Brought to you by:

Symantec

The GDPR & Managing Data Risk

for dummies®
A Wiley Brand

Understand the GDPR

Find technology that can help with compliance

Protect user data and privacy

Andrew Moore

Symantec Special Edition

About Symantec

Symantec Corporation (NASDAQ: SYMC), one of the world's leading cyber security companies, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit **www.symantec.com** or connect with us on Facebook, Twitter, and LinkedIn.

The GDPR & Managing Data Risk

The GDPR & Managing Data Risk

Symantec Special Edition

by Andrew Moore

for dummies®
A Wiley Brand

The GDPR & Managing Data Risk For Dummies®, Symantec Special Edition

Published by: **John Wiley & Sons, Ltd.,** The Atrium, Southern Gate Chichester, West Sussex, www.wiley.com

ISBN 978-1-119-48774-6 (pbk); ISBN 978-1-118-48775-3 (ebk)

Printed in Great Britain

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. For details on how to create a custom *For Dummies* book for your business or organization, contact info@dummies.biz or visit www.wiley.com/go/custompub. For details on licensing the *For Dummies* brand for products or services, contact Branded Rights&Licenses@Wiley.com.

Some of the people who helped bring this book to market include the following:

Editorial Manager: Rev Mengle

Acquisitions Editor: Katie Mohr

Business Development Representative: Frazer Hossack

Production Editor: Magesh Elangovan

Table of Contents

Introduction

If you're in the IT industry or a technology director or executive and you need to know what the European Union's (EU's) General Data Protection Regulation (GDPR) is all about and how it impacts your business — you've come to the right place.

The GDPR is a regulation adopted by the European Union that becomes effective on May 25, 2018, and that impacts not only businesses that are located in the EU, but any organization that does business with countries in the EU and/or collects data from people or businesses that reside in the EU.

The GDPR is designed to create a harmonized data protection regime throughout the EU that will make it easier to comply with data protection regulations instead of navigating a patchwork of data protection requirements in the various nations that compose the EU.

In this book, I outline the main concepts of the GDPR, how it impacts your business, and how you can be prepared to comply with the GDPR throughout the data protection life cycle.

About This Book

This book is designed to explain important concepts of the GDPR and its impact on your business and how you can prepare to comply with this data protection regime. In this book I don't intend to give a comprehensive treatment of the GDPR, but I give you an overview of the important concepts that will help you on your journey to GDPR compliance.

Legal disclaimer: The information contained in this book is not intended to provide, and does not constitute or comprise, legal advice on any particular matter and is provided for general information purposes only.

You should not act or refrain from acting on the basis of any material contained in this presentation, without seeking appropriate legal or other professional advice.

Icons Used in This Book

In this book, you see the following four icons to give you a hint about things in the GDPR or general data security of which you need to be aware.

REMEMBER

When you see this icon, I point out core information that you should take away from a topic, such as the GDPR or data security.

WARNING

When you see the Warning icon, I give you challenges or pitfalls of which you need to be cognizant.

TECHNICAL STUFF

The Technical Stuff icon gives you some extra information related to technical details of the GDPR or data security. What you see is information that isn't essential to understanding these topics but gives you some additional context you may find helpful.

TIP

When you see the Tip icon, I give you information that gives you important insights into the GPDR or a data security topic that will make your job easier.

IN THIS CHAPTER

- Looking at GDPR basics
- Examining how the GDPR protects data
- Seeing how the GDPR affects your organization
- Looking at data privacy and security
- Asking some questions
- Taking a look at the framework approach

Chapter 1
The GDPR Is Here: What You Need to Know, Now!

In this chapter, I introduce you to the EU's new data protection regime known as the General Data Protection Regulation (GDPR). This regulation has a wide-ranging impact on organizations both inside the EU and organizations that reside outside of the EU, but do business and/or collect data on entities and individuals within the EU.

This chapter isn't intended to give an exhaustive treatment of the GDPR, but it gives you an overview of key data protection considerations and security controls, and what you need to know right now to prepare your organization for its implementation.

The GDPR Is for Everyone

The GDPR is a reality, and it could apply to you — even if you're not in the European Union (EU). Starting on May 25, 2018, any organization that processes personal data related to individuals located in the European Economic Area (EEA) must fully comply with the GDPR. So, don't be fooled into thinking that the GDPR

applies only to organizations inside of the EU. The GDPR is truly global in scope and applies to any organization without regard to where it is based.

In today's globalized world, it's easy to see how the GDPR's impact is felt throughout the world.

REMEMBER

Don't think of May 25, 2018, as a "drop dead" date where there's sort of a final exam to determine if your organization is prepared for the GDPR. Instead, think of this date as the start of a new world where your organization must consistently maintain an up-to-date data security readiness and demonstrate this readiness through well-documented policies and procedures.

Understanding the GDPR

The EU's GDPR is a regulation that the European Union intended to harmonize data protection and data privacy laws throughout the member states of the EU. This regulation was adopted on April 27, 2016, and is enforceable from May 25, 2018.

The GDPR takes the 28 implementations of the EU's 1995 Data Protection Directive and combines them into a single, updated data protection *regulation* across all EU member states. The GDPR equips member states to enforce this regulation by each nation's data protection authorities (DPAs). The GDPR also imposes strict penalties on organizations that fail to comply.

Authorities may impose fines at different levels under the GDPR:

- For violations of most technical rules, up to 2 percent of the global annual turnover or €10 million, whichever is higher.
- For violations of the basic principles, and under aggravating circumstances, such as failure to comply with data protection authorities' instructions, repeat violations, or unauthorized international data transfers, a higher penalty of 4 percent of the global annual turnover or €20 million, whichever is higher, can be levied.

The authorities may also levy nonfinancial penalties, including requiring a complete cessation of data collection or processing.

In the event your organization's data has been compromised — something security professionals note is becoming increasingly inevitable — the GDPR compels your organization to report data breaches to data protection authorities within 72 hours of discovery or face some of the penalties mentioned here.

WARNING

The penalties levied by the authorities aren't the only repercussions from having poor data privacy practices or mishandling a data breach. Your organization may also suffer negative headlines, lower sales, and negative impact on stock values.

Your organization may be penalized or subject to sanctions even if a breach hasn't occurred — the GDPR requires meeting privacy obligations at all times (for example, by always maintaining an appropriate level of security for the personal data you control or process).

WARNING

If you suffer a data breach and you deliberately fail to report it within 72 hours of discovery, you risk facing the maximum penalties provided by the GDPR. You may be tempted to not report a data breach to avoid harm to your organization's reputation, but in the long run, your organization risks suffering both a damaged reputation and facing the higher end of the penalties allowed by law.

Understanding the Key Roles in the GDPR

The GDPR defines some key roles, or players in the data protection scheme. In this section, I define some of these roles so you can understand them better in the context of the GDPR. Figure 1-1 illustrates these roles in the GDPR.

Data controllers and processors

Data controllers and processors are specific GDPR terms. A *data controller* is an entity that is responsible for collecting and/or using personal data on customers, prospects, employees, or other individuals as part of its operations. *Data processors* are entities that handle data on behalf of data controllers — examples of processors include outsourced organizations that have been given the data to do something with it (like a call center) or application or infrastructure providers used by the controller to share or store data (think of cloud infrastructure and application providers).

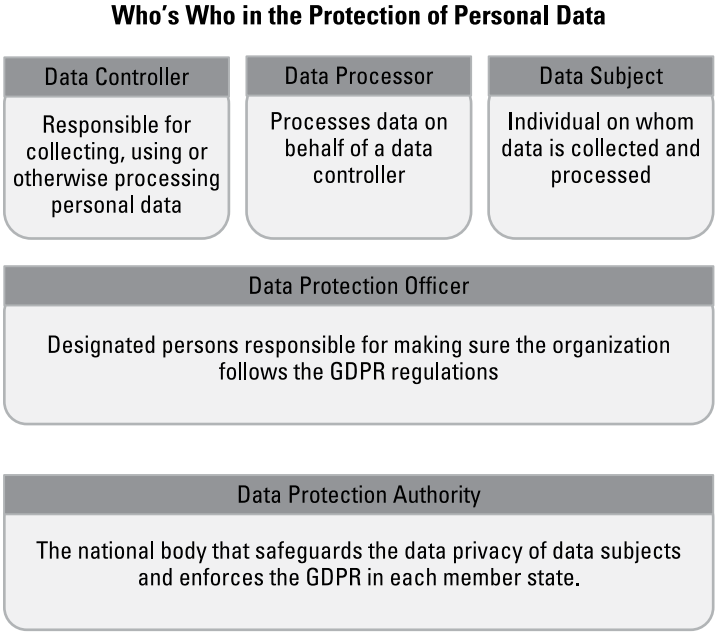


FIGURE 1-1: The who's who in data protection.

In today's digital economy, your organization in all likelihood either collects and uses personal data (you're a controller) or receives data from another entity to handle it for them as part of your business (you're a processor).

REMEMBER

The GDPR places data privacy obligations on both data controllers and processors. Later in this chapter, I discuss some examples of how the GDPR may apply to these entities.

TECHNICAL STUFF

If you're curious, you can see how the EU defines these entities (GDPR Article 4) which you can find at `http://eur-lex.europa.eu/eli/reg/2016/679/oj`.

So, now that I've summarized the definitions of these entities, how does the GDPR apply to them? Take the example of a company called ABC News that is based in Ireland but covers all of Europe. Here, the data controller is ABC News, because it's the organization that is collecting and using for its own purposes data on users — defined in the GDPR as *data subjects*. ABC news subcontracts its email marketing to a company that provides it

with mailshots and other marketing tools and a cloud provider that hosts and stores ABC News data. The marketing company and cloud provider are considered as *data processors* in the GDPR.

The GDPR introduces direct obligations for data processors

The data protection directive that precedes the GDPR contained very few obligations for data processors. Under the GDPR, data processors are subject to penalties and civil claims brought by data subjects.

Although data processors are now potentially liable, that doesn't absolve data controllers of all responsibility after data leaves their systems: The GDPR now requires data controllers, the customers of data processors, to choose only data processors that comply with the GDPR or risk penalties themselves. This requirement applies to data processors outside of the EU, such as call centers based overseas. Because data protection authorities enforce penalties on controllers for not properly vetting data processors, data processors may now find themselves obligated to obtain independent compliance assurance to reassure their customers, or find themselves subject to audit by their data controller.


TIP

The GDPR will likely ensure much closer collaboration between data controllers and data processors. It is also likely that the GDPR will push more scrutiny on the supply chain of data both in Europe and outside of Europe because companies that are located outside the EU but want to compete for EU data processing business would need to accept GDPR compliance contractually.

Data protection officer (DPO)

Under the GDPR, most data controllers and data processors will be required, or at least well advised, to appoint an officer to oversee data protection. This officer is known as the *data protection officer* (DPO). The DPO should be a senior advisor to the highest level of management in the organization who should have enough clout and independence to drive change and organization-wide data protection compliance.

Data protection authority (DPA)

The data protection authority (DPA) is the national body that safeguards the data privacy of data subjects and enforces the GDPR

in each member state. In Ireland, for example, the DPA body is known as the Data Protection Commissioner.

The DPA has jurisdiction in its member state to enforce compliance with the GDPR and issue sanctions to organizations that fail to comply. It is also the organization that represents its country on the European Data Protection Board.


TIP

Depending on which country of the European Union your organization has located its main business activity in, the local DPA will likely be the lead DPA for all administrative matters related to your organization. If you're a multinational organization or there are breaches or investigations that span multiple countries, the DPAs of several countries may be involved under the coordination of one lead DPA.

Data subjects

The *data subject* in the GDPR refers to the individual on whom data is collected. Data subjects can be an organization's customers, contractors, vendors, and even employees.

Understanding the GDPR's Impact on Your Organization

This section outlines the application of the GDPR to your organization. Scope (who/what) and jurisdiction (where) are discussed here. So, who's affected by the GDPR? Any organization that processes personal data of individuals located in the EEA must comply with the GDPR. Personal data includes data collected on that organization's employees and customers. If your organization collects personal data on an EU resident, the GDPR applies to you.

What does personal data include?

The scope of personal data goes beyond what you might think. Personal data can include the following:

- Human Resources (HR) data or customer data
- Business contact information

- Behavioral information, including website visitors' data (logged in-house or stored remotely; for example, cookies)
- IT network traffic and communication logs

Some examples of personal data can be: professional habits and practices, banking details, medical information, or even data captured from video surveillance. As a general guide, if a piece of information can be used to identify an individual (directly or via correlation, by you or even by anybody else), there's a good chance that it qualifies as personal data under the GDPR.

There is also a requirement to protect data that can be correlated with other data to reveal a person's identity. For example, combining someone's first name with his or her job title and company could allow you to identify an individual.

REMEMBER

You don't decide what's personal data; the GDPR decides. You may need to protect other types of sensitive data, not just EU-defined personal data such as intellectual property, strategic plans, or financial data. Although the GDPR doesn't govern how you handle these other types of data, the GDPR framework can help you keep it safe.

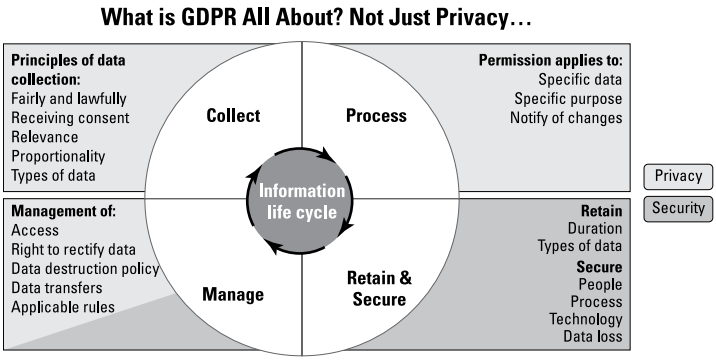
Distinguishing between Data Privacy and Security

The GDPR regulates the complete life cycle of information and isn't limited only to the protection of consumer privacy. Remember that privacy and security are often intertwined. Privacy is often focused on policies and processes that define "what" your organization does around data protection, while security represents "how" you do it by means of technical controls and capabilities.

Figure 1-2 outlines an information life cycle model that can help you with the GDPR.

- **Collect:** You must have a valid, legal business purpose for the data you collect. You must notify all data subjects of the types of data and the purpose for the data you're collecting and in general should obtain their consent to collect data.

- **Process:** If you process data in a new way or collect additional data, you must get new permission from the data subjects or rely on another ground defined as lawful by the GDPR. You must also ensure that the data is accurate and that you only collect the least amount necessary (*data minimization*). You should also endeavor to pseudonymize data (remove its direct identifiability).
- **Retain and secure:** You must consider how you store data, for how long, and the holistic steps you take to secure it. Ensure you consider people, process, technology, and information (data loss).
- **Manage:** You must put processes in place that allow for the data subjects to access their records and change them, including amending data records and requesting the deletion of records (right to be forgotten). You must also put in place a strategy to handle the case where data is lost.



Source: Symantec

FIGURE 1-2: The GDPR Information Life Cycle.

REMEMBER

Both information privacy and security risk management are ongoing projects, not a single point-in-time activity. They involve an ongoing process to ensure that risk is reduced and the risk is fully managed. It's important to ensure that any requirements from the privacy operational life cycle are built into information security management and compliance processes. Privacy shouldn't lead to separate information security projects just for compliance but should be built into overall cyberrisk and resilience management.

Answering Seven Essential Data Security Questions

You have only so much time and budget to devote to your organization's data protection.

There are seven essential questions you must ask to determine whether your organization's people, processes, and technologies are up to the task of securing data in preparation for GDPR compliance:

- What broad areas do we need to focus on for the GDPR, such as improving auditing procedures and communicating policies to all employees?
- How do we manage and report on our information risk management practices?
- What personal data is out there and where is it? Who can access personal data and who has accessed it?
- Can we monitor and, if necessary, control who can access specific personal data?
- How can we ensure protection for data wherever it resides?
- Can we detect unauthorized access or breaches of personal data?
- Can we quickly and thoroughly notify in the event of a breach?

The questions listed are designed to prompt further investigation, as they encompass broad topics. I go further into these topics in the coming chapters.

Introducing a Framework Approach to Data Security and the GDPR

In this section, I introduce a framework approach to data security and the GDPR. In this framework, there are four pillars to support

GDPR compliance across data security and privacy. These four pillars are as follows:

- **Prepare:** In this pillar, your organization should begin with getting full data visibility and then understanding the risk factors associated with data security and privacy. In this pillar, your organization is engaging in risk assessment and management of data protection and associated technologies as well as user behaviors.
- **Protect:** Here your organization is putting into place the necessary data protection and security technology and policies that reduce the risk of data breaches and ensure compliance with GDPR security requirements.
- **Detect:** Here your organization is putting into place technology and services to support your management systems and policies that enable timely detection of data security breaches or other compliance problems.
- **Respond:** Once a data breach has been detected, the GDPR requires you to notify the authorities within 72 hours if you are the data controller, or your customer immediately if you are the data processor. Your organization must be prepared to respond to and control data breach incidents in a timely fashion or risk the heavy sanctions imposed by the GDPR.

REMEMBER

These four pillars of data security are not meant to be approached in a sequential manner; instead, they are an ongoing and repeatable approach to GDPR compliance.

You must be prepared for changes or additions to the technology controls and capabilities used for each pillar to account for changes to your organization, data collection and usage, or the threat landscape. They are also by no means the only things you need to do in order to comply with the GDPR. They are, however, essential components in building a structure that brings together information security and data governance while addressing some of the key challenges that the practical implementation of the GDPR puts on data privacy and security professionals.

IN THIS CHAPTER

- Uncovering data risk and challenges
- Discovering technology to help you find personal data to assess data risk
- Understanding compliance systems and issues
- Discovering tools for assessing and managing your risk

Chapter 2
Get Prepared!

In this chapter, I discuss preparing your organization for GDPR compliance. Here you'll discover what your organization must do to prepare itself for complying with the GDPR and ultimately identify what you should do to secure and protect personal data and avoid the hefty sanctions of this regulation. Preparing for GDPR compliance isn't a one-time event, but is rather an ongoing effort by your organization to be in compliance. There are two topics I explore; the first is knowing your data, and the second is managing your compliance system.

If you're ready to find out how your organization can prepare for GDPR compliance and the technology that can get you there, read on!

Knowing Your Data

When it comes to data, you need to know who has it, why they have it, and where it goes. You also must know which data is important, and what personal data is and where it is located.

REMEMBER

There are a number of different technologies available, from Symantec and other security vendors, and only so much time and budget that your organization can devote to data protection. To quickly gauge your data protection risk factors and priorities,

as well as the value of technologies that can help you with the GDPR, ask yourself the following questions and determine whether your organization's existing people, processes, and technology are up to the task of answering them.

What personal data is out there, where is it, and who has accessed it?

One of the big challenges organizations face before they can adequately protect data is to just understand what data the company currently processes, where it goes, and who can access it. This is an especially difficult task for data that runs through cloud applications — both official ones and shadow IT apps — where IT has little security visibility or control. Without understanding this, it's hard to determine the data risk and what needs to be addressed to achieve compliance. For more on shadow IT, see the "Securing Your Data in the Cloud" section.

How well can we control what personal data is accessible and who can access it?

Once you have visibility over personal data, the job has only begun. Data governance is critical to building out a strong and compliant data protection capability. Encryption and tokenization technologies also make sure that only legitimate users can see the data; anyone who obtains the data in an illegitimate manner will not be able to do anything with it, negating the consequences if this data is stolen or accidentally exposed.

TIP

Multifactor authentication capabilities can help your organization limit access to important personal data resources so that you can minimize exposure to attacks and misuse.

How much data resides outside my network or outside the EU?

A major aspect of data protection is being able to first see and then control where data resides — in both a physical and logical sense — so as to prevent it going somewhere where the risk of compromise is too high or where it is impossible to maintain adequate data protection.

Data Loss Prevention (DLP) and Cloud Access Security Broker (CASB) technologies can logically prevent specific kinds of data from being shared with risky users or applications, on-premise or in the cloud. Cloud data protection technology can replace personal data within the forms of cloud applications with meaningless tokens, preserving the functionality of the cloud application while ensuring that the personal data never leaves the corporate network (let alone the country); this has the benefit of easing compliance risk with regard to data transfers.

REMEMBER

The GDPR identifies encryption and pseudonymization as ways to protect personal data when it's at rest or when it's in transit in and out of your network.

How quickly can we detect unauthorized access or breaches of personal data?

Numerous sources have shown that in the case of major data breaches, the targeted organization has taken over 200 days to detect that it has been breached, and in many cases, that breach was identified by external parties, not the breached organization itself. Reducing the average time to detection is one of the best ways to mitigate the impact of a data breach.

In the Prepare phase, it's important to broadly assess your organization's ability to rapidly detect threats and breach incidents. As I discuss in Chapter 4, there are many sophisticated technologies designed to help detect and block advanced attacks, including advanced threat protection (across email, endpoint, and the network), sandboxing, security analytics, SSL visibility, and malware analysis. Additionally, cybersecurity services can help support your company with round-the-clock monitoring, threat intelligence, incident response, and cyberexpertise. You should also consider technologies that contain advanced behavioral analytics or that can perform a detailed analysis of who has access to documents containing personal data.

Can we quickly and thoroughly notify in the event of a breach?

When a breach does happen, the GDPR has laid out specific requirements that data controllers need to follow within 72 hours

of discovery in terms of notifying authorities and (potentially) affected data subjects. If the organization is not a data controller but a data processor, the requirement for notification is different: The data processor's customer (typically the controller) needs to be informed, "without undue delay," well before the 72-hour limit.

In the Prepare phase, you should be trying to determine if you're able to gather sufficient data within the 72-hour period in order to understand the nature of the breach and provide a thorough notification to the authorities.


TIP

Additionally, cybersecurity services can again support your company with such capabilities, including incident response services that monitor your security operations center (SOC), fly to site incident response, and user education programs, if your organization requires this expertise. In Chapter 5, I discuss the technologies that can help you quickly respond to breach incidents and notify authorities.

Securing Your Data in the Cloud

The GDPR makes no distinction between data stored in the cloud or on the local network. However, the nature of cloud applications means that organizations have limited visibility and control, making it much harder to ensure secure and compliant data protection once the data leaves the network.


TECHNICAL STUFF

Businesses have increasingly turned to cloud products and solutions to streamline their processes and to enhance the efficiency of employee collaboration. Products such as Microsoft's Office 365 for office productivity, Salesforce for Customer Relationship Management (CRM), and Box for content management have largely replaced their desktop equivalents for use in organizations.

In a cloud threat analysis survey performed over the first half of 2017, Symantec discovered some insightful statistics about organizational use of cloud services. See Figure 2-1.

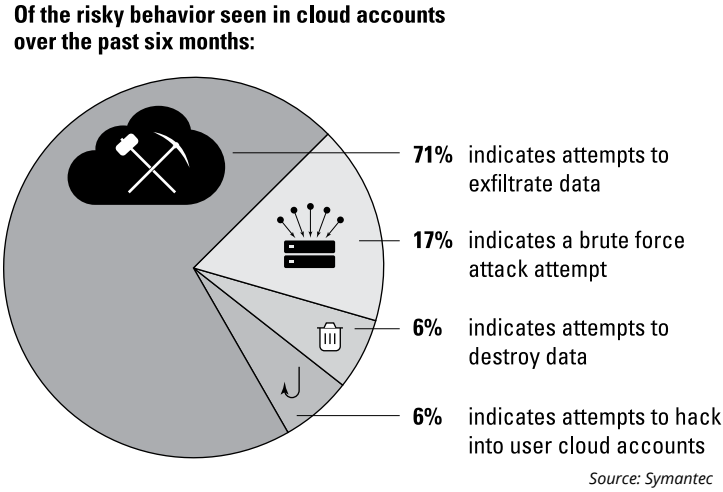


FIGURE 2-1: Some info on the risky behavior seen in cloud accounts.

Additionally:

- CIOs typically think they use 30-40 cloud applications, yet the average enterprise actually uses 1,232 cloud applications.
- Forty seven percent of organizations have active high-risk users.

Shadow IT poses a growing challenge to preventing noncompliant exposure of sensitive corporate data. Shadow data comprises all the unmanaged content that users are uploading, storing, and sharing; not only by using unsanctioned cloud apps, but sanctioned ones as well. For example, cloud storage designated as a repository of public facing documents with correspondingly lower security controls being misused to store confidential internal documents.

Even if an organization were to successfully limit employees to the use of secure, IT-approved file sharing applications, this limitation would not mean the company has fully mitigated the risk of data loss or compliance violations. Smart data governance practices such as identifying and categorizing all cloud data, then enforcing policies around its use, are sensible ways to prevent the leakage of personal data.

Cloud applications and services provide unprecedented levels of collaboration and business enablement that can help your employees and organization become more productive and efficient. They can do this while keeping your sensitive data secure — if you take the proper steps to maintain security and compliance over the entire cloud security life cycle.

The term *shadow IT* sounds like something out of spy fiction where secret agents come to mind, but it's anything but fiction. Shadow IT, in the context of the cloud, refers to the use of cloud applications and services by employees and business units without the IT department's oversight or consideration of security requirements. Symantec's Shadow Data Report shows that this is a highly underestimated risk with organizations finding they have 20 to 30 times more cloud applications in use than they expected.

Cloud Access Security Broker (CASB)

Cloud Access Security Broker (CASB) technology enables organizations to extend security visibility, control, and threat protection to the cloud.

A CASB solution sits between users and cloud services to monitor activity, assess risk, identify threats, and enforce security policies. You can deploy a CASB solution in your organization to perform various services such as, but not limited to, monitoring cloud application usage, warning administrators of potentially hazardous actions or overall risk, enforcing security policy compliance, and taking automated action for malware detection.

CASB shadow data assessment

Shadow IT in the cloud exposes your organization to large compliance risks. A CASB shadow data assessment provides you visibility into shadow IT usage by analyzing logs from your proxy, firewall, and endpoints to identify the cloud services in use in your organization and provides an executive summary to IT and business decision-makers. This assessment's flexible log format can analyze almost any type of logfile.

A CASB shadow data assessment identifies risky cloud applications based on a number of security attributes. This assessment also detects personnel using these services and how much

they're using them. You can use the intelligence gathered from this assessment to coach business units and users to select safer alternatives and use them or implement security controls to limit this behavior or mitigate its risk.

A CASB shadow data assessment allows you to control access to — and block unapproved — cloud services while allowing access to those that meet your security guidelines. You can apply granular controls directly from the proxy management console.

You can identify risk factors in cloud application traffic by uncovering threats in firewall, proxy, and endpoints by employing behavioral analytics and advanced data science.

An added benefit of the CASB shadow data assessment is that it allows you to compare cloud services and helps you make well-informed recommendations to business units to consolidate cloud services and accounts, while reducing cloud risk, saving money, and reducing complexity.


TIP

Finally, the CASB shadow data assessment generates infographics and executive audit reports with the click of a button. You can set up custom scheduled reports to be sent via email to critical stakeholders in your organization.

Data Loss Prevention

A Data Loss Prevention (DLP) solution is designed to protect your organization from data loss that can cause your data to end up in the hands of unauthorized persons, possibly with malicious intent.


WARNING

A majority of an organization's information is unstructured, and the growth of this type of data is exploding. In fact, analysts predict the growth of unstructured data will continue at over 60 percent year over year. Unfortunately, IT often lacks critical insights into the data and how it's being used. This lack of insight can lead to significant challenges in managing an organization's data governance objectives — protecting important business data, maintaining regulatory compliance, and driving down costs to manage this rapid data growth.

DLP technology can provide data insight features that help organizations improve data governance through data owner identification and visibility into usage and access permissions. This intelligence into the data enables effective data management to reduce costs, protect sensitive information, and achieve compliance.

DLP intelligence enables you to increase operational efficiency and reduce costs. To keep up with unstructured data growth, IT departments are buying more storage. If, however, organizations had a better handle on data usage and ownership, storage could be used more efficiently. DLP helps you to identify data owners, locate inactive or orphaned data, and determine file types to help guide cleanup, retention, and archiving efforts.

Protecting unstructured data against loss and misuse is a vital component to a data governance program. Data insight technology is integrated with DLP to discover sensitive data (including GDPR regulated data), identify data owners, and understand permissions and detailed access history to enable an effective data protection process.

DLP can assess which folders are at greatest risk and supports automated user notifications to facilitate data cleanup. Using an intuitive web-based interface, you can understand who is accessing data and how often they're accessing it, which helps with security investigations and audits. Access alerts identify suspicious or irregular access of sensitive data. Additionally, you can pinpoint which data is at risk, such as folders or shares that have overly permissive access rights. This information allows the data owner to lock the data down and limit access of sensitive data to only those individuals who have a business need.

TIP

Your organization needs to maintain compliance on data access and entitlements. Data insight technology identifies data owners and custodians that need to be engaged for compliance efforts. Data insight automates the process of reviewing who has accessed custodians' data — a requirement for regulatory compliance. Custodians also face the challenge of complying with data retention guidelines. Data insight technology classifies the data based on owners, groups, or roles and provides custodians the capability to automatically review stale and orphan data. These capabilities facilitate data cleanup or deletion and retention efforts.

Managing Your Compliance System

The second key area to consider is your process and system for managing compliance. Failure to comply with the GDPR can lead to the heaviest penalties.

Assessing how well you manage and report on information risk management practices

How well you manage and report on information risk management practices is a fundamental issue you need to address for GDPR compliance. Does your organization's compliance team recognize which key areas of their data handling procedures require attention, as well as what technologies can get them in shape to comply with the GDPR?


TIP

The GDPR also requires that all facets of your data protection program are documented so that they can be assessed and improved.

Leveraging tools to prepare for GDPR compliance

Preparing for GDPR compliance is no trivial matter. In fact, Article 32 of the GDPR requires organizations to manage evidence of data security compliance. The effort of navigating the GDPR and determining exactly what data is collected, where it's stored, who has access to it, and where it goes can be a daunting, months-long process.


TIP

To manage your compliance program, you may find technology that can automate IT assessments helpful, especially where they offer specific reports tailored for GDPR compliance. If you have a single view of your state of readiness across servers and applications, and have the capability to track people and process elements, the administration effort required becomes much simpler and reporting gaps are reduced.

Compliance assessment manager

Technology like Symantec's Control Compliance Suite (CCS) enables you to automate Information Technology (IT) assessments with prepackaged content for servers, applications, databases, network devices, and the cloud from a single console based on security configuration, technical procedures, or third-party controls. Such compliance assessment manager tools can also identify misconfigurations and prioritize remediation.

Automate compliance

One advantage that compliance management technology provides is that it allows you to perform a single assessment and report against many regulations, mandates, and best practice frameworks, including the GDPR.

Using technology like Symantec's CCS GDPR Readiness Assessment may help organizations to evaluate their level of understanding of the regulation, and estimate their current readiness on the path toward compliance with the GDPR. The overall outcome of this assessment will help organizations gauge how far they are from meeting certain important requirements of the GDPR. Based on the results of the assessment, action plans can be put in place.

Organizations can also benefit from an automated approach to managing their compliance with the GDPR. This can provide a cost effective and holistic way to monitor and track progress toward compliance.

Your organization needs a way to demonstrate compliance with the GDPR. Automation makes demonstrating compliance much more efficient. The Control Compliance Suite helps organizations implement a cost effective and holistic approach to procedural compliance automation, monitoring and tracking progress using the following CCS modules:

- **Symantec Control Compliance Suite Policy Manager** simplifies policy management with out-of-the-box policy content for multiple mandates, automatically mapped to controls and updated on a quarterly basis.

- **Symantec Control Compliance Suite Standards Manager** is an industry-leading configuration assessment solution designed to evaluate if systems are secured, configured, and patched according to standards.
- **Symantec Control Compliance Suite Assessment Manager** simplifies the evaluation of procedural controls by providing automated web-based questionnaires. These questionnaires can also be used to evaluate overall employee security awareness.

Endpoint management

Ultimately, personal data will be viewed from or stored on devices, making it important to ensure that an endpoint compromise doesn't lead to a data breach. Endpoint management solutions are able to help administrators manage endpoint configuration securely across Windows, Mac, Linux, UNIX, and virtual environments so you can know what devices are being used and who is using them.

Before you can effectively manage and protect endpoints, you first need an accurate picture of the environment. What software and devices are being used, who is using them, how much do they cost, and do they have the latest patches and updates?

REMEMBER

Symantec IT Management Suite discovers, inventories, and tracks all the hardware and software assets in your IT infrastructure and manages the relationships between them in the Configuration Management Database (CMDB). Armed with this information, your team can quickly identify problems, apply solutions, and document compliance.

Successful compliance with the GDPR requires your organization to uncover the risks and challenges that go with securing your sensitive data. Data Loss Prevention (DLP) and Cloud Access Security Broker (CASB) technologies help you discover and protect your sensitive data both on-premise and in the cloud. Your organization must also put in place data security compliance assessments to demonstrate GDPR compliance at all times. Compliance assessment manager and endpoint management technologies make implementing compliance assessments much more efficient.

IN THIS CHAPTER

- Applying complete data protection
- Keeping your systems safe
- Finding some tools

Chapter 3
Protect Your Data!

In this chapter, I show you how to protect your personal data — and the systems where that data is stored — to ensure your organization can achieve and maintain consistent compliance with the GDPR. Protecting data is an ongoing endeavor that goes to the heart of GDPR compliance and one that should not be taken lightly. Here you discover some strategies and automated tools that'll help you stay in compliance.

This chapter is set in two parts. The first part discusses data protection from cradle-to-grave, covering key technologies to protect you from unauthorized access, including protecting data in the cloud. The second part of the chapter explains how to protect data systems from threats such as malware.

It's natural that you will be inclined to focus on the protection methods and technologies described in this chapter. Although they're critical, protecting data extends beyond just these capabilities — you also need to ensure you're well *prepared* by understanding the key risks (see Chapter 2) and you have strong breach *detection* (see Chapter 4) and *response* (see Chapter 5) processes in place.

According to IT analysis firm IDC, the total volume of data worldwide will increase tenfold by 2025, driven by the usage of cloud and mobile applications. Organizations must figure out how to protect both their existing data that may be scattered across

on-premise repositories, cloud services, and user devices as well as new content. As the total amount of unstructured data grows, so too does the risk of losing control over what is truly sensitive.

Along with balancing the need to protect a diverse range of sensitive and valuable information — regardless of whether the data is on-premise, on a user's device, or in the cloud — organizations need to allow collaboration among employees, partners, customers, suppliers, and investors, spanning organizations and locations worldwide.

Data protection must be engrained into your organization's culture. You must ensure that your people are trained how to detect and protect valuable data, supported by technology to automate, simplify, educate, and mitigate errors in their data handling decisions.

Applying Cradle-to-Grave Data Protection

To comply with the GDPR, you must be able to show that your organization's personal data is being adequately protected from the time it is created until the time it is destroyed. Additionally, personal data must be protected when it is at rest, in transit, and in use.

WARNING

Protecting data generally involves a number of risk factors, including:

- Users may not recognize that data is regulated. Where they do, they often forget, or lack the tools to protect data on their own.
- Valuable data can often move to shadow IT cloud services, or is stored on unmanaged devices or accessed by unintended users; all of these scenarios involve sensitive data moving beyond the relative safety of corporate-controlled IT resources.
- Even if data has been properly encrypted, it is often difficult to ensure that the data is only shared with intended legitimate users and can't be decrypted by unintended recipients.

» Many organizations' data protection strategies have focused on securing data held on devices and systems. They have not adequately considered how to protect data throughout its life cycle. In addition, the security of those devices and systems is managed in isolation of the data protection risk.

Encryption and tokenization

In today's information economy, organizations collect and share data with users across multiple organizations and locations, and this makes it increasingly difficult to keep that data safe and usable. Increased regulation, customer scrutiny, and risk awareness are driving the need to protect information. Attackers take advantage of the fact that personal data is externally shared and stored and look for security flaws that can allow them access for their own purposes. Therefore, organizations need to take measures to ensure data that falls into the wrong hands is still protected. The GDPR recommends the use of *encryption* and other *pseudonomization* technologies (for example, tokenization) to achieve this.


TECHNICAL STUFF

Encryption is the process of applying mathematical algorithms to encode data so that only those authorized can view the data. Encryption involves the use of cipher keys that are known only by the sender and receiver. The keys scramble and unscramble the data so that the authorized parties can view the data, while anyone without the right key will not be able to do anything with the data.

Tokenization is an alternative *pseudonomization* process. There are a number of tokenization techniques, and here I describe Symantec's approach. Sensitive data is replaced with a token that has no relationship to the original data. A token vault, controlled by a secure gateway, maps the sensitive data to the new unique token. Therefore, the only way to restore data is through the secure gateway, which retrieves it from the token vault that is retained within the organization's network. This technique is very powerful for storing data in the cloud, because you can store tokenized data in the cloud, with the assurance that the sensitive or regulated data is still under your direct control, in a physical location of your choice.

This reduces the risk of exposure by, for example, a SaaS provider being breached. Naturally, it is important to adequately protect the token vault to keep it safe from potential attackers.

Secure user access

Another critical aspect of protecting data is to ensure that only the right people can access it. Securing user access is essential to keeping your personal data out of the wrong hands.

REMEMBER

With Data Loss Prevention (DLP) it is also possible to control data transfers to untrusted recipients and third-party organizations that may not be GDPR ready; together with a Cloud Access Security Broker (CASB), geolocation restrictions can be applied to control users trying to access data in the cloud. Finally, access to data can also be revoked at any time from a cloud-based management console.

Multifactor authentication (MFA) is a method of access control in which a user is granted access only after successfully presenting multiple separate pieces of evidence to an authentication platform. MFA generally involves users authenticating from the following categories: knowledge (something they know), possession (something they have), and inherence (something they are). For example, a user entering a password, then entering a randomly generated access key from a hardware token or an authentication application on the user's mobile device.

TIP

MFA is an important tool for securing user access because, for example, if a user's password is compromised, an unauthorized person is still not able to gain access because another piece of evidence is required (such as a phone or other device) for that. The other advantage is that if people have reused passwords across many systems, a breach in one system doesn't compromise the others because the additional authentication element is still secure.

Data monitoring and tagging

To ensure all the right data is properly protected, organizations must also engage the content creators and editors in the decision-making process because their judgment and knowledge are critical to properly identify and ascribe context to the sensitive data you must protect.

Earlier in this chapter, I describe the benefits of a user-based classification model. Symantec offers classification technology that also integrates with DLP. Symantec Information Centric Tagging (ICT) seamlessly integrates into the user interface of leading productivity applications, such as Microsoft Office and Outlook, enabling employees to effortlessly apply a classification tag to data.

TIP

Tagging can prevent users from transferring unclassified content and ensure that classified files and messages are automatically encrypted and protected with the application of digital rights and role-based access control that follows the data everywhere — on-premise, in the cloud, on user devices — even when shared with external parties. This ensures sensitive data always stays in the correct hands and reduces data loss and non-compliance risks.

Data protection in the cloud

To protect your organization's data, you must have visibility into it both on-premise and in the cloud. To ensure that you can adequately protect valuable data (including personal data as defined under the GDPR), you need to be able to find it on the network (such as in file share, databases, repositories, and on endpoints) as well as in the cloud. You should have the same level of visibility and control irrespective of where the data is.

DLP solutions can offer you customizable data protection policies that look for specific data types that are subject to regulations, including the GDPR. DLP technology monitors data anywhere it's stored and anywhere it's transmitted, such as via email, the web, or from endpoints (for instance, removable storage or clipboards).

REMEMBER

Advanced DLP solutions can automatically discover a wide range of data types (for example, unstructured data or text in images) through content inspection, not just relying on a classification tag.

For situations where users are generating data that they know is private, DLP allows them to classify data very easily. By engaging the users who create and handle the data to determine what's truly sensitive, information-centric tagging can help reduce data loss prevention "false negatives" and enhance detection of sensitive data with more accurate outcomes, without requiring administrators to author ever-more-complex policies. Once classified, DLP policies automatically protect the data.

In addition, advanced DLP solutions also include analytics tools that can correlate user access records with sensitive data use, providing insight into usual, and importantly, unusual activities or patterns that could be an early indicator of a personal data breach.

New trends in protecting data

Many organizations have security in place designed to protect devices and users, but increasingly organizations have shifted their focus to the data itself.

Symantec's Information Centric Security (ICS) is such a data-centric approach that provides complete protection for personal data throughout its life cycle with policy-driven encryption and access management. It brings together DLP, CASB, data classification, user authentication, and analytics to discover sensitive data and protect it wherever it goes via information centric encryption (ICE; see Figure 3-1).

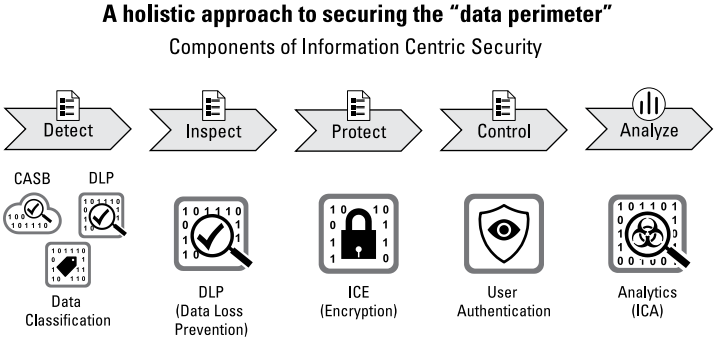


FIGURE 3-1: Components of information-centric security.

REMEMBER

ICE utilizes user identity to provide protection and control. User identity governs whether a file is decrypted, and the degree of access permission granted (for instance, print or save). Coupling this with a two-factor authentication solution reduces the risk of account takeover. Central control is provided as user access records show who accessed which documents, and access can be revoked with the flick of a switch.

Protecting Your Data by Protecting Your Systems

Protecting your data is vital, but you can't protect your data adequately if your data hosting systems don't have the proper protection as well.

Take a look at the parts of your systems that need protection and some tools for implementing that protection in an automated fashion.


TIP

Protecting your data from cradle to grave requires protection of your systems that handle that data: endpoints, mobile, and in the cloud.

Endpoint protection

The constantly evolving nature of today's IT environment has driven attackers to use more sophisticated attacks to infiltrate networks and endpoints, which in turn makes it much easier to get to the data moving across them. Organizations are more concerned about cyberdamage and disruption as ransomware attacks are trending upward, as was evident with the WannaCry and Petya outbreaks in 2017. In addition, the attackers' expanding use of file-less and stealthy attacks combined with *living-off-the-land* techniques (leveraging common IT tools for attacks) threatens the confidentiality, integrity, and availability of endpoint assets.


TIP

So, what can security teams do to address cyberattacks? Managing multiple point products and technologies is overwhelming, and challenges mount when managing security across multiple geographies with diverse operation systems and platforms. With limited resources and limited budgets, security teams want easy to-manage technologies that can integrate with each other to improve overall security.

Symantec Endpoint Protection delivers multilayered protection to stop threats regardless of how they attack your endpoints. Endpoint Protection integrates with existing security infrastructure to provide orchestrated responses to address threats quickly. The single, lightweight Endpoint Protection agent offers high performance without compromising end-user productivity, so that you can focus on your business.

Mobile endpoint protection

Aside from behaving like computers, the nature of mobility means that more data is being collected. Much of this collected information qualifies as personal data, so protecting these devices is vital, especially in the face of growing volume of malware and threats

targeting mobile devices. Despite all of this, mobile devices have generally not received the same attention from security teams.

Symantec Endpoint Protection Mobile's risk-based mobile security approach uses a multilayered system to defend against all detected threats that put business data at risk of exposure, theft, and manipulation, while respecting users' need for privacy, productivity, and a great mobile experience. Symantec's Endpoint Protection Mobile identifies threats and takes deliberate actions in real time, leveraging machine learning to protect devices, their users, and the resources to which they connect.

Cloud workload protection

Enterprises are rapidly moving their information systems to public cloud services such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform to increase business agility, relieve pressure on understaffed IT departments, and save money.

WARNING

However, without careful thought, just relying on the public cloud secure infrastructure may not give you the degree of control, consistency, and protection you need to meet the requirements of the GDPR, especially as data controllers have shared responsibility.

Symantec Cloud Workload Protection (CWP) allows you to view, monitor, and protect all your workloads and the personal data in them from a single intuitive console. CWP automates workload security, providing discovery, visibility, and protection against advanced threats to personal data and other valuable information.

Advanced threat protection

Today's advanced malware and zero-day attacks fly under the radar of traditional security technologies. Thousands of new malware samples appear every day and advanced zero-day threats, sophisticated malware, social engineering, and targeted attacks from outside sources or even employees are constantly increasing in size and scale. Traditional blocking strategies simply aren't effective against advanced attacks. To tackle this, a mutlilayered security model is needed that protects endpoints, email, networks, and the cloud.

Symantec's Integrated Cyber Defense Platform offers a range of technologies to prevent traditional malware, as well as advanced threats.

Employing advanced threat intelligence

Through securing endpoints, email, web, and cloud environments, Symantec gathers lots of security telemetry that powers its Global Intelligence Network, enabling a richer understanding of the actual threat environments, the nature of attacks, and the appropriate responses. This data powers many of the security technologies offered by Symantec, enabling it to offer a wide portfolio of products and services. Symantec continually updates this intelligence base and uses it as a source of continuing product innovation.

Symantec solutions are supported by Symantec's Global Intelligence Network (GIN). Over 8 billion security requests from 80 million web proxy users, 163 million email users, and 175 million endpoints provide comprehensive threat telemetry.

Symantec's threat intelligence approach covers the complete security life cycle, from risk assessment to data discovery, protection, and access control. This threat intelligence ensures threats can be anticipated in order to maximize protection, and advanced detection techniques correlate data across attack vectors to allow rapid identification, isolation, and remediation — all enhanced by Symantec's GIN, its civilian cyberthreat intelligence network, allowing it to see and protect against the most advanced threats.

This is an essential asset for data controllers and data processors who, under the GDPR, are required to stay abreast at all times of their data risk exposure, and to dynamically adapt their security posture accordingly.

IN THIS CHAPTER

- Identifying leaks
- Prioritizing and analyzing data leak incidents
- Analyzing the role of threat intelligence

Chapter 4
Detect Data Breaches

In this chapter, I discuss tools and techniques for detecting and analyzing data breach incidents as early as possible so that you can take action to minimize the impact of the breach and mitigate the damage to individuals, to your organization's reputation, and to customer goodwill, as well as the potential penalties under the GDPR.

Today, attackers use a number of techniques to infiltrate their target organizations, whether by exploiting vulnerabilities, through social engineering, via phishing websites, or some combination of all of them. Once inside the victim's infrastructure, targeted attacks traverse endpoints and the network to access key systems, steal credentials, and connect with command-and-control servers, all with the goal of compromising the organization's most critical systems and data.

This problem is only growing. In 2016, 357 new malware variants were found along with about 4,000 zero-day vulnerabilities. Today, preventing threats is simply not enough. Attackers are moving faster. At some point, they will find their way through. Research in 2015 showed that it can take organizations 120 days on average to remediate found vulnerabilities. Undetected threats and slow remediation can leave customers' organizations exposed and result in significant cost, including but not limited to, the loss of intellectual property and sensitive data, financial losses, and

reputation damage. On top of that, significant amounts of alerts and the user impact from infection could raise IT overhead and disrupt customers' business.

TIP

The threat landscape is constantly evolving. To find the latest Internet Security Threat Report (ISTR), visit `https://www.symantec.com/security-center/threat-report`.

Read on to discover more about detecting data breaches!

Discovering When Data or Systems Are Compromised

The GDPR goes beyond just protecting data subjects' personal data, requiring your organization to also monitor effectively all personal data in your custody, and most importantly, to detect and record any breaches and to notify the authorities and those involved in a timely fashion if the breach creates a risk to data subjects. You have some important questions to consider:

- Can you detect advanced and stealthy threats that are active in your environment?
- Can you detect a data breach as it's taking place and assess its scale?
- Can you rely upon your existing, traditional cyberdefenses to pinpoint an attack in real time and protect your personal data assets? Can these defenses be enhanced with new tools that can improve your ability to detect signs of a breach?
- Can those systems "learn" from past attacks to better identify threats and breach incidents in the future?

REMEMBER

Typical data breach events involve the attackers being on the network for over 200 days, according to Symantec's ISTR and Verizon. During this time, they can inflict massive damage and will have enough time to plunder virtually all the data they want. Improving your capability to detect data breaches early can greatly reduce the time and freedom they have and the amount of data they can steal, reducing the impact a data breach has on the persons concerned and, of course, on your organization.

Advanced Threat Protection

An Advanced Threat Protection (ATP) solution is a unified platform that uncovers, prioritizes, investigates, and remediates advanced threats across multiple control points from a single console. Each control point represents a vector that attackers can take advantage of to invade an organization and compromise its data assets. Typically, there are four control points that an ATP solution can evaluate:

- Endpoint
- Network
- Email
- Web traffic

Each of these modules sends event information from different control points to the ATP platform that correlates and prioritizes all the malicious events, allowing security analysts to focus on what matters the most. Symantec's ATP uncovers stealthy threats that others miss by leveraging one of the world's largest civilian threat intelligence networks combined with local customer context, thereby providing state-of-the-art protection for GDPR-relevant data across the organization's infrastructure.

TECHNICAL STUFF

ATP also provides you with granular attack details and allows you to remediate all instances of threats in minutes.

Here's what ATP technology can help you do:

- Detect, prioritize, investigate, and remediate threats across multiple control points in a single console before any data breach materializes.
- Uncover stealthy threats across endpoint, network, email, and web traffic, giving you full visibility into the various systems where personal data may be found.
- Prioritize what matters the most by correlating across events from all Symantec-protected control points for complete visibility and faster remediation so as to quickly zoom to high priority events like GDPR-relevant data incidents, which require expeditious reporting, the failure of which could expose the organization to hefty penalties.

- Contain and remediate any attack artifact in minutes, with a single click so as to minimize the risk of negative impact on individuals concerned, thereby mitigating the requirement to notify the incident.
- Customize incident response flow with public APIs and third-party Security Incident and Event Management System (SIEM) integration so as to streamline, expedite, and possibly even automate mandatory data breach recording and notification procedures.

One of the challenges that incident responders face today is that they're overwhelmed with too many alerts, which makes it very possible for a major data breach incident to be masked by the sheer volume of alerts and go ignored — even if it's been detected! An Advanced Threat Protection (ATP) solution leverages correlation technology that aggregates suspicious activities across all installed control points, prioritizing threats based on various attributes, including the type, scope, complexity of a threat, and more.

REMEMBER

Once an event has been identified as malicious, ATP allows you to remediate all instances of the threat in minutes. With a single click of a button, you can quickly delete a file, whitelist or blacklist a file or a domain, or isolate an endpoint from communicating to the rest of the organization and the Internet.

Symantec offers ATP technology to correlate data from endpoints, networks, and email in order to identify sophisticated attacks, using security analytics to help you focus on the most risky.

Symantec's ATP platform also provides unique visualization of related Indicators-of-Compromise of an attack, including a complete graphical view of how all Indicators-of-Compromise are connected to each other. An analyst can easily find out the impact of an incident and see all files used in an attack, all IP addresses, and URLs where the file was downloaded from, and all affected registry keys with the graphical view. She can then remediate any of these attack artifacts with one single click, effectively containing the spread of an attack. This allows you to quickly establish the extent of a personal data breach, gauge its likely consequences, and document the remediation actions taken. These are all important elements to report to authorities in cases where the breach is worthy of being notified under the GDPR.

Security Analytics

Security Analytics is like a security guard observing and extensively documenting what goes on in your network. It enables you to identify malicious or suspicious activities and payloads hiding within the network, giving you complete visibility and context before, during, and after a compromise. A Security Analytics solution also offers you advanced network forensics, anomaly detection, and real-time content inspection for your network traffic to identify when protected personal data assets may be on the path to being misused or compromised in any way or form.


TIP

Using a Security Analytics tool, you can better understand the full scale and context of an incident, enabling you to resolve it faster. This is key for you to be able to manage data breaches in line with the GDPR's tight breach notification schedules and requirements.

With the push of a button, you can see what's happening on your network, including critical areas such as the amount of encrypted traffic crossing your network, as well as any signs of malware, data exfiltration, or other suspicious behavior that is being hidden inside that encrypted traffic. You can also see the presence of risky applications on the network, and network behavior that falls outside of the normal traffic behavior of your network.

Although many incident responders and security operations teams need to manually trawl through various logs and status windows to piece together evidence that a breach is taking place, Symantec's Security Analytics brings all of this information into one place and helps to piece it together to point security teams toward major incidents in a proactive, automated manner. Symantec's Security Analytics can proactively search for potential hidden threats and gaps across your network, endpoints, and servers, to enable security teams to identify and remove threats before they can launch an attack.

Behavioral analytics

Behavioral analytics helps you identify risky traffic patterns and high-risk activities, allowing you to view and prioritize threats by quickly identifying anomalous events that can point to account takeovers, data exfiltration, and data destruction attempts. You can cross-correlate data collected with associated detailed logs to verify suspected incidents such as personal data breaches. If any

users have been targeted by the attack, you can create policies (1) to protect those users from further damage and (2) to block compromised user accounts from accessing the service to prevent fraudulent data access or loss. Some examples of metrics that behavioral analytics uses to compute a threat score include:

- Invalid logins
- Surprising geography
- Long sessions
- Sudden location changes
- Suspicious location

TIP

Behavioral analytics can be very powerful and privacy-enhancing with the right safeguards in place.

Behavioral analytics can trigger alerts for further investigation, or you can craft policies to prevent unwarranted uploading and sharing of these documents. You can use policies to control how this data is handled and track for further follow-up any attempted compliance violations.

TIP

Behavioral analytics can coach users on appropriate technology use (on-premise through to cloud) and automatically alert users when they attempt high-risk behavior and inform them of security response actions. An example alert might inform users that they are attempting to share GDPR-protected personal data outside of the organization in violation of policy.

You can detect risky activities and malicious attacks such as brute force attacks or ransomware with behavioral analytics and quantified threat scores. You can use this information to trigger controls to block, quarantine, or alert on accounts with high-risk activity.

Malware is a scourge that impacts many organizations around the world. A strong Cloud Access Security Broker (CASB) can use behavioral analytics can defend your organization from malware using advanced protection complete with file insight, antimalware, file analysis, and sandboxing techniques.

Malware sandboxing refers to the use of a safe, isolated environment (typically emulated or virtualised) to simulate a computer and run suspicious files, scripts, and so on to determine if they are malicious. This way, new malware and threats can be discovered without actually infecting real systems.

Endpoint Detection and Response (EDR)

Endpoint Detection and Response technologies help you stop attacks on endpoints from becoming wide-scale breaches. An EDR solution should detect, isolate, and eliminate intrusions across all endpoints using Artificial Intelligence (AI) and advanced threat intelligence. EDR can help you expose advanced attacks in real time and mitigate their impacts quickly by performing such tasks as:

- Detecting file-less and memory attacks
- Capturing and studying endpoint activity for ex post verifications
- Extending EDR to remote users
- Correlating incursions across endpoint, network, and email control points

Symantec's EDR solution allows you to detect and expose stealthy attacks using its Advanced Threat Protection (ATP) at the endpoint. Symantec's EDR solution detects and exposes these attacks by using the following features:

- Machine learning and behavioral analytics to detect and expose suspicious activity, and prioritize incidents
- Automatically identifying and creating incidents for suspicious scripts and memory exploits
- Leveraging the Symantec Endpoint Protection agent

Cyber Security Services (CSS)

Cyber Security Services (CSS) employ human experts, advanced machine learning, and a host of other advanced capabilities to assess and strengthen your organization's cybersecurity posture. When assessing your organization's cybersecurity posture and deciding

if you could benefit from Cyber Security Services, especially in the perspective of the GDPR, you should ask yourself the following questions:

- Are we able to rapidly detect breaches, or can we be better?
- Do we have the necessary technologies and expertise to detect breaches as rapidly and comprehensively as possible?
- Are our in-house capabilities as cost- and resource-effecient as they can be?
- Does our threat intelligence program provide us with a current and complete picture of the threat landscape?
- Do our security operations diagnose critical threats in real time?
- How quickly and effectively do our teams respond when faced with an incident?
- Are we developing our people to protect our organization from an attack?

TIP

You need a robust threat intelligence program and a clear understanding of the current and emerging threat environment to create a proactive and effective defense as required by the GDPR. Cyber Security Services can provide you a full view of the threat environment so your team can create the right strategy for managing cyberattacks.

To have an effective cybersecurity posture, your organization must have a security program monitoring your environment 24 hours a day, 7 days a week using global threat intelligence to detect advanced attacks. Cyber Security Services should provide you technology and human expertise, supplemented by the latest threat intelligence to help you better manage your organization's cybersecurity so as to stick to the state-of-the-art benchmark defined by the GDPR.

When your organization handles incidents correctly, it drastically reduces the cost, duration, and exposure to your business and minimizes the impact not just on you, but also on those whom the GDPR seeks to protect first and foremost: the data subjects. With Cyber Security Services in place, your organization can move from ad-hoc reactions to a repeatable, optimized program so you can react decisively when an incident occurs and learn from every attack to defend better against the next one.

Symantec offers Cyber Security Services, which provides your organization a purpose-built portfolio of human expertise and advanced machine learning capabilities and technologies all powered by global threat intelligence.

Cloud Access Security Broker

Most organizations use or are adopting cloud applications and services. Office 365 and Google Suite provide a range of business applications. Box and Dropbox focus on collaboration boosting file sharing. Salesforce, ServiceNow, and others provide platforms for specific functions. Infrastructure services such as AWS and Azure provide the foundation for even bigger enterprise cloud IT initiatives.

Detecting threats in the cloud requires leveraging either real-time gateway detection for unsanctioned and sanctioned cloud apps or APIs to get near-real-time detection of incidents in select sanctioned cloud applications. Detecting threats and attacks is no easy task because the attackers have become increasingly sophisticated.


TIP

Symantec's CloudSOC Securlets use APIs to integrate with many popular cloud applications like Salesforce, Dropbox, Box, Office 365, and many others. Securelets allow you to monitor and protect your GDPR-relevant personal data stored in these cloud applications as well as traffic between these applications and your organization. CloudSOC Securlets extend your existing DLP policies and workflows to the cloud without having to re-create them for cloud stored and shared data, to gain consistent visibility and control over shadow data on-premise and in the cloud.

Quick detection of data breach attacks requires the right tools and processes

By the time you discover a data breach attack, it's likely that the attackers have had access to your network resources and data for a long time! With enough time, sophisticated attackers can wreak havoc — accessing your valuable customer data and causing harm to your customers, employees, and your organization's brand and reputation.

The best way to mitigate the risk of data breaches is to reduce the time that it takes to detect a data breach incident. Technologies like Advanced Threat Protection (ATP), Security Analytics (SA), behavioral analytics, and Endpoint Detection and Response

(EDR) applied in your organization automate the tasks of detecting attacks by monitoring the threat vector and applying analytics to determine changes in system behavior that indicate an attack is in progress. Behavioral analytics can be used to monitor users' behavior for suspicious activity that may indicate an attack is in progress, or at least indicate that users are engaging in risky behavior when handling data. Behavioral analytics can also be used as a coaching tool to guide your users to safer data handling processes. CASB technology helps your organization detect data breaches on the cloud by applying the same technologies you can use to detect data breaches in your on-premise systems.

Attackers have become much more sophisticated in their tools and methods. You need the right technology and processes in place in your organization to detect attacks the moment they start — before attackers can destroy your organization's reputation and harm your customers.

IN THIS CHAPTER

- Plugging leaks by rapid response to data breaches
- Notifying interested parties of a data breach
- Remediating data breaches
- Documenting lessons learned

Chapter 5
Respond to Data Breaches

Hackers have become more sophisticated in their tactics and technologies. In recent years, you've probably heard about the large data breaches in the news like the data breach at Equifax in 2017 and Target stores in 2015, but what about the breaches you don't hear about? According to research performed by Symantec in 2015, roughly three quarters of data breaches contain data for fewer than 25,000 identities and data breaches on the scale of Target and Equifax are actually outliers — irregular occurrences that fall outside of the norm. Therefore, it's a mistake to assume that you are too small to be breached. Automation and the growing hacker community make any organization with valuable data a viable target.

In this chapter, I give you some information about responding to data breaches. A core part of the GDPR is the requirement for data controllers to notify the authorities of a data breach within 72 hours of its discovery and for data processors to notify their customers as soon as possible. However, being able to notify about breaches is only one part of responding to them. You also need to be able to resolve (stop) the breach and take steps to improve your defenses so that a similar event can't happen again. In fact, a breach notification isn't truly complete if it doesn't contain information about these elements of investigation and remediation.

WARNING

Failure to notify the authorities of a data breach within 72 hours of its discovery will jeopardize your compliance with the GDPR, increasing the risk of you facing penalties under the regulation (which, in the most serious cases, could amount up to 4 percent of your global turnover or €20 million, whichever is highest).

You're reading this chapter because you want to avoid these penalties and damage to individuals as well as your organization's brand and reputation, so read on to discover how you can respond quickly to data breaches and remain in compliance with the GDPR, as well as inspire ongoing trust with your customers. Maintaining a GDPR compliance posture is not just a one-time endeavor — it's an ongoing process where your organization consistently analyzes its data breach response capabilities and applies lessons learned to continuously improve.

Stopping the Attack and Restoring Your Systems

After spending years focusing almost exclusively on preventative cybersecurity, IT professionals recognize that network and data security incidents will happen. No organization or business is immune from increasingly sophisticated attacks from around the world. The data you collect is valuable and there's no shortage of people who'd love to get their hands on it for their own gain, and if you give a skilled and highly resourced adversary enough time, it will eventually find a gap in even the most resilient security postures. Therefore, your organization must be prepared to not only prevent attacks, but detect them and mitigate their effects. And with the GDPR, there is the added requirement to be able to understand the extent of what happened and notify the authorities within 72 hours of detection if you are a data controller, and if you're a data processor, you need to inform your customers (the data controllers) in even shorter cycles.

REMEMBER

Although many data breaches are carried out by malicious parties accessing customer information, data breaches can also happen when insiders make mistakes. For example, an employee losing a data-rich laptop at the airport could also be considered a breach.

Much like when you detect water coming from the ceiling due to a burst pipe, your first response must be to call the plumber while plugging the leak in the pipe to keep more water from doing further damage. Even before that, you might want to shut off the water! The same holds true for a data breach. Once you've discovered the breach, you must take immediate action to prevent more data from being compromised (for instance, by being accessed by hackers or unintended recipients). The less damage done, the fewer customers or employees who will be harmed by the breach and the less damage to your organization's business and reputation.

Just like in the plumbing scenario mentioned, you first must know from where the leak comes; or in the case of a data breach, from where in the system the data loss occurred.

Once you've figured out the source of the breach, you must plug that hole right away! To prevent further damage, you may first need to revoke the unauthorized access to the data or quarantine infected systems. If you've implemented some of the advanced breach detection capabilities I describe in the previous chapter, you should be able to rapidly detect the breach, isolate its nature, and take remediative measures.

In order to remediate data breaches quickly, you must have the right tools and technology in place. Also, it's vital that you get any compromised devices quarantined and restored as quickly as possible.

Remediate breaches at the device level with Endpoint Detection and Response (EDR)

Rapid response to a breach comes with great preparation. First, as discussed in the previous chapter, you must have tools in place to monitor your network, applications, and devices to detect the breach in the first place. Once detection has occurred, you can use the knowledge gained by these tools to identify indicators of compromise (IOCs) and connect them to understand not just the root cause of the breach, but also how it developed and what happened as a result.

Endpoint Detection and Response (EDR) systems help you contain and respond to threats more precisely using Advanced Threat Protection (ATP) techniques. ATP not only monitors your endpoints

(and wider network) for threats, it can also help you prioritize the most critical and then mitigate the effects of a data breach.

When ATP detects a threat, it can help you gain visibility into the attack history by continuously monitoring activity and analyzing process logs that help you see exactly what has happened over time so you can determine the length and extent of the attack.

ATP hunts for threats by searching for indicators of compromise across your organization in real time. When ATP detects indicators of compromise it, for example, seals off affected endpoints by isolating them from your network so that you can begin your investigation without further damage. ATP systems can also provide cleanup, deleting malicious files and their associated artifacts from all compromised endpoints and getting these endpoints back in service — sometimes in minutes.


REMEMBER

In earlier chapters, I discuss the processes of encryption and tokenization of data. Encryption prevents unauthorized users from reading data and tokenization removes the identifiability from personal data, making it *pseudonymous.* Both processes are extremely important because if you can demonstrate that the data accessed by hackers isn't exploitable (for example, because it is encrypted or tokenized), it's more likely that you won't have to report the data breach and remediation will be much easier, too. The personal data you hold (and other sensitive data) should be encrypted whenever appropriate so that in case attackers access your data, they won't be able to exploit it for their gain and harm the subjects of the data accessed.

If you employ an integrated solution, such as Information Centric Encryption (ICE) combined with Data Loss Prevention (DLP), you can selectively encrypt files that contain personal data. This reduces negative user experience and keeps data safe through monitoring and controlling data access in real time. With ICE you can:

- Restrict what level of access to personal data any particular user has using digital rights management.
- Revoke access to personal data if a malicious insider or hacker obtains it.
- Monitor personal data and usage access patterns to identify suspicious behavior or unauthorized access.

Indicators of compromise could be obtained by a variety of data sources, but the analysis of such a vast and diverse set of information is resource-intensive. Behavioral analysis provides extensive data protection telemetry that analyzes data from multiple feeds, including user access (identity telemetry), corporate asset data, and alerts from other security systems (threat telemetry).

Symantec Information Centric Analytics (ICA) is such a behavioral analysis system that helps identify an anomalous behavior of a specific account or machine, which can expose a malicious insider or an account takeover. With drill-down functions connecting the account to DLP incidents, you gain visibility into what specific sensitive data was exposed and why. Central monitoring of data access enables organizations to track sensitive data and to identify by whom and from where sensitive data is accessed after the breach. Even if data was exposed from authorized user accounts, it is then possible to rapidly revoke access. Information Centric Security helps to investigate a data breach and respond quickly. Symantec CloudSOC also provides behavioral analytics capabilities that can be used to detect anomalies in cloud application usage.

Cyber Security Services — making your security team a dream team

Not all organizations have the means to detect, let alone respond to, a data breach. Many IT departments are already overtaxed and aren't prepared when a breach has occurred and yet they must quickly respond and mitigate the damage done.

Cyber Security Services (CSS) assists organizations to help them remediate and respond to data breaches using state-of-the-art technology and experts in the cybersecurity industry.

Imagine if your organization had at its disposal a team of over 1,000 certified, carefully vetted and continuously trained cybersecurity professionals who have, on average, over 12 years of in-field experience tracking over 700,000 threat actors and groups globally. CSS contains a hand-picked army of security professionals recruited from organizations and government agencies around the world to offer your organization the expertise to address every phase of the attack life cycle.

Consider this. The worst-case scenario has happened and your organization has experienced a data breach and you need both to report the data breach and to immediately stop the attack from continuing. A "dream team" of cybersecurity professionals can respond at a moment's notice and get to work straightaway to stop the attack, respond appropriately, and get your system up and running as soon as feasible.


TIP

Based on where your organization's breach detection and response capabilities currently are, and where you want them to be, you could decide to rely on CSS on a permanent basis, or on a transitional basis until your own incident response technology and expertise is up to the job.

Responding Quickly and Effectively to Data Breaches

According to the GDPR, if you are the data controller you must notify the data protection authority of any significant data breach within 72 hours of discovery. If you are a data processor, you need to act even more quickly to inform your customer (the data controller), so it in turn can notify the incident to authorities within 72 hours. The report to authorities must include likely consequences of the breach and the action you will take to mitigate adverse consequences to the data subjects. Specifically the notification of a breach must:

- Describe the nature of the personal data breach, including the **categories and rough number of data subjects** concerned and the **categories and estimated number of data records** concerned (including whether that data was protected, for example, by encryption, or not).
- Recommend **measures to mitigate** the possible adverse effects of the personal data breach.
- Describe the **consequences** of the personal data breach.
- Describe the **measures** you propose to take or have already taken **to address** the personal data breach.

Security Analytics helps you detect and respond to data breaches quickly

With the increasingly sophisticated threats targeting your organization, you need increasingly intelligent defenses that enable you to quickly and effectively respond. A quick and effective response requires full visibility into your network traffic and insightful security intelligence capable of uncovering breaches, so they can be quickly contained and remediated. Security analytics or network forensics solutions enable your organization to conduct comprehensive retrospective analysis, and react to security issues in real time to protect your workforce, your customers, partners, and other stakeholders; fortify your network; and improve your security processes.

Security Analytics are a key part of incident response and forensics solutions. Security Analytics can capture and index network traffic, and can even reconstruct files or webpages in order to gain full visibility into what happened. It is vital that this data is stored in an optimized and highly secure file system for rapid analysis, instant retrieval, and complete reconstruction to support all your incident response activities, such as reducing the time it takes to resolve security incidents and conduct swift forensic investigations.

Symantec's Security Analytics deliver:

- **Application classification:** More than 2,800 applications and thousands of descriptive metadata attributes, including content types, filenames, and more are classified for easy analysis and recall.
- **Real-time threat intelligence:** Direct access to the latest threat intelligence, via tight integration with intelligence services and the Symantec Global Intelligence Network, a network of thousands of customers and millions of users worldwide, as well as numerous third-party threat reputation services.
- **Anomaly detection:** Advanced statistical analysis on your captured data and baseline of your organization's network traffic and activity. Security Analytics alerts you to anomalous patterns where you can pivot to the anomaly investigation view to see when the anomaly occurred, how often, and which parts of the network were involved.

- **Emerging, zero-day threat detection:** Automatic brokering of unknown files to malware analysis or third-party sandboxes for detonation and threat scoring helps you incriminate or exonerate suspicious activity in your environment.


REMEMBER

Security Analytics can give you the insights you need to understand the context of security events in your environment, so you can quickly contain and remediate the full extent of a security incident and support post-breach forensics activities.

Cyber Security Services (CSS) can quickly analyze and report data breaches

CSS experts can provide management support and communications, empowering your executives to make the right business decisions related to response actions. CSS follows generally accepted forensic procedures to collect, preserve, and analyze evidence in accordance with your objectives. These procedures include a variety of techniques such as log analysis, network and systems forensics, advanced malware analysis, and security intelligence to determine the root cause, timeline, and extent of the incident.

Documenting Lessons Learned

Data breaches are scary and keep IT department leaders and executives awake at night. The thought of individuals suffering harm and the perspective of financial penalties inflicted by authorities along with the diminished brand reputation and possible costs of civil litigation make quite a compelling case for investing in superior security and response capabilities.


TIP

Nevertheless, if a data breach does happen, it is vital that your organization take advantage of all possible lessons that can be learned from the incident to give your organization a strengthened security posture going forward to reduce the likelihood of data breaches occurring in the future.

Once the data breach notification and remediation activities have concluded, the CSS team of security experts can provide your organization a comprehensive report of the response investigation

with recommendations and proposals on how to avoid future incidents from observed on-site issues and behaviors, including executive and board-level summaries of its findings.

Security experts can equip your staff to be better able to avoid and respond to security incidents in the future by training your security operatives with tools like incident response readiness assessments, tabletop exercises, advanced threat hunting, and attack simulations such as sending expertly crafted phishing emails to employees of your organization to train them not to fall for them.

CSS security experts can train your personnel to be more aware of data security and to change their behavior to avoid security incidents in the future. CSS experts work with your IT department to create and maintain incident "playbooks" that your organization can use both to simulate and to respond to real-world data security incidents. These playbooks define specific steps to follow that are unique to distributed denial of service (DDoS) attacks, advanced persistent threats, malware outbreaks, web server compromise, and so on.

It's possible (and even necessary) to harden your security posture against future incursions by patching vulnerable systems, updating threat databases to be aware of the latest malware and attack techniques, or even blocking high-risk applications or websites.

TIP

How your organization responds to a data breach incident can make the difference between a minor security incident that can be easily remediated or a full-blown data breach incident with many thousands or millions of customer records being compromised and the ensuing individual harm, public relations disaster, and financial hardship that come along with it. If your organization is prepared with the expertise and technology necessary to detect, mitigate, and respond to a data breach incident in a timely fashion, it is highly probable that your organization can survive the incident and remain protected from those consequences. Taking these measures and accompanying them with thorough documentation will also give you a much better chance to avoid potentially heavy fines imposed by data protection authorities, while maintaining your brand's reputation.

IN THIS CHAPTER

» Ten things about the GDPR

Chapter 6
Ten Things about the GDPR You Need to Know

In this chapter, I show you ten key things to know about the GDPR and how you can leverage data security to help maintain privacy and compliance.

The GDPR is a comprehensive data protection regulation that replaces 28 different data protection regulations in the European Union (EU). Much more than any past data protection legislation, the GDPR provides for strong enforcement mechanisms and empowers protection authorities to levy heavy fines on organizations for noncompliance.

The contents of this book have sought to provide some comprehensive guidance, but if you're new to the GDPR and want a quick brief on what you need to know about the network and information security and incident response requirements of the GDPR, you've come to the right place.

Although the following ten points are designed to help as you prepare your organization for compliance before the May 2018 deadline, remember that GDPR compliance demands an ongoing process, so use these guidelines as you engage in continual improvement of your data risk and security postures to maintain your GDPR compliance.

- Starting on May 25, 2018, the GDPR is enforceable. The GDPR allows all the member states to enforce compliance on all organizations that operate in, or target the European Union's (EU) internal market. Enforcement also affects organizations that may not reside in the EU but do business in or collect data on individuals physically located in the European Economic Area.
- The GDPR allows authorities to impose fines of up to 2 percent of an organization's global annual turnover or €10 million, whichever is higher. Under aggravating circumstances, such as failure to comply with data protection authorities' instructions, repeat violations, or unauthorized data transfers to third countries, a higher penalty of up to 4 percent of the global annual turnover or €20 million, whichever is higher, can be levied. Nonfinancial penalties may also be levied, including a cessation of all data collection and processing activities.
- The GDPR requires organizations that are data controllers to detect, record, and, in case of significant privacy risk, report data breaches to the data protection authorities within 72 hours of detection. Controllers may also need to inform the individuals impacted by the breach. Organizations that are data processors handling personal data on behalf of other data controllers are required to inform such controllers of any data breach immediately.
- In the context of the GDPR, personal data not only consists of data your organization collects on its customers, but also includes identifiable data collected and maintained on its employees, vendors, and even unknown third parties such as unique website visitors. A GDPR compliance audit and management system is a must to ensure you have identified the major risk factors and can track progress to compliance.
- The GDPR requires that personal data be protected (for instance, using appropriate encryption, pseudonymization, or tokenization techniques) at rest and in transit, and also to be secured while in use. Data encryption can complicate the capability of your users to share and access data efficiently, so your organization must have a solution that allows them to encrypt and decrypt personal information efficiently. Beyond encryption and pseudonymization, controlling access to the data with strong authentication is essential to keeping data protected.

- Protecting, monitoring, and reporting on personal data stored and transferred to the cloud is a difficult challenge for organizations to comply with the GDPR. Your organization could benefit from a Cloud Access Security Broker (CASB) solution to secure, monitor, and detect security issues, and to detect, record, and potentially report data breaches.
- Knowing where your data is can be complex, and the proliferation of shadow IT usage by employees creates further challenges for your organization. Data discovery technology can help you identify GDPR-protected data, wherever it is, giving you a true perspective on the scale of the issue. For example, you can leverage CASBs to produce shadow IT audits to discover data in the cloud. Additionally, you can use DLP to identify personal data across all data loss channels, in order to develop a strong risk reduction plan.
- To comply with the GDPR's data protection requirements, it is important to not only protect your personal data, but also your underlying IT systems that store, process, and transfer your data. You should review the effectiveness of cybersecurity protection at the endpoints, in the cloud, on the network, and on mobile devices. A blended security approach built on a common platform will deliver strong protection and be simpler to deploy and manage.
- To detect data breaches, you must be able to monitor data at all points in your systems, including on the network and in the cloud. You can use technology (for example, Security Analytics, CASB, or Advanced Threat Protection) to assist your security teams. Alternatively, you might consider the use of outsourced managed security services to monitor the security of your systems.
- Responding to an incident can be overwhelming, especially where resources are limited. Using an outsourced incident response team can ensure a speedy resolution to a breach, and minimize the disruption. Alternatively, ensure your own staff are appropriately trained and participate in regular training exercises.

Find out what you need to know about the GDPR!

If you're concerned about data privacy and need to know what the EU's General Data Protection Regulation (GDPR) is all about and how it impacts your organization, then this book is for you. The GDPR represents a single data protection regulation that is harmonized across all EU member states. Even if you are outside the EU, you may be subject to the GDPR if you handle data on European individuals. This book covers the regulation, describes how it applies to organizations, and shows how leading technology and services can help you comply.

Inside...

- See how the GDPR affects your organization
- Learn the data protection framework
- Find personal data everywhere
- Keep your systems and users safe
- Detect, respond to, and recover from data breaches

Go to Dummies.com®
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-48774-6

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.