PONDURANCE

5 Ways To Invest Your Remaining Infosec Budget

pondurance.com

Introduction

For a variety of reasons, you may find that you have unspent funds in your annual IT budget. These funds could have come from not investing in software or hardware as planned or, more likely, from negotiating the price of software and services down from the planned amounts. Regardless, you will want to spend it as wisely as possible.

All spend within information security should be to manage risk more effectively. You can structure your spend to reduce the impact of a cyber incident should it happen, decrease the probability of an incident occurring in the first place, or both.

In this eBook, we cover our top five picks for investing any remaining use-it-or-lose-it funds in ways guaranteed to yield an improved security posture. A 24/7 managed detection and response (MDR) service, threat intelligence, or tabletop exercises can reduce impact by speeding up your incident management, while penetration testing, vulnerability scanning, and multi-factor authentication (MFA) can reduce the probability of a successful attack.

PONDURANCE

Start or Expand Your Investment in Multi-Factor Authentication

As reported in the annual Verizon Data Breach Investigations Report, credential theft is the most common cause of a data breach over the past few years. This is because passwords are easily stolen or guessed. MFA helps reduce the risk of that threat by providing you with a code, most often cryptographically sent to a specialized app on a mobile device, that is impossible to guess and hard to steal.

Avoid solutions that send this code via SMS message to your phone or via email, as neither SMS nor email are secure methods of sending sensitive authentication data. A more secure approach uses client certificates to authenticate the devices on your network. This cryptographically superior technique is more secure against phishing than other MFA technologies, and phishing is the most common way to steal credentials. Most MFA solutions will run between $30 and $50 per user per year.

Solutions run between
$30 and $50
per user per year and are a great option to prevent phishing attacks.

PONDURANCE

Adding a Threat Intelligence Feed

Threat intelligence feeds add external context to internal events and provide visibility into both discussions about your company and corporate data for sale on the dark web. They provide indicators of compromise that can be matched against the traffic you're seeing on your networks, servers, and infrastructure. Good providers will structure this to the MITRE ATT&CK framework to allow you to hone your defenses. Threat intelligence can speed up detection of a sophisticated attack and help you identify how best to respond to the attack.

Many threat intelligence feeds specialize in providing specific, targeted information from the dark web, such as a listing of credentials that have been compromised, so it makes sense to leverage different feeds from organizations that provide different intelligence. These can cost from as little as $1,500 a year for a specialized feed to $10,000 per year for a more data-rich feed.

A threat intelligence feed can speed up detection of a sophisticated attack **costing between $1,500 (specialized feed) - $10,000 (data-rich feed) per year.**

PENETRATION TEST
$15,000 per two-week engagement
to test your survival against a skilled attack.

VULNERABILITY MANAGEMENT
$20,000 - $40,000 per year to see how your organization is perceived by those looking to attack.

Penetration Test or Vulnerability Scan for an Important, Exposed System

A penetration test is an attack simulation against your defenses. This allows you to test how well you'd survive a determined and skilled attack and how quickly your monitoring can detect and alert you on attacks targeted at your organization. The most important thing about a penetration test is that if the testers gain access to sensitive information, they will let you know how it happened so that your team can shore up your defenses.

A third-party vulnerability scan can show you how your organization looks to those who wish to attack it. While it lacks the attempt to penetrate your defenses, a vulnerability scan can readily identify those issues used by attackers at a fraction of the cost with the benefit of being able to repeat the scans as needed.

While penetration tests often cost about $15,000 for a two-week engagement, vulnerability management may be $20,000 to $40,000 for a year's worth of results.

Tabletop Exercises

Tabletop exercises provide expert training for your staff on how to handle the worst of incidents. They will use experience from incidents that other organizations have faced to educate your entire organization on how to detect, respond to, communicate internally, and communicate externally regarding a variety of incident scenarios. Good scenarios to explore are ransomware response, a data breach, or even the simulation of a disaster. Some organizations will use gaming concepts, such as a zombie attack, to help you develop a pandemic response plan.

Make certain to involve not only your information security team but also your IT staff, human resources department, legal team, and marketing team, as all of these groups would be involved in a real incident. These exercises can cost between $15,000 and $30,000 if you engage a good organization.

$15k-$30k

PER YEAR

to prepare your organization for the worst case scenario.

24/7 Managed Detection and Response

24/7 MDR uses the expertise of a company that specializes in searching for and identifying malicious traffic to establish monitoring of your entire infrastructure, servers, and applications for attacks. With the high cost and sparsity of expert security analysts, this gives you a team that can quickly detect an attack or malware in your environment and escalate to your staff for a swift and knowledgeable response. A good partner can even spot gaps in your defenses through their observation and analysis of the traffic on your company's networks. They'll use both machine learning and user behavior analytics to identify the unusual or the obscure.

Many MDR providers charge based on the volume of data they analyze; others charge a fixed fee. While the fees may be $200,000 or more per year, the cost is typically far less than what it would take to procure the equipment and tech platforms and maintain the staff to support this level of service yourself.

Fees may be
$200,000 OR MORE PER YEAR,
far less than procuring the equipment and tech platforms and maintaining the staff to support.

PONDURANCE

While there are countless ways to spend funds and enhance the effectiveness of your information security program, investing in any of the recommendations above is guaranteed to reduce cyber risk, which is the primary goal for any information security program.

Interested in putting your spare funds to use? Contact us to discuss where it may be best to invest.

CONTACT US

PONDURANCE

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

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