WHITE PAPER

CYTEX™
Unified Resilience Platform

A RISK BASED APPROACH TO CYBERSECURITY IN 8 STEPS

hello@cytex.io | https://cytex.io

Risk based cybersecurity

The news cycle these days is replete with organizations of all sizes getting hit by ransomware, data breaches, and other cyber-attacks. Cybersecurity budgets have been increasing for the last few years and will likely continue to increase for the foreseeable future. This spending has obviously resulted in organizations purchasing more cybersecurity capabilities, both as products as well as services. So, a valid question to ask is: why has the increased spending not resulted in an improved cybersecurity posture? It can be argued that the current approach to acquire more capabilities as products has increased the cybersecurity risk through application sprawl, misconfiguration risk, and alert fatigue. This might be the right time for organizations to transition from a feature-based approach to cybersecurity and adopt a risk-based approach.

A feature-based approach to cybersecurity is common and perhaps the most accepted one. For instance, an organization might implement an initiative to monitor all network traffic to reduce data exfiltration. But, in doing so, the organization will likely deploy monitoring queues to observe captured traffic, application logs, and access logs. The increase in applications will also result in workload for analysts responsible for observing and interpreting this data. Does an action like this really reduce the cyber risk or improve the security posture? Or would it have been better to selectively pick a smaller number of critical applications to observe? This leads us to tackle this as approach as a risk evaluation instead of a feature to deploy additional monitoring capabilities.

Many organizations attempt to correlate their cyber maturity with a reduction in risk. For instance, an organization that has implemented a DLP program on 30% of its assets may incorrectly assume that its data breach has been reduced the same amount. A risk-based approach to cybersecurity should focus on business value and use a common language among the stakeholders to link enterprise risks to controls and therefore help executive decision making.

Cyber risk is just another kind of an operational risk. Organizations of all sizes are adept at dealing and mitigating operational risk so cyber risk reduction should not require a new paradigm. However, cyber risk should be distinct and separate from cyber threats and vulnerabilities. Vulnerabilities and cyber threats are specific dangers that can be exploited to cause cyber risk that leads to a financial loss, data breach, reputation damage, or other impact. A common accepted definition of risk is:

Risk = Likelihood of a threat * Impact of a loss

Impact →

Likelihood ↑

	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low	Moderate	High	High	High
Likely	Low	Moderate	Moderate	High	High
Possible	Low	Low	Moderate	Moderate	High
Unlikely	Low	Low	Moderate	Moderate	Moderate
Very Unlikely	Low	Low	Low	Moderate	Moderate

The following 8 steps provide a guidance framework for organizations that want to start a risk-based cybersecurity program.

1 » Establish the risk

Establish the risk baseline by aligning the organization's objectives, resources, and risk tolerance threshold. An organization can use a framework like NIST 800-53, NIST CSF, ISO 27001, or other to identify the risk that could compromise the confidentiality, integrity, or availability of the information assets.

2 » Identify the risks

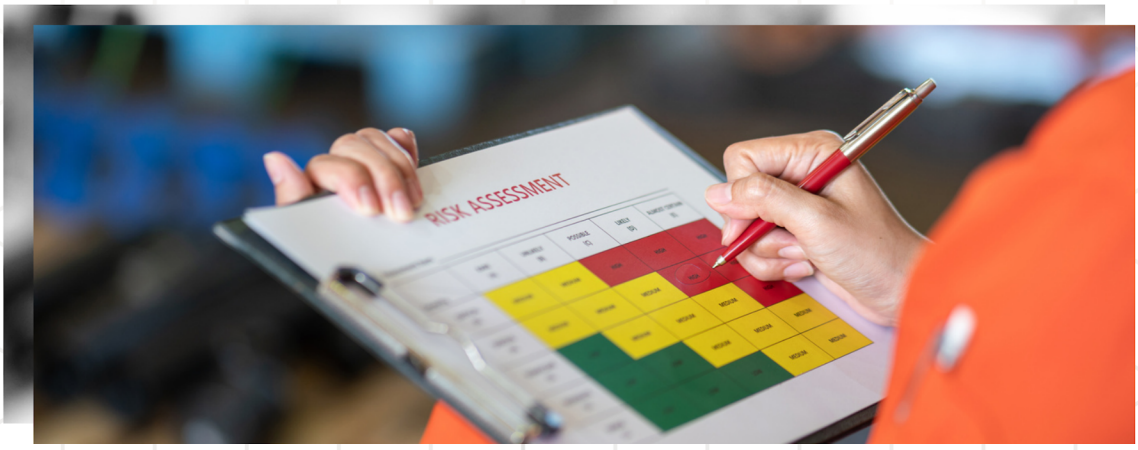
In this step, the organization should identify the source of the risk by identifying the vulnerabilities and the likelihood of these vulnerabilities to be exploited. It is important to perform a thorough review of all potential risks and vulnerabilities in on-premises devices, on-premises applications, cloud applications, and data supply chain.

3 » Estimate the risks

Risk estimation should include consideration of the causes and sources of risk in the form of threats and vulnerabilities, their impacts in term of a loss of confidentiality, integrity, availability of information, and the likelihood that the risk would materialize.

4 » Evaluate the risks

Using the risk levels computed in the previous step, the organization should establish an acceptable risk threshold to stratify the identified risks. Identification of the risks that are outside the acceptable threshold provides a pragmatic approach to prioritize the remediation process.



5 Establish the risk

For each of the evaluated risks, the following options can be considered:

- Risk reduction: Reduce the risk impact by remediating the vulnerability that may be exploited to result in this risk.
- Accept the risk: If the risk impact is within the acceptance threshold, then a risk may be accepted without any remediation.
- Risk avoidance: Identify the activity that may result in this risk and avoid it.
- Risk transfer: It may be determined that a risk can be transferred to another party, who will be responsible for the risk reduction or acceptance.

6 Risk acceptance

For every risk that is accepted, the organization must accept review, approve, and monitor the risk treat plan and continuously evaluate the residual risk to determine if it still within acceptable limits.

7 Risk monitoring

The risk monitoring process should review the security risks.

8 Risk consultation

Develop a risk communication and consultation plan with all the stakeholders early in the process. The plan should include a discussion of the risks, causes, impact, remediation steps, and task assignments.

Cytex Risk Assessment Tool

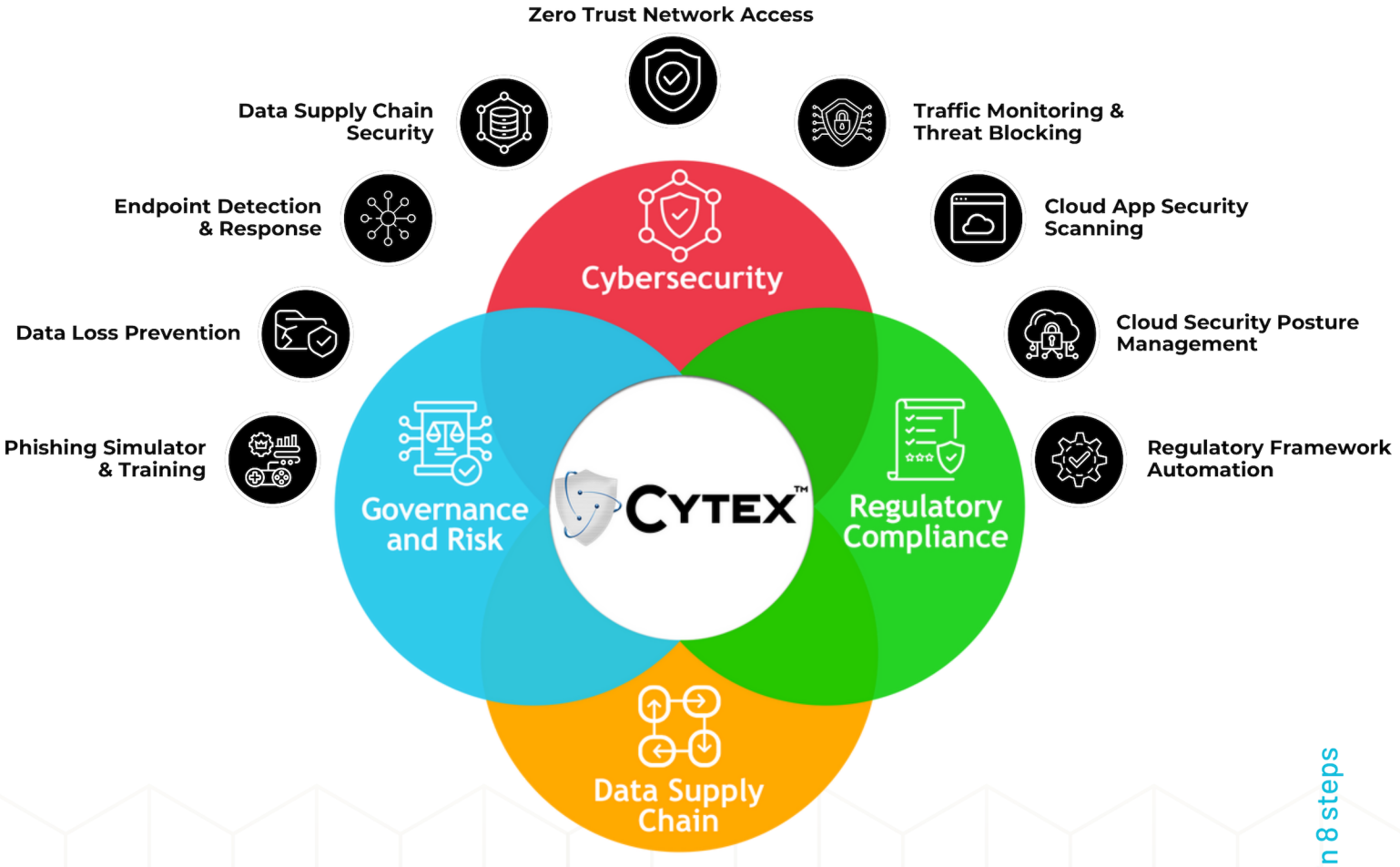
Take the next steps towards adopting a risk-based approach by utilizing a dynamic risk assessment tool developed by Cytex, Inc.

Take the guess work out & identify areas that need to be strengthened.

https://risk.cytex.io

CYTEX™

Unified Resilience Platform



https://cytex.io hello@cytex.io @cytexsmb @cytexsecure cytex-inc