When a Risk in Not a Risk

Is choosing tiramisu over a lemon tart a risk or a choice?
Is a forgotten password a risk or an inconvenience?
Is an unauthorized access a risk or an incident?
Is an unpatched server a risk or a vulnerability?
Is a flying pigeon a risk or a threat?
Is a broken arm a risk or a problem?

In an everyday setting, we don't pay much attention to how we use the term "risk," and being precise does not enhance its interpretation. However, in an organizational setting, the risk your executive management needs to hear about is rarely reduced to a simple choice between the delicate taste of espresso-soaked ladyfingers and the creamy freshness of lemon curd in a crumbly crust.

Within an organization, the differentiation between specific "risks" informs a decision-making process that can make or break a company. It positions an organization to weather future crises or appropriately evaluate an opportunity. It enables faster identification of critical matters, fosters faster allocation of resources, and informs appropriate organizational levels to allow for meaningful and engaging discussion.

Not every event is a "risk," and not all events are equally important—nor do they apply to every audience. Organizations must differentiate not just between different "risks," but also between different levels of criticality and impact an event may have (e.g. low, medium, or high).

For example: The leader of a Security Operations Center (SOC) needs to know about all incidents; the CIO needs to act on all high issues; and the governing body (i.e. board of directors and executive management) needs to know about and understand all high risks. In

contrast, the governing body can do little about every single incident that occurs, and the SOC leader can do even less about high organizational risks. In short, every risk should be evaluated based on the entity that needs to get involved with it.

DIFFERENT "RISKS"

Risks, issues, incidents, vulnerabilities, threats, exploits, failed controls, and findings are not all the same. They have specific meanings, and their differentiation is important. Their various effects on an organization can be driven by probability, time, severity, and speed.

The terms below were defined by many individuals, organizations, and institutions. There is no universal definition for any of them; however, most sources do agree to an extent, and these definitions reflect that agreement. The following list is geared toward IT and security teams and is not exhaustive; it is simply exemplary of common risk-related terms.

RISK - An event that did not occur yet but is likely to impact an organization. The "impact" can be positive or negative.
Examples:

- Primary data center might become inoperable
- Investment in passwordless authentication
- Evolving or changing regulatory requirements

ISSUE or PROBLEM – An event that already occurred and is negatively impacting the organization.
Examples:

- ERP system implementation delayed
- Mobile devices deployed without data protection measures
- Systematic back-up failures

INCIDENT – An event that already occurred and is actively or potentially harming the organization or violates organization's rules.
Examples:

- Executive's computer is locked, and data held for ransom
- Unauthorized access to restricted data
- Excessive upload, download or printing of files

VULNERABILITY – A weakness that could be exploited or misused. (Most often refers to security.)
Examples:

- Unpatched servers
- Untrained or uninformed workforce
- Overprivileged or unmonitored access to privileged data

THREAT – An occurrence that could have a negative impact on an organization by exploiting a vulnerability. (Most often refers to security.)
Examples:

- Malware, ransomware, spyware/adware
- Criminal enterprise/scammers
- Malicious internal users (insider threats)

EXPLOIT – A means by which a threat is acting on a vulnerability. A program or technique that takes advantage of a vulnerability. (Most often refers to security.)
Examples:

- Email with the link to a download that contains a virus (phishing)
- Phone call requesting a user to reveal secret credentials (social engineering)
- Use of trusted access

Example: A scammer (threat) calls a CEO's administrative assistant (vulnerability) and poses as the company's help desk (exploit). The scammer exploits the untrained assistant to access the CEO's email account credentials. Needless to say, the CEO's emails contain vast amounts of sensitive data.

It is not uncommon for IT and security teams to track compliance-related findings as risks. However, in those cases a control failure has already happened—so the findings cannot be considered risks. The below classifications offer more accurate descriptions of compliance-related outcomes.

FAILED CONTROL – A documented management control that does not operate as designed or intended

FINDING – Non-conformity with audit criteria; where audit criteria is different from management's documented controls

OPPORTUNITY FOR IMPROVEMENT – A concern over a weak practice

CONCLUSION

Risks, issues, incidents, vulnerabilities, and compliance-related events should be differentiated and tracked in order to improve day-to-day prioritization and strategic positioning. Threats and exploits must be evaluated within the context of vulnerabilities for likelihood estimation.

To continue the conversation about governance, risk management, and compliance, contact:

Evelin Biro
Risk Management Enthusiast and Founder
evelin@biroconsulting.com

Visit us at www.biroconsulting.com