DATA PROTECTION FUNDAMENTALS:

BRIDGING THE GAPS IN DATA SECURITY MANAGEMENT

In today's climate of escalating security risk and increasingly high stakes, boards can't leave security to chance.

In 2017, hackers stole social security numbers and other personally identifiable information from Equifax, implicating over 143 million people. In 2019, Capital One announced a massive data breach where hackers accessed sensitive information from more than 100 million Americans. These are well-known examples, but security breaches like these happen to organizations around the world every year. This is why state-of-the-art encryption, data storage, and access controls are key in protecting companies from attacks and vulnerabilities against their most important assets: their data.

Boards of directors and executive teams need an extra layer of security to ensure their governance information and materials remain safe and secure at all times, but many are unaware of the basic data protection fundamentals and gaps in their security processes which leave them vulnerable.

Understanding common data protection attributes, where those controls exist today, and how those solutions should be applied in an enterprise environment are critical in bridging security gaps to protect companies' most sensitive information and privacy.

Equifax security breach resulted in personal information of 143 million people stolen.

Diligent

Data protection fundamentals

Data protection from a technical standpoint is about access control. Organizations need to protect their data throughout its lifecycle by using different tools and techniques to reinforce this access control (such as encryption, masking, anonymization tokenization, obfuscation, randomization, or null). It's a simple concept, but difficult to do correctly with the diverse systems found in most organizations, so understanding the fundamentals is key.

Data classification

To understand the level of access control required for various information, companies need to first classify their different data assets. Common commercial data classifications (from highest to lowest) include:

Sensitive
Data that requires the most limited access and the highest degree of integrity. This kind of data can do the most damage to an organization if it's disclosed.

Confidential
Data that might be less restrictive within the company but might cause damage if disclosed.

Private
Private data is usually compartmental data that might not do the company damage but must be kept private for other reasons, like human resources data.

Proprietary
Proprietary data is data that's disclosed outside the company on a limited basis or contains information that could reduce the company's competitive advantage, such as technical specifications for a new product.

Public
Public data is the least sensitive data used by the company and would cause the least harm if disclosed. This could be anything from data used for marketing to the number of employees in a company.

Information owners should be responsible for assigning classifications to their information assets so they can be labeled and handled correctly by others. Based on these data sensitivity classifications, the protocols for treating each category of data will vary.

Data labeling

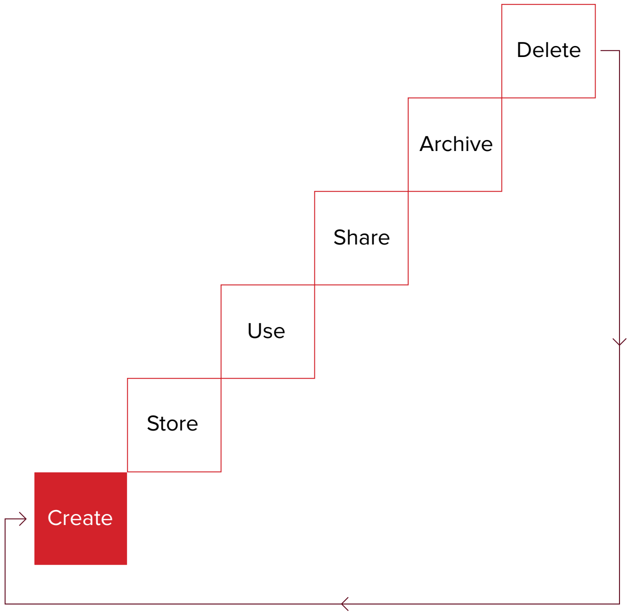
In order to provide a sound security framework with the right protocols for treating these different data classifications, information must be labeled accordingly. Common data labels include:

- Data classification labels
- Date of creation
- Handling
- Distribution instructions
- Source
- Access limitations

Labeling restricted information allows data owners to stipulate how data should be handled, and by whom. They can block certain actions like printing or copy and pasting while enabling employees or any other data-user to understand how the information should be treated. For example, policies requiring personally identifiable information to be labeled as "Company-Confidential" or watermarking proprietary information with the text "Internal Use Only" help ensure the access and distribution of private documents are safeguarded. Put simply, employees are rarely bad actors, but organizations need to take the guesswork out of how to maintain security.

The data lifecycle and handling

Finally, the data lifecycle needs to be understood so sensitive information remains protected at all times.



Data Lifecycle

With the correct data classification and labeling, companies can ensure data is handled correctly throughout its lifecycle. For example, once restricted-use and client-confidential data are created, they must be securely stored at all times or destroyed, whether in hard-copy or electronic form. If personal identifiable information or other sensitive data that requires special handling is in transit, it must be encrypted in-transit using secure protocols such as TLS to ensure only those authorized to access it can do so. Similarly, if the data is at rest, it must be encrypted at the whole disk, file system, folder, file, and record level to preserve its integrity.

Collaboration across functions and individuals is imperative to modern governance, but it must happen within a locked-down environment that mitigates the risk of data leakage, human error, or attacks. By understanding the necessary data classifications, labeling, and how they dictate the way sensitive information is treated throughout its lifecycle, companies can develop the processes and adopt the solutions necessary to enhance their security ecosystem.

Common gaps in data security management

Common gaps in data security management exist due to the fact many organizations don't have a deep understanding of their data based on classifications, how it's created, used, and shared, which prevent them from developing sound protection policies. Security is a complex topic, yet solutions are often presented as silver bullets. In reality, data protection is more than just encryption or digital rights management (two common controls used to protect data). It requires a data-centric viewpoint that takes into account the cloud access security broker and data leakage prevention, with a multi-layered defense network architecture to ensure no vulnerabilities arise.

Key risk factors arise in common consumer or commercial products:

- **Basic SMS text messages and messaging platforms**. SIM card hijacking attacks create very high data leakage risks where communication is not encrypted. Even with platforms like WhatsApp that are considered more secure, authentication is a key risk factor—it doesn't provide federated identity integration with enterprise customers.

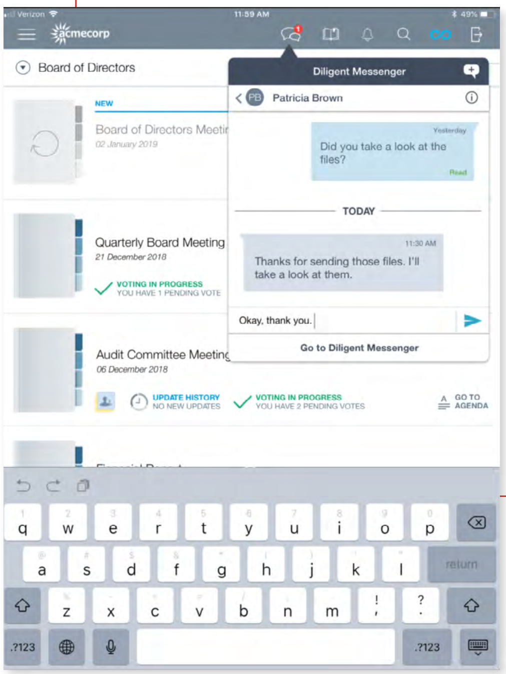
- **Consumer emails like Gmail**. The next most vulnerable to data leakage risks, they're subject to account take-over attacks due to poor authentication methods chosen by users and the contents downloaded from webmail platforms are often disk undecrypted. Overall, consumer emails cannot enforce strong user authentication methods like MFA, which is a key risk factor.

  For sensitive information sharing and discussions, **Diligent Messenge**r, a highly secure messaging tool, prevents cyber breaches and mitigates data leakage risks.

- **Widely used platforms like Dropbox or Box**. These tools have inherent data leakage risks that customers may not fully realize. The control of data contents resides within the customer's responsibilities and misconfigured sites can result in data leakage. Even with platforms like Microsoft Azure Information Protection (AIP), misclassified data can result in unintentional data leakage. This stems from the fact that documents are only individually protected and data classification is manually required by the data owner.

  In this case, **Diligent Secure File Sharing**, a secure data storage, sharing, and collaboration solution can support Microsoft AIP to provide an additional layer of robust security.

For sensitive information sharing and discussions, Diligent Messenger, a highly secure messaging tool, prevents cyber breaches and mitigates data leakage risks.



Did you take a look at the files?

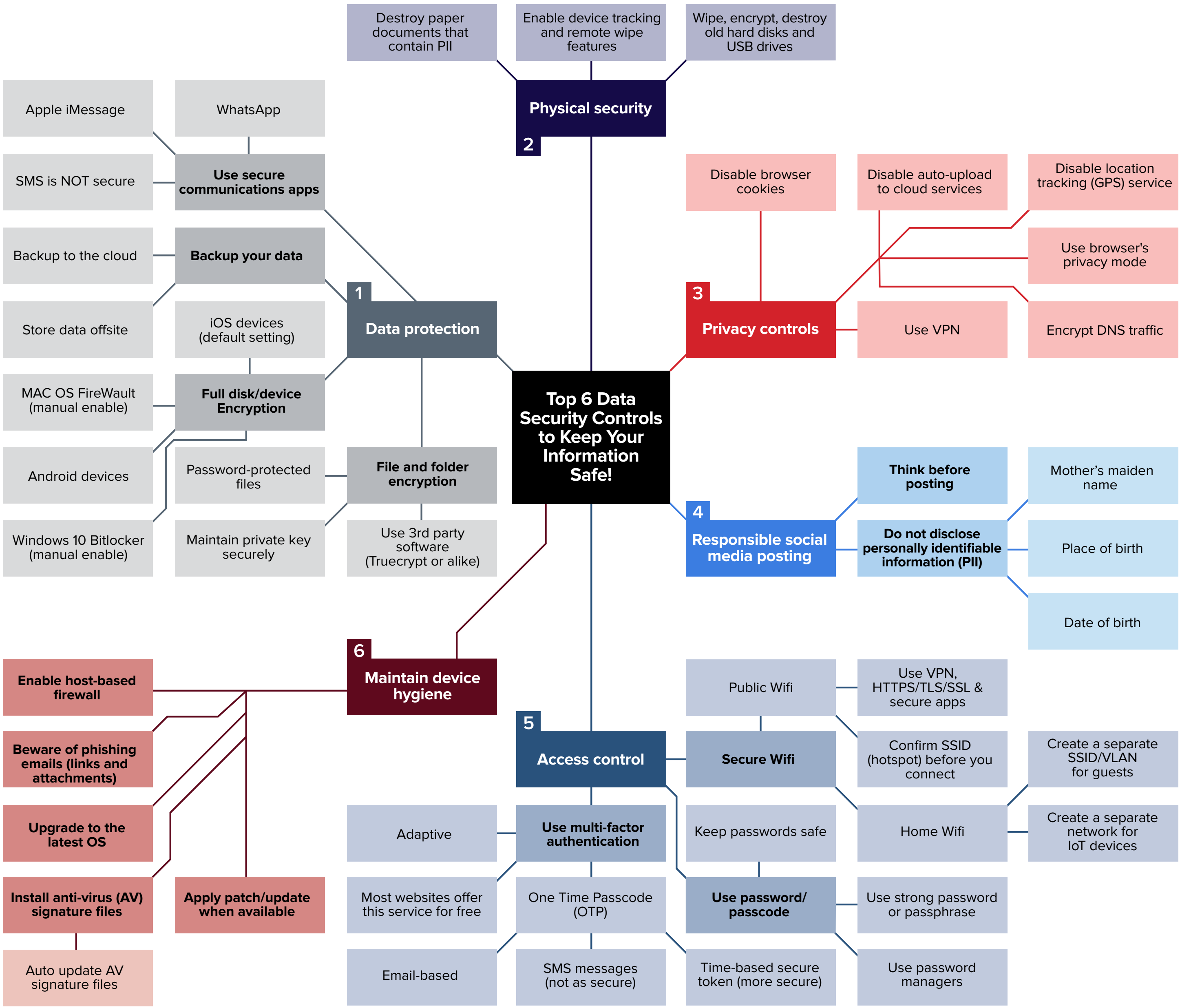
Thanks for sending those files. I'll take a look at them.

Okay, thank you.

Diligent

Top 6 data security controls to keep information safe

Keeping your company's information safe stems from access control. From a high-level, there are six key avenues for organizations to consider when it comes to protecting their information.



Top 6 Data Security Controls to Keep Your Information Safe!

1 **Data protection**

- **Use secure communications apps**
  - Apple iMessage
  - WhatsApp
  - SMS is NOT secure
- **Backup your data**
  - Backup to the cloud
  - Store data offsite
- **Full disk/device Encryption**
  - iOS devices (default setting)
  - MAC OS FireWault (manual enable)
  - Android devices
  - Windows 10 Bitlocker (manual enable)
- **File and folder encryption**
  - Password-protected files
  - Maintain private key securely
  - Use 3rd party software (Truecrypt or alike)

2 **Physical security**

- Destroy paper documents that contain PII
- Enable device tracking and remote wipe features
- Wipe, encrypt, destroy old hard disks and USB drives

3 **Privacy controls**

- Disable browser cookies
- Disable auto-upload to cloud services
- Disable location tracking (GPS) service
- Use browser's privacy mode
- Use VPN
- Encrypt DNS traffic

4 **Responsible social media posting**

- **Think before posting**
- **Do not disclose personally identifiable information (PII)**
  - Mother's maiden name
  - Place of birth
  - Date of birth

5 **Access control**

- **Secure Wifi**
  - Public Wifi
    - Use VPN, HTTPS/TLS/SSL & secure apps
    - Confirm SSID (hotspot) before you connect
  - Home Wifi
    - Create a separate SSID/VLAN for guests
    - Create a separate network for IoT devices
- **Use multi-factor authentication**
  - Adaptive
  - Most websites offer this service for free
  - One Time Passcode (OTP)
    - Email-based
    - SMS messages (not as secure)
    - Time-based secure token (more secure)
- **Use password/passcode**
  - Keep passwords safe
  - Use strong password or passphrase
  - Use password managers

6 **Maintain device hygiene**

- **Enable host-based firewall**
- **Beware of phishing emails (links and attachments)**
- **Upgrade to the latest OS**
- **Install anti-virus (AV) signature files**
  - Auto update AV signature files
- **Apply patch/update when available**

1. Data protection

Protecting sensitive data includes:

- File and folder encryption
- Full disk or device encryption
- Database or data field level encryption
- Backing data up
- Using secure communication apps with end-to-end encryption

File and folder encryption includes maintaining private keys securely, having password-protected files, and using third-party software for on-the-fly encryption.

Full disk encryption includes encrypting employees or data users, iOS, Windows, MAC, or Android devices for as long as they serve the company. In the event of lost or stolen devices, ensuring that data on a secure cloud has been backed up or stored securely offsite is equally important. Finally, as mentioned above, using communication tools with end-to-end encryption (i.e. never using SMS when discussing sensitive data) is key, with other safeguards in place to compensate for any intrinsic vulnerabilities.

2. Physical security

If sensitive information can't be stored securely (i.e. encrypted) in a physical form it must be destroyed. Paper documents should never have personally identifiable information (PII) on them and confidential data on USB drives or other physical media should be sanitized properly to ensure no information can be accessed from it in the event that it's reused or discarded.

Similarly, laptops and cellphones should have device tracking and remote wipe features enabled so that if stolen or lost, sensitive information can be destroyed. These physical security measures require sound policies and procedures from leadership that employees and third-party vendors are aware of so they can be maintained and enforced.

3. Privacy controls

There are a few best practices for privacy controls that companies can educate employees and data users on leveraging. For starters, disabling auto-uploads to cloud services and location tracking (GPS) services is a great step to keep information safe. Reminding individuals to use a browser's privacy mode (i.e. Chrome Incognito or MS Edge InPrivate) is also a good habit to instill.

Finally, disabling browser cookies, using a VPN, and encrypting DNS traffic are important privacy controls for maintaining data integrity.

4. Responsible social media postings

This may seem obvious, but without proper information security policies and education, data leakage can occur through social media postings. It should be very clear to every data user how to treat different classifications of data so access to sensitive information doesn't become available.

Without an understanding of the data security fundamentals, opportunities for human error, and data leakage arise. Instructing employees or data users to think before they post isn't enough—communicating how even sharing information like their mother's maiden name, place or date of birth, or other PII that can compromise security is imperative.

5. Access control

Access control is a key driver in maintaining the security and integrity of data. Using multi-factor authentication (MFA), passwords, and secure WiFi are the three main controls to leverage. Two-factor authentication is offered on most social, email, and payment accounts with one-time passcodes sent as time-based secure tokens (note: enabling this via SMS is not very secure). Adaptive MFA is a way that multi-factor authentication can be configured and deployed such that the identity service provider system will select the right multiple authentication factors depending on the user's risk profile and behavior as part of an ongoing process, instead of applying risk evaluation and elevation only during the authentication process once. Essentially, it adapts the type of authentication to the situation.

In regards to passwords, password managers are a best practice because they ensure passwords are strong and kept safe. When it comes to secure WiFi, data users need to use a VPN, HTTPS/TLS, or other secure apps when using public WiFi and confirm the SSID (hotspot) before connecting. At home, data users should create a separate SSID or VLAN for guests and a separate network for IoT devices like thermostats, which can be hacked.

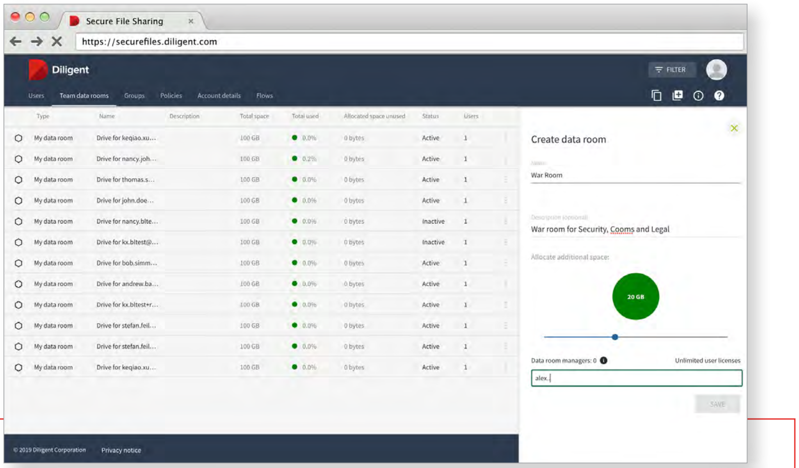
6. Device hygiene

Maintaining device hygiene is imperative to keeping information safe. Being diligent about phishing emails and having processes in place for data users to notify leadership about security threats is table stakes. Similarly, communicating with employees or any data user about the importance of upgrading to the latest operating system, applying updates, installing anti-virus (AV) software, and automatically updating AV signature files is best practice. Furthermore, enabling host-based firewalls are a granular way to protect individuals from viruses, malware, and to control the spread of harmful infections throughout a network.

Being intentional about data protection has never been more important.

In an increasingly remote-first world, organizations need to ensure connectivity and business continuity online while protecting themselves from security gaps and breaches. This requires sound policies and procedures from leadership with additional security solutions to back it up.

Diligent's products are backed by the world's leading security standard with secure data centers globally. In an age of increased cyber risk, your organization needs an extra layer of security to ensure that sensitive information and materials remain safe and secure at all times, which is why **50% of Fortune 1000 companies use Diligent to protect their most sensitive information**.



	Type	Name	Description	Total space	Total used	Allocated space unused	Status	Users
○	My data room	Drive for keqiao.xu...		100 GB	● 0.0%	0 bytes	Active	1
○	My data room	Drive for nancy.joh...		100 GB	● 0.2%	0 bytes	Active	1
○	My data room	Drive for thomas.s...		100 GB	● 0.0%	0 bytes	Active	1
○	My data room	Drive for john.doe...		100 GB	● 0.0%	0 bytes	Active	1
○	My data room	Drive for nancy.blte...		100 GB	● 0.0%	0 bytes	Inactive	1
○	My data room	Drive for kx.bltest@...		100 GB	● 0.0%	0 bytes	Inactive	1
○	My data room	Drive for bob.simm...		100 GB	● 0.0%	0 bytes	Active	1
○	My data room	Drive for andrew.ba...		100 GB	● 0.0%	0 bytes	Active	1
○	My data room	Drive for kx.bltest+r...		100 GB	● 0.0%	0 bytes	Active	1
○	My data room	Drive for stefan.feil...		100 GB	● 0.0%	0 bytes	Active	1
○	My data room	Drive for stefan.feil...		100 GB	● 0.0%	0 bytes	Active	1
○	My data room	Drive for keqiao.xu...		100 GB	● 0.0%	0 bytes	Active	1

Create data room

Name
War Room

Description (optional)
War room for Security, Cooms and Legal

Allocate additional space:
20 GB

Data room managers: 0 Unlimited user licenses
alex.

SAVE

© 2019 Diligent Corporation Privacy notice

Learn more about how your organization can check every security box while improving governance, compliance, and overall performance through Diligent's suite of integrated solutions.

LEARN MORE ▸

For more information or to request a demo, contact us today:
Email: info@diligent.com | Call: +1 877 434 5443 | Visit: diligent.com