globalscape®
securely connected

Out of Order! The Risks of Being Out of Compliance

TABLE OF CONTENTS

"The average cost for organizations that experience non-compliance related problems is nearly $9.4 million."

- Ponemon Institute, True Cost of Compliance

Data privacy matters to people, and it's a core reason why compliance regulations are in place. You, your customers, employees, and business partners all value your right to the privacy of your data—which makes it no surprise that the cost of non-compliance is exceedingly high. Non-compliance often indicates that an organization doesn't even have the bare minimum security measures in place to protect the data they manage. This very situation would scare any individual from engaging with an organization that would put their data privacy at risk.

We are all very protective of our own individual data profile. In this day and age, our personal and professional data follows us, from home to work, the grocery store, the doctor's office, the bank, pretty much any and everywhere. If we lose control of our data, and it's stolen or lost, the repercussions can be extremely damaging on many levels, financially and emotionally.

Whether your organization handles credit or debit card data or sensitive customer and employee information, at the bare minimum your organization is required to comply with data and IT infrastructure security mandates to avoid heavy fines, lawsuits, time-consuming government audits, lost revenue, or damaged reputation. Failure to comply—even unintentionally—can also be a leading indicator of security vulnerabilities within your organization's IT infrastructure.

In this guide, we discuss common compliance regulations, how compliance risks evolved across the enterprise, the top six consequences of failing to comply with industry or government regulations, and the role of data management in helping facilitate or maintain compliance.

COMMON COMPLIANCE REGULATIONS

Do you know which compliance mandate you are required to meet and maintain? Here's a look at a few compliance mandates that may relate to you and your organization, based on the data your organization manages:

Payment Cared Industry Data Security Standard (PCI DSS)

PCI DSS is a security standard for organizations that handle major credit cards such as Visa, MasterCard, American Express, Discover, and JCB.

Who does PCI DSS apply to?

Any company that accepts credit card payments is required to comply with PCI DSS standards.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA refers to a data privacy legislation that established the first national standards in the United States to protect patients' personal health information (PHI).

Who does HIPAA apply to?

HIPAA applies to organizations such as health plans, healthcare clearinghouses, and healthcare providers. In addition, HIPAA requires covered entities that work with a HIPAA business associate to produce a contract that imposes specific safeguards on the PHI that the business associate uses or discloses.

Health Information Technology for Economic and Clinical Health Act (HITECH)

The HITECH Act set meaningful use of interoperable Electronic Health Record (EHR) adoption in the health care system. In 2015, hospitals and doctors began to be subjected to financial penalties under Medicare if they are not using electronic health records.

Who does HITECH apply to?

HITECH amends HIPAA. HIPAA applies to "Covered Entities" and "Business Associates" of covered entities. "Covered entities" under HIPAA generally include health care providers, health plans, and health care clearinghouses.

Sarbanes-Oxley Act (SOX)

The SOX Act of 2002 is legislation passed by the U.S. Congress to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise, as well as improve the accuracy of corporate disclosures. The U.S. Securities and Exchange Commission (SEC) administers the act, which sets deadlines for compliance and publishes rules on requirements.

Who does SOX apply to?

All U.S. public company boards, management and public accounting firms must be SOX compliant. There are also a number of provisions of the Act that apply to privately held companies, for example the willful destruction of evidence to impede a Federal investigation.

Federal Information Processing Standard Publication 140-2 (FIPS 140-2)

FIPS 140-2 is a U.S. government computer security standard used to approve cryptographic modules. The National Institute of Standards and Technology (NIST) issued the FIPS 140 Publication Series to coordinate the requirements and standards for cryptography modules that include both hardware wand software components.

Who does FIPS 140-2 apply to?

Government agencies require FIPS 140-2 compliance for any commercial systems that are used to protect the integrity of data moving across their networks. It's also becoming a security standard for many public-sector organizations.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a regulation by which the European Parliament, the European Council, and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Who does GDPR apply to?

The regulation applies if the data controller or processor (organization) or the data subject (person) is based in the EU. Additionally, the regulation also applies to organizations based outside the European Union if they process personal data of EU residents. The regulation does not apply to the processing of personal data for national security activities or law enforcement.

THE EVOLUTION OF COMPLIANCE RISKS ACROSS THE ENTERPRISE

Enterprise risk has grown dramatically in both scope and complexity since the dawn of the digital era. Cybersecurity represents only one branch of risk management in today's business world. Companies are also tasked with regulatory compliance demands and operational challenges that can only be tackled by IT departments. As executive boards seek to address these evolving strategic components, the role of technology becomes even more inextricable from the foundations of the corporate outlook.

This shift has put additional strain on corporate budgets and has left many organizations uncertain about their risk assessment strategies at large.

Network Risks Continue

As the frequency and severity of cyber-attacks and information leakage incidents continue to rise, perhaps the most hazardous risk in the contemporary enterprise landscape is data loss. According to Verizon's latest Data Breach Investigation Report, 2015 was defined by an ongoing torrent of high-profile database intrusions, insider misuse and privacy incidents, physical theft and loss, point-of-sale-system attacks, and a range of additional cybercriminal activity across nearly every professional sector. This pivotal year marked a massive uptick in cybersecurity awareness, and many enterprise leaders have dedicated efforts to bolster their defensive measures and avoid falling victim to cybercriminals.

Evolving Regulatory Standards

While governing boards seek to protect businesses and organizations with strict compliance requirements, failing to meet these demands constitutes a substantial portion of enterprise risk as well. The regulatory landscape has been dramatically expanded in the past 20 years, with deep-seated implications in every area of the digital world.

Decision-makers must understand the nature of these compliance standards and adjust their technology profiles accordingly to avoid the repercussions of falling short of the demands. Thankfully, the right data management solution can proactively address many of the requirements laid out by these organizations, taking the pressure and the uncertainty out of the equation for IT and business leaders.

THE COMPLIANCE PROBLEM – 3 WAYS COMPLIANCE PROBLEMS NEGATIVELY AFFECT YOUR BUSINESS

1. Shadow IT - Privileged or proprietary data is placed at risk

Compliance regulations exist to protect people and their data. Shadow IT methods—or the use of unsanctioned applications—can unintentionally expose a back door into your system. In short, your system and data is at risk of data loss, breach, or theft.

2. Compliance reporting processes are broken

Compliance requirements are very strict. If your processes are unreliable, slow, or inaccurate, then you will find yourself extremely challenged when it comes to dealing with a compliance audit. Data management is crucial in this aspect, as it helps ensure the secure and efficient management of the processes and workflows necessary for facilitating compliance.

3. IT has no visibility into their data

You can't fix or prevent issues that you can't see or understand. Compliance requires visibility into your IT infrastructure, data activity, and data accessibility. Any solution or issue that obstructs this visibility not only indicates a compliance failure—but also indicates a security failure.

Gaps in compliance are inevitable, and it would be impossible to expect that you could achieve perfection at all times. Compliance is a dynamic entity that evolves and changes over time in response to the environment. Security risk factors always change, and compliance regulations are designed to adapt to the environment so that organizations can better prepare themselves to protect their data and IT infrastructure, which in turn will better protect their consumers, employees, patients, partners, and others.

When and where you find failures within your system can also be an opportunity to close those compliance gaps. Having a proactive and flexible mindset when it comes to compliance will encourage a more compliance-friendly and transparent culture, where you and your team can learn from your mistakes and correct any failures before they become an expensive and damaging consequence of compliance failure.

THE TOP 6 CONSEQUENCES FOR FAILING TO COMPLY

Failing to meet local, industry-specific, and/or federal guidelines for compliance can result in serious consequences for your business, in addition to lawsuits, audits, fines, or even the dissolution of your business entirely. What follows are the top six consequences for failing to meet compliance mandates.

Consequence #1: Compensation and Remediation Costs

Once you lose the trust of your customers, employees, and the general public, it can be difficult to get it back. In some cases, rebuilding that trust may have to come with some form of compensation and remediation. Reassurance may need to take shape with providing a free service like credit monitoring or identity theft insurance, or maybe a combination of the two. When the national retailer Michael's confirmed the theft of their consumers' credit card information, the company compensated their

customers in this fashion. That "free" reassurance for their customers wasn't free for the retailer. At the same time, internal remediation comes with additional costs including costs to determine what happened, how it happened, who was responsible, and the final steps in fixing the security of your IT infrastructure.

Consequence #2: You Open Yourself Up to Lawsuits

We're living in a material and litigious world. Lawsuits have become the norm. Are you prepared to face lawsuits, the very expensive and highly publicized kind? Victims of a data breach want justice, and if a lawsuit seems like the best avenue for justice, then who do you think they will target? It certainly will not be the anonymous, impossible-to-find hackers. Lawsuits are expensive to deal with, regardless if you win or lose your case. A law firm in Tampa, Florida is currently building a case against Yahoo! for their 2016 data breach that accounted for more than 500 million stolen user accounts. Their 2016 data breach, along with the discovery of years and years of prior data breaches, has also had a negative effect on the value of Yahoo! during their acquisition with Verizon.

Consequence #3: Bank Fines

When your customers' credit cards are used to fraudulently purchase items, the banks are on the receiving end in terms of responsibility. The good news is that your customer's confidence in you isn't shaken. The bad news is that although the banks "foot the bill," they will most likely pass along those charges to you in the form of fines or added fees.

Consequence #4: If You Don't Audit, the Government Will

The Federal Trade Commission (FTC) often monitors high profile cases where organizations have failed PCI DSS compliance and where a large number of U.S. citizens were negatively affected. Compliance failures can put your organization in the spotlight, and the FTC can quickly decide to audit your organization regularly. Or the FTC may determine that your organization should pay a heavy fine—and be audited regularly. Federal audits are generally increasingly stringent when it comes to compliance.

Consequence #5: You Will Lose Revenue

Each of the previously mentioned consequences of compliance failure points to a very high price to pay, but it doesn't stop there. Compliance failure can also lead to lost revenue. Data breaches and compliance failures all make great news fodder, and the daily news cycle and social media certainly help bad news travel faster. If people can't trust you to protect their sensitive data, be it their credit card information or patient health information, then they won't trust you with their business. They will take their wallets elsewhere. When retail chain Target experienced a massive data breach, they say their profits took a nose dive by $440 million dollars during the fourth fiscal quarter after the breach.

Consequence #6: Damaged Reputation

One thing is clear: a data breach is a PR disaster. Companies often spot the intrusion too late, and cannot respond adequately, resulting in falling sales and media outrage.

Customers often vote with their wallet. UK-based fraud prevention company Semafone found that the overwhelming majority of people would not do business with a company that had been breached, especially if it had failed to protect its customers'

credit card data. In the survey, conducted by OnePoll, 86 percent of 2,000 respondents stated that they were "not at all likely" or "not very likely" to do business with an organization that had suffered a data breach involving credit or debit card details. Damage on this scale can never be fixed. At best, it can be mitigated with countless hours of reputation management, marketing, and PR.

You can see how the total costs of a data breach can easily reach into the millions. For big companies, the figure could top $1 billion over time. With consequences like these, you don't want to risk a compliance failure.

THE ROLE OF DATA MANAGEMENT AND COMPLIANCE

Data management is an inherent part of facilitating compliance, and is especially helpful with the common compliance regulations described in an earlier section of this guide. Facilitating compliance requires the proper strategy, tools, and processes that will encourage the secure and efficient management of an IT infrastructure and its data. For that reason, it's critical for your organization to design a secure system within your IT infrastructure that enables full control and visibility of your data, along with the efficient, accurate, and reliable management of your data. The process and system behind facilitating compliance should not be a set-it-and-forget-it strategy. It should be a strategy that combines security policies, training, and technologies. Data management can streamline your processes and simplify an endeavor that can otherwise get complicated.

> "On average, non-compliance cost is 2.65 times the cost of compliance […]"
>
> – Ponemon Institute, True Cost of Compliance

Spending less time planning and implementing your compliance strategy—or not spending any time on compliance at all—is a sure-fire way to end up facing one or all of the top six consequences of compliance failure. Dealing with the consequences of compliance failure will cost more time and money than the proactive and prevented cost of a well-planned strategy, implemented with the right tools and technologies.

MANAGE YOUR DATA, MANAGE YOUR COMPLIANCE: WHY SYSTEMS MATTER

Data management plays a crucial role with an organization's security and compliance strategy. The methodologies and tools that support secure data management—especially when it comes to facilitating compliance—helps organizations reduce security and productivity vulnerabilities. Through a secure system of policies, procedures, and technologies, a secure managed file transfer (MFT) solution can enable you to enforce and facilitate compliance mandates with greater efficiency and visibility over the data and IT Infrastructure that you want to protect.

If you are evaluating solutions to help you facilitate compliance, consider the following MFT-supported functionalities:

1. Automated Data Workflow and Processes: Today's end users may be aware of the compliance standards to which their organizations are held, but

when performing daily tasks such as sharing data, messaging, and email, the need to comply with regulatory measures is not necessarily top of mind. In fact, employees focused on productivity may take some shortcuts to accomplish more in a given day, circumventing best practices in the process. For profit-minded business leaders, it's hard to enforce data management standards while maximizing user performance.

An MFT solution should automate processes with all key applications and services with appropriate compliance functionality. This lets end users remain at the top of their game while all security and tracking processes are performed automatically in the background.

2. Centralized Control and Visibility: Executives, department heads, and managers need a view of an array of business management-focused insights derived from the movement of files and data. Not knowing what's happening in your network can be dangerous. Oftentimes, the most pervasive compliance pitfalls stem from a shortage of administrator insight into a sprawling, changing IT infrastructure. With today's network dynamics shifting so rapidly and encompassing new technologies all the time, transparency into these environments is critical if IT teams want to ensure everything checks out with regulatory expectations. Only when IT leaders can see the big picture, investigating and closing compliance gaps in a proactive manner, will a company truly be averse to risk and maintain a clean record.

A robust MFT solution offers IT administrators an unprecedented level of transparency into the data in the entire network, empowering strategists with perspective and control that no manual processes could provide. This top-down view of the infrastructure is a primary component of compliance excellence, and can also alleviate a number of other security and performance risks.

3. Custom Compliance Profiles and Reporting: It's important to understand how data moves throughout your organization. Every organization has its own set of regulatory expectations to uphold. Therefore, a one-size-fits-all data management solution won't do much for a highly specialized compliance profile. Luckily, today's best solutions offer customized data workflows and configurations that ensure every data transfer is performed and tracked to the highest possible degree of adherence.

Whether a company is striving to uphold excellence in PCI DSS, HIPAA, or standard SOX accountability, a tailored MFT solution can simplify and strengthen its data management capabilities.

With each of these functionalities, an MFT solution simplifies what can easily be a complicated endeavor when it comes to meeting compliance mandates. The right MFT solution will also go beyond traditional IT considerations to provide real opportunities to achieve greater operational efficiency, enhance your security posture, and provide data management and integration capabilities, producing measurable effects on ROI within your organization.

Compliance is undoubtedly a complex and dynamic endeavor. With a secure MFT solution and a strong data management policy, you will be better equipped to help your organization track, monitor, and report on compliance efforts so that you can proactively catch and mitigate any potential risks.

For more information please visit our website today.

globalscape®
securely connected

GlobalSCAPE, Inc. (GSB)
Corporate Headquarters
4500 Lockhill-Selma Road, Suite 150
San Antonio, TX 78249 USA
Sales: 210-308-8267 / Toll Free: 800-290-5054
Technical Support: 210-366-3993
Web Support: www.globalscape.com/support