QUICK START GUIDE

Quick Start Guide to Security Compliance

Powered by

IT Security COMMUNITY

CompTIA

Which of your customers are subject to compliance mandates? Before you answer that, take a moment to consider factors outside their primary industry – geographic scoping, service provider implications, and sensitive consumer data. Technology has flattened the world and requirements now exists that many people are simply unaware of and do not know apply. This covers the gamut of US state, federal and international laws, as well as regulatory bodies, and private-party business agreements. Cybersecurity compliance touches every US-based business to some degree.

If you take one concept from this guide, please let it be that compliance does not equal security. It never has and it never will. However, if you create a security-minded culture in a company, then compliance is relatively easy to achieve. As an example, liken building a security-minded culture in a company to assembling LEGO pieces - once a few building blocks are in place, they starting coming together and soon enough you've build something great!

In your chosen profession, would you argue that you are only as good as your current IT knowledge? For most people in the technology fields that is a given, since change is the only constant and IT professionals have to keep abreast of the latest technologies. How is your cybersecurity knowledge? The best IT service providers understand key cybersecurity concepts and are able to leverage compliance-related requirements to create opportunities. This is a "win-win" since it provides customers with peace of mind, while also creating valuable revenue opportunities. This guide won't make you an expert, but it will provide you with immensely valuable information and references that you can use. CompTIA wants you to take advantage of this opportunity to help your business, as well as protect your customers.

For technologists, many in our industry focus on selling and implementing the "bright & shiny" technology solutions. For some IT service providers, that is their business model and it has traditionally worked. Is that wrong? No. However, they miss the forest because of the trees – they are blind to the bigger concept of providing comprehensive risk management, as compared to just selling products. This blind spot can be catastrophic if a customer feels an IT service provider "was supposed to make me secure" and they suffer a security-related incident. This is now a public relations nightmare for the IT service provider.

According to a report from the website RetailCustomerExperience.com, Americans tell an average of nine people about good experiences and nearly twice as many (16 people) about poor ones – making every individual service interaction important for businesses.[1] Consider how a local or regional IT provider's business would be impacted by the negative ramifications of bad publicity associated with an unhappy client from a security-related incident.

Skeptical? Two of the most recent high-profile data breaches in the US are blamed on outsourced IT service providers. In 2014, hackers broke into Target via a HVAC service provider that led to a data breach affecting roughly 40 million customers. In the end, Target agreed to a $39 million settlement with several US banks, settled with Visa for $67 million, and had to address a federal class action lawsuit brought by customers for $10 million.[2] Also in 2014, hackers used the credentials of an IT service provider to enter the perimeter of Home Depot's network that led to the compromise of 56 million debit and credit card numbers of its customers.[3] To date, the Home Depot disclosure made that incident the largest retail card breach on record. Both companies pointed to IT service providers as the springboard into their network that led to the breaches.

These kinds of headlines are going to be the "new normal" for the foreseeable future. What this takes is to reset thinking to view cybersecurity as merely the management of operational risk, just as businesses handle risk management in the rest of their business. Cybersecurity is coming out of the shadows from being relegated to an "IT function" to a business focus, since what businesses don't know has a proven ability to hurt them. That concept is starting to take off and it benefits IT service providers who can market their services from the perspective of risk reduction.

1 http://www.retailcustomerexperience.com/articles/survey-twice-as-many-people-tell-others-about-bad-service-than-good/
2 http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/
3 http://krebsonsecurity.com/tag/home-depot-breach/

Understanding Negligence

When things go bad, lawyers are usually involved. That is why it is important to understand what negligence is and how it can be avoided.

What is required to avoid negligence is for IT service providers to understand their role and responsibilities in securing client networks. In all cases, it involves ensuring that communications or other documentation exists that can prove how an IT service provider fulfilled its duties to its clients. This goes back to having strong customer service capabilities, which really need to expand upon situational awareness updates to clients, since the client's awareness of technical issues and recommendations helps take liability away from an IT service provider.

When negligence is claimed, it falls under tort law, since it deals with civil court proceedings to address wrongs. In tort law, both businesses and individuals may be liable for injuries caused due to negligent behavior. A business may be found guilty of negligence for a number of reasons, all of which involve breaching duties that the business has toward others. Breach of duty comes into play when a loss or injury occurs due to the possible negligence of another party. Negligence usually includes doing something, or not doing something, that an ordinary, reasonable, and prudent person would not do, when considering the circumstances and the knowledge of parties involved.

Negligence lawsuits generally name businesses or individuals as defendants, claiming that the business or individual was responsible for harm due to a lack of care. Negligence cases rely on assumptions about how reasonable people would act and under tort law, a negligence case must claim that a defendant's lack of care caused actual harm to a plaintiff.

Duties for businesses change based on employee special skills or levels of expertise. For example, an IT service provider that employs trained and licensed technicians has a higher duty of care to its clients than an unskilled defendant. This means that an IT service provider may be held liable for a cybersecurity incident at a customer if a reasonable technician would have deemed a server/firewall/application/website/database to be insecure, even if a reasonable person without technical training would have deemed it secure.

Still skeptical? Invite your insurance agent for a cup of coffee and share this document to get his/her perspective to see how your insurance coverage protects, or doesn't protect, your business from the risk of a negligence-related lawsuit. Many "cybersecurity insurance" policies do not cover non-compliance related costs. While the range of fines and lawsuits following a cybersecurity event are vast and potentially expensive, the game plan of obtaining cybersecurity insurance and working to remain in compliance with all applicable laws does greatly reduce the backend risks associated with cybersecurity incidents.

One of the most common pitfalls for IT service providers is the assumption that "unless my clients tell me that they have a compliance mandate, I assume they don't." Secure Designs, Inc. CTO, Ron Culler, notes "The compliance landscape is changing all the time in response to new and ever expanding breaches and attempts to secure protected data. As advisors to your clients you should be aware of the impact this can have and be prepared to discuss it with your clients before it's too late."

Of special note from Secure Designs, Inc. is the expansion of the Internet of Things (IoT). "I think one of the greatest risks that businesses are missing today is the impact of non-traditional IT channel technology entering their client's networks. IP enabled technology (IoT) is rapidly entering businesses and without a clear understanding of 'What, Why, and How' these technologies are being implemented and secured" states Ron. The clients are at risk and IT service providers are going to be left trying to answer the questions of "What happened?" and "Why didn't you know?"

It's not just about PCs and servers anymore - Point of Sale (POS), IP video, embedded sensors, VoIP, and BYOD are just a few of the evolving technologies that must be secured. The threat landscape is expanding at an astonishing rate and with it comes the need to understand the risk, potential compliance issues, and how security is applied. The first step is start having higher level conversations with clients about their business in order to help them understand technology is a tool and not the solution. This will help create steps to select the correct secure for the requirement.

Building A Cybersecurity Program

Getting back to the LEGO analogy from earlier, if you've ever played with LEGOs before, you can build nearly anything you want – either through following directions or using your own creativity. It all comes down to understanding how the various LEGO shapes snap together. Once you master the fundamentals, it is easy to keep building and be creative since you know how everything works. Cybersecurity really isn't much different, since cybersecurity is made up of numerous building blocks that all come together to build the maturity of a company's cybersecurity program.

Each of the various components that make up a cybersecurity best practice essentially is a LEGO block. Only when the following building blocks come together and take shape do you get a real cybersecurity program:

- **Documented policies, procedures & standards**
- **Asset management**
- **Identity & access controls**
- **Risk management**
- **Vendor management**
- **Physical & environmental security**
- **Compliance**
- **Privacy**
- **Remote access**
- **Data backups**
- **Data destruction**
- **Etc**.

If you closed your eyes for a moment to envision your company's or your clients' cybersecurity programs as a LEGO creation, what would they look like? Is it a hobbled-together assortment of blocks without structure or is it an awe-inspiring fortress? A valid excuse if that you didn't have a set of instructions – that is understandable and is a common point of frustration. CompTIA is here to fix that for you!

When you start discussing the topic of "best practice frameworks" for cybersecurity, the two names at the top of the list are ISO and NIST. The International Organization for Standards (ISO) 27001/27002 frameworks tend to dominate multinational or non-US companies. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 framework dominates within the US healthcare, financial services and government contractor segments. These two frameworks are essentially the instruction manuals that a company uses to create a "reasonably expected" cybersecurity program.

Keep in mind that it is rare to have to a requirement for verbatim compliance with the entire ISO or NIST requirements, since some controls might not be applicable to some organizations. This usually provides companies with room to be flexible and craft cybersecurity programs that, while aligned closely with ISO or NIST, are customized to the specific needs of the company. With the mind of flexibility and creativity, you can build your LEGO fortress to suit your specific needs and that is ok.

Fundamental Cybersecurity for Businesses Not In Regulated Industries

Keep in mind that ignorance is neither bliss, nor is it an excuse! Arguably, one of the biggest risks for businesses is being within scope for a statutory, regulatory or contractual compliance requirement and not knowing it. The following section covers cybersecurity requirements that are unbound by industry verticals. These topics should be talking points for your salespeople!

FEDERAL TRADE COMMISSION (FTC)

One of the most shocking revelations for more IT professionals is that the FTC can and does investigate companies for deficient cybersecurity programs as part of its mandate to regulate "unfair business practices" under Section 5 of the FTC Act that prohibits "unfair or deceptive acts or practices in or affecting commerce."

The FTC Act defines "unfair acts or practices" as those that cause or are likely to cause "substantial injury to consumers which (are) not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." FTC's recent move into cybersecurity fills the vacuum left by the US government's inaction related to data security oversight and the perceived inability of traditional civil litigation to alter the security behavior within businesses.

Nearly every business sector finds it necessary to collect, maintain, analyze and monetize user data. If a business mismanages that data, the FTC may come knocking. Once a company finds itself in the FTC's crosshairs, that company is often forced to expend substantial resources on compliance costs and legal fees. In addition to financial damages that arise from a "consent decree" with the FTC, companies may also be "asked" to overhaul data security practices, hire third-party auditors, notify affected customers, and be subject to continual FTC oversight up to 20 years!

FAIR & ACCURATE CREDIT TRANSACTIONS ACT (FACTA)

The Fair Credit Reporting Act (FCRA) is a federal law, which, among other things, provides individuals the right to examine their own consumer files maintained by consumer reporting agencies to ensure the accuracy of such information. The Fair and Accurate Credit Transactions Act of 2003 (FACTA) amended the FCRA in numerous respects. It is designed to prevent identity theft and it established a requirement for the secure disposal of consumer information, which has a technology implication for the secure destruction of electronic media.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

You may think you know all you need to know about PCI DSS, but have you considered how you affect the compliance of YOUR CUSTOMERS' compliance with PCI DSS?

The Payment Card Industry Security Standards Council (PCI SCC) is a non-governmental organization, launched in 2006, that is responsible for the development, management, education, and awareness of the Payment Card Industry Data Security Standard (PCI DSS) and other payment-re-

lated requirements. The Council's five founding global payment brands (American Express, Discover Financial Services, JCB International, MasterCard, and Visa) have agreed to incorporate the PCI DSS as the technical requirements of each of their data security compliance programs, so it is an industry-wide standard.

As an IT service provider, you very well may have your clients' "keys to the castle" since many IT service providers manage the critical technologies for them. While PCI DSS addresses systems that store, process, or transmit cardholder data, IT service providers manage components such as routers, firewalls, databases, physical security, and/or servers and that bring the IT service providers within scope for their PCI DSS compliance as a third-party service provider!

What does this mean for you as an IT service provider? Service providers are responsible for demonstrating THEIR compliance with PCI DSS. According to the PCI SCC, there are two options for third-party service providers to validate compliance with PCI DSS: (1) Annual assessment: Service providers can undergo an annual PCI DSS assessment(s) on their own and provide evidence to their customers to demonstrate their compliance; or (2) Multiple, on-demand assessments - if an IT service provider does not undergo their own annual PCI DSS assessments, they must undergo assessments upon request of their customers and/or participate in each of their customer's PCI DSS reviews, with the results of each review provided to the respective customer(s).

For the IT service provider's PCI DSS assessment, it must cover the services applicable to their customer(s) and that the relevant PCI DSS requirements were examined and determined to be in place. The specific type of evidence needed to be provided by the IT service provider to their customers will depend on the agreements/contracts in place between those parties.

GENERAL DATA PROTECTION REGULATION (GDPR)

The European Union (EU) released the GDPR in May 2016 and it goes live in 2018. The regulation applies to any business that has personal information of EU residents, so it is not geographically-tied to having operations in the EU. This also applies to both employees and consumers, so it expands the scope of data and privacy requirements to internal operations.

The GRPR has wide-ranging implications for businesses. One of the most forward-thinking components to the GDPR is the concept of building in cybersecurity from early on in any process, as compared to cybersecurity being an afterthought and having a "bolted-on" solution to keep data secure.

Of particular concern to IT service providers is the increased focus on the control of data flows, since it is necessary to document where data actually exists. There are numerous requirements for data protection, record keeping, breach notifications, and more, so it is worthwhile for IT service providers to educate their workforce on this regulation.

MA 201 CMR 17.00

In 2009, Massachusetts passed the most stringent data security law within the US called MA 201 CMR 17.00, also known as the Standards for the Protection of PII of Residents of the Commonwealth. The law applies to any business that has Massachusetts residents as clients, so it is not geographically-tied to having operations in the state. The law calls out the duty of businesses to protect sensitive information, as well as specifying expected cybersecurity practices for businesses to follow.

One key point in this state data security law is it coined the term "written information security program," or WISP. The law recognized that businesses require more than just a single security policy and it necessitates a comprehensive program to address cybersecurity risks.

Additionally, this state law marked the turning of the tide for vendor management. Requirements in the law specify the oversight of service providers through documented contracts and on assessing "reasonably foreseeable internal and external risks." In terms of data security laws, this state law is a game changer and it is reasonably expected for other states to both follow and expand upon this law.

Healthcare (HIPAA/HITECH)

There are many misperceptions about HIPAA/HITECH compliance. Often heard from medical providers is that HIPAA interferes with patient care, according to Mike Semel, from Semel Consulting, a firm that specializes in healthcare related technology consulting. "When I ask for specifics, I almost always find out that they do not understand HIPAA basics, but just assume things or listen to other people with little knowledge."

HIPAA allows caregivers and health plans to share patient information with each other for the treatment, payment, and the operations of their organizations. While the Security Rule does have some security requirements, the amount of inconvenience and extra work is not much different than requiring a doctor to wash their hands or wear gloves and goggles when treating a patient. HIPAA is far more procedural for the medical staff than a technology compliance issue.

Of most importance to IT service providers is compliance with HIPAA is categorization as a Business Associates (BA). This including IT service providers that support health care clients. A common misperception is that BA are compliant just by signing a Business Associate Agreement. In fact, that is just the beginning of compliance, since BAs are required to implement full cybersecurity compliance programs, including employee training, maintaining documentation, and delivering HIPAA-compliant services. BAs are now directly liable for data breaches and BAs are now in scope for audit if their healthcare clients are audited. From Mike Semel's perspective, "there is more risk than ever before, but also more opportunities if you embrace compliance as a competitive differentiator."

Additionally, beware of "HIPAA-in-a-Box" or online portals that make HIPAA compliance easy. Mike Semel was recently was shown an online HIPAA management system that included an automated risk assessment module where "the vendor showed me how easy it was to upload a software inventory, and how the 'compliance score' increased once the inventory was uploaded." Mike asked, "What if the software on the list is old, unsupported, and no longer complies with HIPAA?" The vendor had no answer because their system only cared if you uploaded a list and not what was on the list. These "compliance tools" provide a false sense of security and compliance.

Financial Services

The 2008 financial services meltdown triggered a renewed focus on regulatory compliance. But that's not an entirely new trend. Established IT service providers in the financial vertical have successfully navigated compliance requirements such as the Gramm-Leach-Bliley Act (GLBA) for more than a decade.

Enacted in 1999, GLBA ensures financial institutions have security programs in place, at a scale appropriate to the needs of the business. Moreover, GLBA ensures financial institutions protect consumers' non-public personal information.

Among those navigating this compliance landscape, Dave Cava, COO and co-founder of Proactive Technologies. The New York-based IT service provider's clientele includes hedge fund operators and private equity financial services that are 40 users or less. "What a lot of people don't realize about financial services compliance is that these companies are concerned first and foremost about making the correct impression on potential investors," said Cava. "They are at least as worried about due diligence audits from funding sources as they are interaction with the SEC or another regulatory body. These companies die without growing outside investment and not getting funded is a much greater direct threat to their businesses than the SEC."

Still, Cava hears some common compliance questions over and over again. They include:

- **"What do investors look for when evaluating compliance readiness as part of the due diligence process?"**
- **"What are similar firms of type and size doing for compliance?"**
- **"What kinds of data should we be capturing? How are they captured? What is the proper retention time?"**

Government / Department of Defense (DoD) Contractors

Two of the most significant, recent changes to impact IT service providers working for the US federal government deal with cybersecurity compliance.

The National Institute of Standards and Technology (NIST) published Special Publication 800-171 that provides requirements to ensure that sensitive federal information remains confidential when stored in nonfederal information systems and organizations. This impacts government contractors and sub-contractors, since compliance requirements are being written into contracts. As an IT service provider, if you cannot comply with NIST SP 800-171, you simply may not have a seat at the table to even bid on government contracts.

NIST SP 800-171 does not re-invent the wheel for cybersecurity requirements. NIST even went so far as to map SP 800-171 requirements with both SP 800-53 rev 4 and ISO 27002 controls. Interestingly, ISO 27002 "out of the box" will not comply with SP 800-171 requirements and it clearly favors the use of a subset of SP 800-53 rev 4 controls that equate to a "moderate" controls baseline. NIST SP 800-171 essentially created a minimally-accepted cybersecurity benchmark for private businesses.

Specific to DoD contractors, updates to the Defense Federal Acquisition Regulation Supplement (DFARS) require that a contractor designated as "operationally critical" must report each time a cybersecurity incident occurs on that contractor's network or information systems. It also expands protection of a broader collection of data and information described as "covered defense information" and adverse effects on a "contractor's ability to provide operationally critical support." The previous definition of "controlled technical information" remains, but the expanded provision includes many new definitions, the most pertinent being Covered Defense Information (CDI). That term is defined as unclassified information that is "(i) provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or (ii) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract"

Cloud service providers and contractors wishing to employ cloud resources should be aware that DoD will only accept cloud computing services using commercial terms and conditions that are consistent with Federal law, and an agency's needs. Accordingly, a cloud provider must have received provisional authorization by the Defense Information Systems Agency. Furthermore, any "government data" stored in the cloud and not resident on a DoD installation must reside on servers in the United Sates unless otherwise authorized. Contractors will also be obligated to advise the government of intent to use cloud services for their government data.

Outside Experts

IT service providers don't have to navigate the complex compliance landscape on their own. CompTIA, for instance, offers channel training in vertical markets (e.g., government IT, healthcare IT), business credentials, and conference discussions focused on compliance.

The bottom line: At first glance, compliance issues can seem overwhelming. But in reality, compliance expertise actually provides new revenue opportunities rather than business inhibitors for IT service providers.

About CompTIA

CompTIA is the voice of the world's information technology (IT) industry. As a non-profit trade association advancing the global interests of IT professionals and companies, we focus our programs on four main areas: education, certification, advocacy and philanthropy. Our purpose is to:

- Educating the IT channel with our educational resources that are comprised of: instructor-led courses, online guides, webinars, market research, business mentoring, open forums, networking events, as well as helping our members advance their level of professionalism and grow their businesses.
- Certifying the IT workforce as we are the leading provider of technology-neutral and vendor-neutral IT certifications, with more than 1.4 million certification holders worldwide.
- Advocating on behalf of the IT industry. In Washington, D.C., we bring the power of small and medium IT businesses to bear as a united voice in helping our members navigate regulations that may affect their businesses.
- Giving back through philanthropy, our foundation enables disadvantaged populations to gain the skills needed for employment in the IT industry.

Our vision of the IT landscape is informed by more than 25 years of global perspective and more than 2,800 members with more than 2,000 business partners spanning the entire IT channel. We are driven by our members and led by an elected board of industry professionals.

All proceeds are directly reinvested in programs that benefit our valued members and the industry as a whole. Headquartered outside of Chicago, we have offices across the United States; as well as Australia, Canada, China, Germany, India, Japan, South Africa, and the United Kingdom.

For more information, visit CompTIA.org.

CompTIA

Powered by

IT Security
COMMUNITY

CompTIA.org