PONDURANCE

Risk-Based Cybersecurity Protects **What's Most Important**

pondurance.com

PONDURANCE

Introduction

Your company has its own unique set of cyber risks. Your lines of business, your technical infrastructure, threats, employees, third-party vendors, and other variables all factor into your cyber risk profile. Each year, risks continue to grow more complex and new threats raise their ugly heads. Though you can't control the evolving cyber landscape, you can control your cybersecurity strategy. But what's the best strategic approach to cybersecurity today?

Many companies take a generic approach to cybersecurity where they adopt a standardized program and simply check the boxes as they reach predetermined security milestones. Other companies use a "random acts of security" approach where they reactively put new technologies in place without having a strong strategy behind their actions. However, neither of these approaches considers what the company truly needs in a cybersecurity program. But risk-based cybersecurity does.

This ebook helps define a risk-based approach to cybersecurity and outlines the steps you need to consider.

WHAT'S THE RISK?

R= Likelihood X Business Impact

- **Inventory**
- **Vulnerabilities**
- **Threats**
- **Exposure**
- **Compensating Controls**

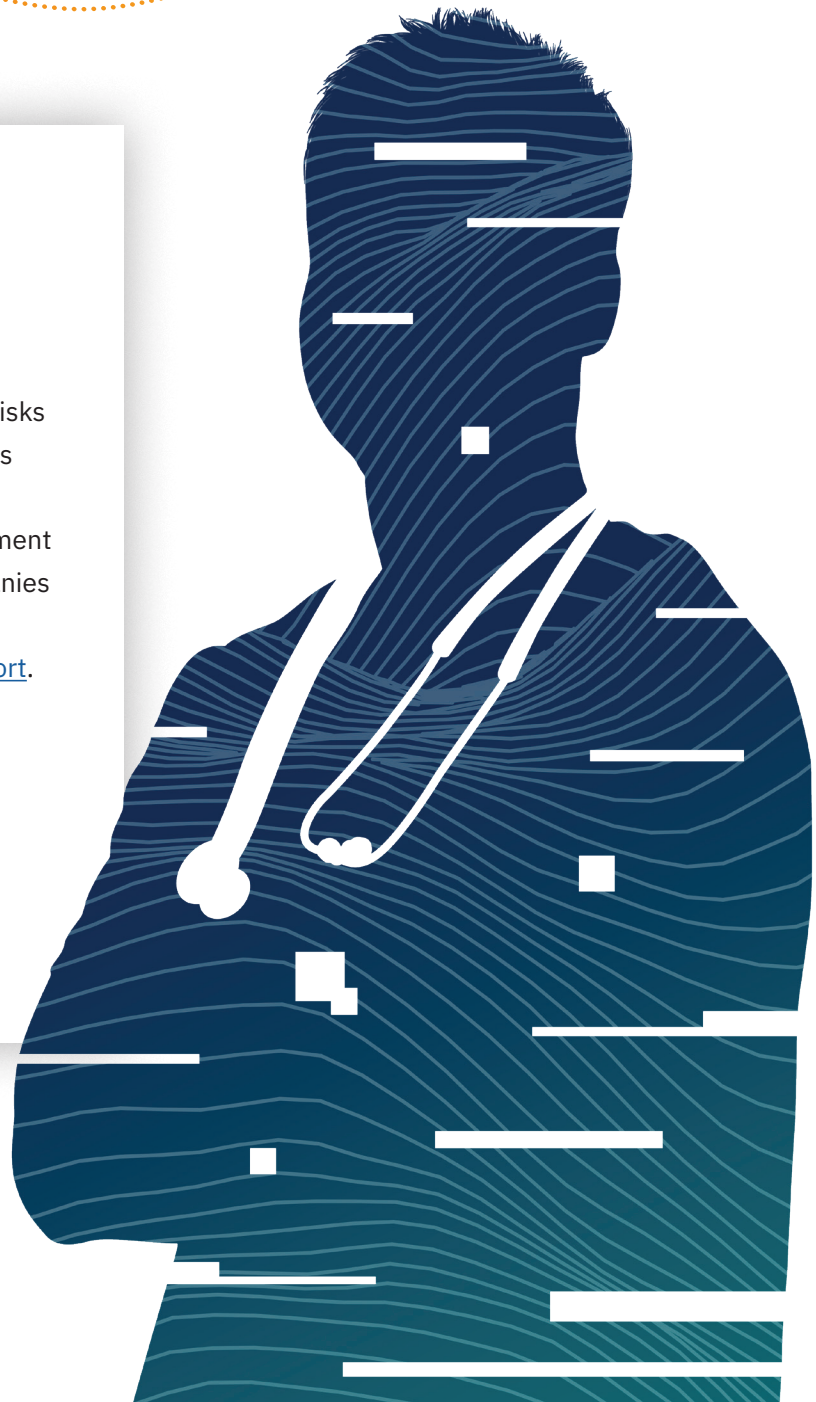
f

- **Confidentiality**
- **Availability**
- **Integrity**

Risk-based cybersecurity

Risk-based cybersecurity is a modern approach that focuses on a company's specific cyber risks and considers what the company wants to accomplish and wants to protect. Many companies don't use a risk-based approach because they don't understand their risk profile, are lacking security professionals and effective technology, and have limited budgets and time to implement it. However, companies that do use risk-based cybersecurity reap the benefits. These companies stop three times more attacks outright, find over 50% of incidents within one day, and see impactful breaches reduced from 76% to 28%, according to an Accenture cybersecurity report.

A risk-based approach is not an add-on approach; rather, it's built into the core of your cybersecurity strategy. Using risk-based cybersecurity, you will identify the specific cyber risks for your company, prioritize the most important risks, and then find the most impactful ways to protect your company against those risks.



Identify risks

Every company has specific gaps and vulnerabilities. For example, with each passing year, companies add more and more IoT devices to their networks, increasing the attack surface for cybercriminals. As a first step, you need to identify what your company's gaps and vulnerabilities are. Performing a risk assessment is the best way to proactively find those blind spots and weaknesses — and it's necessary to find them before the cybercriminals do.

A risk assessment analyzes your security controls and processes to determine where your company is vulnerable to an attack. You must fully understand the threat landscape, your internal risks, and your assets.

PONDURANCE

Prioritize risks

CEOs view cyber risks (49%) as the top threat negatively impacting companies in 2022, just above health risks (48%), according to a PwC global survey. Those CEOs were most concerned about how cyber risks will impact their ability to sell products and services.

But every company is different. Once your company identifies its own cyber risks, you'll want to prioritize those risks. No company can eliminate all risk, but you can focus on where you can reduce it. Ask yourself what risks the company is willing to take, what risks pose the greatest risk for your company, and what risks require the most protection. You'll want to consider how the risks impact your growth potential, online sales, regulatory compliance requirements, remote workforce, return on investment, and any other aspects of your company.

In particular, small to midsize companies, which make up 98% of all cyber insurance claims, may want to pay special attention to their cyber risks in terms of cyber insurance requirements. Since cyber insurance premiums are up, coverage limits are down, and cyber insurance providers are imposing greater scrutiny on clients, cyber insurance can be a key consideration when prioritizing risks.

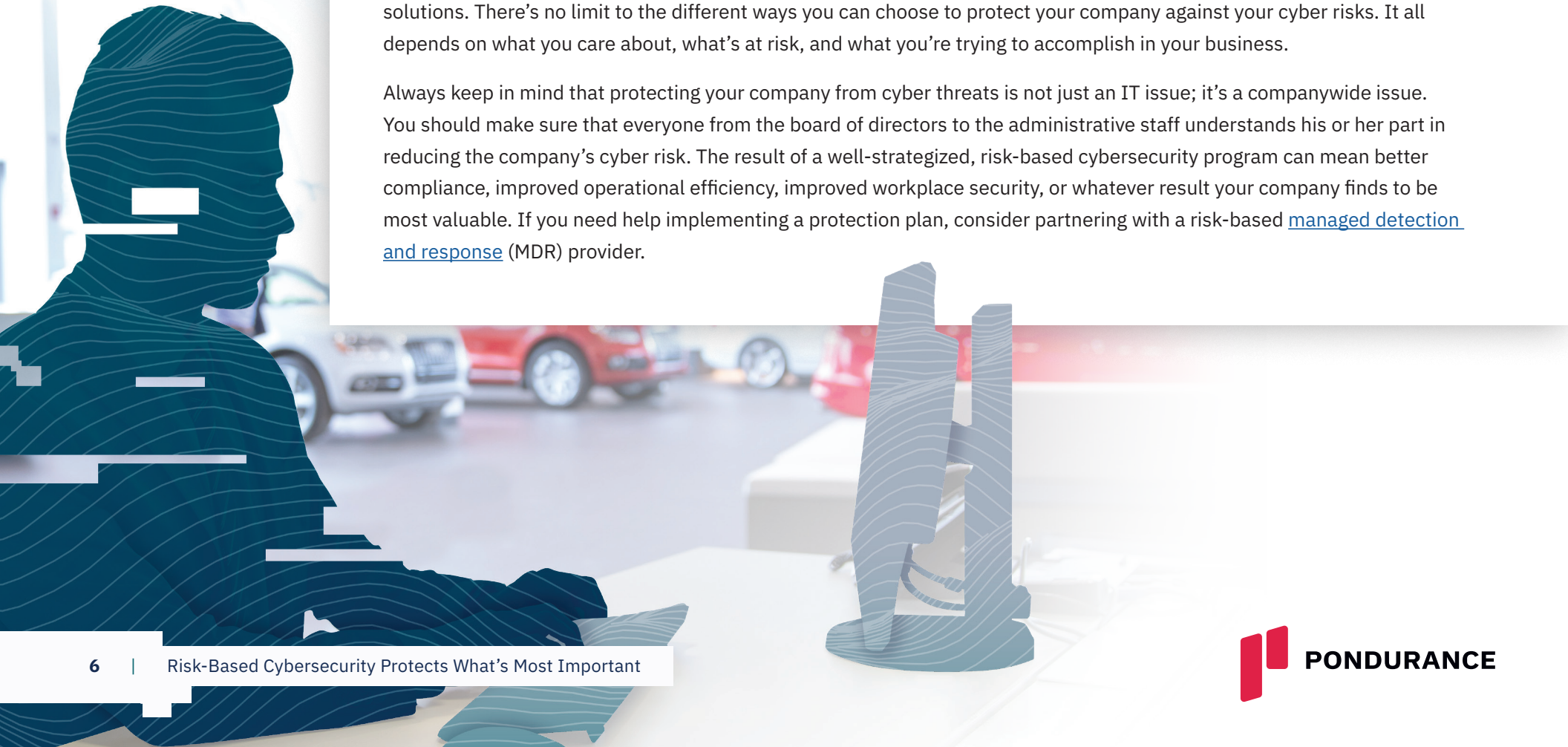
Once you've considered the priority of all cyber risks, you'll want to rank them in order of importance to your company. Keep in mind that you need to prevent immediate problems first, then work on ongoing solutions. This ranking will give you a precise and thorough guideline for how to move forward in protecting your company from cyberattacks.

Protect against risks

In business, it's wise to know the impact of every risk you take — and cyber risk is no different. At this stage of risk-based cybersecurity, you want to find the most impactful ways to protect your company against cyber risks.

To start, you can create a road map to address the gaps and vulnerabilities that you prioritized for your company. You want to put measures in place to fix these cyber risks in a way that makes the most sense for your company and within your budget. You can establish new controls for the vulnerabilities, secure additional people or technology to address any gaps, provide data transparencies so you have a better idea of what's going on behind the scene, or any number of other solutions. There's no limit to the different ways you can choose to protect your company against your cyber risks. It all depends on what you care about, what's at risk, and what you're trying to accomplish in your business.

Always keep in mind that protecting your company from cyber threats is not just an IT issue; it's a companywide issue. You should make sure that everyone from the board of directors to the administrative staff understands his or her part in reducing the company's cyber risk. The result of a well-strategized, risk-based cybersecurity program can mean better compliance, improved operational efficiency, improved workplace security, or whatever result your company finds to be most valuable. If you need help implementing a protection plan, consider partnering with a risk-based managed detection and response (MDR) provider.

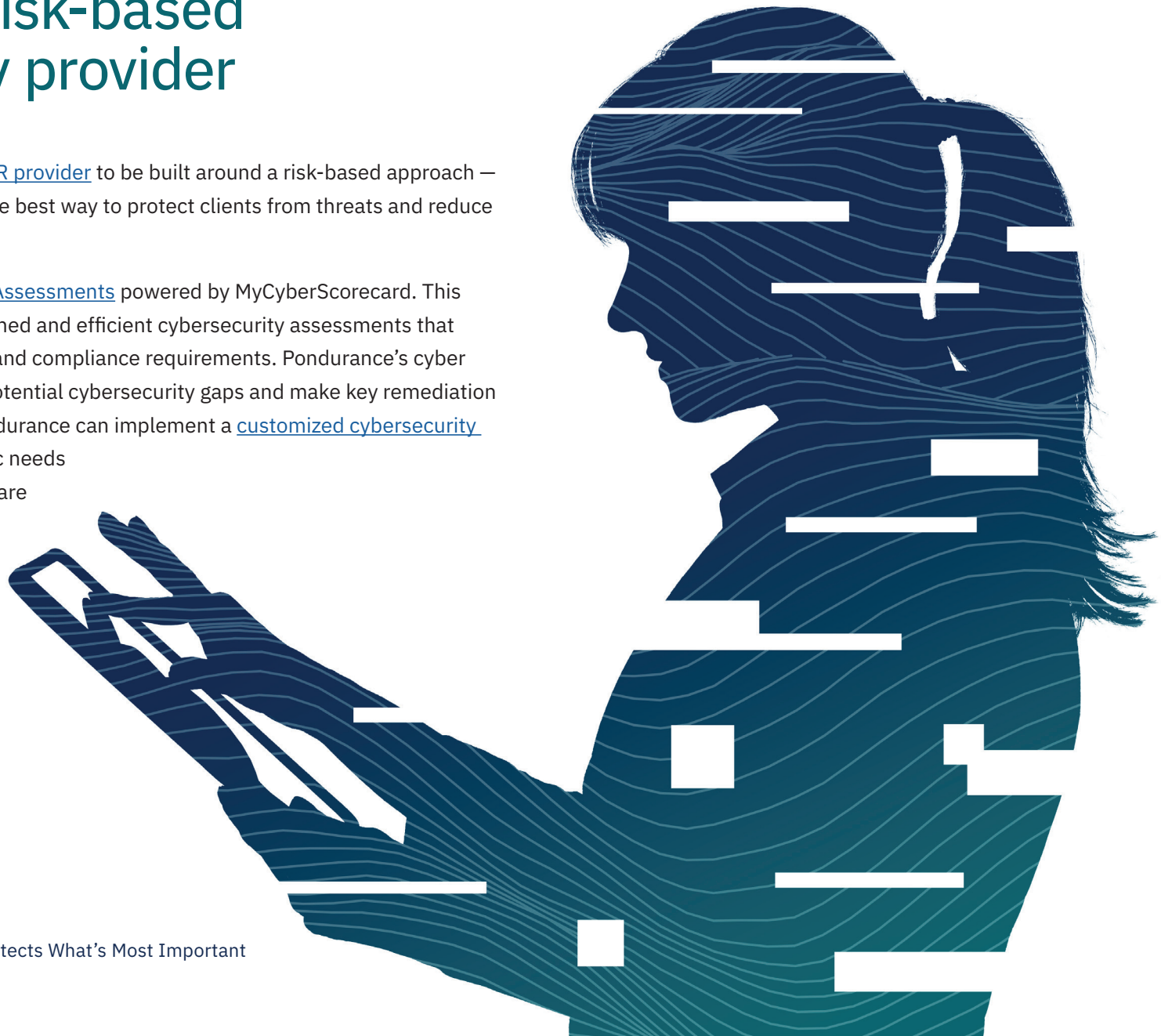


PONDURANCE

Work with a risk-based cybersecurity provider

Pondurance — the first and only MDR provider to be built around a risk-based approach — believes a risk-based approach is the best way to protect clients from threats and reduce their exposure to attacks.

The process starts with Cyber Risk Assessments powered by MyCyberScorecard. This all-in-one solution delivers streamlined and efficient cybersecurity assessments that coincide with regulatory standards and compliance requirements. Pondurance's cyber risk experts analyze and visualize potential cybersecurity gaps and make key remediation recommendations. From there, Pondurance can implement a customized cybersecurity program for your company's specific needs in alignment with the priorities that are most critical for your company.



Conclusion

Your company has its own unique set of cyber risks, and you want to address those that are most important to your business. A risk-based cybersecurity approach will allow you to identify the specific cyber risks for your business, prioritize the most critical, and find the most impactful ways to protect your company. It's a cybersecurity strategy that maximizes your company's needs and wants and reduces your exposure.

Watch this video with Tom Field, Senior Vice President at Information Security Media Group, and Lyndon Brown, Chief Strategy Officer at Pondurance, to learn more about risk-based cybersecurity.

How Pondurance can help

Our mission is to ensure that every organization is able to detect and respond to cyber threats — regardless of size, industry, or current in-house capabilities. We combine our advanced platform with decades of human intelligence to decrease your risk.

CLOSED-LOOP MANAGED DETECTION AND RESPONSE

Recognized by Gartner, Pondurance provides 24/7 U.S.-based security operations center services powered by analysts, threat hunters, and incident responders who utilize our advanced cloud-native platform to provide you with continuous cyber risk reduction. By integrating 360-degree visibility across log, endpoint, and network data and with proactive threat hunting, we reduce the time it takes to respond to emerging cyber threats.

Pondurance MDR is the proactive security service backed by authentic human intelligence. Technology is not enough to stop cyber threats. Human attackers must be confronted by human defenders.

INCIDENT RESPONSE

When every minute counts, organizations need specialized cybersecurity experts to help them respond to a compromise, minimize losses, and prevent future incidents.

Pondurance delivers digital forensics and incident response services with an experienced team capable of guiding you and your organization every step of the way. This includes scoping and containing the incident, determining exposure through forensic analysis, and helping to quickly restore your normal operations.

SECURITY CONSULTANCY SERVICES

Our specialized consultancy services will help you assess systems, controls, programs, and teams to uncover and manage vulnerabilities. Our suite of services ranges from penetration testing to red team exercises, along with compliance program assessments for highly regulated industries. We provide security incident response and business continuity planning to put you in the best position to defend against and respond to cyberattacks.

PONDURANCE

500 N. MERIDIAN ST., STE 500
INDIANAPOLIS, IN 46204

About Pondurance

Pondurance delivers world-class **MDR** services to industries facing today's most pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements, and digital transformation accelerated by a distributed workforce. By combining our advanced platform with our experienced team of analysts, we continuously hunt, investigate, validate, and contain threats so your own team can focus on what matters most.

Pondurance experts include seasoned security operations analysts, digital forensics and incident response professionals, and compliance and security strategists who provide always-on services to clients seeking broader visibility, faster response and containment, and more unified risk management for their organizations.

Visit **www.pondurance.com** for more information.