously-bad-at-assessing-risk/