PONDURANCE

Cyber Priorities: 6 Cybersecurity Investments You Should Consider in 2022

pondurance.com

Table of contents

Introduction

You may have fewer employees and lower revenues, but small and midsize organizations like yours are just as likely to be targets of cybersecurity threats as large enterprises. In fact, 43% of all data breaches involve small and midsize businesses, and 61% of all small and midsize businesses have reported at least one cyberattack during the previous year.[1]

A global increase in cybersecurity attacks is ratcheting up the need to dedicate more resources to the problem, and large enterprises are doing just that. According to PricewaterhouseCoopers, 55% of enterprise executives planned to increase their cybersecurity budgets in 2021, and 51% added full-time cyber staff.[2] For small and midsize businesses, though, it's a different story. In a recent survey of organizations like yours, they cited budget constraints as the top cybersecurity challenge.[3]

With limited cybersecurity resources, your organization needs to be judicious with spending. You need to balance tactical and strategic investments so you can see both immediate and long-term benefits. You need to prioritize investments based on the specific risks facing your organization. And you need to maximize efficiency while minimizing complexity. This eBook will help you make the most of your organization's cybersecurity budget.

The next six chapters explore six cybersecurity investments that you should consider prioritizing in 2022 as you work to strengthen your security posture. To assist in planning purposes, this eBook provides ballpark pricing and implementation timelines.*

43%

OF ALL DATA BREACHES
invovle small and
midsize businesses

* Please note that these numbers are rough estimates based on historical data. Actual pricing and timelines vary depending on the size of the organization, the size and composition of the infrastructure, the complexity of the environment, the regulatory requirements in play, the use of in-house versus external resources, the specific needs of the organization and more.

PONDURANCE

INVESTMENT #1:

Cybersecurity Competency

Bringing in cybersecurity competency – the capabilities provided by a chief information security officer (CISO) – should be your first investment, before you decide on or make other technology investments. In some cases, the recommendation to appoint a CISO comes directly from regulatory guidelines.[4]

Not to be confused with technology competencies, your CISO should have the knowledge to establish a foundational cybersecurity program, confirm compliance and adhere to regulatory guidance and industry best practices. Critical functions of the cybersecurity competency include conducting risk assessments, aligning your cybersecurity strategy to risk assessments, understanding and interpreting regulatory prescription, directing resources in the appropriate way and advising your executives on security matters.

Despite its importance, a full-time in-house CISO is not always possible or practical. Your organization may not have the financial resources — or the need — to source a full-time CISO, and if you do, you may find it difficult due to the cybersecurity workforce shortage and competitive staffing environment. When that happens, outsourcing in the form of a virtual CISO (vCISO), CISO as a service or a fractional CISO is a smart alternative.

Engaging a vCISO offers your company numerous benefits. It's more cost-effective than a full-time in-house CISO, which can cost you an average of $227,000 per year.[5] It provides geographic flexibility, a consumption-based model and a broad range of expertise and capabilities. And it allows you to dramatically accelerate security program maturity, improve compliance and reduce the risk of threats as well as the risk of fines and penalties.

BALLPARK COSTS AND IMPLEMENTATION TIMELINE

- vCISO services provided by a team of experts from Pondurance typically start at $25,000. With our vCISO services, you also gain access to other security experts within our company who can weigh in on your specific needs.
- vCISO services can begin almost immediately, with the goal of ultimately integrating into the environment to provide valuable leadership-level insight to security objectives. The deliberate program management follows either an assessment timeline, an initial observation or inquiry of the current security state and/or policy and procedure and regulatory compliance alignment.

INVESTMENT #2:

Cyber Risk Assessments

A cyber risk assessment is a key investment, as it is the starting point in developing your cybersecurity framework. There are several types of assessments, such as NIST Cybersecurity Framework, NIST 800-53, NIST 800-171, Cybersecurity Maturity Model Certification (CMMC), New York State Department of Financial Services, (NYDFS) and more. These assessments are designed to identify your gaps for different types of risk exposure, providing answers to fundamental questions:

- What assets do you have, including data, devices, cloud and on-premises infrastructure, software and networks?
- Who would want them?
- Where do the assets live, how do they interact within specific workflows and how do they move through the organization?
- What business processes depend on those assets?
- What threats could impact those assets and how likely are those threats?
- Who touches them (including third-party providers)?
- What would the impact be if the assets were lost, unavailable or compromised?
- How are you protecting them?
- Where are the gaps in protection?
- What risks do your third-party vendors pose?

Conducting a comprehensive risk assessment offers both immediate and long-term benefits. It enables risk-based prioritization and decision-making, ensuring the best use of your cybersecurity resources from the outset. It prevents over- or under-engineering your security solutions, and it can directly inform mitigation strategies and incident response planning.

While timely execution of your risk assessment is critical, bear in mind that remediation doesn't have to wait until the assessment is complete. Areas of high risk that are identified can and should be addressed along the way.

BALLPARK COSTS AND IMPLEMENTATION TIMELINE

- Pondurance offers cyber risk assessments powered by MyCyberScorecard depending on the need. Our solution helps identify your organization's gaps and prioritize improvements with skilled experts, consistent assessment processes and a powerful platform.
- Rapid risk assessments start at $10,000 and can be completed within days.
- Comprehensive NIST-based risk assessments and assessments of third-party and vendor risk typically come in between $25,000 and $75,000 and can take anywhere from six to 12 weeks depending on the complexity of the organization.

PONDURANCE

INVESTMENT #3:

Managed Detection and Response

It's hard to understand the true potential of a cyberattack until it happens to you, but today's reality is that a small or midsize organization can be shut down by a single cybersecurity attack.[6] Unfortunately, many small and midsize businesses lack the security expertise or budget to implement 24/7 monitoring and detection, and many lack the tools to monitor and detect malicious activity across their infrastructure. If this sounds like your organization, Managed Detection and Response (MDR) could be the answer. It's an affordable and highly effective way to get access to the same security operations center (SOC) capabilities that large enterprises enjoy.

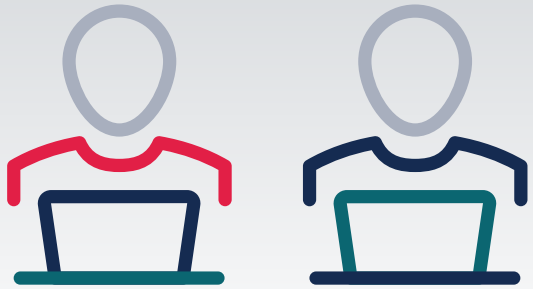
MDR services should include:

- High-fidelity, 24/7 monitoring, with 360-degree visibility into networks, logs, endpoints and cloud infrastructure
- Artificial intelligence (AI), machine learning and global threat intelligence integrated with human threat hunting and intervention
- The ability to immediately and seamlessly transition from monitoring to response, with the expertise and capabilities to quickly contain and eradicate threats

Augmenting the capabilities and capacity of your security team with MDR is a smart cybersecurity investment for small and midsize businesses. MDR enables you to:

- Stop security incidents through proactive, around-the-clock detection and response
- Reduce the time it takes to respond to emerging cyber threats, helping minimize the business impact of an incident
- Decrease time spent on false positives while helping avoid the dangers of "alert fatigue"
- Protect data and assets and improve compliance across the organization

BALLPARK COSTS AND IMPLEMENTATION TIMELINE



- It typically takes one to three months to fully deploy and fine-tune MDR services with Pondurance, which integrates U.S.-based SOC services with your existing infrastructure and controls.
- Our MDR services are modularized for maximum flexibility, and costs can vary from $5,000 to $20,000 per month for a midsize organization.

INVESTMENT #4:

Incident Response Planning

Incident response planning is a crucial investment because there's simply no way to prepare for and prevent every possible attack. Successful incident response planning can help your organization identify, prevent, and respond to business disruptions and avoid millions in losses.

Effective incident response planning reflects specific scenarios that are relevant to your organization, including those identified during your risk assessments. It engages cross-functional teams in hands-on plan development, exercises and testing, including the executive team, technical teams, forensics, human resources, legal, finance, employee communications, public relations, suppliers, partners and customer service. The goal is to create a situation where you can get the right people in the right place at the right time to receive critical information and make the best decisions.

Your incident response plan should also prepare you to comply with the legal obligations that arise in the aftermath of a cyberattack, especially to individuals affected by the incident, state attorney generals and other regulatory bodies. If it sounds like a tall order, keep in mind that many small and midsize organizations often need outside help getting incident response planning off the ground.

An experienced cybersecurity partner can help you simplify the process, leveraging their expertise in the development of an initial plan that covers these components and more:

- Response preparation
- Incident detection and identification
- Threat containment
- Threat eradication
- Operational recovery
- Learning and plan validation

BALLPARK COSTS AND IMPLEMENTATION TIMELINE

- Pondurance can help your team develop a base Incident Response plan in two to three weeks, although a more comprehensive rollout across roles and with proper testing takes longer.
- Costs can run anywhere from $10,000 to $50,000 depending on complexity, company size and the testing required.
- In addition to incident response planning, you can retain Pondurance to lead the response in the event of a cyberattack.

INVESTMENT #5:

Attack Surface Reduction

You can quickly and dramatically reduce your attack surface by investing in a handful of tactical security solutions, including:

- Multifactor authentication (MFA) – an authentication method that research shows can protect against 99% of account attacks[7]
- Domain controller protection – a personalized mix of strategies such as Remote Desktop Protocol (RDP) controls and Server Message Block protection
- Mobile disk encryption – automatic hardware-based encryption that protects data on mobile devices
- Next-generation antivirus software – algorithm-based programs that use heuristics instead of relying only on threat signatures to provide protection from viruses

You can also quickly assess and address your vulnerabilities at any point in time by investing in penetration testing. Research shows that 1 in 3 cybersecurity breaches are caused by the exploitation of an unpatched vulnerability.[8] But pen testing allows you to test for common configuration issues, identify flaws not easily discovered by automated tools and evaluate the effectiveness of your security controls.

Just remember that relying on pen testing alone can leave you vulnerable during the time in between, but you can proactively mitigate risks between pen tests by investing in an ongoing vulnerability management program. Robust vulnerability management should include comprehensive vulnerability scanning and classification of vulnerabilities, detecting and prioritizing findings related to unpatched systems and misconfigurations, and verifying any misconfigurations and confirming there are no legitimate business reasons for them.

BALLPARK COSTS AND IMPLEMENTATION TIMELINE

- Penetration Testing with Pondurance typically costs between $15,000 and $30,000 and takes four to six weeks to implement. Some of our clients conduct pen tests every few weeks, and some test annually.
- Adding Pondurance vulnerability management services to pen testing brings the total cost to between $20,000 and $40,000. External vulnerability scanning can be implemented almost immediately, followed by a scheduled rollout of internal scanning.

INVESTMENT #6:

Security Awareness Training

Employees are the first line of defense, and when it comes to sophisticated social engineering, phishing and ransomware attacks, sometimes they are the only line of defense. A recent study reveals that 88% of data breaches are caused by user error. Nearly half of the respondents surveyed said they are “very sure” or “pretty sure” they have made an error at work that could lead to a security issue.[9]

Add to that the fact that nearly 90% of organizations in a recent global survey were targeted with business email compromise and spear-phishing attacks in 2019, and you can see that employee security awareness training is no longer a “nice to have” in the security budget.[10] It’s now mission-critical.

Effective user awareness training is an investment that has been proven to help our clients prevent cybersecurity breaches and the downtime and costs associated with them. Security awareness training provider KnowBe4 has reported that, pre-training, 31.1% of users are prone to phishing attacks. After 90 days of ongoing training, that number comes down to 16.4%. After a year of ongoing training, the number comes down to 4.8%.[11]

What makes user awareness training effective?

- It’s comprehensive, accessible, consistent, engaging and ongoing
- It measures security knowledge and awareness and tracks changes over time
- It provides real-world testing through routine simulated attacks

BALLPARK COSTS AND IMPLEMENTATION TIMELINE

- KnowBe4, a Pondurance Select Technology Partner, currently provides comprehensive security awareness training for $13 to $18 per employee per year. Companies with more than 500 employees pay even less.
- In addition to a customizable and automated security awareness program, this offering includes unlimited phishing security tests and ongoing security awareness emails.
- KnowBe4 security awareness training is 100% in the cloud, so users can get started right away.

Learn more about proactive cybersecurity solutions

Today, you have to stretch your organization's budget like never before, protecting your assets while adapting to an ever-changing cybersecurity landscape. Pondurance can help you make the most of your cybersecurity investments by providing you with proactive, cost-effective solutions based on the specific needs of your organization. No matter what your company size, partnering with an innovative cybersecurity vendor like Pondurance can help you minimize complexity while instantly boosting your cybersecurity readiness.

Contact us to get started, or visit our website to learn more.

PONDURANCE

PONDURANCE

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 customers seeking broader visibility, faster response and containment, and more unified risk management for their organizations.

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

SOURCES

1 10 Small Business Cyber Security Statistics That You Should Know – And How To Improve Them, Cybersecurity Magazine, May 2021.

2 The Best Cybersecurity Predictions For 2021 Roundup, Forbes, December 2020.

3 How SMBs are overcoming key challenges in cybersecurity, TechRepublic, September 2020.

4 Passing The Cybersecurity Baton To A vCISO, Forbes, June 2019.

5 Chief Information Security Officer Salary in the United States, Salary.com, November 2021.

6 6 times when hackers forced companies to go bankrupt and shut down, PrivacySavvy, December 2020.

7 Microsoft: Multi-Factor Authentication Is 99 Percent Effective...And Other Small Business Tech News This Week, Forbes, September 2019.

8 Cybersecurity: One in three breaches are caused by unpatched vulnerabilities, ZDNet, June 2019.

9 "Psychology of Human Error" Could Help Businesses Prevent Security Breaches, CISOMAG, September 2020.

10 Security Awareness Training – Keys to Delivering a Successful Program, Security Magazine, June 2020.

11 Report: KnowBe4 Phishing By Industry 2021 Benchmarking, KnowBe4, 2021.

pondurance.com

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