PONDURANCE

Privacy Is Hard To Enact Without Security

Protecting data privacy begins with cybersecurity.

INTRODUCTION

Data has become a valuable asset for any organization in today's economy. Organizations are producing and collecting larger volumes of data than ever before. Data collection is being used to manage information and make informed business decisions across a variety of verticals. Some experts even argue that raw data is more valuable than oil.[1] Data is an engine for growth. It is worth billions — solidifying its place in our modern economy.

Data has become a lucrative business worth billions to those who can "extract and refine it,"[1] which is why protecting consumer and employee PII is critical for any organization. Data breaches and the rising costs are no laughing matter. The average cost of a data breach can reach upward of $3.86 million per incident.[3]

Statista forecasts created, captured, copied, and consumed **data** to increase rapidly, reaching 149 zettabytes **by 2024** (149 trillion gigabytes)[2]

The volume of data created, captured, copied, and consumed worldwide is expected to double in the next three years.[2] With global data and its value rapidly increasing, it is no surprise that hackers or insider threats are motivated to gain access to consumer personal identifiable information (PII), employee PII, and intellectual property. Pondurance predicts that ransomware will keep leading the headlines and that the exfiltration and weaponization of intellectual property will become a focus area for nation-state attacks.

52% of breaches in 2020 were caused by malicious attacks[3]

In recent years, privacy regulations have been put in place to protect consumer data in the European Union, Brazil, and the U.S. to ensure individuals have the right to protect their valuable data. However, before data privacy can be protected, organizations must focus their defenses on securing all forms of sensitive data, starting with data security and ending with data privacy.

DATA PRIVACY IS NOT DATA SECURITY

The basics of data protection start with a comprehensive cybersecurity program. The measures an organization takes to prevent an unauthorized individual from accessing sensitive consumer PII, employee PII, or intellectual property are data security. The regulatory and compliance factors of data focus on how to properly manage, collect, share, and delete data at the consumer's request are data privacy.

For an organization to properly protect data and comply with the minimum requirements set forth by data privacy laws, both data security and data protection need to be prioritized.

PONDURANCE

DATA PROTECTION					
DATA SECURITY			DATA PRIVACY		
Encryption	Access Control	Data Loss Prevention	Discovery & Classification	Data Minimization	Subject Access Request
MDR	Human Intelligence	Breach Response (IR)	Consent	Policies	Data Deletion

Data Security and Transparency

As the number of data breaches making headlines increases, consumers are becoming more concerned about how their data is being protected. Organizations that are transparent and communicate how they are taking adequate measures to protect consumer and employee data can significantly benefit from making these changes.

If you are collecting data, implementing the following cybersecurity measures could reduce your organization's chances of a data breach:

Encryption

If organizations are online and collecting information, chances are they are handling data. With more businesses storing data in the cloud, encryption is necessary when it comes to securing digital assets in transit and at rest. Encryption can protect sensitive information by using algorithms to scramble or code sensitive information, making it readable only with a decryption key. This makes it difficult for adversaries to read confidential or sensitive information if it is intercepted in an attack or through a data breach.

Access Control

Who should have access to sensitive information in the company? Implementing access control policies is a method of guaranteeing that users are who they say they are and have the right level of access to certain systems and information within an organization. For example, the domain controller, the heart of any distributed network, responds to security authorization requests. If access to the domain controller falls into the wrong hands, adversaries have access to everything on the network including users, accounts, and sensitive information. Therefore, only individuals who need absolute access to this system should be allowed.

Data Loss Prevention

A strong data loss prevention program is key to protecting sensitive data and digital assets. An organization must prioritize and classify its data by segmenting the data by types such as intellectual property, financials, and PII. Understanding what is sensitive in your data and when it is at risk can help organizations determine what needs to be encrypted and protected by endpoint and network-based security controls.

Managed Detection and Response (MDR)

The threat to data is constant and data security should be full time. This means having deep visibility into all networks, logs, and endpoints, including 24/7 detection and response to ensure any nefarious activity within the organization's ecosystem is detected and addressed right away. Endpoints are where data can be most vulnerable, and having 360-degree visibility on and beyond endpoints is critical.

$3.86 million is the average cost of breaches caused by nation-state attackers[3]

Human Intelligence

The human element is a critical component of data security. While technology and automation are essential, human intuition and ingenuity play a big role. Human analysts, threat hunters, and incident responders acutely trained to monitor and detect malicious activity must be part of the data security solution. Understanding the consequences associated with violating data privacy regulations is a key factor in knowing which systems and data to prioritize.

PONDURANCE

Breach Response (or Incident Response)

When it comes to a data breach, every minute counts. It is critical to have a devised breach response plan for identifying, triaging, and analyzing a compromise that could affect an organization. Having a comprehensive response plan can help companies better prepare to successfully mitigate threats, assess the damage associated with any sensitive information that was seized during the attack, and improve defenses.

DATA PRIVACY STARTS WITH TRANSPARENCY

Building a comprehensive data privacy rights strategy begins with transparency. Some companies that are open with their data practices reap the benefits of long-term customer relationships, while others that choose to keep consumers in the dark run the risk of sacrificing their reputations for short-term benefits. Certain data privacy laws, like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), have similar privacy policies that organizations should follow including:

Discovery and Classification

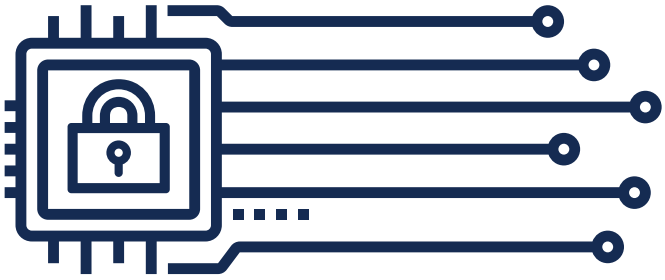
Organizations must have a firm understanding of all avenues of data collection. This means discovering and classifying their data are the foundational components of a comprehensive data privacy strategy. Data discovery is the process of scanning your digital ecosystem to determine where both structured and unstructured data resides, while data classification is more of a daunting task due to the complex level of data mapping involved to identify the types of data within an organization. Classification involves using a predefined set of patterns, keywords or rules, and classification tags or labels. These steps are tedious, but they must be done.

Data Minimization

As data collection increases year over year, organizations do not need every ounce of data collected. Data minimization includes measures put in place by organizations to limit the amount of personal data collected and set thresholds for data retention policies. By implementing a data minimization strategy, it allows an organization to minimize its data footprint that can also reduce its compliance and security risks.

Subject Access Requests (SARs) — Intake Requests

Consumers and employees that have the right to access their data under privacy laws are known as subjects. It is important for organizations to educate their consumers and employees on how they can submit a SAR to obtain access to the information an organization collects, shares, and sells about them. There are certain requirements in place to ensure an organization makes it as seamless as possible for an individual to request this data from an organization within a certain time frame to avoid further fines and penalties.



Consent

Transparency is at the heart of consent management when it comes to data privacy. Users want to know what organizations plan to do with their data, and before they grant access to this data, it is required they opt-in or opt-out to give consent to personal data. Some privacy regulations require organizations to gain consent from consumers and/or employees for marketing communications, administrative communications, and the use of their personal data.

Policies

Communication is key to creating a privacy policy. Depending on the types of data an organization collects, it could fall under multiple regulations, which is why it is critical to know where data is coming from and the sources. To ensure the right policies are in place, it is important for organizations to reach out to their legal counsel to draft their internal- and external-facing policies.

Data Deletion

In addition to knowing what types of data an organization manages, collects, retains, and shares, it is important to have a mechanism in place that can delete data at the consumer's request.

PONDURANCE

DATA PRIVACY REGULATORY LANDSCAPE

As businesses continue to lean on data analytics to understand more about consumer behavior, consumer PII will continue to be a risk that business leaders must take into account as the regulatory landscape rapidly evolves. Data privacy is centered around how data should be properly managed, and data protection laws around the world aim to give consumers control over their data.

In 2019, the European Union initiated the first data privacy regulation, the General Data Protection Regulation (GDPR), that set the framework for the U.S. to enact its own privacy rights and regulations. Since then, a number of other policies have surfaced, including:

- 2020 California Consumer Privacy Act
- 2020 Lei Geral de Proteção de Dados Pessoais
- 2023 California Privacy Rights Act
- 2023 Customer Data Protection Act

As more states and countries implement new privacy laws, it is only a matter of time until there is a patchwork of individual state privacy laws to comply with, making it more challenging for businesses to comply with future regulations.

INDUSTRY SPOTLIGHT: HEALTHCARE

The healthcare industry leverages data for a multitude of purposes, especially in the current COVID-19 era to help slow the spread of the virus. The value of stolen healthcare records continues to increase, with the average cost of a data breach within the healthcare sector reaching $7.13 million per incident.[3]

HEALTHCARE DATA	FINANCIAL DATA	INDUSTRIAL DATA
$7.13 million per incident	**$5.85 million per incident**	**$4.99 million per incident**
***263 days** to identify a healthcare data breach*	***177 days** to identify a financial data breach average time*	***220 days** to identify a financial data breach average time*[3]

pondurance.com
500 N. Meridian St., Suite 500, Indianapolis, IN 46204

PONDURANCE

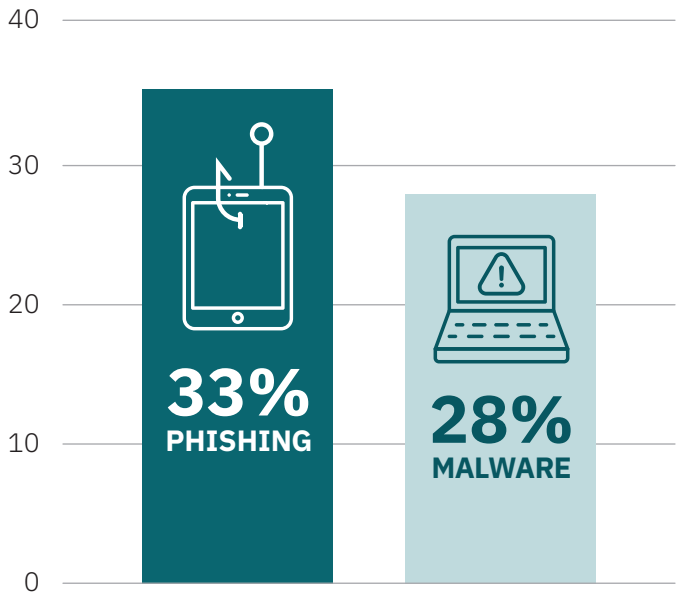
COMMON THREATS

Phishing continues to be an attack that adversaries utilize to gain access to sensitive consumer data and intellectual property. In fact, the Pondurance 2021 Quarterly Report identified 33% of attacks detected by our analysts and incident responders as phishing attacks, while 28% were identified as malware.[4]

Human error and misconfigurations continue to be the leading causes of data breaches.

Human error and misconfigurations can lead to much larger and more severe attacks such as ransomware. Implementing strong access control policies by limiting access to critical systems and using multi-factor authentication can reduce the risk of compromised credentials. As more organizations move to the cloud, organizations can easily lose sight of shared responsibility within the cloud and experience a breach due to misconfiguration. For example, cloud providers are responsible for the security of the cloud, which involves the infrastructure and the software, while the customer is responsible for securing what is in the cloud.

Top Attack Vectors



Root Causes of a Data Breach

PONDURANCE

CONCLUSION

As companies mature so should their data protection strategies. Bridging the gap between data privacy and data security could be the differentiating factor between you and your competition. Cultivating trust among your consumers, employees, and business partners is a key result of incorporating a comprehensive data cybersecurity strategy.

As businesses leverage technology to improve the quality of data and make informed decisions, the human element should always remain a critical component of comprehensive data security. Whether a business has an internal security operations center or incorporates an MDR service, having a strong data security plan in place to protect consumer data is critical.

Pondurance MDR services will provide your business with the 360-degree visibility needed to monitor and protect your intellectual property and customer data on a 24/7 basis.

ABOUT PONDURANCE

Pondurance delivers world-class Managed Detection and Response services to industries facing today's most pressing and dynamic cyber security 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 team can focus onwhat matters the 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 Pondurance.com for more information.

Sources:
1. As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants, The New York Times, Dec. 2018.
2. Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2024, Statista, May 2020.
3. Cost of a Data Breach Report 2020, IBM, 2020.
4. Pondurance Security Operations Report: 2021 Q1, Pondurance, April 2021.