CYBALT

The Growing Compliance Challenge

Cybalt Inc. Suite #510, 2701,
North Dallas Parkway, Plano, TX

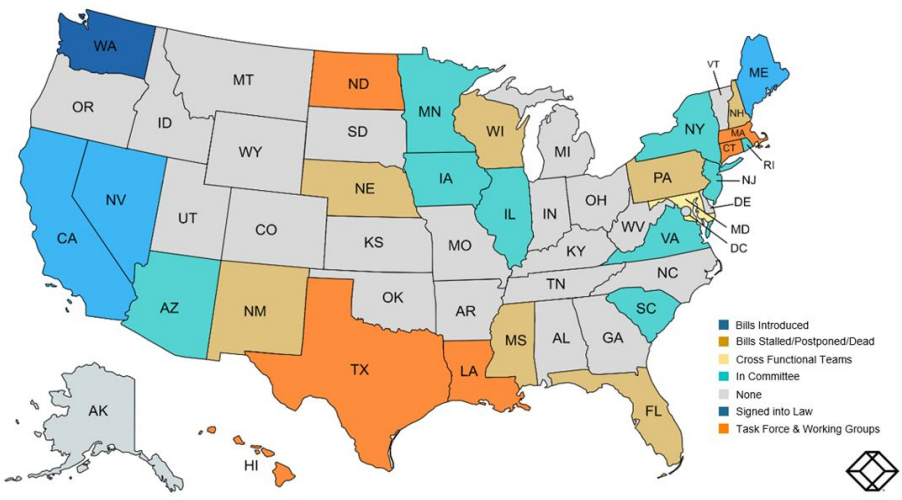
discover@cybalt.com

The Growing Compliance Challenge

Information security management encompasses risk protections like cloud security, perimeter protection, application security, encryption, and disaster recovery. IT security becomes more challenging when compliance, regulations, and global standards such as PCI-DSS, HIPAA, and GDPR are business mandates. With the huge increase in cyberattacks over the last three years, compliance has become much more than avoiding fines and penalties – compliance has become a fundamental requirement to conduct business.

Enterprises in today's marketplace face three new compliance developments making IT security governance a precondition to conducting business and amplifying the challenges to meet compliance requirements:

1. Steep legal fines and penalties now in effect by the new state-level privacy regulations in the United States and what might soon be America's version of the European General Data Privacy Regulation (GDPR).
2. As losses mount due to the industry's exponential growth in ransomware incidents, cyber insurance brokers are making it significantly harder for their policyholders to maintain cyber liability insurance. Cybersecurity insurance providers are reducing their amounts of liability coverage, or exiting the cybersecurity insurance business altogether.
3. The drive to offload services including Cloud-as-a-Service, MSSP, and third-party network operations giving providers access to an organization's confidential data. An organization may not have to abide by any regulatory compliance standard, for example, PCI-DSS. However, if you want to be in a business-to-business partnership with your client, they are now asking for the first time that you "attest" or "prove" that you have the controls in place to protect their confidential data. If your company cannot provide the evidence that you will be a proper data custodian of customer data, your customer will do business elsewhere.



After the California Consumer Privacy Act passed in 2018, the state-level momentum for comprehensive privacy bills is at an all-time high. In the United States, more than 32 states are in some form of committee or development of privacy provisions. So far, three states including California, Colorado and Virginia have enacted comprehensive data privacy laws. These provisions are broken down into two categories – consumer rights and business obligations.

The California Consumer Privacy Rights Act (CPRA) approved November 2020, and effective January 01, 2023, expands the consumer data privacy laws. The new law permits consumers to prevent businesses from sharing personal information, correct inaccurate personal information, and limit a business's use of "sensitive information." Some of the new criteria considered personally identifiable information include geolocation, race, ethnicity, religion, and genetic data such as your DNA which may become the next-generation identity management.

Cyber Insurance Providers are Running for Cover

According to Insurance Business America, cyber insurers are hiking up their premiums and lowering coverage limits. Mr. Edward Ashby, Global Head of Distribution at Axis Insurance states that even with cybersecurity mitigation strategies in place, organizations are finding it impossible to secure 2021 cyber coverage at 2020 rates. Carriers are hiking premiums, some as high as 300% at renewal, and lowering coverage limits on sectors that have been hardest hit by cyber crime. The hardest hit industries for cyber insurance premium increases include education, government, healthcare, construction, and manufacturing.

According to January, 2022 report released from RPS, *U.S. Cyber Insurance Market Outlook,* insurers are not just raising their premiums but also lowering coverage limits. Insurers that were happy to issue$5 million in liability coverage on policies in 2020 have reduced back to limits of $1-3 million in 2021, even on renewals.

For underwriters of these liability policies, the requirements of an organization to obtain coverage have become much more strict and comprehensive. For example, RPS says that multi-factor authentication (MFA) has become a must to qualify for cyber coverage. Insurers are also increasingly incorporating the same scanning technology used by hackers into their own underwriting processes in order to better control their loss ratios.

Privacy Protects Profitability

Your organization may not be in an industry that is regulated and thus, compliance has been off the radar of your Executive Management team. Your client however, is under a regulatory mandate or is simply trying to maintain its cyber liability coverage. Thus, your client must now provide evidence that all third-parties they choose to do business with align and agree to its data handling and data protection guidelines. If your company cannot *attest* or provide evidence of its information security protections you will lose your business contract with the client or they can no longer renew its services agreement with you for the next calendar year. Protecting privacy has now becomes a requirement to protect your company's profitability.

How to Overcome the Compliance Challenge

General George S. Patton said "Accept the challenges so that you can feel the exhilaration of victory." The new privacy laws, changes in cyber insurance liability, and outsourcing IT services have brought new compliance challenges and have altered the path to victory. Winning the war of compliance can be achieved however with a few fundamental steps:

1. Be able to answer the *what*, *how*, and *when* questions of IT security governance.
2. *What* are you trying to protect? Be able to show the auditor that you have a data classification policy that defines "data confidentiality". And have a data handling policy that defines how you handle confidential data, who accesses it, and the procedures to restrict or limit access.
3. *How* did you protect it? Be able to show the auditor how you enforce your data confidentiality policy. This could be opening your drawer and pulling out the network drawing of your firewall architecture or showing a representation of your public cloud infrastructure and how you secure it.
4. And the *When* your organization enforced policy to some auditors is the most critical artifact they will want to see. Your security program needs to be able to create a report showing when your IT security policy was enforced. For example, your organization's Internet proxy blocked this user from accessing this restricted application according to IT security policy.

Having the administrative controls (policies), enforcement controls (technologies), and reporting tools ensures that you are a good way down the path of achieving compliance to the newly changing IT security requirements. The only way however to be completely sure of your organization's ability to protect privacy, maintain its cyber liability insurance, and verify your outsourced IT services meets your clients requirements is to undergo an assessment by an independent outside agency.

The IT security and risk management experts at Cybalt can help baseline and assess your organization's ability to adhere to the pertinent privacy laws applicable to your firm. Cybalt's highly credentialed security consultants can verify your organization's ability to protect confidentiality and stay ahead of the exacting risk management requirements needed to maintain cyber liability insurance. And finally, whether your IT services are cloud-based or delivered by a MSSP, Cybalt's team of cybersecurity experts can attest your firm's' ability to protect client data.

Cybalt is a global cybersecurity practitioner assisting organizations with all their cybersecurity needs including security consulting, best-in-class security technologies, global SOC, vulnerability and device management.