PONDURANCE

Practical Cybersecurity: A Roadmap for Your Business



pondurance.com

INTRODUCTION

You can tell from the news headlines that cybersecurity attacks are increasing in both frequency and sophistication. But you don't have to be a household name to be an attractive target for today's cybercriminals. In fact, for the first time in its 14-year history, the Verizon Data Breach Investigations Report shows that small and midsized businesses (SMB) are now experiencing almost as many breaches as large enterprises.[1]



Still, some of these organizations may feel that they are not at risk of a cyberattack, especially compared to their large-enterprise counterparts. But with fewer resources to devote to cybersecurity, these businesses can actually be more vulnerable to attack. And when an attack happens, it can have more serious consequences than you might realize. Research shows that SMB business leaders tend to grossly underestimate the cost of mitigating a data breach. More than half of SMB leaders surveyed believe a data breach would cost them around $10,000, when in actuality the average SMB breach costs 15 times that.[2]

Protecting your business is an ongoing process, and it requires careful planning. But with the right people, technology and policies in place, you're more likely to find and fix vulnerabilities, detect and thwart threats and avert disaster. Getting there isn't necessarily easy, but you don't have to do it alone. This eBook can help you cut through the clutter, complexity and confusion.

In the next five chapters, we'll explore the five key components of a sound cybersecurity foundation based on the NIST Cybersecurity Framework.[3] And we'll cover industry best practices and solutions like risk management, incident response (IR) planning and managed detection and response (MDR) – tools you can use to build out an effective, practical threat management strategy.

Chapter 1: Identify

You can’t protect what you can’t see, and the first step in the threat management lifecycle is about making sure you see into every corner of your organization. You’ll identify your assets, their risks and vulnerabilities, their priority levels and, finally, your specific plans to protect them.

Before you can begin to make those plans, you have to know what apps you’re running and on what devices, how your network is structured, what data you’re using and storing and how your users are accessing it all. You have to know the risks associated with each asset and prioritize those assets so you can manage risks accordingly.



The SonicWall Security Center reported 304 million ransomware attacks in 2020 alone and has reported another 304 million just in the first six months of 2021.[4]

PONDURANCE

Chapter 1: Identify

YOUR ROADMAP:

- ☐ Identify your assets, including data, devices, cloud and on-premises infrastructure, software and networks, by conducting a comprehensive inventory. Prioritize assets or asset groups based on business value.
- ☐ Determine and document your cybersecurity policies and procedures for operations, backup and recovery / business continuity, risk management and compliance. These documents should include your cadences for routine threat management activities such as backups, vulnerability scans, updates and patches, and training.
- ☐ Set identity access management (IAM) policies across all assets, then remove unauthorized devices, systems, software and users from the network.
- ☐ Find the attack surfaces and specific risks in your environment by conducting a comprehensive vulnerability assessment, including penetration testing.
- ☐ Develop and test incident response plans that include step-by-step instructions for handling different incidents and types of attacks based on your specific environment.

The success of your cybersecurity strategy relies on comprehensive testing and planning. The objective expertise of a third-party vendor can be valuable at this stage, especially when it comes to uncovering your blind spots. Consider exploring your options for risk management, internal and external security testing, compliance consulting and virtual CISO (vCISO) services.



Phishing attacks continue to be the top attack type representing a third of all attacks detected by Pondurance security analysts in 2021.[4]

Chapter 2: Protect

Protecting your organization is an ongoing and multi-threaded effort. Taking a risk-based approach is key to bringing your routine threat management activities to life, as documented in your cybersecurity policies and procedures.

PONDURANCE

Chapter 2: Protect

YOUR ROADMAP:

- ☐ Implement IAM controls based on the principles of least privilege and separation of duties. Review these controls quarterly.
- ☐ Configure systems, software and devices for security, implementing built-in safeguards such as firewalls, data encryption and multi-factor authentication. Apply uniform configurations to like devices and disable unnecessary features.
- ☐ Equip and monitor every endpoint device with effective and up-to-date antivirus software.
- ☐ Create regular secure backups on a frequency consistent with your recovery time and recovery point objectives.
- ☐ Update your asset inventory monthly.
- ☐ Conduct routine vulnerability scanning, with weekly vulnerability threat feeds, monthly external scanning, quarterly internal scanning and annual penetration testing.
- ☐ Keep systems and software updated and patched based on vulnerability scan results and as directed by vendors.
- ☐ Routinely test and update your backup and recovery mechanisms as well as your business continuity plan.
- ☐ Provide foundational cybersecurity awareness training to all employees, followed by refresher training and phish testing on an ongoing basis to keep cybersecurity top of mind.

For some organizations, these ongoing action items are more than can be managed with in-house resources. Despite best efforts, critical activities can fall through the cracks, leaving gaps in your cybersecurity strategy. As a result, businesses of all sizes often turn to security services providers to augment the capabilities and capacity of the security team. Consider outsourcing security testing and controls validation activities such as penetration testing, vulnerability management and application security testing.

Chapter 3: Detect

Organizations with even the strongest security controls can be compromised, but the faster a security incident can be identified and contained, the lower the costs associated with it. Bad actors such as ransomware groups can have your systems encrypted within an hour of gaining entry.[5] That's why detecting incidents as soon as possible is crucial.

Unfortunately, it can take months to detect and contain a breach. According to the 2021 IBM Cost of a Data Breach report, it takes 287 days on average – 212 days to identify a breach and another 75 days to contain it. A breach with a lifecycle over 200 days costs an average of $4.87 million versus $3.61 million for one with a lifecycle of less than 200 days, representing a difference of almost 30%. The differences in impact are substantial when you can detect and contain a threat in minutes versus hours, days or even months.[6]

According to recent research, smaller organizations are less likely to detect breaches in a timely manner than larger ones. Regardless of the size of the organization, 80% of breaches are discovered by external parties, a number that clearly indicates the need for organizations to put more emphasis on threat detection and response operations.[1]

AVERAGE TIME TO IDENTIFY AND CONTAIN A DATA BREACH

287 Days to Identify and Contain



PONDURANCE

Chapter 3: Detect

YOUR ROADMAP:



- ☐ Maintain full visibility into data, devices, logs, cloud-based and on-premises systems infrastructure, software and networks.
- ☐ Implement 24/7 monitoring for threats and incidents across all environments.
- ☐ Know how data normally flows through your organization. Deploying a network sensor can help, alerting you when data is suddenly flowing in an unexpected direction/path—a strong indicator that something could be amiss.
- ☐ Maintain and monitor logs that record events such as IAM activity, changes to systems or accounts and the initiation of communication channels.
- ☐ Deploy security tools such as security information and event management (SIEM) that can aggregate these logs and look for deviations from expected network behavior.
- ☐ Consider implementing other security tools such as endpoint detection and response (EDR), file integrity monitoring (FIM) and intrusion detection system (IDS).
- ☐ Consider implementing next-generation firewalls, which can provide in-depth information such as deep packet inspection as well as intrusion prevention capabilities.
- ☐ Separate real incidents from the noise of alerts so you can prioritize anomalies for investigation. Fine-tuning your SIEM can help reduce false positives, resulting in a more manageable volume of alerts to investigate.
- ☐ Test and tune your detection mechanisms on a regular basis.

Large, well-resourced organizations would typically build a Security Operations Center (SOC) to address these key areas and other threat management functions. However, if you lack the security expertise or budget to implement 24/7 monitoring and detection, or if you lack the tools to monitor and detect malicious activity across your network, endpoints, logs and cloud, consider leveraging an MDR services provider as an affordable and highly effective alternative.

MDR services are also ideal for organizations that are getting bogged down with false positives and suffering from “alert fatigue.” Acting as an organization’s SOC, MDR providers can use context and historical timelines to identify the threats that truly require the attention of security resources.

Chapter 4: Respond

When a breach happens, it's critical to have an incident response plan in place that can immediately guide you through each stage of response. During an incident is not the time for determining your policy on paying a ransom or identifying your key stakeholders. That's what your incident response plan, discussed in Chapter 1, is for.

Your incident response plan is not a one-and-done exercise. It's a living document that must be tested and updated regularly. Each person must understand their role and responsibilities in order for your organization to respond effectively. It's also not a one-size-fits-all document. Your planned response to ransomware will be different than your response to a data breach, which will be different than your response to a lost or stolen device. Your incident response plan should include different playbooks to reflect different potential risks and scenarios.

It should also reflect different potential threat vectors. Malicious data breaches occur through a wide range of threat vectors, including compromised credentials, cloud misconfigurations, vulnerabilities in third-party software and phishing. In fact, according to IBM research, those vectors account for nearly 75% of all malicious data breaches.[6]

"It's critical to have an incident response plan in place that can immediately guide you through each stage of response."

PONDURANCE

Chapter 4: Respond

YOUR ROADMAP:

- ☐ Review the security event to confirm it's not a false positive and then work quickly to triage the incident to investigate the type and source of the attack and assess the potential scope of the impact.
- ☐ Stop the incident immediately to reduce the impact on business operations. Contain the threat by isolating or shutting down the affected systems, networks, servers, databases and devices to prevent further spread to your network.
- ☐ Preserve evidence and collect critical information while it's still available. Gather logs, memory dumps, audits, network traffic reports and disk images – any evidence that can be used to analyze the origin, impact and intention behind the attack.
- ☐ Eradicate the threat and prevent future occurrence. Patch the entry point to ensure the attacker cannot regain access.
- ☐ Determine if any sensitive information was breached or data loss occurred.
- ☐ Initiate communications with internal and external stakeholders, as outlined in your incident response plan. Work with your communications team on the content and timing of public statements.
- ☐ Engage with your legal team and examine any compliance or regulatory risks to determine potential violations. Contact law enforcement and any other required government agencies.
- ☐ Perform a root cause analysis to determine the attacker's steps to gain access to your systems and update protection and detection mechanisms accordingly.
- ☐ Perform a company-wide vulnerability analysis to ensure all vulnerabilities have been addressed.
- ☐ Keep a log of all incident response activities and results of investigations.

Chapter 4: Respond

It often makes sense for an organization to seek outside expertise at this point in order to minimize the damage of an attack. Having access to SOC and incident response capabilities can dramatically shorten your mitigation and recovery time. Ideally, you've engaged an MDR provider that can move seamlessly into incident response when the time comes.

"A key value proposition of MDR is performing most of the incident response process," says Toby Bussa et al. in Gartner's Market Guide for Managed Detection and Response Services. "Timely and accurate incident response takes time and skill, which many organizations just don't have, especially when multiple threats need to be addressed simultaneously."[7]



PONDURANCE

Chapter 5: Recover



“The goal of recovery is to move from the immediate aftermath of an incident to full restoration of normal systems and operations,” says the National Cybersecurity Alliance.[8] Like all of the other components of the threat management strategy, it requires thoughtful planning to fully restore normal systems and operations. Recovery often begins immediately on the heels of – or overlaps with – incident response.

PONDURANCE

Chapter 5: Recover

YOUR ROADMAP:

- ☐ Confirm that all the necessary forensic evidence has been collected.
- ☐ Fully restore normal systems and operations. Repair, restore or replace affected components, whether that means restoring system images, restoring data from backups or replacing potentially compromised controls such as passwords or encryption keys.
- ☐ Leverage evidence and other critical information collected during the incident for post-incident analysis and reporting. Discuss the effectiveness of the incident response plan, and make adjustments accordingly.
- ☐ Capture lessons learned that would reduce the risk of a future incident, minimize the severity of a future incident or improve incident response time. Incorporate these improvements into your policies and procedures for operations, backup and recovery / business continuity, risk management and compliance. Update employee training and the incident response plan accordingly. Communicate these updates to all stakeholders.



Companies that find themselves in this position are actually the lucky ones – the ones that are still in business after a security breach. Cyberattacks cost companies $200,000 on average, which is enough to put some out of business.[9] Take this opportunity to put renewed emphasis on security across your organization and take the necessary steps to improve your security posture.



Learn more

Developing and implementing a practical threat management strategy is not optional for today's businesses. Cyber attackers are creative, opportunistic and motivated individuals – and even businesses and nation states. They have access to the latest tools, and they are constantly looking for available targets. Your best defense is a strong cybersecurity foundation that includes 24/7 security operations.

To learn more about MDR, watch our on-demand webinar, "Demystifying MDR for Security Conscious Buyers," or download our MDR info sheet.

To talk to an MDR expert or see a demo, contact us.

PONDURANCE



PONDURANCE

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

Copyright © 2021 Pondurance

About Pondurance

Pondurance delivers world-class managed detection and response 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. "2021 Data Breach Investigations Report," Verizon, 2021.
2 Lee, James, "The Impact of Data Breaches and Cyberattacks on SMB's and Their Employees," National Cybersecurity Alliance, October 15, 2020.
3 NIST Cybersecurity Framework.
4 "SONICWALL: RECORD 304.7 MILLION RANSOMWARE ATTACKS ECLIPSE 2020 GLOBAL TOTAL IN JUST 6 MONTHS," SonicWall, 2021.
5 "Incident Response Planning," Pondurance.
6 "Cost of a Data Breach Report 2021," IBM Security, 2021.
7 Bussa, Toby, et al., "Market Guide for Managed Detection and Response Services," Gartner, August 26, 2020.
8 "Cybersecure My Business," National Cybersecurity Alliance.
9 Steinberg, Scott, "Cyberattacks now cost companies $200,000 on average, putting many out of business," CNBC, October 13, 2019.