FROM TECHNICAL ANALYST TO BUSINESS ENABLER:

What CISOs Must Have to Lead the Company

ProcessUnity

PROCESSUNITY WHITE PAPER

CONTENTS

ProcessUnity

01 INTRODUCTION

If You're Not Leading, You're Losing

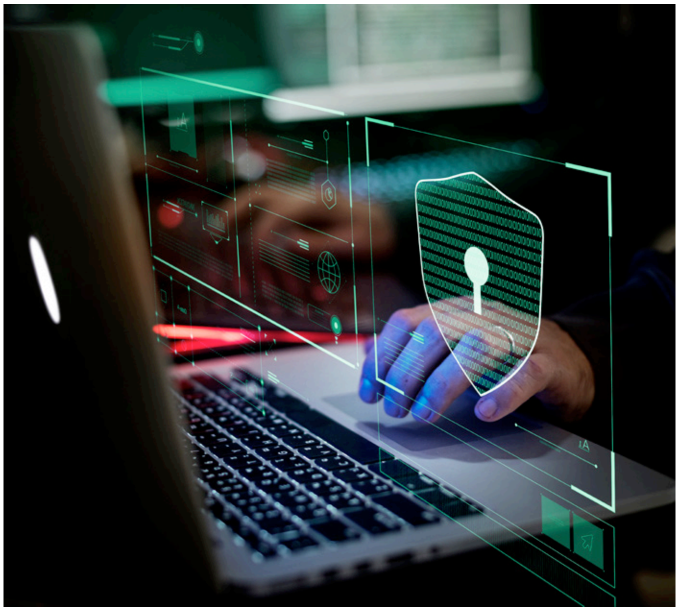
Not that long ago, the people responsible for cybersecurity labored behind the scenes, called to the front office only when the status quo had been compromised.

Today, many third-party risk managers have been elevated to Chief Information Security Officers (CISOs), achieving a significant status within the status quo itself.

Yet many forward-looking CISOs are hindered by workflows rooted in the past. Despite enormous changes wrought by the sheer increase in threat volume and the influence on key business decisions, many CISOs continue to act tactically when they are required to think, manage, and communicate strategically.

To some extent, this leadership gap can be attributed to novelty: the CISO is a new executive role whose parameters are still being defined. But to an even greater extent, the CISO has been hampered by tools designed to address the old problems risk managers face, not the new responsibilities CISOs have.

In this paper, we'll explore the changing role of the CISO, articulating why tactical management must be replaced by strategic leadership, and how CISOs can apply a new generation of technology to bridge the gaps between raw data collection and the actionable insights decision makers need to lead.



02 CHANGING ROLE OF CISO

A Transformed Landscape Means A Transformed Role

If CISOs want to lead, they can't continue to function from the back room. The nature of the role has changed precisely because the nature of the challenge has changed:

Addressing The Increasing Complexity of The Risk Landscape

There are simply more threats (phishing, ransomware, ID theft, etc.) coming from more actors from differing angles. The proliferation of a greater variety of devices (mobile, tablets, IoT) and the expanded reach of cloud computing and cloud-based applications has exponentially increased the surface area of risk exposure. In response, cybersecurity relies on a greater variety of tools deployed in a wider range of environments. Today's CISO can no longer rely on tools alone, but must manage a complex team of experts monitoring a much broader risk landscape.

Going Beyond Tactics and Into Strategy

Before, risk managers looked backwards (logs and reports) to protect current assets. This challenge remains, but it is now complemented with a new responsibility: help the business look ahead, not just by monitoring risk trends, but by being able to contribute security insight to new and emerging business initiatives. The CISO's executive colleagues don't just want to know "what happened"; they need to understand how the firm's security posture positions (or fails to prepare) them for road maps ahead and want to know what measures they need to take now for their future growth.

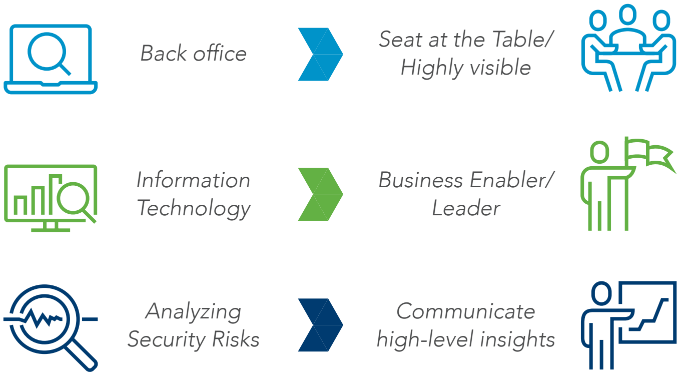
Translating The Technical Into The Actionable

Among the C-suite leadership team, the CISO sits in a unique place between the raw security data flooding into and among the organization, and the strategic intelligence executives need to make informed business decisions. The implications of this bridging role are dramatic: CISOs must simultaneously master an ever-growing set of complex data from multiple sources while being prepared to communicate high-level insights and answers to less tech-savvy colleagues.

Fulfilling Responsibilities Efficiently and Cost-Effectively

Just like every other executive, the CISO has to fulfill exceptional security obligations with limited budgets and resources. For any system to be genuinely useful, it must reduce, not increase, the complexity of the management environment itself: power and simplicity must go hand in hand.

Transforming Roles



03 CHALLENGES

Larger Responsibilities, Bigger Challenges

The CISO's changed and changing role presents challenges beyond the reach of individual tools and fragmented policies. As the point person for security, the CISO has responsibilities over an increasingly complex web of threats, risk frameworks, assets that demand protection, and third-party relationships that extend risk–and their necessary controls–beyond the walls of the organization itself.

Key responsibilities, and the special challenges they impose upon the CISO, include:

Assessing Threats

Every institution needs to know what the threats are, where they are coming from, and how they can be ameliorated. As noted earlier, the growing variety and scale of the threats continues to increase, resulting in more data analysis, metrics, and monitoring that the CISO must master.

Challenge: Map Potential Threats To Relevant Business Processes and Objectives

As with any large set of data, incoming risk reports must be understood and abstracted to a level that distills the false positives, categorizes the incidents, and elevates the results to action. That's why the CISO must not only monitor a large panel of threats, but needs to map threats to the business's unique processes, policies, assets, and objectives. By mapping threats to business issues, the CISO can identify priorities that merit the greatest attention from executive colleagues and can make informed recommendations for appropriate security investments.

Challenges the CISO's Face

- Mapping potential threats to relevant business processes and objectives
- Asserting control over disparate controls
- Monitoring protections and priorities that can evolve over time
- Controlling potential risks among external resources

Mastering Frameworks

The CISO is responsible for conforming to multiple frameworks (ISO/NIST/CSF), each with their own standards and their own requirements for demonstrating compliance. CISOs must account for the controls in place, monitor their effectiveness across a complex array of assets, and prepare reports that meet each framework's rules.

Challenge: Asserting Control Over Disparate Controls

With multiple regulations demanding multiple controls, it is all too easy to miss gaps and violations that fall between the gaps of organization silos. CISOs need a centralized matrix of recordable checks and balances, with appropriate cross-references, to gain at-a-glance mastery of complex obligations.

Managing Assets

Between the frameworks and the threats lay multiple layers of policies, systems, and applications that must be assessed and controlled through an assertive program of workflows, established processes, and enterprise-wide awareness and training. The CISO has ultimate responsibility for their implementation and fulfillment.

Challenge: Monitoring Protections and Priorities That Can Evolve Over Time

As assets change–through mergers, acquisitions, new product and service launches, and more–and threats evolve, the corresponding risk management programs, protocols, and technologies must change with them. CISOs need the power to survey work in progress, audit and test controls, and obtain insight on potential gaps, weak areas, and new vulnerabilities that require program changes and/or new controls.

Monitoring External Partners

Getting one's house in order now means asserting control beyond your own doors. The increasing prevalence of cloud computing, SaaS applications, and outsourcing, has shifted a significant proportion of the enterprise's workload among a wide variety of third-party partners and vendors who may hold and manage sensitive data–the company's and its customers'.

Challenge: Controlling Potential Risks Among External Resources

Today, managing risk is no longer just an internal affair, but a coordinated process that encompasses both internal and external assets. CISOs need to expand their controls to determine which vendors/third parties merit attentive cybersecurity measures, assess the degree and potential impact of vulnerabilities, establish protocols, and assess, monitor and report on third-party compliance.

04 COMMUNICATE AND CONTROL

Enable Your Business By Enabling Your Leadership

Now that CISOs have a seat in the boardroom, what will they bring to their peers? At the highest levels of governance, raw data fails to provide the actionable insight business leaders need. The effective CISO serves as a bridge between the complex pool of data generated by various cybersecurity initiatives, and the decision-making needs of executive and board leadership.

In essence, CISO leadership means translating data into insight, and making informed recommendations, not just for managing current assets safely, but for blazing secure trails ahead as the enterprise grows, morphs, and embraces new directives. The CISO is no longer a master of obscure technology in a remote part of the organization, but a highly visible communicator who must be prepared to articulate essential cybersecurity intelligence to fellow executives and board members, including (but not limited to):

Nature of Threat Landscape

The successful CISO can not only assert control over all dimensions of the threat landscape (including among external partners) but can identify and prioritize the most significant threats to the business and its ambitions.

Status of Cybersecurity Assets

CISOs should be able to describe the progress of cybersecurity controls for non-technologically sophisticated audiences, helping them understand what's working and what merits improvement.

Safety of Third-Party Relationships

Senior leadership needs to understand the nature and extent of third-party relationships, and the controls in place to assess risk, assure compliance, and monitor cybersecurity status.

Effectiveness of Policies and Procedures

CISOs are entrusted with policy stewardship and should be prepared to articulate what the policies are, how they are implemented and enforced, and what, if any, procedural changes must be made to meet current and anticipated threats.

Employee Engagement and Training

In addition to communicating to leaders, CISOs must communicate policy and procedures to employees and partners throughout the enterprise, establishing both the resources for awareness and training, and various means of assessment to record and report on the effectiveness of these initiatives.

05 CONCLUSION AND CHECKLIST

Do You Have The Tools You Need To Lead?

Most CISOs are already equipped with a wide range of technologies that help them and their teams address threats and monitor assets. Yet few, if any, have the tools they need for leadership: the effective mastery of every dimension of cybersecurity, and the ability to communicate activity in a way that is meaningful for executive leadership.

Fortunately, ProcessUnity has filled the gap with a Cybersecurity Program Management solution that helps integrate cyber-risk management into one tool for documenting, monitoring, and communicating the full scope of CISO responsibilities.

To see how you can benefit from a comprehensive Cybersecurity Program Management solution, use the following CISO Leadership Checklist, then contact a ProcessUnity Cybersecurity expert to discuss how the right tools can help you assert more effective leadership.

CISO Leadership Checklist

- ✓ Do you have a complete list of your organization’s assets – and understand their relative importance/priorities?
- ✓ Have you assembled all policies, procedures and standards in one centralized location?
- ✓ Can you monitor all threats or risks from one pane of glass?
- ✓ Is your controls inventory easy to access and monitor?
- ✓ Are you able to manage your risk registry and issue remediation through an integrated tool?
- ✓ Can you document and record employee awareness and training protocols?
- ✓ Do you have the means to assess and monitor third-party cybersecurity compliance?
- ✓ Do you have the power to quickly assemble coherent reports to fellow leaders and board members?
- ✓ Can you account for all cybersecurity frameworks and monitor your performance against their standards?
- ✓ Do you have the means to fulfill your duties efficiently and cost-effectively?

Get meaningful answers, fast. **Contact** ProcessUnity today or visit us **online** for more information.

ProcessUnity

www.processunity.com

info@processunity.com

978.451.7655

Twitter: @processunity
LinkedIn: ProcessUnity

ProcessUnity
33 Bradford Street
Concord, MA 01742
United States