PROCIRRUS™
cloud technologies

Alphabet Soup – IT security in and out of the cloud

By Ronny Loew, National Sales Director, ProCirrus Technologies

Whether driven by client requirements or scary headlines, IT security and compliance has risen to the forefront of firm planning and concern. Complying with the alphabet soup of regulators from GLBA and GDPR to HIPAA can feel like an expensive and overwhelming hoop-jumping exercise. The reality is, becoming compliant with these types of requirements is actually an important step to protecting the very continuity of your business. It can even become a competitive advantage.

Regardless of the firm's IT model (cloud, hybrid or on premise), it is important to develop and publish a clear security policy. The goal of the security policy is to ensure that sensitive information (i.e. data) is not physically lost or accessed by unauthorized parties.

Define what protected data means to you and educate your users

The first step is to clearly define your protected data and to educate your users on how to protect it. This can be as simple as defining three categories:

1) Public Data – this is data that is publicly available like your website information
2) Proprietary Data- this is data that may be specific to your firm (like a client list) but not confidential in a regulatory sense
3) Confidential Data – This would be all client work product as well as very specific items like social security numbers, patient identifying numbers, health information, financial information etc.

When developing a security plan, most think in terms of the nefarious external hacker. Although that is certainly a risk, in reality the primary risk is the intentional or unintentional behavior of company's end users.

Create policies and systems to protect your data

If you have ever seen a security questionnaire with over 300 inarticulate control points from a client, like a big bank, it is easy to become overwhelmed. However, at its heart, the goal of the security policy is simply to ensure that sensitive information (i.e. data) is not physically lost or accessed by unauthorized parties.

It helps to simplify things by thinking in terms of protecting your data in three key states: at rest, in use and in transit.

Protecting data at rest

Data at rest is data when it is being stored, like on a server hard drive, a PC hard drive, laptop, a mobile device or a thumb drive.

1) Clearly define to your associates where your protected data can stored and require that all storage is encrypted and by what protocol (i.e. AES-256).

2) Remember that email is protected data. So in addition to encrypting drives you should maintain mobile device management (MDM) to protect mobile content as well.
3) Protect your data physically. If your firm maintains on premise servers, make sure they are locked from general access.
4) Have a disaster recovery plan including robust off-site backups (also encrypted).
5) Maintain best practice antivirus and patch updates on all hardware.

Protecting data in transit

Data in transit is data that is in motion, like an email. Your policy should require that protected data is transmitted securely and accessed by only authorized individuals.

1. You should provide an encrypted email option and define its usage requirements.
2. Deploy other services like DLP (Data Loss Prevention) to protect against user errors. Most commonly, these are services at the firewall and/or email server level that detect protected words or patterns (i.e. ###-###-####) and quarantine email before it is sent.
3. Maintain current firewall security software and regularly penetration test your network.

Protecting data in use

Data in use is about protecting data when it is actively being accessed from an authenticated user or a system service (like a database).

1) Maintain a robust password policy that includes:
    a. Length greater than 8 digits
    b. Complexity that includes upper and lower case, numbers and symbols
    c. Change frequency of no more than 90 days
    d. System lock out after three failed login attempts
    e. Forbid the use of any external password for work (i.e. Facebook). *Phishing schemes or insecure external sites are the most common way user credentials are exposed*
    f. Forbid the sharing of credentials or storing passwords in unencrypted states (i.e. plain text, post its)
2) Deploy Multi Factor Authentication (2FA). Multi-factor authentication requires an additional key to access system resources, like a text. It is biggest bang for your security buck!
3) Deploy auditing system for file, database (i.e. SQL) and active directory changes.

The Bottom Line

Best practices security is always a multi-layered and redundant approach. By thinking in terms of protecting your data, where ever it is, you can create the policies and practices that will not only protect your data but also the very existence of your firm.

It can seem overwhelming. A competent cloud partner can certainly relieve the majority of your overall compliance burden. However, regardless of the size of your firm, it is important to remember that protecting your data is up to you. Every step you take toward that end is the right move.