FASTCOMCORP™

Discover Potential, Empower Success

Cyber Risk Management

Fastcomcorp Collective

introduction

Every organization has its own unique set of business objectives, compliance requirements, policies, processes, and technology solutions. As a result, organizations also have their own unique set of threats, vulnerabilities, and risks.

Nevertheless, embracing IT security and compliance simply isn't an option in today's world anymore. Customers and partners expect organizations from retailers to government agencies to actively address vulnerabilities associated with technology, as well as with people and processes.

This is because consumers are increasingly concerned about the privacy of data shared how is shared and how is managed than ever before. According to Pew Research. Nine out of ten Americans worry about online privacy and data security, with 54% citing identity theft and 16% credit card fraud as top concerns.

In the European Union, consumers have been concerned for quite some time about the privacy of how their personal is shared, and how it is managed. EU Parliament solution was GDPR which set a strong standard for privacy and data protection because it empowered people to truly control their personal information.

There is no distinction between personal data about an individual in their private, public, or work roles. It is all are covered by this new compliance regulation. GDPR impacts people, process, and technology for all. This compliance regulation inspired the State of California in the United States to pass a law in June 2018. The California Consumer Privacy Act (CCPA). AB 375 allows any California consumer to demand to see all the information a company has saved on them, as well as a full list of all the third parties that data is shared with. In addition, the California law allows consumers to sue companies if the privacy guidelines are violated, even if there is no breach.

FASTCOMCORP™

non-compliance consequences

This is why recent damaging cyberattacks and streams of suspicious digital communications have made data security a top concern due to non-compliance. A recent study by Carbon Black found that 88% of UK businesses were breached last year (2018), It just shows how widespread the threat is.

Based on a recent report by research firm the Ponemon Institute and security company GlobalScape, **the annual cost of non-compliance to businesses now runs an average of $14.8 million**, a 45% increase since 2011. The range can be anywhere from $2.2 million to $39.2 million.

Gramm-Leach-Bliley Act of 1999

There are many business who are not in compliance with GLBA. This law applies to all businesses, regardless of their size, that are "significantly engaged" in providing financial products or services to consumers. GLBA calls for severe civil and criminal penalties for noncompliance, including fines and imprisonment. If a financial institution violates GLBA:

The institution will be subject to a civil penalty of not more than $100,000 for each violation.

The institution and its officers and directors will also be subject to fines in accordance with Title 18 of the United States Code or imprisonment for not more than five years, or both.

Officers and directors of the institution will be subject to, and personally liable for, a civil penalty of not more than $10,000 for each violation.

FASTCOMCORP™

compliance law

DFARS – Defense Federal Acquisition Regulation Supplement

All contractors working for DoD, even subcontractors must comply with DFARS 252.204.7012. This clause is in direct response to data breaches and cybersecurity threats

CMMC – Cybersecurity Maturity Model Certification

In 2020, all contractors working for the DoD, even subcontractors must pass a CMMC Audit to ensure appropriate levels of cybersecurity controls and processes are adequate and in place to protect controlled unclassified information (CUI) on DoD contractor systems.

GDPR – General Data Protection Regulation

For companies collecting data from EU citizens (whether or not they are based in the EU), GDPR means ramping up their company's data collection systems, improving accountability, and in most cases, hiring or promoting a data control officer, whose primary responsibility is ensuring that the company's proper data collection protocols are followed.

FISMA – Federal Information Security Management Act

FISMA was introduced to reduce risks involving federal information and data while also managing federal spending on information security programs and procedures. The importance of FISMA is summarized as a means to protect sensitive information in a timely and costly manner.

SOX – Sarbanes-Oxley Act

The Sarbanes-Oxley Act came into force in July 2002. SOX applies to all publicly traded companies in the United States as well as wholly-owned subsidiaries and foreign companies that are publicly traded and do business in the United States. SOX also regulates accounting firms that audit companies that must comply with SOX.

GLBA – Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.

HIPPA - Health Insurance Portability and Accountability Act

HIPPA established national standards for processing electronic healthcare transactions. It requires healthcare organizations to implement secure electronic access to health data and to remain in compliance with privacy regulations set by HHS. This is also extended to those who handle healthcare data.

PCI – Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes. The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council.

CCPA - California Consumer Privacy Act

CCPA - The law goes into effect on January 1, 2020. All companies that serve California residents and have at least $25 million in annual revenue must comply with the law. Allows any California consumer to demand to see all the information a company has saved on them, as well as a full list of all the third parties that data is shared with.

FASTCOMCORP™

internal threats

A lot of attention is given to external threats that businesses face through identification, authentication, encryption and a variety of software and hardware security systems. Yet, **little attention is directed towards internal threats** that can easily become real threats to an organization.

Internal threats are one of the biggest threats to businesses. Considering that employees have direct access to your business data, systems and hardware, the possibility of dealing with internal theft cases that involve data and even equipment should never be taken lightly. Untrustworthy or disgruntled employees are particularly a great risk. According to claim data released by Willis Towers Watson, a global advisory, broking and solutions company. **Two-thirds of cyber breaches arise from internal threats**,

The data reveals that employee negligence or malicious acts account for two-thirds (66%) of cyber breaches, where only 18% were directly driven by an external threat, and cyber extortion accounted for just 2%.

FASTCOMCORP™

social engineering

"All of the firewalls and encryption in the world can't stop a gifted social engineer from rifling through a corporate database. If an attacker wants to break into a system, the most effective approach is to try to exploit the weakest link—not operating systems, firewalls or encryption algorithms—but people. - Kevin Mitnick

Today, regardless of the maturity and periodicity of a company's security awareness plans, social engineering remains **the number one threat in breaching security defences**. Social Engineering is the act of using various methods of manipulation to gain access to information through human interaction – often by tricking an individual into breaking normal security procedures.

These methods may involve phishing emails, bogus telephone calls, gaining unauthorised access to the premises and obtaining information through accessing the company's network.

Hacking minds

Social Engineers are absolute masters at getting what they want: credit card numbers, social security numbers, bank accounts, health records, secret government documents, critical business data, client lists and your identity. They **target individuals, and often refer to sob stories, such as a divorce or the death of a spouse, to manipulate customer service agents into providing account information**.

FASTCOMCORP™

an integrated cybersecurity vision

At their core, all business and financial services are based on trust. In order to win and maintain the trust of customers, businesses have to demonstrate consistent dedication to preserving confidentiality, confirming the availability of systems and services, and maintaining the integrity of data.

Putting cybersecurity at the heart of business strategy will help the businesses maintain and even enhance the trust of consumers, regulators and the media. For a start, the C-suite can no longer assume that cybersecurity is solely the responsibility of the information security (IS) or information technology (IT) departments. Instead, companies must make cybersecurity a core part of business strategy and culture.

Cyber attacks are inevitable, it is important for organizations to have systems and strategies in place to reinstate business as usual in the fastest possible way, learn from what happened in an incident, and adapt and reshape the organization to improve cyber resilience going forward. Businesses need to adopt a centralized, company-wide cyber breach response program that will bring together the wide variety of stakeholders that must collaborate to resolve a cyber incident. This initiative needs to be led by someone who is experienced with technology, and able to manage the day-to-day operational and tactical response.

FASTCOMCORP™

risk mitigation

At Fastcomcorp, our clients are central to everything we do. We look at cybersecurity from your point of view. Cybersecurity has a lifecycle starting with risk assessment, moving through strategy formulation, designing a solution, everyday control, and on-going management. We have consulting services aligned with every stage in the lifecycle, and you can join at whatever stage is right for you.

Our consulting services help you manage cybersecurity from every angle throughout the lifecycle by:

Consulting	Strategy	Architecture	Controls	Management
• Business requirements • Workshops and interviews • Risk analysis • Gap analysis • Technical analysis • Recommendations	• Business alignment • Vision and strategy • Roadmap	• Evaluation • Optimisation • Design • Deploy	• Platform • Automation • Configuration • Integration • Consumption • Threat intelligence	• Operations • Maintenance • Support

FASTCOMCORP™

This document is produced by consultants at Fastcomcorp as general guidance. It is not intended to provide specific advice on your circumstances. If you require advice or further details on any matters referred to, please contact your Fastcomcorp representative.

FASTCOMCORP™