



3967945  
2.126548  
1.312658  
8.674424

**CREATING A  
RESULTS-ORIENTED  
CULTURE BY  
MEASURING WHAT  
MATTERS**

The background is a dark blue gradient with various data visualization elements. On the left, there is a list of numbers: 3967945, 2.126548, 1.312658, and 8.674424. Below these numbers are several line graphs and bar charts. In the bottom right corner, there is a large, faint icon of a padlock, symbolizing security or protection.

**Jack Nicholson**

# CONTENTS

<b>03</b>	<b>INTRODUCTION: THE PROOF IS IN PERFORMANCE</b>
<b>04</b>	<b>STEP 1: BE PROACTIVE &amp; FOCUS ON WHAT MATTERS</b>
<b>05</b>	<b>STEP 2: KNOW YOUR STAKEHOLDERS</b>
<b>06</b>	<b>STEP 3: CREATE A PLAN</b>
<b>07</b>	<b>STEP 4: IMPLEMENT &amp; REPORT</b>
<b>08</b>	<b>GET STRATEGIC SECURITY SUPPORT NOW</b>
<b>09</b>	<b>ABOUT THE CISO</b>

# THE PROOF IS IN PERFORMANCE

---

As an information security leader, you're all too familiar with the challenges that impede progress inside your remit.

## Past & Future Budgeting

As with other organizational leaders, information security executives and managers must account for how the past year's budget was spent and make a business case for the following year's budget. Sadly, this is often a catch-22. On the one hand, the perception is that the absence of cybersecurity incidents doesn't justify more budget (and even creates curiosity into why you have as much budget as you do). On the other, you can't get more budget for preventive tooling or team growth when nothing has happened to justify them.

## Presentation & Communication

InfoSec leaders looking to grow their departments and capabilities must make their case to boards and other executives. And for the reasons listed above, this is often more difficult than it seems. Their perception is that you don't need more when all is well, and yet you know the only reason all is well is because your team and tools prevented threats from becoming actual problems. Being able to share the story of what you've accomplished and using that as a framework for the future is not a resource technology leaders often have, let alone a communication skill set to present effectively.

## Team Accountability & Reporting

At all times throughout the year, there are countless projects and tasks that your teams must tackle — security-related or not. Many come up as emergencies — distracting tech teams from what they should be doing. All too often, it can be difficult for technology leaders to demonstrate progress on their strategic goals because of this. In order to demonstrate progress, you and your team must take accountability for your projects, put processes in place to measure them, and be ready to say "no."

**In this white paper, we'll break down four steps tech leaders can take to overcome these challenges, creating a results-oriented culture built on a foundation of metrics and reporting that supports its own long-term goals.**

# STEP 1: BE PROACTIVE & FOCUS ON WHAT MATTERS

As an InfoSec leader, change starts with you.

## Be the Leader Your Team Needs

The first step in this journey is to understand that your team itself won't solve these challenges for you. Whether they're already rockstars in their own ways, or if they could use some improvement, "better" must begin with you stepping up as their leader. Remember, "There are no bad teams. Only bad leaders." (Jocko Willink)

While the goal of this process is to create a framework of metrics for reporting and change, the first metric you need to track is yourself. You will need to shift your focus from trying to influence the things you can't control (e.g. outside needs) to the things you can control (e.g. department goals). Use the framework below to evaluate your efforts each day.

Manage Yourself		Evaluate Yourself
Where/how do you spend time/energy each day?	What concerns you and what can you influence?	Ask yourself these three questions every day.
1. _____	1. _____	1. Did I do my best to spend my time on things I can influence?  2. Did I do my best to set and communicate clear goals?  3. Did I do my best to make progress toward goal achievement?
2. _____	2. _____	
3. _____	3. _____	
4. _____	4. _____	
5. _____	5. _____	
6. _____	6. _____	

Connect items that correlate between all three columns with a line. Each line represents a success. Through this exercise, you'll begin to discipline yourself to focus on higher priority tasks and goals. In doing this, you'll remove complexity from your list, be able to prioritize what matters, and focus on the things that provide a bigger return.

# STEP 2: KNOW YOUR STAKEHOLDERS

What matters to stakeholders must matter to you.

## Know How to Solve the Right Problems

The aim of InfoSec is protecting assets in the stewardship of others. This crosses company and customer lines, as you're responsible for protecting the business' technology infrastructure (which connects with its bottom line) as well as customer data (the loss of which can bring a company to its knees). Understand the responsibility given to you, and ensure that what you're focusing on as an InfoSec leader is what protects and supports it.

But how can you learn what matters most to stakeholders? Effective leaders will take the time to understand stakeholders and their pain points. This is where the human part of your role comes in. Whether through interviews, meetings, or surveys, make an effort to understand what your stakeholders' greatest concerns are. Below are some questions designed to guide the conversation to help you get to the root of the problem.

Questions To Ask Stakeholders		What Their Responses Might Mean
1.	Tell me more about the problem.	Longer responses may demonstrate severity.
2.	Can you be more specific or provide examples?	Examples prove it's a real business challenge.
3.	How long has this been a problem?	Long-term problems may reveal deeper challenges.
4.	What's been done about the problem already?	Reveals whether others feel it's a priority, too.
5.	Did those efforts work? Why or why not?	Reveals what solutions to try or avoid.
6.	How much has this problem cost you?	The more money spent, the greater the priority.
7.	How does this problem make you feel?	Demonstrates how the problem impacts their goals.
8.	Have you given up trying to solve this problem?	Is it a priority anymore? Or an opportunity for a win?

Remember, "The day people stop bringing you their problems is the day you have stopped leading them." (Colin Powell) Don't forget that the stakeholders and employees you're serving are your customers. They will forget what you did long before they forget how you made them feel. Treat them well, and they will become your advocates and supporters, helping you improve your efforts and supporting the solutions you put in place.

# STEP 3: CREATE A PLAN

---

Use plans to drive results and share successes.

## Creating a Problem Statement

A problem statement clarifies the current situation by identifying the problem and its severity, likelihood, and impact. It also serves as a communication tool — helping to get buy-in and support from others. Note that depending on your challenges, you may have one or more statements of varying complexity. Some may be more strategic than others.

While defining a problem is half the challenge, it's important to not fall into the trap of inaction. The problem statement is meant to be the springboard for what comes next. Often, this can be difficult to map out. Here are some recommendations for next steps following the development of the problem statement.



**Invest Time in Planning** — Time spent clarifying and understanding the problem is never wasted. Spend time planning the project parameters and goal and doing your due diligence so you and your team know what to do and what to expect.



**Create a Project Charter** — Once you fully understand the problem and what lies ahead, formalize the plan with a charter. Clearly state the scope, objectives, participants, and success measurements.



**Create a Work Breakdown Structure** — Projects can be difficult for teams to process, so creating a graphical representation of scope broken down into chunks with defined deliverables and accountabilities will give your team clarity.



**Use Lean Principles** — Originally created for manufacturing, lean also applies to cybersecurity. Lean focuses on the process (not the person) when a problem arises. It also measures what you want to improve — not just measuring for the sake of it.

## Things to Consider

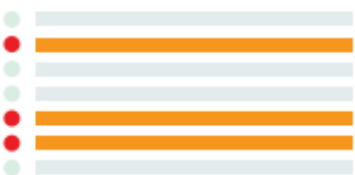




How you prioritize work to solve challenges must consider what's truly urgent — i.e., in alignment with stakeholder concerns. These efforts must come first. The metrics you include in your problem statement must be measured over time as well. Not monitoring them as you move forward could lead to project derailment. Monitoring them also empowers your team to stay on track and streamline the path to success.

# STEP 4: IMPLEMENT & REPORT

Creating the culture of shared success — not blame.

## Lead Your Team and Work Together to Solve Problems

With your problem statements identified, it's time to get to work. Remember, you're not meant to do all of the work yourself or move forward without tracking progress. Set recurring meetings and standups at intervals that make sense to check progress. Only focus on what needs to be addressed now to move projects forward. Below are some reporting solutions that support this effort so you can keep your team charging ahead.

	<p><b>The Pain Points Board</b></p> <p>Each team should have a project board that shows pain points and where work stands to solve them. Tasks should be marked green or red. In each meeting or standup, focus only on red (i.e. at risk, urgent, needs input).</p>
	<p><b>Pareto Charts</b></p> <p>The Pareto Principle states that, for many events, roughly 80% of effects come from 20% of causes. The same goes for cybersecurity. Identify the problem causes and prioritize solving them (aligned with stakeholder concerns). This will help reduce incidents and vulnerabilities.</p>
	<p><b>Internal Report Cards</b></p> <p>Services are available that can grade your security efforts on the A-F scale. The aim should be obvious: as many As as possible. This creates a public feedback loop that keeps teams motivated and focused on what matters.</p>
	<p><b>Industry Report Cards</b></p> <p>Internal report cards are great for supporting teams, but industry report cards help board members understand how your company stands in relation to others. These can also be used to motivate teams internally.</p>
	<p><b>Nist Cybersecurity Framework</b></p> <p>The National Institute of Standards and Technology built this framework as guidance for improving the ability to prevent, detect, and respond to attacks. It features best practices and has become a baseline for best practices by companies in assessing legal or regulatory exposure.</p>

# GET STRATEGIC SECURITY SUPPORT NOW

You're not alone in this effort. We're here to help.

## Inversion6® Partners with Leaders Just Like You

Never before has cybersecurity been so strong a focus for company boards and executive teams. With just one mistake or oversight, companies' operations can be brought to an immediate halt as the public and regulatory agencies apply pressure to solve the problem once and for all. With countless data records and millions of dollars at stake with each vulnerability that goes unaddressed, now is the time to partner with cybersecurity experts to both support and extend your internal cybersecurity capabilities.

Inversion6® is a leading provider of CISO services, managed security, network support, and storage solutions. Headquartered in Northeast Ohio, we've been partnering with companies in multiple industries to support their leadership teams and cybersecurity leaders in developing strategy and tactical response for more than 30 years.

## How We Can Support Your Efforts

We Support Your Strategy	We Bring the Solutions with Us
Your organization has strategic goals. Cybersecurity should protect and support them. We partner with your leaders to understand what you're looking to achieve and implement solutions to ensure those goals are met securely.	MRK Technologies has partnered with numerous security solutions providers, allowing us to implement the security systems you need for threat detection, vulnerability scanning, email security, network scanning, and more.
We Emphasize Communication	We Create Security-Focused Cultures
Our CISOs are more than cybersecurity experts — they're proven leaders with decades of experience in helping boards, executives, and employees understand and manage cybersecurity strategy throughout the entirety of an organization.	From incident response planning and tabletops to complete security program management, our team is committed to helping you identify the risks present in your technology environment and helping everyone do their part to prevent them.

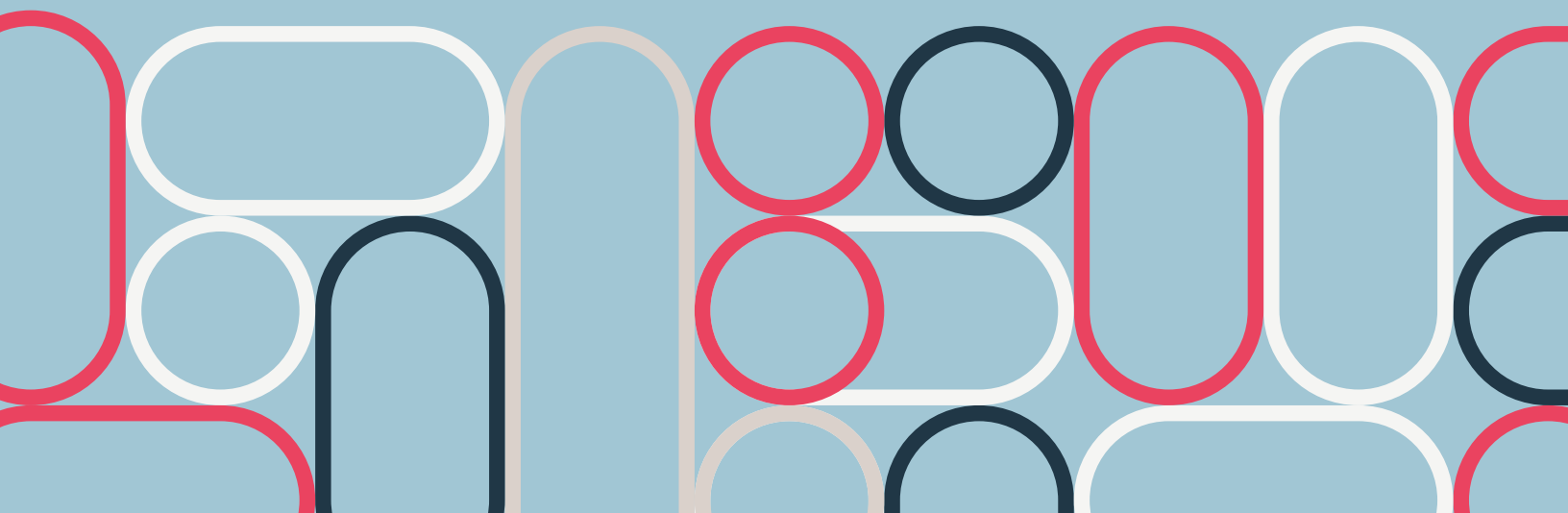


# ABOUT THE CISO

## **Jack Nicholson** CISO

Jack Nicholson is an experienced CISO practitioner and technology executive with 25 years of experience in the government, financial and manufacturing sectors. His roles have included leading transformation and management of information security and IT infrastructure, data management and more for organizations in numerous industries. Jack earned recognition as one of the People Who Made a Difference in Security by the SANS Institute and received the CS050 award for connecting security initiatives to business value. He's been a CISO for Inversion6® since 2018, and now leads our efforts as a CMMC Registered Practitioner. Jack holds an Executive MBA from Baldwin-Wallace University, where he is an adviser for its Collegiate Cyber Defense Competition (CCDC) team.

Connect with Jack on LinkedIn





## ABOUT INVERSION6®

Inversion6® provides customized security solutions to support your internal security efforts. Whether you're looking for CISO, MSSP, or security software guidance, Inversion6® partners with you to keep your company safe. Dedicated to long-term service, Inversion6® will work to protect your organization relentlessly — every hour of every day — by investigating and detecting potential threats, then communicating those concerns and finally by eliminating security issues.

With an entire suite of services and programs, we provide a managed security solution that will monitor and resolve information security threats around the clock to add a new level of protection for your organization.

With our innovative CISO for Hire platform, we partner clients with high-level information security executives to manage and guide your security needs and responses alongside your own team. We also offer network solutions, forward-thinking security measures, and dedicated storage solutions as part of the breadth and width of services and products we provide.

### Get in touch

216.535.4100

[info@inversion6.com](mailto:info@inversion6.com)