WHITE PAPER

OVERCOME YOUR COMPLIANCE CHALLENGES

Meeting the demands of industry regulations requires an effective strategy.

EXECUTIVE SUMMARY

Security- and privacy-related regulations used to be mainly specific to a single industry, such as healthcare or finance. Today they increasingly cover much wider areas, including any organization handling personal information on consumers, and many states and localities have their own regulations or pending legislation. Determining which regulations an organization must comply with, identifying the organization's compliance requirements, and being prepared to remediate issues and produce evidence of compliance on demand are tough challenges for nearly every organization today, especially in the increasingly dynamic and distributed environments most organizations have.

Fortunately, there's a clear path forward: Be proactive when it comes to compliance. Taking a strategic approach, where the organization focuses on addressing its security and privacy risks first, then identifies gaps between its collective compliance requirements and the controls it has implemented, minimizes duplication of effort and wasted resources — not just now, but for many years to come. Compliance requirements are not going away. The sooner they're tackled, the better.

This white paper addresses the following questions to help organizations plan their next steps:

- What does the regulatory landscape look like for organizations in a variety of industries?
- What are the key challenges to complying with these regulations?
- What are the key elements of a compliance strategy?
- What solutions and services can be effective in helping organizations meet their compliance objectives?

A Changing (and Demanding) Regulatory Landscape

The regulatory landscape changes frequently, almost always growing in size and complexity. Being aware of existing requirements is vital, as is knowing what new requirements may be imposed in the near future. Numerous industries must comply with a variety of regulations administered by a wide array of entities, such as government agencies and industry leadership organizations. Below are summaries of four regulations that affect a variety of organizations. Each summary explains the basics of the regulation and its key requirements, which organizations it applies to, and possible penalties for violations.

Health Insurance Portability and Accountability Act of 1996: The U.S. law known as HIPAA defines a wide variety of requirements related to health insurance and healthcare. Healthcare providers, insurance companies and other healthcare-related organizations must protect the security and privacy of patients' healthcare data, in paper and electronic formats. HIPAA defines high-level administrative, physical and technical controls that organizations must have and use. HIPAA itself has not changed over the years, but subsequent laws such as the Health IT for Economic and Clinical Health (HITECH) Act have added requirements. The U.S. Department of Health and Human Services (HHS) investigates reported violations of HIPAA, and it may fine noncompliant organizations or, in extreme cases, recommend criminal investigation.

Payment Card Industry Data Security Standard: The PCI DSS defines security requirements for banks, retailers and other organizations that handle credit or debit card data for several major card brands, including Visa, MasterCard, Discover and American Express. The PCI DSS strives to prevent retail fraud by making it more difficult to steal card data. The standard requires protecting not only credit and debit card data, but also the computers, networks and other systems that handle the data, as well as computers, networks and systems that directly interact with them. It was first released in 2004 and is updated every few years to take into account changes in security risks and risk management. Although the PCI DSS is not a law or regulation, many contracts require organizations to comply with it, and organizations that fail to fully comply can be fined or even lose the ability to handle credit and debit card data, which could be fatal to many businesses.

General Data Protection Regulation: GDPR, a data privacy law from the European Union, took effect in 2018. It does not just apply to businesses located in the EU; it applies to any organization anywhere in the world that has certain types of data on any citizens of the EU. The GDPR covers a wider range of personal information than most other data privacy laws, so it applies to organizations that might not otherwise be concerned about privacy. There are many requirements in the GDPR, including protecting the confidentiality of personal data, reporting any data breach within 72 hours, and giving people the opportunity to opt in before delivering any content to them. Through the GDPR, the EU can fine organizations for breaches of EU citizens' personal

Nearly
250,000

The number complaints of potential HIPAA violations the Health and Human Services Department has received since April 2003. HHS has fined offending companies over **$111 million** and referred more than **800 cases** to the Justice Department for criminal investigation.[1]

Source: [1]HHS, "Enforcement Highlights," December 2019

data, even if the organization was not at fault (for example, a third party handling the data on behalf of the organization might have been responsible), and these fines can be large.

California Consumer Privacy Act : On January 1, 2020, CCPA took effect. It applies to larger organizations doing business with California residents, plus any organization doing business in California that acquires, sells or shares personal data for at least 50,000 people, or that gets at least half its revenue from selling personal data. The CCPA defines "personal data" broadly, so it considers information such as IP addresses that could be associated with a person or household as personal data that must be protected. The CCPA also requires numerous consumer protections, such as allowing people to prohibit the sale of their personal data and requiring organizations to delete all personal data for a consumer upon request. Organizations violating the CCPA can be fined, and organizations with data breaches may be required to pay damages to each affected California resident via class action lawsuits.

Many organizations are affected by more than one of these regulations, such as a healthcare provider in California that handles credit card payments. These organizations face the additional complexity of achieving and demonstrating compliance with multiple regulations, but fortunately, they're likely able to apply much of their effort for compliance with one regulation to others as well.

Settlements and Fines for Compliance Violations

Failures to comply with regulations can result in companies paying huge settlements and fines, especially when data breaches have occurred. Here are some notable cases from the past few years.

- In 2019, British Airways paid a $230 million fine for violating the GDPR. Failure to properly secure customer data led to the theft of sensitive customer data and credit card information for 500,000 people.
- Equifax paid a $575 million settlement, including $100 million in fines, for a data breach exposing personal information for 147 million people. The fines in part stemmed from Equifax failing to comply with the Gramm-Leach-Bliley Act, which requires businesses to protect their customer data.
- Marriott was fined $124 million for GDPR violations involving a company it acquired in 2016. Marriott did not take the necessary steps to ensure the acquisition followed sound security practices, so hundreds of millions of customer records were exposed for years.
- Uber failed to secure customer data, leading to a data breach affecting 57 million people, then failed to disclose the breach for a year. Uber paid a $148 million settlement to 50 U.S. states and the District of Columbia for violating data-breach notification laws.

In addition to fines and settlements, which multiple jurisdictions often levy, noncompliant companies have many other expenses, such as paying for credit monitoring services for people affected by a breach. These expenses, along with damage to a company's reputation and loss of revenue, can be overwhelming. For example, in 2019, the American Medical Collection Agency filed for bankruptcy in the aftermath of a data breach affecting more than 20 million patients.

The Challenges of Compliance

Complying with all applicable regulations is challenging and costly. Simply determining which regulations currently apply and identifying new and emerging regulations can be time-consuming and require the expertise and diligence of legal and compliance professionals, especially for organizations with international customer bases. And that's just one aspect of the many challenges of compliance.

Aspects of various compliance requirements differ from others, and many requirements are high level or otherwise vague, with room for interpretation. This can be good, because it provides flexibility, but understanding the requirements and determining how to meet them become more time-consuming. There's also the risk of unnecessary duplication of effort if the organization's compliance efforts are not centralized or at least centrally coordinated. Different parts of an organization addressing different regulations may implement controls that do the same thing, or even implement the same security technology more than once.

Implementing security controls to meet requirements almost always involves protecting data — identifying the data that needs to be protected, such as customer personal information or credit card numbers, then preserving the confidentiality of that data no matter where and how it is processed, stored or transmitted. Third parties acting on behalf of the organization also need to protect the organization's data, and the organization may be responsible for ensuring that those third parties comply with the requirements.

Some regulations require even broader protection of data. One possibility is safeguarding data not only in digital formats, but also in physical formats: data displayed on screens and observed by unauthorized people, data printed out and left in unsecured areas, and conversations about data made within earshot of people not authorized to hear that information. Another requirement in regulations such as GDPR and CCPA is that organizations must be able to identify all the data they have for a person on request, provide that data to the person within a set time period and destroy someone's personal information if they request it. Many organizations don't have data asset inventories, let alone the capability to pull it all together on demand, and would be hard-pressed to comply with requests from consumers.

Further complicating compliance is that it often requires securing not just the data the regulations specifically address, but also the systems, networks, physical facilities and other

elements of the organization's environment. Even if regulations don't specifically call out those elements as needing to be secured — although some do — it's often implied and more often an absolute necessity. Using strong encryption and other robust security controls to safeguard data is only part of compliance — if anyone can easily guess a default password and gain administrative access to a database server, the robust security controls don't matter.

Additional considerations organizations commonly face in addressing regulations:

- Organizations should monitor their compliance status at all times; an organization can fall out of compliance at any time. It's the organization's responsibility to be constantly vigilant, identify instances of noncompliance, and address them quickly to restore compliance.
- Organizations should be prepared to respond quickly and effectively to noncompliance notifications from regulators. This generally involves assessing the deficiency, remediating it, ensuring that the deficiency no longer exists and providing evidence of this to regulators. If customers or others have been adversely affected or could have been adversely affected, the organization should be prepared to formally notify regulators, customers, the public and others.
- If legacy systems need to be secured, it may be difficult or even impossible to achieve some requirements because the legacy systems can't support the necessary security controls. Sometimes an organization can find other ways to meet a regulation's requirements, such as performing security monitoring and maintenance tasks manually instead of automatically. Sometimes it may be necessary to upgrade or replace a legacy system to ensure that data is sufficiently protected.

There's one final challenge to keep in mind: "Compliance" is not the same as "security." Just because an organization, or systems and networks within an organization, comply with a regulation does not mean they are adequately secured. These regulations are intended to address security and privacy issues, but they aren't by any means the equivalent of having sound security and privacy programs or risk-management capabilities. While compliance is certainly important, holistic security efforts are ultimately more important.

Strategy, Solutions and Services for Compliance

Experts recommend that organizations take a more proactive approach to compliance. In years past, a tactical approach was most common, in which organizations would react to individual regulatory mandates. But with the number of regulations most organizations now need to comply with, the sheer complexity of all the requirements, and the always-accelerating rate of change in technologies, reactive approaches can't keep up anymore.

There's also increasing recognition that compliance shouldn't be the primary driver for security and privacy. Focusing on compliance first typically causes organizations to implement a large number of individual security and privacy controls without coordinating the controls throughout the enterprise. This means duplication of effort and wasted resources not only for initial deployment, but throughout the entire lifecycle of the controls. Every time another regulation becomes relevant to the organization, the reaction is to implement another wave of security and privacy controls, which only increases the control complexity and long-term effort needed.

A more effective approach to compliance involves strategically analyzing relevant security and privacy risks, using data from that analysis to predict issues, and then addressing those issues within an organization's security and privacy programs. This gets the organization ahead of compliance requirements. By the time regulations emerge, the organization has already put the appropriate measures in place, and ensuring compliance with new regulations should not require much effort. An organization's compliance program and its security and privacy programs should work closely together and ultimately be fully integrated as the organization's compliance maturity improves. An effective compliance strategy will break down silos within an organization and create an atmosphere of

Maintaining Compliance in a Changing Environment

Circumstances regarding regulatory compliance change frequently. Organizations must plan to keep up with these changes or risk noncompliance. Here are examples of some of the types of changes to track:

- **REGULATORY CHANGES:** Some compliance requirements, such as PCI DSS, change periodically, and organizations must adjust their operations to account for these changes. Also, the generally accepted interpretation of some requirements may shift over time. For example, as a particular security control becomes a best practice, organizations may be expected to add it to their environments.
- **TECHNOLOGY CHANGES:** As an organization's technology changes — whether adding new technologies or upgrading existing systems to enable new capabilities — an organization may need to reassess its compliance requirements and achieve some requirements differently — or even achieve some requirements that didn't apply before.
- **BUSINESS CHANGES:** An organization's presence and scope may change, such as acquiring new companies, expanding the customer base to additional states or countries, or adding new types of product or service offerings that are subject to other regulations.

knowledge sharing and collaboration that benefits everyone involved.

Starting a Compliance Program

As an organization starts a compliance program, it should include these steps:

1. Determine which regulations and which requirements apply to the organization, and identify which parts of the organization each requirement affects (databases, systems, geographic locations, etc.) Whenever feasible, map requirements across regulations to minimize duplication of effort (such as checking more than once for compliance with the same requirement).
2. Assess the state of the organization's security and privacy controls that help meet the regulatory requirements. Conduct a gap analysis to identify any compliance requirements that the organization does not fully meet.
3. Plan to address all gaps, making sure to prioritize actions within the plan appropriately. It's critical to include the security and privacy programs in the planning because they are responsible for doing the actual control implementations, monitoring and maintenance. In some cases, changing how the organization operates, such as outsourcing a particular function to a third party and contractually transferring responsibility for compliance to that third party, or reducing the data provided to third parties, may be the best way to address a gap.
4. Work with the appropriate personnel (for example, security and privacy professionals, lines of business) to implement the plan.
5. Reassess the state of the organization's controls and verify that no gaps remain.

Building and Maintaining a Compliance Program

A successful compliance program brings together people and processes throughout an organization. Participation and cooperation among teams such as marketing, sales, billing, customer support and legal are critical. Ultimately, compliance involves everyone in an organization. Everyone's roles related to compliance must be clearly defined, and everyone must be trained on their compliance responsibilities. And as the details of compliance change over time, roles must be redefined, and training updated or augmented to reflect changes in responsibilities. The organization should also engage experts such as lawyers and compliance consultants where needed to supplement the skills and knowledge of the compliance program's staff and other personnel.

Another key element of a successful compliance program is executive support. If executives don't fully buy in to the

The Role of Chief Compliance Officer

As regulatory compliance has become a more important and larger responsibility, some organizations have added the role of chief compliance officer. A CCO is in charge of compliance activities throughout an organization for all regulations, particularly security- and privacy-related requirements. This includes analyzing regulations and determining how the organization should meet their requirements, monitoring compliance, and responding to internally detected or externally reported instances of noncompliance.

Not every organization needs a CCO, but a CCO should be particularly helpful for an organization that matches any of the following criteria:

- The organization operates in a highly regulated domain, such as finance or healthcare.
- The organization operates in a line of business that pending legislation would apply to (for example, state legislatures have many consumer privacy regulations under consideration).
- The organization has numerous components, such as discrete business units or divisions in different geographic regions, and there is insufficient coordination of compliance activities across those components.
- The organization has recently been cited and fined for noncompliance with one or more security or privacy regulations.

Security: A Top Legislative Priority in Recent Years[2]

2019

- **43** Number of U.S. states and territories that considered bills or resolutions that dealt with cybersecurity
- **Nearly 300** Number of bills or resolutions considered
- **31** Number of states that enacted cybersecurity-related legislation

2018

- **35** Number of U.S. states and territories that considered bills or resolutions that dealt with cybersecurity
- **365** Number of bills or resolutions considered
- **22** Number of states that enacted cybersecurity-related legislation

2017

- **42** Number of U.S. states and territories that considered bills or resolutions that dealt with cybersecurity
- **240** Number of bills or resolutions considered
- **28** Number of states that enacted cybersecurity-related legislation

Source: [2]National Conference of State Legislatures, Cybersecurity Security Legislation 2019, January 2020

need for a compliance program and make it clear to the rest of the organization how important compliance is, it's unlikely the compliance program will accomplish what it needs to. It's important to make executives aware of the potential penalties the organization could face for noncompliance — and that they as individuals could face penalties in some cases.

It's also important to keep executives informed of major data breaches and other noteworthy issues involving other organizations, especially competitors, to highlight what the consequences could be of not having a strong compliance program. Similarly, it's quite helpful to be able to demonstrate the benefits of a compliance program. Quantifying benefits helps to show that being compliant prevents breaches and other issues, and that the ounce of prevention is worth a pound of cure.

Finding Solutions and Services for Addressing Compliance Needs

Addressing an organization's compliance needs means leveraging automated solutions that provide support at all times. The scale of compliance can't be handled through manual means. Automated solutions that are particularly helpful include:

- **Asset management technologies** that track what and where an organization's data assets are and what systems and services (both internal and external) the organization uses
- **Security technologies** that protect data, prevent data breaches, and identify problems, such as cloud, network and endpoint security products; email encryption utilities; and vulnerability scanners
- **Disaster recovery solutions** that minimize operational disruptions while also ensuring data remains properly protected
- **Governance, risk and compliance (GRC) solutions** that monitor the enterprise to identify potential security problems so they can be remediated before a breach occurs

Specific services can also help organizations address their compliance needs. For example, CDW offers gap analysis services, during which CDW experts assess an organization's gaps in meeting the requirements of security and privacy regulations. CDW and its partners also offer compliance assessment services in which they look at how effectively and efficiently an organization carries out its compliance responsibilities, then recommend how the organization can change its technologies, processes, policies and other components to improve its compliance program.

We Get Compliance

No matter which regulations your organization must comply with, CDW can help. With a large and experienced staff of security and industry experts who know security and privacy regulations for industries such as healthcare, finance and retail, we can help optimize your compliance strategy to best fit your organization's requirements.

Our experts can help you choose and implement the solutions and services to fulfill your strategy and improve your compliance. Through analysis of current and future needs, we help organizations find the right solutions and bring them together to better identify potential issues and create a robust defense-in-depth environment. Also, CDW can help organizations manage third parties that store, process, transmit, or otherwise handle sensitive data on their behalf. This includes consulting services for assessing your organization's cloud-service options and needs, as well as its security and privacy risks.

CDW Can Design, Orchestrate and Manage a Comprehensive Infrastructure Strategy

CDW's simple, smart, scalable and flexible services portfolio provides a fully automated and managed infrastructure across your entire network, whether on-premises, hybrid or in the cloud.

DESIGN For The Future
Consult with our team of technology experts to plan a unique solution that fits your unique needs and optimizes business impact.

ORCHESTRATE Progress
CDW Amplified™ Infrastructure services help you build and deploy your custom infrastructure utilizing best practices.

MANAGE Operations
Our world-class, certified staff monitors and manages your infrastructure 24/7/365 to ensure operational efficiency and security.

Sponsors

Cisco Partner tenable Carbon Black.

Learn more about how CDW solutions and services can help you meet your security and compliance challenges.

CDW PEOPLE WHO GET IT®