eBook

Prioritization Secrets of Top CISOs

What makes the difference between a good CISO and a top CISO?

Balbix®

The Eisenhower Decision Matrix, also known as the Urgent-Important Matrix, is a powerful tool for time management and prioritization, widely attributed to Dwight D. Eisenhower, Supreme Commander of the Allied Expeditionary Force in Europe during WWII and the 34th President of the United States. It's a simple yet effective framework that helps leaders, including Chief Information Security Officers (CISOs) prioritize tasks based on their urgency and importance. The difference between a good CISO and a top CISO often lies in their ability to apply such principles of ruthless prioritization and delegation to their cybersecurity strategy and operations.

As a political and military leader, Eisenhower had a few insights into security as well as leadership:

Eisenhower Decision Making Matrix

Given the evolving nature of the threats and limited cyber resources, security teams can never be able to achieve perfect security. However, through prioritization and optimization CISOs can maximize the effectiveness of what they do have, turning a rag-tag assortment of technologies, processes and people into a well organized and effective fighting force.

So, what are those top CISOs' priorities?

The Balbix research team recently surveyed a number of top Fortune 1000 CISOs to determine how they prioritize and delegate tasks to achieve better cyber risk outcomes and organizational resilience. This blog details the results and implications of their responses.

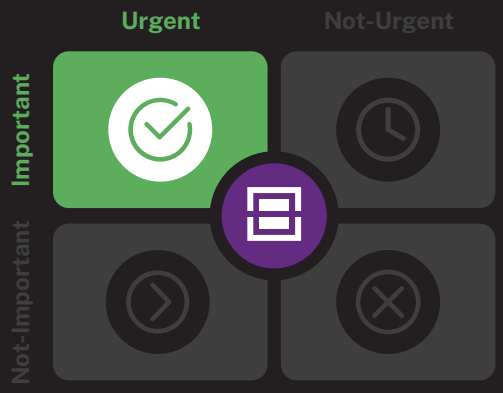
The Eisenhower Decision Matrix Explained

The matrix divides tasks into four quadrants based on two criteria: urgency and importance.

	Urgent	Not-Urgent
Important	**Do-It Now** These tasks are critical and require immediate action. For a CISO, this includes responding to breaches, compliance deadlines, or immediate threats to the organization's assets.	**Schedule It** Essential for long-term resilience, these tasks don't need immediate action. They include developing cybersecurity awareness, planning infrastructure upgrades, or new security policies. Top CISOs focus here, planning and investing in their organization's future security posture.
Not-Important	**Delegate It** These tasks, while requiring attention, minimally impact security strategies. They often involve operational activities or minor issues that other team members can address. Delegation enables the CISO to concentrate on strategic matters.	**Eliminate It** These tasks offer little to no value and can be considered distractions. This could include redundant reports, unnecessary meetings, or tasks that could be outsourced. These consume time and do not contribute to the security posture.

Quadrant 1

Urgent and Important
(Do it now)



Survey Question

For an effective cyber risk management program, which activities are urgent and need to be handled immediately by the CISOs themselves?

"I think every CISO would agree that responding to a security incident requires immediate attention, especially in light of the regulatory requirements around breach notifications. Time is of the essence as it pertains to security incident response activities."

Dina Mathers,
CISO at Carvana

CARVANA

Top 3 responses (activities)

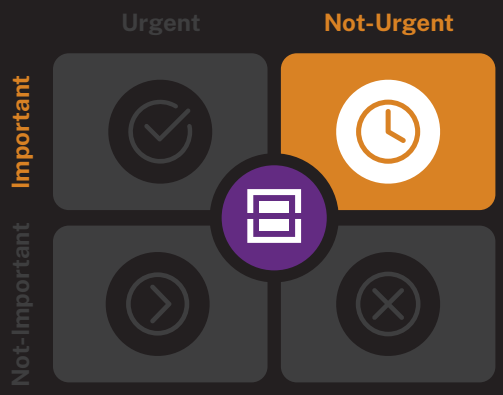
- Respond to a recent breach, ransomware or disruption.
- Build and deliver board reports.
- Determine materiality for SEC 8-K and 10-K reporting

Insights

The top activities in this quadrant emphasize the critical nature of immediate action and personal oversight by CISOs in the face of active threats and compliance. Responding to breaches showcases the necessity of swift, decisive action to mitigate damage. The emphasis on board reports and SEC filings underlines the importance of communication and transparency with stakeholders regarding the organization's cybersecurity posture. This highlights a strategic aspect of the CISO role, balancing hands-on crisis management with navigating regulatory requirements and maintaining trust at the executive level.

Quadrant 2

Important but Not Urgent (Schedule it)



Survey Question

For an effective cyber risk management program, which of these activities do you consider essential but not urgent? As a CISO, you would do these yourself but need to schedule time for them rather than do them immediately.

Top 3 responses (activities)

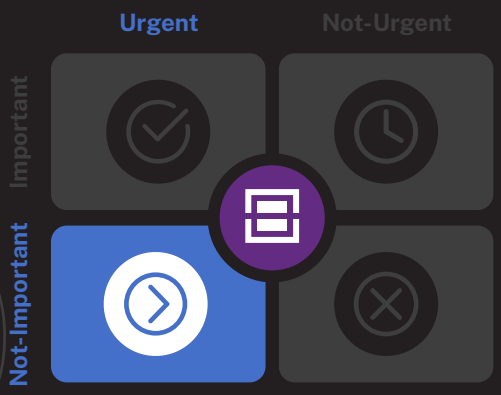
- Establish and report KPIs to show the effectiveness of the cybersecurity program.
- Measure maturity against NIST and other similar frameworks.
- Identify and plan for emerging security threats.

Insights

The top activities in this quadrant reflect a strategic, forward-looking approach to cybersecurity. Establishing and reporting KPIs, measuring against frameworks like NIST, and planning for emerging threats are all critical for long-term cyber resilience. These tasks require thoughtful analysis and planning, underscoring the importance of a proactive and metrics-driven approach to security. By scheduling these activities, CISOs can ensure continuous improvement and alignment with best practices, ultimately strengthening the organization's cybersecurity framework without the pressure of immediate deadlines.

Quadrant 3

Urgent but Not Important (Delegate it)



Survey Question

Which of the following activities would you delegate to the security team?

Top 3 responses (activities)

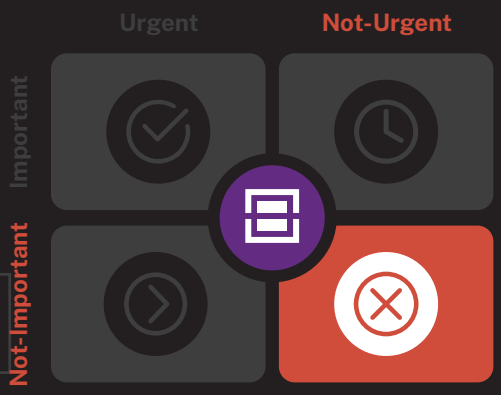
- Automate vulnerability remediation and find a tool for it.
- Automate security alerts and resolution.
- Regularly review and update security policies and procedures.

Insights

The top activities in this quadrant underscore the significance of automating operational cybersecurity tasks to enhance efficiency and effectiveness. By automating vulnerability remediation and security alert resolutions, CISOs can delegate these critical yet time-consuming tasks to technological solutions, freeing up valuable time to focus on more strategic initiatives. This automation ensures that the organization can swiftly address potential threats without necessitating constant manual oversight, thereby maintaining a robust security posture with optimized resource allocation. The emphasis on regularly reviewing and updating security policies and procedures highlights the importance of keeping the organization's cybersecurity framework adaptive to evolving threats and compliance requirements. Delegating these reviews to trusted team members ensures that policies remain current and effective, while allowing the CISO to oversee strategic cybersecurity direction rather than getting mired in the details of policy management.

Quadrant 4

Neither Urgent Nor Important (Eliminate it)



Survey Question

Are there any activities or tasks that CISOs and security teams do that should be deleted?

Top 3 responses (activities)

- Outsource training
- Focus less on technology, more on the business.
- Focus less on prevention and response, more on resilience and recovery.

Insights

The activities that should be eliminated from the security team indicate a need to shift focus towards more strategic elements of cybersecurity management. Outsourcing training suggests a move towards efficiency and leveraging external expertise. The advice to stop focusing solely on technology points to the importance of a holistic view encompassing people, processes and technology within the business context.

Finally, the shift from prevention and response to resilience and recovery reflects a strategic pivot towards ensuring business continuity and adaptability in the face of cyber threats. These insights recommend reevaluating priorities to eliminate outdated practices and focusing on actions that contribute to the organization's resilience.

Three Ways The Matrix Helps CISOs Make Better Decisions

Enables Strategic Focus and Prioritization

The matrix helps CISOs distinguish between tasks that are critical for immediate action and those that, while important, do not demand immediate attention. By identifying tasks that are urgent and important, CISOs can prioritize actions that directly mitigate cybersecurity risks or comply with regulatory requirements, ensuring that resources are allocated to the most pressing issues first. This prioritization not only aids in immediate threat mitigation but also ensures that strategic projects, such as planning for emerging security threats or measuring maturity against frameworks like NIST, are scheduled appropriately without being overlooked in the daily operational demands.

Facilitates Efficient Resource Allocation

By categorizing tasks into quadrants, the matrix allows CISOs to make informed decisions on resource allocation, including time, personnel, and budget. For instance, tasks that are urgent but not important can be delegated to other team members or automated, as suggested by responses advocating for automation of vulnerability remediation and security alerts. This delegation frees up the CISO's time for more strategic endeavors and ensures that the cybersecurity team's skills are utilized where they can have the most significant impact. Similarly, identifying tasks that neither are urgent nor important highlights areas where resources may be wasted, guiding CISOs to eliminate these tasks and reallocate resources to more valuable activities.

Promotes Proactive Rather Than Reactive Management

The matrix encourages CISOs to engage in proactive management of cybersecurity threats and compliance obligations. By scheduling important but not urgent tasks, such as identifying and planning for emerging security threats, CISOs can shift from a reactive posture to a more anticipatory approach. This forward-looking perspective enables the development of comprehensive strategies to address potential vulnerabilities before they are exploited and ensures that the organization is prepared for future regulatory changes. Additionally, the focus on strategic planning helps build a culture of continuous improvement within the cybersecurity team, fostering innovation and resilience.

How Can Balbix Help CISOs Prioritize?

Balbix aids CISOs in prioritizing and delegating tasks through AI-driven risk assessment, actionable insights, and automated workflows. By highlighting critical vulnerabilities and compliance gaps, CISOs can allocate resources efficiently. Automated workflows streamline tasks like vulnerability remediation, freeing up time for strategic initiatives. With delegation features and customizable dashboards, CISOs can collaborate effectively with their teams and track progress. Balbix ensures informed decision-making and enhances cybersecurity posture, empowering CISOs to address the most pressing issues swiftly and effectively and delegate or eliminate those that are less critical.

Quadrant 1 *Urgent and Important (Do it now)*

Balbix can help you quickly address these high-priority tasks by enabling you to...

- Quickly burn down cyber risk with prioritized patching, streamlined workflows, and gamification.
- Demonstrate the effectiveness of security controls and communicating ROI of your cybersecurity programs to the board.
- Determine materiality to comply with SEC and other cybersecurity regulations.

Quadrant 2 *Important but Not Urgent (Schedule it)*

Balbix can help you prioritize these high-priority, non-urgent tasks by enabling you to...

- Analyze the ROI of your cybersecurity tools and programs by gaining insight into risk reduced with a specific initiative such as improving coverage of EDR.
- Track your progress against a framework such as NIST by providing visibility into assets, vulnerabilities, controls, threats and others that comprise the 'identify' function.
- Evaluate and assess the risk associated with different business units, locations, assets, etc. and then analyze security controls for efficacy against vulnerabilities present in your environment.

Quadrant 3 *Urgent but Not Important (Delegate it)*

Balbix can help your security team members address these urgent, delegated tasks by enabling them to...

- Use severity, threats/exploits, external exposure, security controls, and business impact to prioritize vulnerabilities for efficient remediation.
- Integrate with ticketing platforms to create remediation tickets with fix/patch information, owners, and priority, significantly improving the time to remediate vulnerabilities.
- Generate reports on vulnerabilities, misconfigurations and control gaps by business units, locations, and mission-critical assets to ensure compliance with security policies and SLAs.

Quadrant 4 *Neither Urgent Nor Important (Eliminate it)*

Balbix can help eliminate unnecessary tasks...

- With monetary measures for cyber risk, CISOs can improve communications and credibility with senior executives and better align security budgets with risk to eliminate unnecessary activities and spend that aren't measurably reducing risk.

Conclusion

The distinction between a good CISO and a top CISO lies in their ability to prioritize effectively, focusing on tasks that significantly impact the organization's cybersecurity posture. By adopting the Eisenhower Decision Matrix, CISOs can ensure they are not merely reactive but are proactively steering their organization toward a secure and resilient future. This strategic prioritization is what enables top CISOs to make a profound difference in their roles, transforming cybersecurity from a defensive necessity into a strategic advantage.

"For years, CISOs have been told that in order to have or keep a seat in the boardroom, you must be able to speak the language of the business but most times, there isn't practical guidance on how to do that effectively. Our investment in Balbix takes the guesswork at translating cyber risk into quantifiable impact based on our business context, which allows me to have more productive and effective conversations with various stakeholders across the business by sharing stories on how our overall security program has evolved and matured over time."

CARVANA

Dina Mathers
CISO at Carvana

Request a demo to learn more about how Balbix helps CISOs prioritize cyber risk.

Balbix®