UNITRENDS
A Kaseya COMPANY

Win IT's Newest Challenge: Compliance

Are you sure you can pass the audit?

INTRODUCTION

Compliance is a new and complex challenge for IT. Some of the most sweeping compliance mandates have just emerged, such as GDPR and its detailed requirements for handling EU citizen data just went into effect in May, 2018. IT's challenge comes as mandates require implementing policies and procedures normally performed by professionally trained Records Managers, a job usually found only in Fortune 100 companies, using skills not taught in traditional IT training.

Compliance adds a layer of complexity and a whole lot of work to an already under-budgeted and over-burdened IT department. Compliance challenges are also coming at a time when the volume of data IT is required to manage is exploding. Fortunately there are a new set of tools designed for small to mid-sized businesses to help them to deal with compliance challenges.

SMB COMPLIANCE CHALLENGE

Compliance mandates present a wide range of challenges for small and mid-sized IT managers.

Lack of compliance expertise

IT doesn't know the rules. Trying to learn them by reading manuals is almost impossible as guidelines are written by and for lawyers. Additional confusion is introduced because some mandates legislate very specific directives and some are more "guiding principles". How can IT know for sure they are not leaving their organization exposed to findings of non-compliance?

Hiring external contractors is expensive and not a long term solution. Contractors can help set up a process and maybe even guide you through an audit, however they may not be available long term to deal with changes to the law or your evolving business processes. Outsourcing IT services is not necessarily an answer either, as many compliance regulations, such as SOX apply equally and as stringently to outsourced functions as well as those performed internally.

Compliance adds a layer of complexity and a whole lot of work to an over worked and under budgeted IT staff.

Lack of security policy expertise

Most mandates, such as HIPAA and GDPR, center on protecting personally identifiable information (PII) and/or protected health information (PHI) from exposure or theft. IT has traditionally looked to hardware devices such as fire walls and virus scanners to provide security. But now compliance mandates appropriate business policies outside of traditional IT control. Backup appliances protect data from loss and corruption but do nothing to control how data is accessed by vendors or shared by users.

IT is already maxed out

SMBs typically have between 1 and 5 IT staff. There is little time, energy or budget to invest in compliance programs, particularly those that have open-ended mandates that continue to evolve. And most frightening, the cost of failure can be quite high.

COST OF NON-COMPLIANCE

Being judged non-compliant can lead to heavy fines and loss of credibility. Bad publicity from a compliance violation will negatively affect your customers and trading partners. What is worse is that many compliance regulations are written so that an organization does not even have to knowingly have breached a protocol to be found in violation. HIPAA has a whole category of fines just for those who really don't know what they are doing. HIPAA auditors judge non-compliant enterprises along several categories:

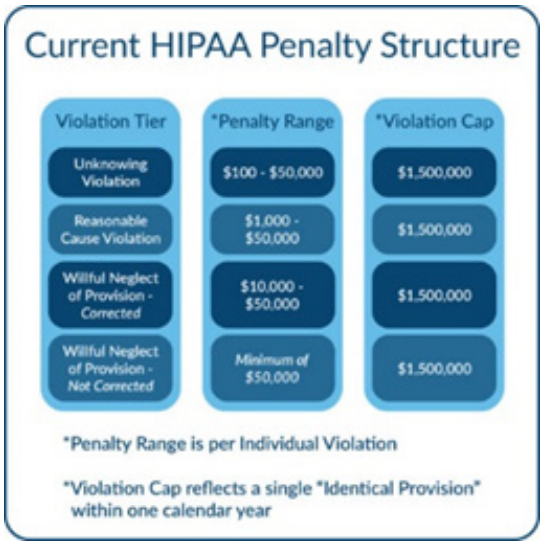
- **Category 1** - A violation that the covered entity was unaware of and could not have realistically avoided, had a reasonable amount of care been taken to abide by HIPAA Rules.

- **Category 2** - A violation that the covered entity should have been aware of but could not have avoided even with a reasonable amount of care. (but falling short of willful neglect of HIPAA Rules).

- **Category 3** - A violation suffered as a direct result of "willful neglect" of HIPAA Rules, in cases where an attempt has been made to correct the violation.

- **Category 4** - A violation of HIPAA Rules constituting willful neglect, where no attempt has been made to correct the violation.

The attached graph highlights the penalty structure for HIPAA. Even "Unknowing Violations" can lead to fines as large as $50,000 per incident per year the violation is allowed to continue. There are hundreds of ways that HIPAA Rules can be violated, with the most common HIPAA violation being impermissible disclosures of protected health information (PHI). The maximum fine per violation category, per year, is $1,500,000.



GDPR also has serious financial penalties. Early in 2019, GDPR changed from an "implementation" phase to one that allows agencies to assess fines. In January, France fined Google 50M Euros for "failing to provide transparent and easily accessible information on its data consent policies".

Fortunately there are now tools that can assess, automate, discover, and report potential compliance violations.

NEW TOOLS TO MEET COMPLIANCE REQUIREMENTS

Compliance mandates are a fact of business life and new requirements are arriving all the time. Fortunately there are new automation tools that can make managing a compliance program easier and less labor intensive.

Bad publicity from a compliance violation will negatievly affect your customers and trading partners

Almost all compliance mandates include requirements to protect data from loss, corruption, or improper storage. Today's best-in-class backup and recovery applinaces address these mandates.

ADVANCED DATA BACKUP AND RECOVERY APPLIANCES

Almost all compliance mandates include requirements to protect data from loss, corruption or improper storage. HIPAA, for example includes standards for the way PHI data is stored and protected, including:

- **Backups**: HIPAA mandates frequent data backups and restores from the most current files.
- **Recovery**: HIPAA-covered organizations must be able to fully restore an exact copy of lost data.
- **Recover Securely**: All security mandates must remain in place during a recovery.
- **Recoveries must be tested**: Regular recovery testing is required, including documentation that demonstrates whether recoveries are within stated goals.
- **Off-site Storage**: Disasters such as a fire or flood will also destroy backups stored locally so backups must be replicated to a remote location
- **Encryption**: Data must be encrypted during storage and while being transferred over a network. Best-in-class backup solutions uses AES-256 Bit Encryption.
- **Documented Backup and Recovery Plans**: HIPAA covered entities are required to have written procedures of backup and recovery procedures.

Today's best-in-class data backup and recovery appliances address these mandates as well as automate other routine data protection processes.

CLOUDS THAT MEET COMPLIANCE REQUIREMENTS

HIPAA requires that all computing resources of covered organizations, including those provided by third parties, meet compliance mandates. If businesses under HIPAA want to use the cloud they are required to find a provider whose cloud infrastructure is HIPAA compliant.

Cloud should be compliant with the mandates of each country in which they operate and meet many industry regulations, such as SOC 1 and SOC 2, HIPAA, CJIS, and GDPR, to name a few. Regular audits ensure that the facilities and associated systems meet industry standards for physical security, encryption levels, network security, configuration management, monitoring, and other control areas.

The cloud provider should also be able to provide a signed Business Associate Agreement (BAA) to you to maintain your HIPAA compliance. The HIPAA Privacy Rule requires all covered entities to have a signed BAA with any third parties they hire that may come in contact with the organization's personally identifiable information

ADVANCED INTRUSION DETECTION MONITORING

One of the major causes of compliance violations is hackers entering enterprise networks and stealing proprietary user information to sell on the dark web. More than 70% of all cyber security incidents today are the result of internal security issues that no firewall or anti-virus could have prevented. Once attackers get past your edge defenses, they can spend months (or years!) undetected on the inside stealing data.

New intrusion detection monitoring solutions will automatically run daily scans to detect and alert IT to suspicious activity such as unauthorized logins or applications being installed on critical servers, new profiles or administrative privileges being added to laptops, or unusual log-ins to important servers at unusual times.

Enterprises may even want to utilize a solution that can scan the dark web for stolen corporate data, including email addresses and passwords, corporate credit cards, and PII information that was sourced from a hack. Many times this will be the first that an organization will find that a hacker has stolen data from their network. Best-in-class dark web monitoring tools will even let IT create a phony phishing email to send to employees to identify who falls for the trick and requires additional security training.

.

Best of all a new family class of applications has been developed specifically to help small and mid-sized businesses meet compliance mandates.

COMPLIANCE GUIDANCE APPLICATIONS

Best of all, a new class of applications has been developed specifically to help SMB organizations meet compliance mandates. Be careful to avoid check-list products on the market that provide you with just a laundry list of tasks you must perform. Superior compliance solutions will automatically perform:

- **An Initial Assessment**: Simply set the software to scan your network and answer a set of resulting questions to quickly determine if requirements are being met, and if not, what needs to be done to become compliant.
- **Recommended Steps for Remediation**: The solution will document and prioritize issues that must be remediated to address compliance-related, fine-worthy vulnerabilities.
- **Produce Approved Documentation**: Perhaps the best feature is that the software will produce all mandatory reports as required by regulators so you can be prepared, in advance, for an audit.
- **Execute Ongoing Compliance Reviews**: For continued protection, the solution will perform regular, automated network scans that will detect any new issues, identify potential threats, and inform administrators of the details.

CONCLUSION

Fortunately this suite of compliance tools will greatly assist in meeting the stringent requirements of industry and governmental auditors. But perhaps the most important aspect of all these solutions is that they are automated to a very high degree. Once set up they run regularly and automatically with little IT involvement unless there are negative findings that need to be addressed.

unitrends.com
PART# WP-2093-ENG-A

UNITRENDS
A Kaseya COMPANY