

DECEMBER 2023

# 7 Steps to Developing a Successful Cybersecurity Program

Dave Gruber, Principal Analyst

**Abstract:** In the fast-paced world of cybersecurity, staying ahead of threats is essential. And while security is, without a doubt, a priority for businesses of all sizes, small and midsize organizations often feel constrained in their ability to effectively secure their operation against the growing cybersecurity threat. Despite their size, these orgs still want and need control and visibility into the security of their entire estate to be able to effectively deliver on availability, reliability, and compliance requirements.

Managed detection and response (MDR) service providers from vendors like Zones are helping to accelerate security program development.

## 7 Steps to Developing a Successful Cybersecurity Program

Building a successful cybersecurity program requires a vision, a series of strategies, and a comprehensive plan to implement and operationalize all aspects of the program. But for smaller organizations, building this program is often a joint task, along with keeping all aspects of the IT operating infrastructure working properly without compromise, in the context of ongoing regulatory requirements. These seven steps frame up what it takes to build and manage a successful program.

### 1. Understand your organization's risk posture and potential cyber-risk

Developing an effective cybersecurity program begins with taking a hard look at your IT operating infrastructure and the potential cyber-risk associated with it. This process requires a deep understanding of the critical operating infrastructure that powers each part of your organization. Ensuring mission-critical systems are protected from potential attack disruption often involves a close look at both upstream and downstream systems.

As the infrastructure grows and changes, so must your cybersecurity controls, so operationalizing your asset and workload asset inventory process is key to continuing success.

### 2. Set achievable goals to improve cybersecurity posture

Developing a security program that fits your individual needs will depend on your organization's specific operating objectives. Regulatory bodies add additional requirements that will help frame your security program.

Setting specific goals begins with the creation of a core vision for how your cybersecurity program will protect your infrastructure over time. Establishing specific program objectives over a one- to two-year period is recommended, focusing on securing the most critical assets first.

### 3. Select strategies that are best suited to your specific organization

While most cybersecurity programs include similar broad capabilities, choosing strategies that best support your individual program may involve several outside factors, such as your program funding, your ability to find and retain skilled staffing, and the frequency and pace of IT infrastructure change you are tasked with protecting. Industry and regulatory requirements will also influence strategies.

Crafting the right mix of security leadership, internal security personnel, and third-party security service providers is core to implementing and operationalizing your security program.

### 4. Architect a scalable security systems architecture and infrastructure

There are literally thousands of security tools and solutions available in the industry. Architecting the right security stack to support your individual organization's needs often means not only considering the scope and scale of your security needs, but also the level of skills available to implement, manage, and utilize cybersecurity technology.

A scalable architecture begins with a set of operating principles that will guide decisions for investments.

### 5. Operationalize your security program

Meeting your ongoing security objectives means operationalizing every program strategy. Best practices are readily available, leveraging standards such as NIST<sup>1</sup> and others.

Managed security service partners can help guide you through this process, in addition to filling gaps in knowledge, skills, expertise, and systems. Selecting a partner that can help you implement the right strategies means finding a partner that is well aligned with security objectives and approaches.

### 6. Implement organizational cyber-resilience readiness

Cyber resilience requires both an understanding and commitment from line-of-business (LOB) leaders throughout your organization. Cyber-attacks can disrupt or paralyze virtually every part of the operation, so operational leaders need to understand and be ready to react when cyber disruption occurs. This means building and rehearsing a crisis response plan, inclusive of IT, security, and LOB personnel.

### 7. Continuously measure and improve

Measuring the effectiveness of your program enables you to measure progress towards overall program objectives and identify gaps that create risk and exposure. Ensuring security leadership can effectively measure, report, and communicate security program progress and posture to senior business leaders is paramount to program success and ongoing support.

## Accelerating Security Program Development

As organizations look for ways to accelerate security program development, recent research from TechTarget's Enterprise Strategy Group reports that 85% of organizations are leveraging managed security service providers for a majority or a portion of their security operations.<sup>2</sup>

The use of MDR services has become a mainstream strategy in modern security programs. But IT organizations shouldn't be fooled by the name: MDR providers are delivering much more than basic detection and response, helping IT and security leaders accelerate program development and improve security posture.

---

<sup>1</sup> Source: NIST, [Cybersecurity Framework](#).

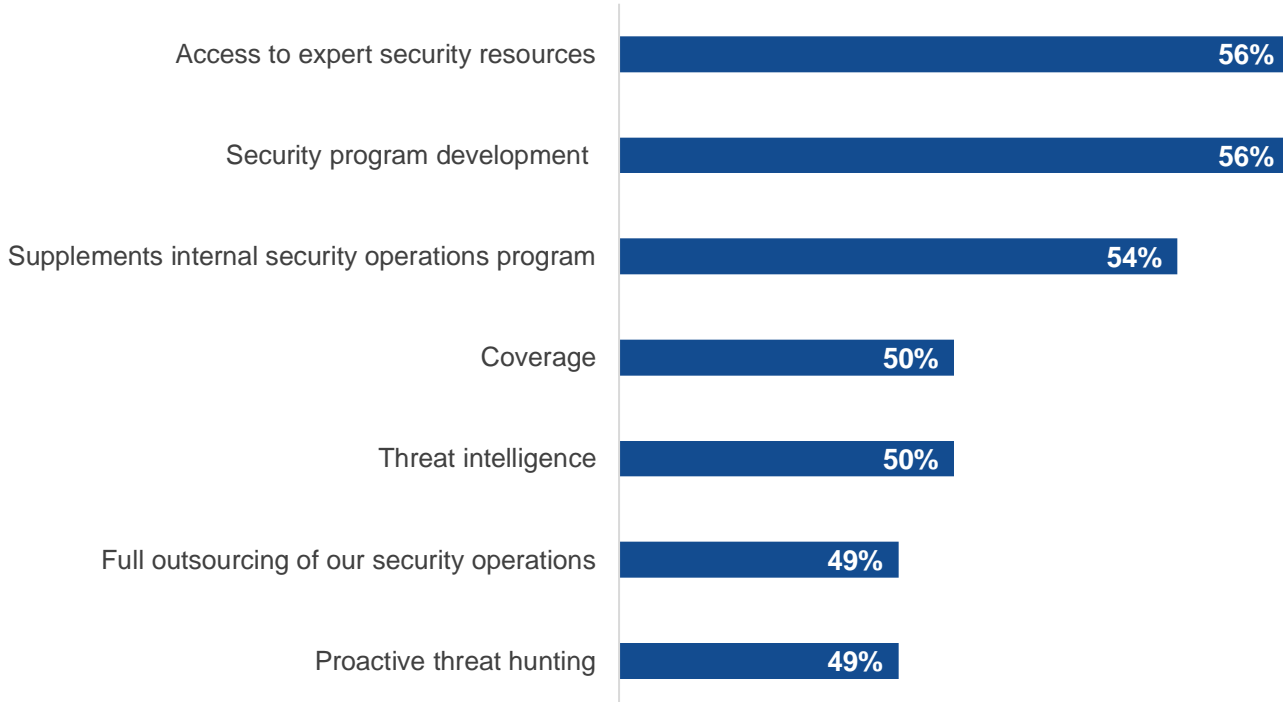
<sup>2</sup> Source: Enterprise Strategy Group Research Brief, [Security Operations Managed Services](#), March 2023.

With no end in sight for the cybersecurity skills shortage, MDR services can bring immediate expert resources online, together with proven, best-of-breed processes and tools that can help security teams gain control and set themselves up for future security program success.

Managed service providers are bringing skilled people, proven processes, and proven systems to help organizations of all sizes secure their organizations. Key use cases supported include access to expert security resources, security program development, threat intelligence, and proactive threat hunting, among others (see Figure 1).<sup>3</sup>

**Figure 1. Key MDR Use Cases**

**What use cases within your organization's security program does MDR apply to? (Percent of respondents, N=373, multiple responses accepted)**



*Source: Enterprise Strategy Group, a division of TechTarget, Inc.*

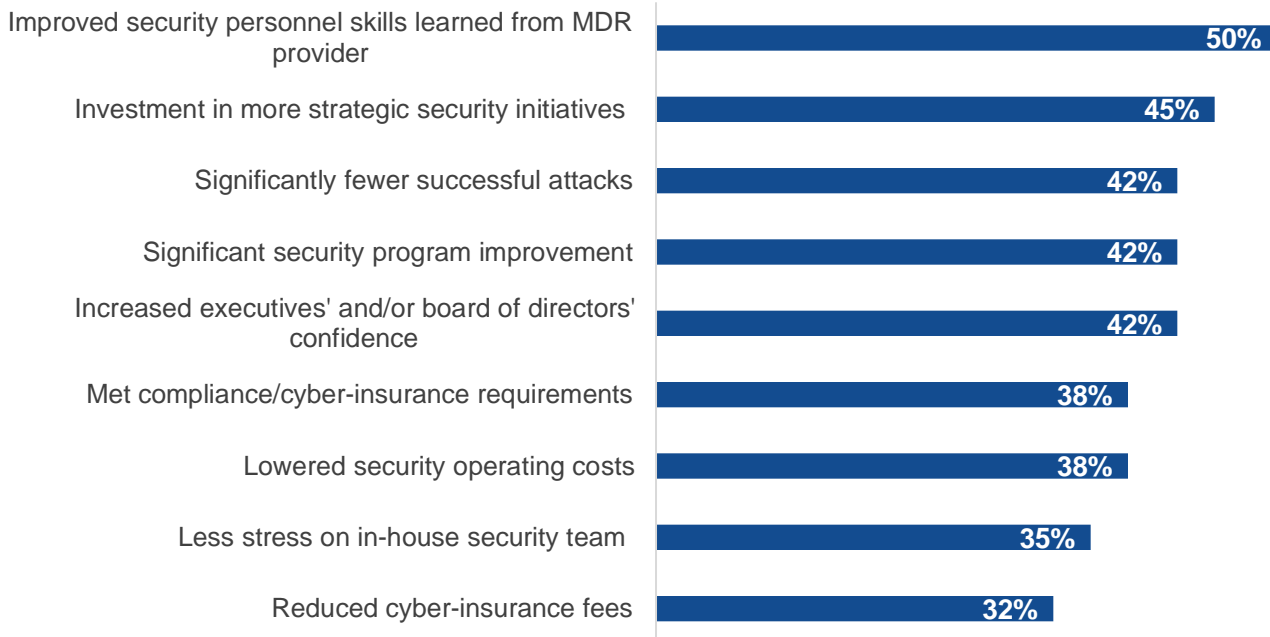
And MDR providers are delivering. Outcomes reported by organizations as a result of MDR provider collaboration include improved security personnel skills, more strategic security investments, significantly fewer successful attacks, and lowered security operating costs, to name a few (see Figure 2).<sup>4</sup>

<sup>3</sup> Source: Enterprise Strategy Group Research Report, [What Security Teams Want from MDR Providers](#), March 2023.

<sup>4</sup> Ibid.

**Figure 2. Outcomes Achieved by Leveraging MDR Providers**

**Which of the following outcomes has your organization achieved by leveraging an MDR provider? (Percent of respondents, N=373, multiple responses accepted)**



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

## Introducing Zones Managed Security Services

Zones differentiates itself from its competitors by being able to comprehensively manage the entire IT estate, including global IT supply chain and operations services, which encompass complete asset lifecycle management, IT service management, managed network services, and managed security that leverages advanced technologies to produce thorough managed detection and incident response services, such as machine learning, augmented intelligence, and other data analysis tools.

Zones now offers full-service managed security, including a comprehensive array of security assessments, security solution implementation services, and operational security services through its security operations center-as-a-service (SOCaaS) offering; security governance, risk, and compliance-as-a-service (GRCaaS) offering; as well as vulnerability and patch management services.

### Why Zones?

- 2700+ employees globally
- Certified, award-winning Minority Business Enterprise (MBE)
- Delivering global security services across 120 countries
- 3000+ hardware and software solution partners
- 300+ service delivery partners
- Broad support for all technologies across cloud and on-premises environments
- Offering migration services

Zones' modular, end-to-end security solutions deliver a complete security management program. Industry-leading partners operate at scale and speed to monitor, identify, evaluate, mitigate, and proactively implement industry best practices to maintain a robust security posture for clients.

Zones also helps its clients transform reactive security management programs into proactive security management programs that improve organizational competency as well as processes, technologies, and overall security culture, thereby helping to minimize attack surfaces, risks, and costs.

## Conclusion

Small and medium-size organizations face an uphill battle to build strategies to keep up with the rapidly changing cyberthreat landscape. With limited budgets and staffing, build-your-own strategies can feel unachievable, motivating many to turn to managed security service providers for help.

Service providers are helping accelerate program development through skilled experts and proven technologies and processes. Enterprise Strategy Group recommends IT and security leaders within small organizations who want to accelerate their security program outcomes explore new solutions from vendors such as Zones.

©TechTarget, Inc. or its subsidiaries. All rights reserved. TechTarget, and the TechTarget logo, are trademarks or registered trademarks of TechTarget, Inc. and are registered in jurisdictions worldwide. Other product and service names and logos, including for BrightTALK, Xtelligent, and the Enterprise Strategy Group might be trademarks of TechTarget or its subsidiaries. All other trademarks, logos and brand names are the property of their respective owners.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.


Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at [cr@esg-global.com](mailto:cr@esg-global.com).

---

### About Enterprise Strategy Group

TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

 [contact@esg-global.com](mailto:contact@esg-global.com)

 [www.esg-global.com](http://www.esg-global.com)