Data Privacy: Between a Rock and a Hard Place

Addressing Today's Data Protection Challenges

cimplifi™

PROTECTING DATA IS MORE CHALLENGING THAN EVER

It seems that just about every day, there's a new jaw-dropping statistic that illustrates the tremendous growth of cyberattacks and data breaches that organizations are facing today. The attacks are not just increasing in number, but they're also increasing in impact to your organization and, most importantly, impacting the sensitive data of your organization's clients. This infographic that illustrates the world's biggest data breaches and hacks in recent years, shows a considerable escalation in breaches involving hundreds of millions of data records per breach. That's your sensitive data and your client's sensitive data at risk.

While it's more difficult than ever to protect your client's data, the stakes for doing so are higher than ever. Data privacy and data breach notification laws continue to be strengthened worldwide, putting more pressure on companies to protect client data and promptly notify them when their data is exposed. When it comes to protecting data and meeting their data protection obligations, organizations today are between a rock and a hard place.

The Challenges of Protecting Data Today

In fact, you could actually say organizations are between a rock and a rock and a hard place, as they are experiencing three difficult data protection challenges, including:

Data Security Threats Are Ubiquitous

Cybercrime is continuing to rise and, despite the emergence of best practices to avoid them, we're seeing more cyberattacks and data breaches than ever. Here are four statistics that illustrate just how ubiquitous data security threats are today:

- In 2020, the FBI's Internet Crime Complaint Center (IC3) experienced a 69% increase in the volume of cybercrime complaints received since 2019 for a total of 791,790.
- It takes an average of 287 days for security teams to identify and contain a data breach.
- In another recent survey of 5,600 IT professionals, 66% of respondents had experienced a ransomware attack in the past year.
- In that same survey, the average ransomware payment grew 470% over the past year from $170,000 to $800,000.

"What happened to the good old days when people just breached contracts?"

cimplifi™

Even as organizations continue to strengthen their practices regarding data security, it only takes one

mistake to become a cybercrime victim.

Identifying Sensitive Data is More Challenging Than Ever

One of the reasons for the continued rise of data breaches is the challenge of identifying sensitive data in organizations. With data in the world expected to rise to 163 zettabytes (163 trillion gigabytes) by 2025, identifying important sensitive data within an organization is becoming increasingly challenging due to the overwhelming volume of redundant, trivial or obsolete (ROT) data and the volume of dark data not used to gain insights for decision making. The amount of ROT and dark data within an organization can be as much as 85%!

Regulations Are Continuing to Evolve

While protecting data is more difficult, the stakes for failing to do so continue to rise and evolve. While GDPR became effective in 2018 to protect data rights for citizens of the EU and CCPA became effective in 2020 to do the same for California citizens, four other states – Virginia, Colorado, Utah and Connecticut – have passed their own data privacy laws in the past fifteen months. In fact, California has already voted to replace their own law effective next year.

Not only that, the Securities and Exchange Commission (SEC) proposed amendments to its rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies includes a requirement for regulated companies to disclose information about a cybersecurity incident within four business days!

Addressing Today's Data Protection Challenges

Protecting your organization's data (and the sensitive data of your clients) requires a combination of (you guessed it!) best practices and leveraging technology. To address today's data protection challenges, your organization needs to: **1)** stay current with regulatory developments; **2)** implement and keep current strong policies and procedures; **3)** apply automation to the privacy compliance function within your organization and **4)** apply automation to the data loss prevention (DLP) function within your organization.

In this whitepaper, we will address each of these four areas of data protection in detail to discuss leveraging these best practices and technology automation mechanisms to protect your organization's (and your clients') sensitive data. With the right combination of data protection procedures and tools, your organization doesn't have to remain between a rock and a hard place forever!

RECENT CHANGES TO THE REGULATORY LANDSCAPE

Organizations are not only between a rock and a hard place, but they are also actually between a rock **and** a rock **and** a hard place, as they are experiencing three difficult data protection challenges. One of those challenges is the ever-changing regulatory landscape to which organizations must continue to adjust. Let's look at some of the recent changes to the regulatory landscape.

SEC Proposed Rules for Cybersecurity Risk Management

On March 9, the Securities and Exchange Commission (SEC) proposed amendments to its rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies (registrants).

The proposed amendments would require, among other things:

- Current reporting about material cybersecurity incidents **within four business days** and periodic reporting to provide updates about previously reported cybersecurity incidents.
- Periodic reporting about:
    - A registrant's policies and procedures to identify and manage cybersecurity risks.
    - The registrant's board of directors' oversight of cybersecurity risk; and management's role and expertise in assessing and managing cybersecurity risk and implementing cybersecurity policies and procedures.
- Annual reporting or certain proxy disclosure about the board of directors' cybersecurity expertise, if any.

The comment period for the SEC proposed rules ended in May, so it will be interesting to see what, if any changes, are made. Regardless, the SEC proposed rules are likely to have a significant impact on how public companies address their cybersecurity obligations.

State Data Privacy Laws

While California adopted the California Consumer Privacy Act (CCPA) in June 2018 (which became effective on January 1, 2020), other states have been slow to adopt comprehensive data privacy laws. In fact, the next state to approve one was…again…California, for which voters approved Proposition 24, adopting the California Privacy Rights Act (CPRA) of 2020, which significantly expands the data privacy rights of consumers over what the CCPA covers and will replace it in January 2023.

However, in the past sixteen months, four more states have approved comprehensive data privacy laws, all of which are set to go into effect next year. They are:

- **Virginia**: Last year, Virginia passed the Virginia Consumer Data Protection Act (VCDPA), which is set to go into effect next January.
- **Colorado**: Also last year, Colorado passed the Colorado Privacy Act (CPA), which is set to go into effect next July.
- **Utah**: This past March, Utah passed the Utah Consumer Privacy Act (UCPA), which is set to go into effect at the end of 2023.
- **Connecticut**: And in May, Connecticut passed the Connecticut Data Privacy Act (CTDPA), which is set to go into effect next July.

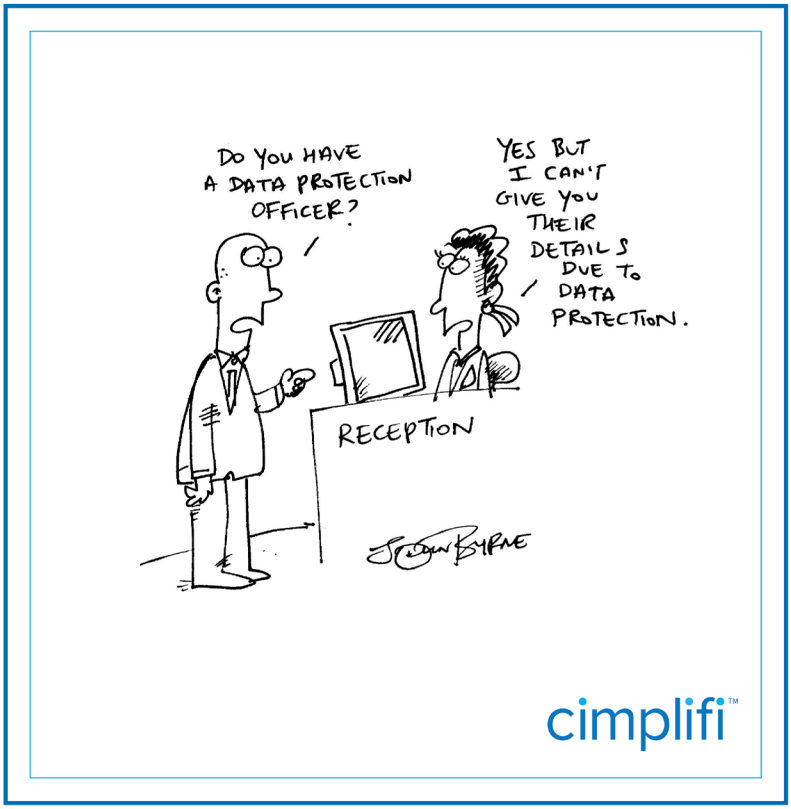
While the state data privacy laws have several similarities, there are also considerable differences as well. For example, California is the only state that offers a private right of action (both CCPA and CPRA include it). Once CPRA goes into effect, Utah will be the only state that doesn't offer the right of rectification or the right against automated decision making. And it will be the only state that doesn't require risk assessments.

With 45 states still to adopt a comprehensive data privacy law, you can imagine there will be plenty of adjustments to come. Currently, Massachusetts, Michigan, New Jersey, Ohio, and Pennsylvania have bills in committee, but that's no guarantee that those bills will proceed into law – 23 states have submitted privacy bills that have failed to gain traction and are currently inactive.

Federal Data Privacy Law

Despite several proposals in recent years, there is no one comprehensive federal law that governs data privacy in the U.S. Instead, U.S. citizens are protected by a combination of laws and regulations that address telecommunications, health information, credit information, financial institutions, and marketing, including:

- Health Insurance Portability and Accounting Act (HIPAA): Governs the collection of health information.
- Children's Online Privacy Protection Act (COPPA): Governs the collection of information about minors.
- Fair Credit Reporting Act (FCRA): Governs the collection and use of credit information.
- Gramm Leach Bliley Act (GLBA): Governs personal information collected by banks and financial institutions.



Although there has been a recent bipartisan compromise draft on potential federal privacy legislation, there is still a long way to go before there is a fully comprehensive data privacy law in the U.S.

State Data Breach Notification Laws

State data breach laws are also changing. Even though all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have laws requiring businesses to notify individuals of security breaches of information involving personally identifiable information, those laws are still being updated periodically.

Recently, Indiana passed House Enrolled Act No. 1351, which requires companies to provide data breach notification "not more than 45 days after discovery of the breach" where the standard was previously "without unreasonable delay". And Arizona recently passed House Bill 2146, which added the Director of the Arizona Department of Homeland Security to the three largest consumer reporting agencies and the Arizona

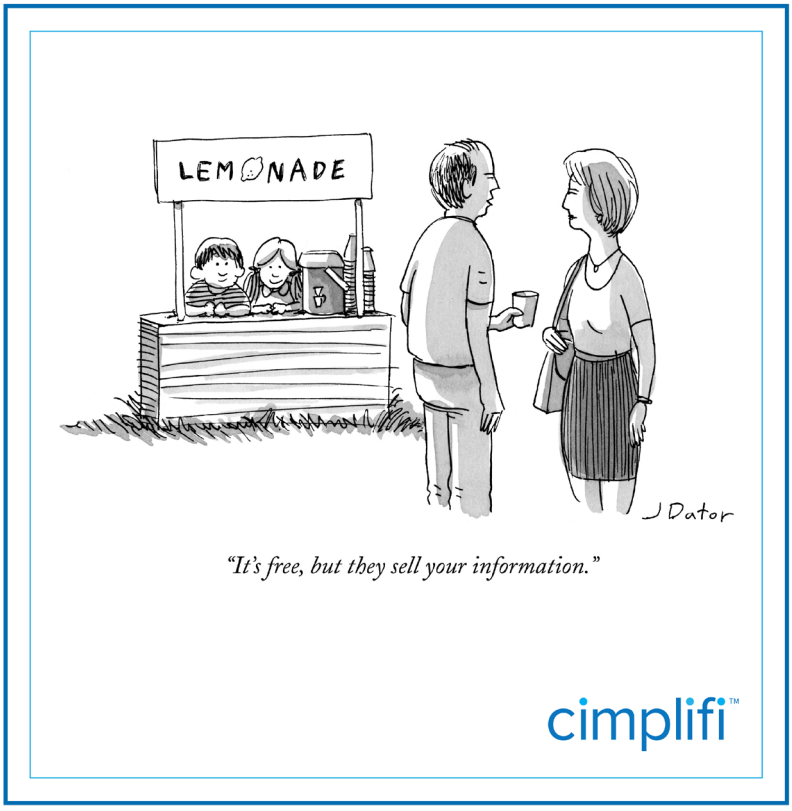
attorney general to be notified when a breach happens. Changes are ongoing here as well.

If we were to write this paper in a few months, the recent changes to the regulatory landscape would likely be different because the regulatory landscape is always evolving! Data security threats continue to rise and identifying sensitive data continues to be challenging so organizations have a tremendous challenge to keep up with changing regulations, especially when the stakes of failing to do so are higher than ever.

It's important to work with experienced professionals who not only know how to address rising data security threats and understand how to identify sensitive data within Big Data collections, but also keep track of the changing regulations so that you can avoid getting stuck between a rock and a rock and a hard place.

SIX BEST PRACTICES YOU CAN TAKE TO PROTECT YOUR DATA

Getting out from between a rock and a rock and a hard place starts with implementing best practices that reduce the risk of exposing sensitive data to cyberattacks. With that in mind, let's look at six best practices that your organization can quickly take to protect its data and (of course) the data of your clients as well. While data protection is an organization wide initiative, there are some best practices your organization can quickly implement to significantly bolster protection of your (and your clients') sensitive data.



Keep Your Software Up to Date

One of the most common ways that hackers can access your sensitive data is through vulnerabilities that are identified. Those vulnerabilities can occur at any layer of software – from the operating system to the applications your organization uses. And they can be discovered by anybody, including hackers.

One example from last December was the Log4Shell zero-day vulnerability (which had been **unnoticed since 2013** until it was discovered) identified in Log4j, which is a Java-based logging utility that is literally found in millions of servers across the world. The patch was issued without much fanfare and many companies were able to apply it before attackers could exploit the vulnerability in their environments. At least one company, however, was hacked within the mere four-day window before they could apply the patch. It's important to keep your software up to date and apply any security patches quickly to minimize exposure.

Disable or Remove Unnecessary OS Services

Most operating systems have certain "out of the box" settings that may need to be adjusted to enhance security. In Windows, for example, removing services that are not required, like Telnet and FTP (which are clear-text protocols) and disabling LAN Manager authentication can reduce potential vulnerabilities. For Linux, disabling unnecessary services and ports, trust authentication used by the ''r commands'' and unnecessary setuid and setgid programs also eliminate some vulnerabilities within the operating system.

Protect the Endpoints

Endpoint workstations and servers are often the route into your data by hackers, so it's important to maximize protection to protect those endpoints. Antivirus software **must** be installed and kept current on all servers and workstations – it's your most critical line of defense! That includes anti-spyware and anti-adware tools as well – often, they are bundled together today. Personal firewalls and Host-based Intrusion detection systems (IDSs) can also provide additional protection. It only takes one vulnerable endpoint to put your data at risk.

Perform Cybersecurity Penetration Tests

Penetration testing is the testing of a computer system, network or web application to identify security vulnerabilities that could be exploited. Penetration testing can either be automated or performed manually and is typically conducted by a security company with experience in identifying security weaknesses. Conducting a penetration test periodically can enable you to find vulnerabilities before hackers do.

Establish Policies for Departing Employees and Third Parties

Your organization's data isn't just vulnerable from outside hackers – it's often the insiders who can do the most damage. In a recent survey, 83% of respondents continued accessing accounts from their previous employer after leaving the company and 56% of respondents said they had used their continued digital access to harm their former employer! In one example, a fired HR executive deleted 17,000 resumes **after** she was fired!

When employees (or even third-party contractors) leave, there must be strong policies for eliminating their access to all systems and confirming that all access has been cut off.

Implement Multi-Factor Authentication Everywhere Possible

Implementing two-factor (2FA) or multi-factor authentication to require at least a second form of authentication for access may be the most important best practice of all. According to Microsoft, your accounts are 99.9% less likely to be compromised when using MFA. If a hacker is able to get your password to a system, but doesn't have your cell phone to accept the authentication code, it doesn't do them much good, does it?

These six best practices can significantly reduce the risk of exposing sensitive data to cyberattacks and it's important to work with experienced professionals who can help you implement these mechanisms.

However, there is more to data protection than just these best practices. A comprehensive data protection program also encompasses best practices for identifying, securing and minimizing sensitive data as well. It also encompasses a thorough program that includes comprehensive documentation and rigorous training of employees and contractors. In the next section, we will look at those programs to take data protection to another level.

SIX PROGRAMS TO TAKE DATA PROTECTION TO ANOTHER LEVEL

Getting out from between a rock and a rock and a hard place requires more than that – it requires another level to provide maximum data protection. With that in mind, let's look at six programs to take data protection to another level, many of which include disciplines beyond cybersecurity. These are organization wide initiatives that need to be addressed.

Identify and Classify Sensitive Data

You can spend a lot to implement various mechanisms to protect your organization's data, but it can be expensive to protect all your data across the entire organization. And you can still fail to protect the data that's most important in your organization.

All data is not the same and shouldn't be treated the same. If you're not protecting the data that is most sensitive to your organization and your clients, your data protection program is a failure. That's why it's important to identify and classify sensitive data within your organization to "right-size" your data protection program.

Data analytics can help to identify sensitive data, such as PII and information about key entities. It can also help identify Redundant, Obsolete and Trivial (ROT) data that your organization can eliminate to make it easier to identify the important sensitive data you need to protect most.

Control Access to Sensitive Data

Once you've identified the sensitive data within your organization, you need to protect it with by controlling the access to it. Access controls can be physical or technical:

- **Physical** controls include everything from security on laptops and mobile devices (in terms of software to protect data and procedures like not using public Wi-Fi hot spots), network segregation, video surveillance in the office and more.
- **Technical** controls include access permissions, access control lists (ACLs), firewalls, proxy servers and more.

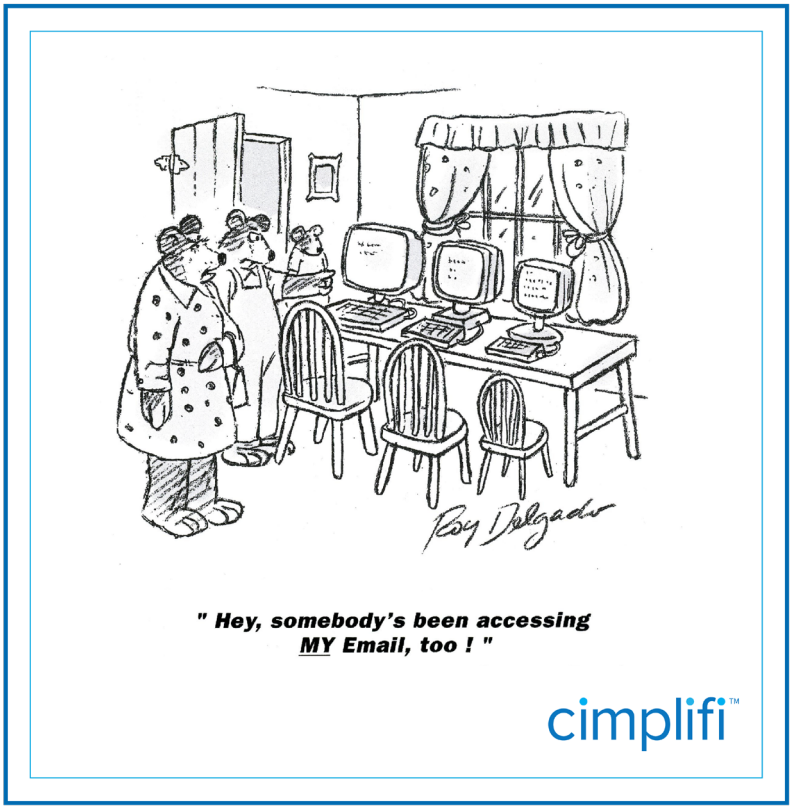
Create a Data Usage Policy

A Data Usage Policy is a legal disclosure of how your organization collects, retains, and shares personally identifiable information (PII). Strengthened data privacy laws like GDPR (which specifies principles for processing data in Article 5, including not keeping the data any longer than necessary for the purposes for which the data is processed) have established an expectation of transparency with regard to how

organizations use personal data. A public Data Usage Policy helps achieve that level of transparency.

Document Your Cybersecurity Policies

While documentation ties into several of these mechanisms, it also is important to mention as an overall procedureas well. Your organization's cybersecurity policies should be well documented, and that documentation should be kept evergreen and up to date as policies change. New employees should be required to read and understand the policies – some organizations even quiz new employees on their understanding after they have read them. Changes in policies should be clearly communicated to all employees and third parties working on your behalf.



Train Your Employees

In addition to well documented policies on data protection, employees need to be trained as well. This includes training for new employees and third parties as well as refreshers and updates for existing employees and third parties. Training should walk-through real-world scenarios and even test employees and third parties on how they handle various situations.

For example, some companies implement periodic phishing tests, which are used by security and IT professionals to create mock phishing emails and/or webpages that are then sent to employees to see if they will be fooled into clicking on the links within them. These fake attacks help employees learn to recognize and avoid clicking on links in phishing emails that can result in malware being installed on their devices. A good training program includes tests to confirm that employees understand best data protection practices.

Perform a Cybersecurity Risk Assessment

A cybersecurity risk assessment is an assessment of an organization's ability to protect its information and information systems from cyber threats. It's designed to identify, assess, and prioritize risks to information and information systems. It helps organizations identify and prioritize areas for improvement in their cybersecurity program.

There are several cybersecurity risk assessment frameworks and methodologies available, including the *National Institute of Standards and Technology (NIST) Cybersecurity Framework* and the *ISO 27001:2013* standard.

While this is the last item on the list, it's really the first item that should be considered as it drives all the best practices and other mechanisms that your organization will implement.

In addition to the six best practices discussed previously, these six programs will help your organization adopt a comprehensive approach to data protection that is "right-sized" to protecting your organization's (and your clients') most sensitive data.

When it comes to data protection, staying compliant with ever-changing data privacy laws is extremely challenging. Next, we will discuss the emergence of technology to automate addressing the continually changing requirements for privacy compliance.

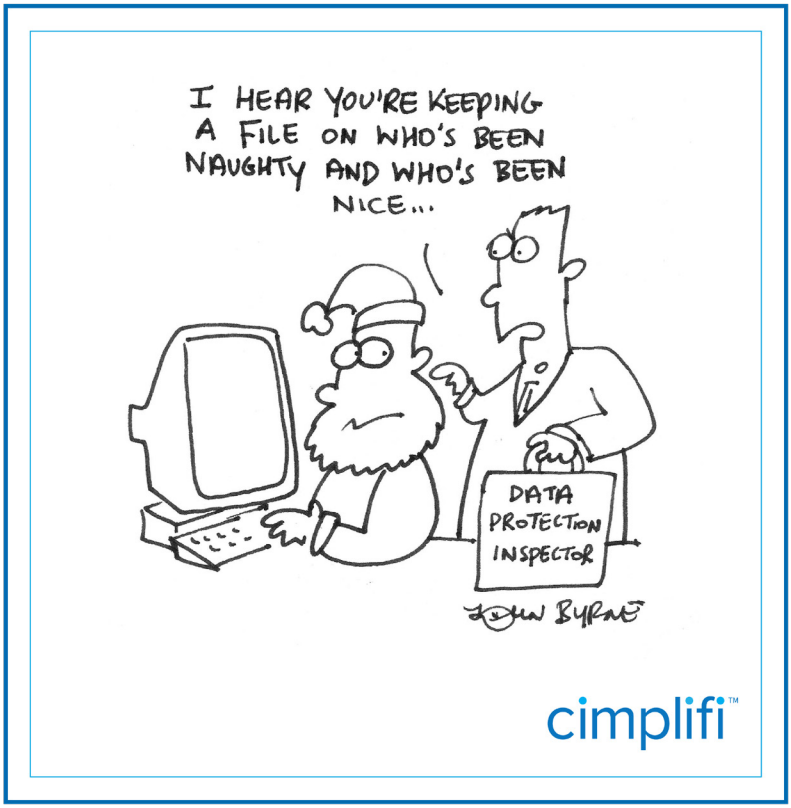
AUTOMATING PRIVACY COMPLIANCE

One of the biggest reasons for protecting your organization's data – and your client's data – is privacy compliance. The good news is that there is technology available today to help automate the process of complying with data privacy laws and regulations.

The Continually Evolving Privacy Compliance Landscape

As we discussed previously, the regulatory landscape for protecting data is constantly evolving. Here are two recent examples since that blog post was published just six weeks ago:

- The recent bipartisan compromise draft on potential federal privacy legislation we mentioned in our blog has advanced, as the House Energy and Commerce Committee voted 53-2 to push forward the American Data Privacy and Protection Act (ADPPA) (R. 8152) to set a national standard for how tech companies collect and use Americans' data.
- New York has become the first state to mandate that attorneys take continuing legal education (CLE) courses in cybersecurity, privacy and data protection.



There are always new developments to consider for privacy compliance that organizations need to address – new laws that are enacted or pending, new regulations and new requirements for professionals. Unless you have a team of privacy lawyers and technologists in house (who can afford that?), you're always getting stuck again in between – you guessed it – a rock and a hard place!

Ten Considerations for Automating Privacy Compliance

Like any other business process, the best way to address changes in business processes both efficiently and effectively is to operationalize and automate. Operationalizing and automating your approach to data privacy is no different – there are technology solutions available today that can help your organization address your privacy compliance efficiently and effectively – while also integrating that approach with other related business functions.

Here are ten considerations to keep in mind when selecting a solution to assist with operationalizing and automating your approach to data privacy:

1. **Easy to Use and Learn**: The system should be easy to use and learn, with customizable policy templates, wizards, and multiple-choice questions to guide you through the process.
2. **Address the Core Questions Quickly**: An automated privacy compliance solution should provide an ability to start with the core questions that will let you know where your organization stands on the most critical areas, what the priorities are, and what you need to do first.
3. **Risk Assessment**: Not all compliance requirements have the same level of risk to your organization, so the solution should provide a rating system for assessing the risks associated with each compliance requirement, from low to severe.
4. **Automated Gap Analysis**: The solution should keep track of open items to be completed so that you can keep track of it all. Spreadsheets are not the answer, especially when you have frequent requests for privacy information.
5. **Collaboration and Workflow Management**: Privacy compliance is a group effort within your organization, and you don't want to search for responses from colleagues in email or use a collaboration tool that is not tailored for privacy compliance. Your privacy compliance solution should enable your team to collaborate and manage workflows directly within the platform.
6. **Track and Re-Use Responses**: Where there are similarities between the privacy laws, or questions on a Request for Information (RFI) to your organization, you don't want to reinvent the wheel each time, so the solution should apply (by default) answers you've already completed to questions that are the same or substantially similar.
7. **Regulation Updates & Alerts**: An automated privacy compliance solution should provide alerts to keep you informed of pending or passed privacy regulations so that you can prepare for the changes.
8. **Automated Reporting to Track Compliance KPIs**: The solution should provide easy-to-read, real-time graphs and charts (easily exportable to PowerPoint for presentation) to show where your organization stands on compliance.
9. **Training & Certification**: The solution should provide modules for training and even a certification program to verify knowledge.
10. **Track and Manage Third Parties**: Finally, privacy compliance isn't just a concern of the employees within your organization – your vendors and even your clients can put you at risk as well. An automated privacy compliance solution should support the ability to track and manage privacy compliance by third parties – at least to the extent that their activities affect your business.

A manual approach to privacy compliance that's based on spreadsheets and email communications is not efficient in the constantly evolving data privacy landscape organizations are faced with today. Consider implementing a solution that operationalizes and automates your approach to data privacy!

To conclude this paper, we will discuss next the emergence of technology to create a data harbor to automate data loss prevention (DLP) within organizations.

AUTOMATING DATA LOSS PREVENTION

Automation can also be applied to create a "data harbor" to automate data loss prevention (DLP) within organizations through an approach that involves next-gen data protection as a service.

Next-Gen Data Protection as a Service

Encryption is a great tool for securing data, and it has been around for decades. But it has limitations, as evidenced by the four cybercrime statistics we provided previously. Think those victims of cybercrime didn't have encryption in their solutions? Of course, they did! Today's data protection challenges require a next-level approach to data protection.

Next-gen data protection as a service, also known as next-gen DPaaS or NGDP, involves three components to end-to-end protection of data:

- Encrypt: Any good data protection program involves encryption of data – at-rest and in-motion.
- Fragment: A second component to protecting data is to fragment that data into valueless pieces. Each of the fragments is encrypted with a different key, so there is no single point of failure if an unauthorized user gains access to a single key.
- Scatter: Take the data fragments and scatter them across multiple separate storage locations, creating a virtual environment known as a "data harbor". That makes it virtually impossible to locate all the pieces of a data set, much less break through encryption of each of the fragments.

Imagine taking important documents and storing them in a secure facility that is difficult to break into. Then, you shred those documents (in a cross-cut pattern, of course!). Then, you take some of those document shreds and you store them in other secure facilities. Imagine how difficult it would reconstitute those documents. You would have to break into multiple places, find all the pieces in multiple locations, then figure out which pieces go to which documents. That's what an NGDP approach does to protect your data.

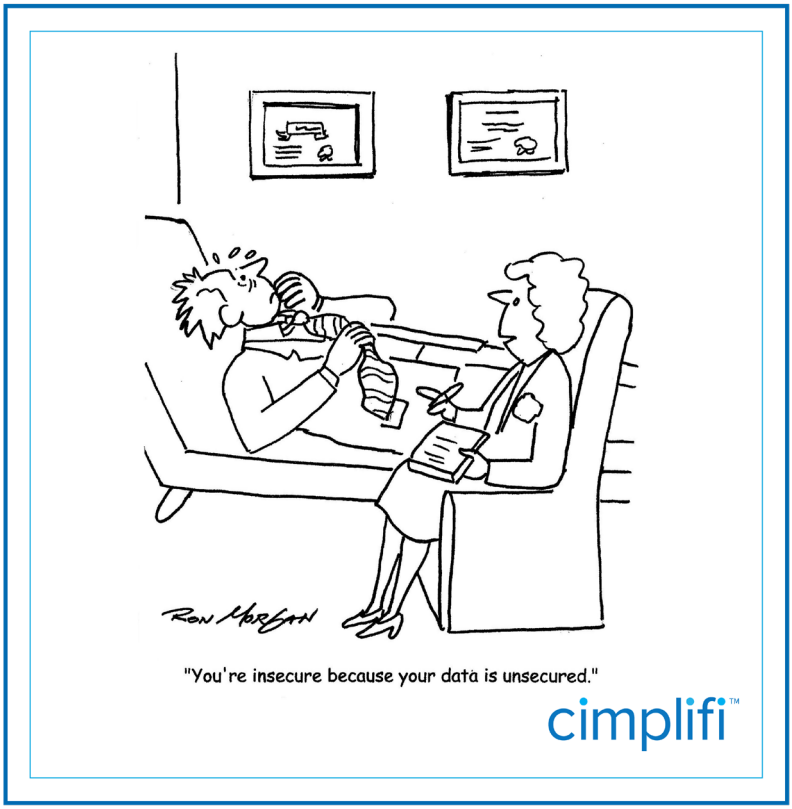
Data Harbor

A data harbor is a collection of geographically and physically separated storage locations used to store data that has been fragmented into valueless pieces whereby no single location contains all the fragments for the data to be reconstructed into its original form. Like an actual harbor that contains a series of boat slips where different boats are docked when they're not in the open water, a data harbor separates the data into different locations, essentially making it necessary to breach each one of them to even have a chance of getting to your organization's data.

Four Characteristics of an Effective NGDP Solution

While a data harbor sounds secure, authorized users still need to be able to access that data in a secure manner when they need it – otherwise, it's not useful. Here are four characteristics that an effective NGDP solution needs to have:

- **Multi-Factor Authentication (MFA)**: A secure solution requires two or more verification factors to gain access, so MFA is a "must have" for an effective NGDP solution today. According to Microsoft, your accounts are 99.9% less likely to be compromised when using MFA.
- **Transparency**: Users of solutions today have enough to worry about without having to worry where their data is stored and how data fragments can be reassembled for use. An effective NGDP solution needs to ensure a transparent user experience with that data.
- **Latency**: Users don't need to be waiting around for data fragments to be reassembled. To be an effective NGDP solution, any latency of retrieving data within systems must be negligible and unnoticeable.
- **Zero-Trust Security**: In 2010, John Kindervag, an analyst at Forrester Research, introduced the term "zero trust," which was based on the idea that an organization shouldn't trust any resource whether it was inside or outside its network. The model of end-to-end, zero-trust security has become a standard expectation of next level security that denies access to applications and data by default. In today's standard remote and hybrid work environments, a zero-trust security philosophy is important to ensure that security is about the data, not the location from which it's being accessed.



CONCLUSION

Automating data loss prevention today requires a next generation approach. An NGDP approach to data protection that effectively encrypts, fragments, and scatters your data for protection – while transparently and quickly assembling that data when it needs to be used – is your best bet to avoid becoming a cybercrime statistic.

Many organizations are stuck between a rock and a hard place when it comes to protecting data and meeting their data protection obligations. An approach that includes leveraging best practices and programs, along with technology automation mechanisms for privacy compliance and data loss prevention to protect your organization's (and your clients') sensitive data is your organization's best bet to get "unstuck" from that position. Best practices + technology = data protection freedom!