



Risk-Centric Cybersecurity Management :

A Methodology to Build Lasting, Intelligent Cybersecurity Programs

A Brinqa eBook

Think InfoSec is ready to keep your enterprise secure through the next transformative tech trend? Think Again!

Over the next 5 years, as technology completely transforms every facet of business, information security organizations will be thrust to the forefront of the enterprise. Most InfoSec organizations, created and structured for what was traditionally a supporting function, are struggling with this new role in the limelight. Rapid digital transformation, proliferation of cloud infrastructure, SaaS, explosive growth of mobile computing power, IOT and other emerging trends have already begun to put tremendous strains on existing InfoSec systems and processes. There is growing pressure on InfoSec organizations to evolve and keep up with this rapid pace of change.



70% OF THE GLOBAL 2000 ARE ILL-EQUIPPED

to securely benefit from the latest transformative trends in technology. As technology becomes a distinct competitive edge, enterprises will be measured by the ability to adapt and take advantage of the latest technological advancements, along with the capability to protect, secure and maintain this crucial, yet vulnerable, agent of change.

So how can InfoSec prepare to better secure the enterprise through transformative experiences?
Read on to learn more about a methodology for building risk programs that deliver lasting value and security.

Increased prominence, dynamic ecosystems, and high-profile breaches demand a paradigm change for InfoSec

Information security organizations and leaders have seen a meteoric rise in significance and prominence as IT ecosystems are changing at a more rapid pace than ever before. In the past few years, there have been a spate of high-profile breaches and attacks that have cost businesses billions of dollars in revenue and inestimable injury to growth and productivity. All of this puts tremendous pressure on InfoSec organizations and leaders to demonstrate that they are taking measures to protect the enterprise.

Lost productivity and lost growth caused by cybercrime led to \$3 Trillion of market value destroyed in 2015 ~ Satya Nadella, CEO, Microsoft

The common response from InfoSec organizations has been to aggressively increase spending for security tools and services. This is an encouraging sign, but when undertaken without a well-defined strategic framework this approach can create more problems than it solves. Most InfoSec organizations and programs suffer from a range of problems symptomatic of this oversight: siloed systems and processes, information overload, lack of consistency in efforts, lack of a cohesive formal security strategy, high operational overheads, lack of communication, and more.



Siloed Systems and Processes



Information Overload



High Operational Overhead



Lack of Communication

'Risk Management' presents the ideal framework to address these challenges and implement strategic planning and tactical management of cybersecurity systems and programs.

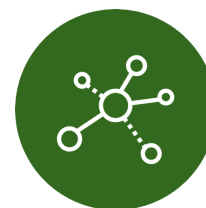
The Why: 'Risk' as an ideal strategic driver and tactical measure for cybersecurity planning & management

With its emphasis on structure, transparency, extensiveness, certainty and adaptability, Risk Management is an ideal model for cybersecurity programs. Core risk management principles such as creating value, being an integral part of organizational and decision-making process, being systematic, processing accurate and extensive information, and continuously monitoring and improving are directly applicable to InfoSec programs.

Cybersecurity programs that put 'Risk' at the core realize tangible benefits



Improve visibility into IT infrastructure and processes



Represent & communicate the relationship between critical business functions and technology assets



Prioritize the most critical, impactful and imminent threats, events and weaknesses



Automate and streamline remediation efforts



Communicate the business impact of security costs and efforts



Improve communication between teams, departments and stakeholders

Vulnerability Management: A Study in Risk

Network and application layers are a prominent attack surface for malicious actors, making vulnerability management one of the most significant components of any InfoSec organization. Vulnerability management refers to the analysis of information from network and application asset repositories and vulnerability scanners to identify weaknesses within the IT infrastructure where security practitioners should focus efforts to secure and harden the IT environment. Since 'Risk' is inherently subjective, a program centered on risk ensures the identification of key stakeholders in the process and resolution of their primary concerns. Consider 3 critical questions that all vulnerability management programs should ask, and what it takes to answer them.



Which vulnerabilities, if exploited, pose the greatest risk of disrupting critical business functions?

Incorporate business context, from CMDB, HR and other business organization systems in the enterprise to understand the real significance of assets and the true impact of vulnerabilities. Incorporate information about business and functional hierarchy - Locations, Departments, Business Lines, Product Lines, Services, Processes, Applications etc.



Which vulnerabilities, if exploited, pose the greatest risk of exposing vital or confidential data?

Incorporate information from existing data protection programs and systems to understand the risks faced by the organization's' lifeblood - internal and customer data. Integrate data from DLP systems, data segmentation, network segmentation, business continuity/disaster recovery (BC/DR), Data Lifecycle Management (DLM) systems and programs.

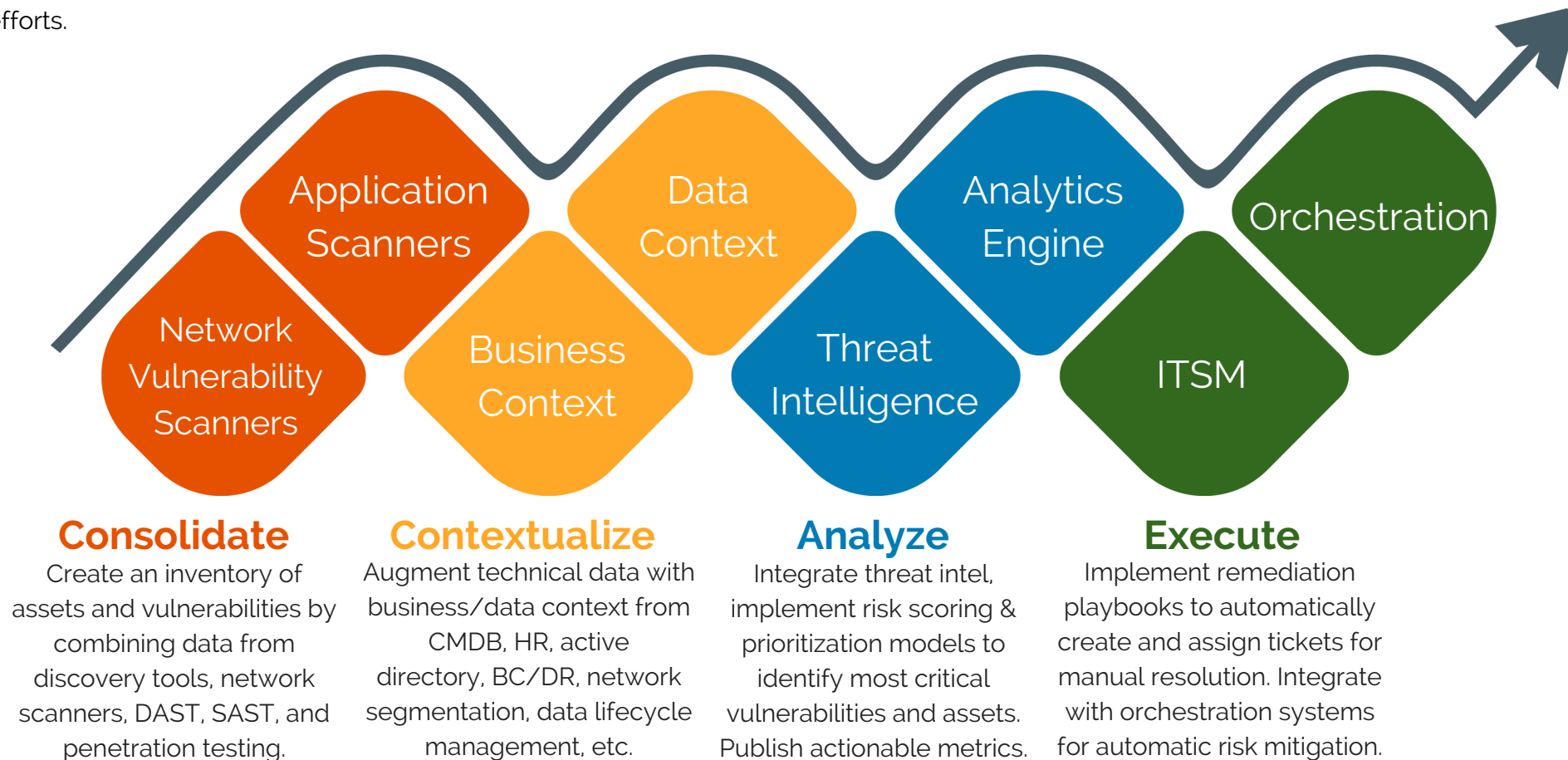


Which vulnerabilities stand the greatest risk of being exploited?

Incorporate organized, analyzed and refined information about current and potential attacks to understand the likelihood of a breach and the urgency with which to address a vulnerability. Incorporate data from the multitude of publicly available and private Threat Intelligence that provide an understanding of the most common and severe threats, such as zero-day threats, advanced persistent threats (APTs) and exploits.

The How: Implementing a Risk-Centric Vulnerability Management Program

After identifying the key stakeholders, primary risk concerns, and the sources of relevant in-scope information, InfoSec organizations can begin to put all these components together into a cohesive program. Central to the program is an analytics system capable of automatically consolidating and correlating all the relevant information sources in scope for the program. The analytics component also defines and implements the algorithms that prioritize assets and vulnerabilities for remediation. The program automatically engages and informs all relevant stakeholders and facilitates prioritized remediation by integrating with systems that manage manual and automated remediation efforts.



Consolidate

Create an inventory of assets and vulnerabilities by combining data from discovery tools, network scanners, DAST, SAST, and penetration testing.

Contextualize

Augment technical data with business/data context from CMDB, HR, active directory, BC/DR, network segmentation, data lifecycle management, etc.











Analyze

Integrate threat intel, implement risk scoring & prioritization models to identify most critical vulnerabilities and assets. Publish actionable metrics.

Execute

Implement remediation playbooks to automatically create and assign tickets for manual resolution. Integrate with orchestration systems for automatic risk mitigation.

The How: Blueprint for a Risk-Centric Cybersecurity Management Program

-  Identify all technology asset types and sources in scope for the program
-  Identify all security monitoring and assessment tools in scope for the program
-  Identify all relevant business, technology, environmental contexts for in-scope asset types
-  Integrate data from asset, monitoring, and assessment sources and correlate all relevant contexts
-  Execute algorithms for risk evaluation, prioritization and insights
-  Identify and engage processes, systems and users to be leveraged for risk remediation
-  Implement play-books and strategies for manual remediation efforts
-  Orchestrate automatic risk remediation
-  Create targeted metrics and dashboards, Inform and engage ALL relevant stakeholders
-  Execute continuously and automatically

Empower InfoSec to be a crucial contributor to secure, sustained business growth

Take Charge Today!

- Empower security professionals and subject matter experts to have a positive impact on business growth
- Implement Risk-Centric Cybersecurity Management to represent the true impact of InfoSec efforts
- Support security leaders with information required to communicate effectively at the highest levels of the enterprise

Brinqa Can Help!

Brinqa Risk Platform is the ideal framework for building risk-centric cybersecurity management applications. With powerful risk modeling capabilities, extensive connectors list, advanced graph analytics, and user-friendly visualizations, Brinqa takes InfoSec programs to new levels of efficiency and productivity. Brinqa Threat & Vulnerability Management, Application Security Risk Management, Vendor Risk Management, IT Risk Management, and Risk Analytics applications are built on the principles outlined in this document and trusted by industry leaders.

Learn more about Brinqa Risk Platform and Applications at www.brinqa.com
Contact Brinqa at info@brinqa.com