RSA BUSINESS-DRIVEN SECURITY™

RISK 101: WHAT IS RISK?

Fundamental Information for Successful Digital Risk Management

CONTENTS

MANAGING DIGITAL RISK TOGETHER

Success Starts with a Common Understanding

In the era of digital transformation, every organization faces both digital opportunity and digital risk. Managing that risk successfully takes an all-hands effort, with risk management and security teams working truly in tandem. But if you ask most technology, business or security leaders for a definition of risk, you are likely to get any number of different answers. There's clearly a gap between the server room and the boardroom when it comes to what the word "risk" actually means.

That gap in meaning reflects a concern of many participants in the 2018 RSA Cybersecurity and Business Risk Study, 69 percent of whom agree that business risk and IT security personnel tend to use different tools and language, and that this can make communication between them challenging. As managing digital risk becomes a more critical challenge for organizations undergoing digital transformation, it is important for all involved to have a common understanding of the meaning of risk. This document is intended to help foster that understanding.

69%

of business risk and IT security personnel surveyed agree business risk and IT security personnel tend to use different tools and language, making communications challenging.

Source: Enterprise Strategy Group, The RSA Cybersecurity and Business Risk Study, April 2018

WHAT ISN'T RISK? MYTHS AND MISCONCEPTIONS

Many terms are often and easily misunderstood as risk, which is reasonable considering the relationship of some of those concepts to risk. Following are a few examples of terms that are often confused with risk. This applies both to risk in the general sense and in the specific context of digital risk.

THREAT

Threats are people, processes or programs that pose a potential for damage, loss or risk. The term "threat" is often used interchangeably, as are specific threats.

Incorrect: *"My firm's biggest risk is ransomware."*

Alternative: *"The threat of ransomware is raising my firm's cyber incident risk."*

VULNERABILITY

Vulnerability is the quality or state of being exposed to the possibility of being attacked or harmed. Vulnerabilities of all types allow threats to negatively affect organizations in various ways, including flaws found in software development and other business processes.

Incorrect: *"The fact we don't have a redundant system is a major risk."*

Alternative: *"Our risk of business disruption will increase without a redundant system."*

ASSET

An asset can be a computer or other device that is subject to threats and vulnerabilities, and ultimately can carry some risk. These terms are often conflated incorrectly, such as in situations where assets may be regarded as fundamentally different.

Incorrect: *"Cloud applications are our company's highest risk."*

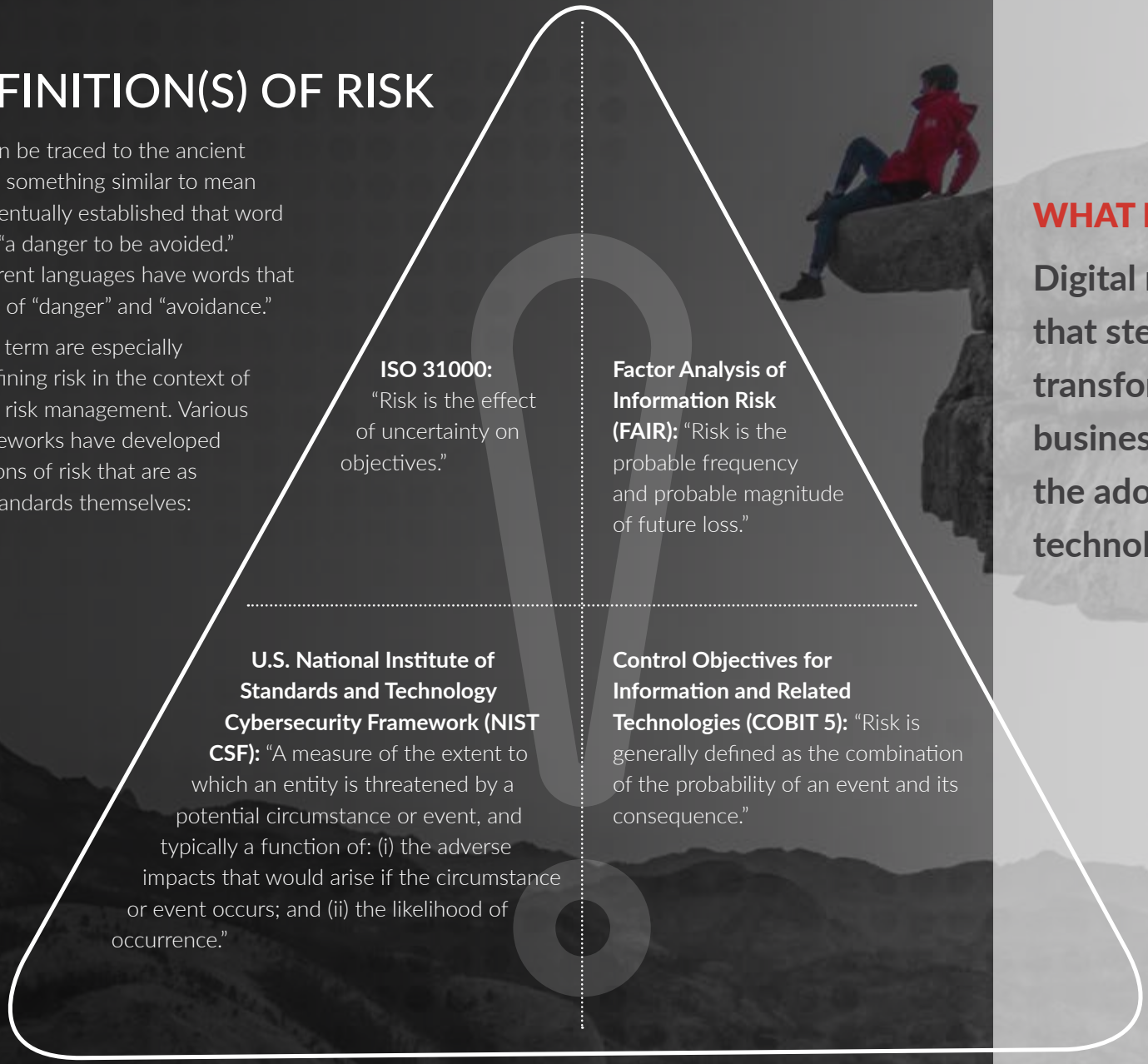
Alternative: *"A compromise of a cloud application we rely on puts us at risk of data theft."*

It is easy to see how such a complex concept can be reduced to a few of its more prominent factors and elements. However, the complexity of risk is exactly the reason it is critical to have a common understanding of the concept, including what it isn't.

THE DEFINITION(S) OF RISK

The term "risk" can be traced to the ancient Greeks, who used something similar to mean "cliff," and who eventually established that word as a synonym for "a danger to be avoided." Today, many different languages have words that carry this concept of "danger" and "avoidance."

The origins of the term are especially relevant when defining risk in the context of cybersecurity and risk management. Various industry risk frameworks have developed their own definitions of risk that are as nuanced as the standards themselves:



WHAT IS DIGITAL RISK?

Digital risk refers to risk that stems from digital transformation, digital business processes and the adoption of related technologies.

KEY CONCEPTS IN DEFINING RISK: LIKELIHOOD AND IMPACT

While the preceding examples of how to define risk offer a number of perspectives from different sources, two core concepts remain intact across them all:

LIKELIHOOD
the probability of an outcome

IMPACT
the effects of an outcome

Essentially, if you aren't thinking in terms of likelihood (probability) and impact (effects), you likely aren't thinking in terms of risk.

Risk is the likelihood and impact of unknown outcomes.

UNDERSTANDING LIKELIHOOD AND IMPACT

The two core concepts within risk—likelihood and impact—are themselves often misunderstood. A clearer view of these concepts is critical to a true understanding of risk.

Likelihood is the probability of an outcome.

"Possibility" is often misunderstood to be probability in this definition. What's the difference?

Probability

Scientific (mathematical) chance of something happening

Possibility

The feasibility of something happening

Probability assumes possibility, and seeks to better predict the outcome. While possibility of unknown developments is important to know when assessing probability, the two are not interchangeable.

Because of its uncertainty, likelihood is often expressed in probability or frequency within a defined period. In its more rigorous forms, likelihood can incorporate elements of certainty (e.g., confidence) and more complex mathematical models (where statistically significant data is available) to account for this uncertainty.

Likelihood is often expressed in probability or frequency within a defined period.

Impact is the practical effect of an outcome.

Impact is a wide-reaching concept, and can be applied in various ways in calculating risk. Given the wide scope of digital technology and risk management dependencies, organizations must consider various factors to accurately assess potential impact. Among other facets, impact can be considered on a spectrum of immediate (i.e., productivity losses due to downtime) and long-term (e.g., litigation) losses.

In business settings, impact is ideally realized as monetary loss, but only some existing models have been able to provide a means for organizations to reasonably measure financial impact of risk. This is the central theme within the FAIR Institute's FAIR framework, which explicitly seeks to provide financial impact as part of its philosophy.

Impact is a wide-reaching concept, and can be applied in various ways in calculating overall risk.

RISK MANAGEMENT CHALLENGES AND CONSIDERATIONS

Not all risks or strategies are created alike. Despite advances over the past 50 years in understanding and measuring risk, there remain real challenges and areas for improvement. Following are a few important considerations in risk management:

Value

An understanding of risk requires an appreciation of business criticality, which is the relative importance of a business function, product, service or asset to the organization. Risk must be evaluated in the context of what is most important or critical to achieving the strategic objectives of an organization and treated accordingly. The calculations for the likelihood and impact of a threat or vulnerability to a business process (and to the technology that supports it) depend on its importance to business objectives. For example, customer data stored in the cloud may be the lifeblood of a retail organization, while information about recreational opportunities for employees is of considerably lower importance.

Industry

An organization's risk-management capabilities may be to some extent dictated by the industry in which it operates. Many industries excel at identifying, assessing and managing specific types or sources of risk, and simultaneously struggle with others. For example, banks, credit unions and others in the financial industry, because of the nature of their business, are likely to be highly attuned to data privacy risk and to have appropriate measures in place to manage the risk. But organizations in other sectors may face greater challenges in recognizing and managing those areas of risk.

Quantification

Measuring the financial exposure related to risk is critical to all businesses and especially for digital businesses. Within organizations looking to better understand their risk, both risk-management and security teams will benefit from practical metrics for quantifying risk. Such metrics make it possible to see risk in terms of calculable impact on areas such as the cost of losses to online fraud or cyber threat, fluctuations in share price and other financial measures of business value. Where a "heat map" visualization may have once been adequate to communicate and consider risk, today's risk-management strategies are best enabled by a quantification of risk, in terms the business can understand and act upon.

Frameworks

Frameworks for assessing and managing risk, including digital risk, can be extremely useful in establishing a baseline for an organization's ability to manage risk—and mapping a path to risk-management maturity. Standards organizations like ISO, COBIT, NIST and FAIR offer a range of approaches that inform their own and other organizations' benchmarks and templates to use for this purpose. These approaches are not mutually exclusive, although many take different paths toward similar goals, and foreground some facets over others in the name of industry- and organization-specific current and desired end states.

CONCLUSION

Understanding risk means understanding business, and the need for business to think both practically and strategically at the same time. In business, the unknown abounds, and organizations of all sizes and stripes spend countless amounts of time, energy and money to understand, anticipate and mitigate the level of risk that comes with pursuing business objectives.

Understanding risk starts with the simple things: a reasonable definition to provide the bedrock of common understanding, and some points for discussion, thought and further research. A common understanding has the potential to change how organizations approach risk, with security and risk-management silos giving way to a united front for managing the risk that comes with taking on digital transformation.

ABOUT RSA

RSA® Business-Driven Security™ solutions provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. With solutions for rapid detection and response, user access control, consumer fraud protection and integrated risk management, RSA customers can thrive and continuously adapt to transformational change. For more information, visit **rsa.com.**

RSA