RiskOptics

WHITE PAPER

FROM THE BACK OFFICE TO THE BOARDROOM:

The Changing Role of the Security Executive

ROB ELLIS, SVP of Strategy

CISOs and other security executives have long been perceived as the "no" people of the organization. When new ideas, tools, or proposals reach their desk (often late in the game), many security executives have taken the approach of shutting them down due to concerns about ineffective compliance and risk management.

But things are changing. Executive boards are no longer confident that they can protect their organizations from attacks, and information security is rightfully and quickly coming to the forefront. Rather than being the consistent voice that says "no," security executives have the opportunity to help the C-suite and board be more forward-looking and proactive by moving from compliance (reactive stance) to risk (proactive stance).

This is a dramatic shift in roles. Once a back-office "doer," the CISO or other similar security executive is now a communicator and influencer in the C-suite and boardroom. In this white paper, we'll look at the forces driving the evolution of the security leadership role and offer concrete advice on the best way to make this shift.

Security leaders face new challenges...

AS NEW CYBERSECURITY CHALLENGES ARISE, COMPLIANCE-FOCUSED ORGANIZATIONS FIND THAT THEY MUST MATURE THEIR RISK MANAGEMENT CAPABILITIES. CHALLENGES INCLUDE:

AN "IMPLEMENT FIRST AND WORRY ABOUT SECURITY LATER" APPROACH to responding to the COVID-19 pandemic, when organizations needed immediate change over a compressed time period. Many chose to put off thorough risk assessments and remediation in the interest of speed to meet the situation's urgency.

A GROWING ATTACK SURFACE, with the move to the cloud, the Internet of Things and hybrid work. Security now has a larger footprint to protect, and COVID exacerbated this issue by dramatically accelerating these shifts.

GREATER COMPLEXITY with hybrid multicloud and a growing supply chain network that can create invisible exposure. As supply chains become more connected, so do opportunities for breaches that can create access to sensitive data. The attack surface is not only larger, but also more complex.

HIGHER STAKES AND PROFILE. Breaches now have "real-world" consequences such as regional energy crunches (Continental Pipeline) and food shortages (JBS meatpacking). The threat of reputational damage, always a concern, is now multiplied by consequences that affect millions of people, make headlines, and attract regulatory scrutiny.

DATA INCREASING IN VOLUME AND VALUE. Data is not only growing, it is also becoming more valuable as companies find ways to mine it for insights. This creates two challenges: How to gain visibility, and also how to protect it from threats such as ransomware.

THE COST OF BREACHES. Every security breach has a cost consisting of detection, notification, lost business, and post-breach response. The average total cost of a ransomware breach, excluding any ransom paid, was $4.62 million according to Ponemon's 2021 Cost of a Data Breach report. Customer personally identifiable information (PII) was the costliest record type, at $189 per lost or stolen record[1].

PRESSURE FROM C-SUITES AND BOARDS to ensure that organizations can meet their growth goals without exceeding their cybersecurity risk appetite. Suddenly, IT security is top of mind at the highest levels of the organization.

THE RAPID PACE OF CHANGE, including a new and increasingly complex global regulatory environment.

A BOOM IN PRIVACY CONCERNS and regulations such as GDPR, which add an entirely new dimension to security.

THE LACK OF TALENT AND RESOURCES to fight on all these fronts. A chronic problem has been exacerbated by a tight talent market and increasing demands on resources.

1 Cost of a Data Breach Report 2021 (ibm.com)

...That are driving a shift from compliance to risk management

WHILE COMPLIANCE REMAINS CRITICALLY IMPORTANT, BY ITS NATURE IT IS INSUFFICIENT TO ADDRESS ALL OF THESE CHALLENGES.

COMPLIANCE IS REACTIVE, which means that the actual security posture in between audits may not capture the true risk.

RISK IS PROACTIVE, so it is built into decision-making before creating potential new exposures.

COMPLIANCE IS TACTICAL. It addresses controls and risks one at a time without fully considering the organization as a whole.

RISK IS STRATEGIC. It looks at threats in the context of the business, to enable growth rather than hinder it.

COMPLIANCE IS BINARY. A control is either in place and effective or it isn't. An organization is either compliant with a particular regulation or not.

RISK IS A CONTINUUM. Because risk evaluates threats in the context of the business and its objectives, it takes into account an organization's risk appetite. For example, a financial institution that relies heavily on customer trust will have a relatively low appetite for risk. A tech startup may have a higher risk appetite.

A seat at the table: The security executive's new role

Just as organizations are evolving from compliance-focused to risk-focused, the security executive's role is evolving in parallel. Where they were once the ones saying "no," they must now be enablers. Where they were brought in at the end of a process (an acquisition, an expansion into a new market, a new product development, etc.), they must now inform decisions from the very beginning. Where they were once doers, they must now be teachers and communicators. Where they once may have reported to the CIO, now they should report to the CEO.

CISOs and other security executives must take on a leadership role, and be prepared to work with the C-suite and the board of directors as peers. They must articulate risk levels in relation to business objectives. Moving from the back office to the boardroom means accepting a higher-profile, less technical role. Security executives should prepare themselves to step out of their comfort zone, but also elevate their reputation and brand within the organization.

In the next section, we'll take a look at how to do exactly that.

How to get there — 5 steps to take

MANY CISOS AND OTHER SECURITY EXECUTIVES WILL HAVE TO GROW INTO THIS NEW LEADERSHIP ROLE. THIS IS TRUE FOR THOSE WHO HAVE RISEN FROM A TECHNICAL BACKGROUND.

1. THINK (AND ACT) PROACTIVELY RATHER THAN REACTIVELY

In its essence, the role that security executives must now take on is an evolution from the tactical to the strategic, so the first step is to adjust your mindset.

The only way to shape strategy is to have a say in its development. You will need to embed yourself in strategic decisions to positively influence outcomes by bringing risk to acceptable levels. It requires embedding security by design throughout the decision-making process to achieve organizational resilience.

All of this is based on another significant shift: from saying "no, period" to saying "yes, but" or "yes, and" in response to strategic proposals. Your new role is to enable strategic initiatives by managing risk from the start rather than hindering it downstream. Think of it as setting a speed limit for the organization so it can reach its destination safely, rather than throwing up a roadblock.

2. EXPAND YOUR COMMUNICATION SKILLS

Embedding yourself and the concept of risk into the strategic decision-making process requires entirely new communication skills. You're no longer a doer who executes and enforces policy, but a teacher at the the topmost echelon who leads by influence.

It is critical to "translate" the language of information security risk into language that the C-suite and Board can easily grasp in order to make strategic decisions. You will certainly be asked to justify your budgetary requirements. You should be comfortable doing so in terms of the roadmap, tools, and people to support the company's goals.

On a more tactical level, you will have to be polished and professional to speak with the board of directors. Have the necessary information at your fingertips so you can illuminate the risks involved in each strategic decision. This will require tools such as a risk dashboard that can serve up the data required. Be able to distill these technical matters into language that people can understand.

The CEO

It's safe to say you won't get anywhere without the ear of the CEO. They are the key to understanding where the organization is going and what its mid- and long-term goals are. They must also back any security-and risk-related initiatives you propose.

The CRO

This is the person who can answer critical questions such as: What products are we going to be selling in what verticals? What jurisdictions will we be entering? Only then can you address new risks and unfamiliar regulations, such as healthcare (HIPAA), government (FedRAMP), credit cards (PCI), and a myriad of offshore regulations and risks.

The CMO

Data is central to marketing, but you need to understand what data your organization is collecting from customers. Why do we need it? What are you doing with it? How are you protecting it? The CMO can provide these answers.

Chief Legal Officer/ General Counsel

Risk, compliance and legal issues overlap considerably. You should have a hand in writing privacy policies, negotiating vendor contracts, and other security-related legal affairs.

Beyond the board room and C-suite, you are now responsible for developing a risk-aware culture, where risk is everyone's responsibility. That will require increasing your visibility across the organization.

3. FORGE NEW RELATIONSHIPS

You certainly won't be able to understand or further the goals of the organization without forging strong ties to the leaders who are setting and progressing those goals. Be prepared to foster positive relationships and open communication with peers across the organization.

Here are just a few examples, but bear in mind that this is just the rudiments of your network.

In addition to these one-on-one relationships, you must also participate in the evolution of the DevOps team into DevSecOps by integrating security across the entire development lifecycle.

4. CULTIVATE NEW CAPABILITIES

Part of the new role is transitioning from a security specialist to a generalist with a hand in different domains: privacy, security, risk, and compliance. While improving your own knowledge in these areas is critical, you can't know everything.

Find new resources inside and outside the organization to roll in these new skills and capabilities. CISOs and other security executives can bring in people with in-demand skill sets like data analytics, risk management, and technical disciplines.

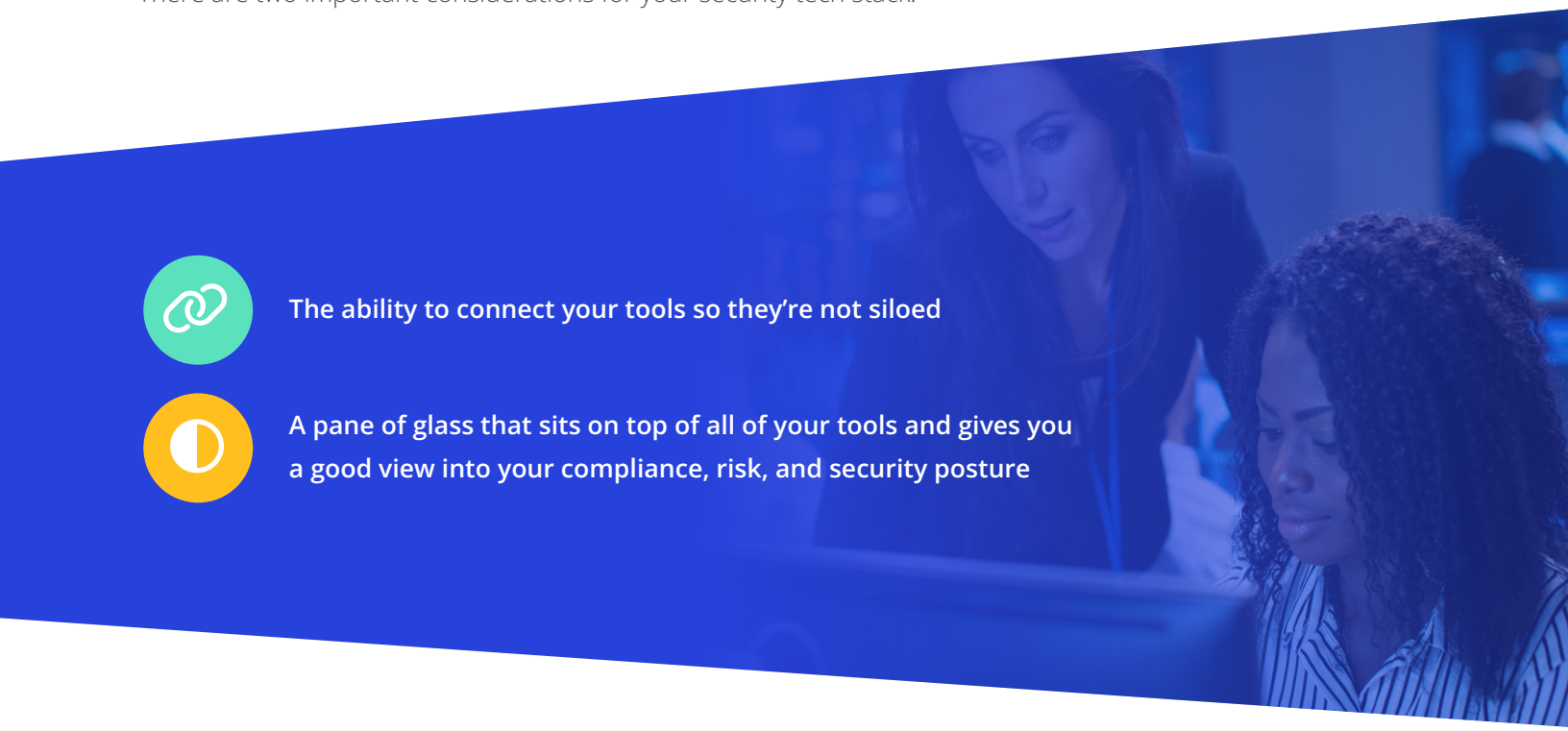
In a recent report, KPMG identified several new roles that security leaders should consider filling to bring in these skills[2]:

2 From enforcer to influencer - KPMG Global (home.kpmg)

5. LEVERAGE TECHNOLOGY PLATFORMS AND AUTOMATION

Talent shortages and resource crunches will place a greater emphasis on sophisticated automation to smooth the transition from compliance to risk, and provide greater visibility into highly complex environments.

There are two important considerations for your security tech stack:



- **The ability to connect your tools so they're not siloed**
- **A pane of glass that sits on top of all of your tools and gives you a good view into your compliance, risk, and security posture**

You and your team need a comprehensive dashboard that puts critical risk information at your fingertips so you can provide informed answers to the questions that your peers in marketing, sales, legal, product, or engineering are going to ask you.

A unified technology platform like the RiskOptics Product Suite helps you to break down traditional silos between compliance, security, and risk management. It can provide a concise set of KPIs and KRIs to monitor and communicate your risk posture. In addition, it can smooth the transition from compliance to risk by automatically creating a risk dashboard from your organization's compliance controls.

In conclusion

The role of the CISO and similar security executives is changing rapidly as organizations shift from a compliance focus to a risk-first approach.

Smart security executives are embracing their new leadership role by cultivating new skills and relationships to enable strategic initiatives with the security necessary to protect sensitive information, engender trust, and maintain brand reputation. As they take on this broader, more prominent role, they need advanced tools to provide the visibility and analysis a risk-first approach demands.

The RiskOptics Product Suite delivers a single, real-time view of risk in context of your business activities, empowering security teams with the actionable insights needed to avoid and mitigate risk, and optimize security. With RiskOptics, you can take your organization beyond "check the box" compliance toward a fully mature risk management program.

Using an AI-powered approach, the RiskOptics ROAR platform allows organizations to unify their risk observation, assessment, and remediation activities for a single, real-time view of risk and compliance in business context. This helps resource-stretched teams with prioritizing and understanding where they can focus resources to achieve their desired business outcomes.

ABOUT RISKOPTICS

RiskOptics is the leader in IT risk management solutions, empowering organizations to convert risk into a strategic business advantage. The fully integrated and automated RiskOptics ROAR Platform provides a unified, real-time view of risk and compliance framed around business priorities, enabling CISOs and InfoSec teams to take a proactive approach to risk management.

RiskOptics customers are able to quantify the impact of risk on their business, communicate that impact to key stakeholders and mitigate expensive data breaches, system failures, lost opportunities and vulnerabilities across their own and third-party data while adhering to compliance requirements.

See Risk Differently

riskoptics.com