In times of technologies such as Cloud Computing, Internet of Things (IoT), Social Mobile Analytics and Cloud (SMAC), many marketers are exposed to large amounts of consumer data and hold responsibility to keep this data secure. Cybersecurity has become a priority of marketers across the globe. They need to amalgamate practices and technologies for protecting programs, networks, and customer data including customer names, phone numbers, addresses, and email addresses.

More than ever before, users all over the globe are now aware about the importance of data security. Furthermore, international regulations such as General data Protection Regulation (GDPR) and ISO 27001 have made it mandatory for industries, including B2B marketers, to take cybersecurity measures. Failing to do so can lead to heavy fines imposed as a result of violation.

For B2B marketers, it is important to employ cybersecurity practices for data protection, since it not only retains customer loyalty but also promotes brand equity.

Let’s have a look at 5 things that B2B marketers need to know about cyber security.

1. **Understanding Cybersecurity Elements**

Cybersecurity refers to protecting all computer systems and digital assets from malicious threats or data breaches. This includes keeping software, hardware, and electronic data secure. Essentially, it has five core elements. Let’s briefly have a look at each of them.

1. **Application Security** – It includes the protection of applications from malicious threats by using hardware, software, and procedural methods. Applications face multiple threats such as modification, unauthorized user access, stealing or deleting sensitive customer data. As modern-day applications are available over a wide variety of networks, it is now more important for B2B marketers to deploy cybersecurity, particularly for software applications.
2. **Information Security** – It mainly refers to risk assessment and management. For B2B marketers, it is important to analyze and prepare for risks they might face. For example, understanding risks associated with access control and using digital signatures to allow access to a user.
3. **Network Security** – it includes all activities that protect users on the internet. It protects integrity, safety, and usability of network data. It prevents against online threats such as malware attacks, zero-day attacks, spyware, identity theft, and Denial of Service attacks.
4. **Disaster Recovery** – Just like any other industry, B2B marketers need to have disaster recovery plans in place. No security system is foolproof, and disasters can still happen even with the best of security. They must prepare strategies to restore data and hardware in case of a disaster.
5. **End-user Compliance** – This element is the backbone of cybersecurity. Even with all security measures in place, if your employees are not on the same page, it can lead to security blunders on their part. It is important to focus on developing their skills to deal with potential threats, deliver regular security awareness trainings, and acquaint them with safe online practices.
6. **Understanding Threats**

There is no single B2B enterprise today that does not use automated systems and computers. We are surrounded by wide array of digital devices and gadgets. Moreover, the ecommerce industry has been booming over the past few years with increased [online shopping](http://www.cardzgroup.com/PvcCard.html) trends and more exposure to threats likewise. Hence, data protection now is more difficult than it has ever been. It is important to understand and estimate the diversity of threat landscape from all areas and implement cybersecurity elements to ensure an efficient and effective threat management process.

1. **Developing Threat Intelligence**

According to Gartner, threat intelligence is, “*evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject’s response to that menace or hazard.”*

B2B employees can develop threat intelligence to leverage cybersecurity effectively. It can be either tactical, automated, or contextual. Tactical threat system tends to manage all external threats such as malware protection, firewalls, email security, and web gateways. Automated threat intelligence makes use of APIs that allow communicating from a device. This supports fast collaboration and quick decision making for cybersecurity matters.

1. **Prioritizing Engagement with IT Teams**

IT departments and marketers typically work in separate setups in an organization. However, since every business is now characterized by its online presence, it is important to emphasize on the need of the two departments working together. For instance, a sustainable cybersecurity awareness program can ensure that all the marketing team knows about latest threats. Furthermore, marketing team must keep IT departments informed about any new tools or applications they use, and how they access enterprise data.

1. **Determining External Application Data Privileges**

To evaluate external sources, it is important to understand their access to the enterprise data. In times when data is constantly exposed to threats, it is important to manage access for third-party applications. They should only be allowed to access data that is absolutely necessary for them to operate. For B2B marketers, this means being aware of where the customer data from email marketing plugins or newsletter signups is being stored, who is accessing them, and what restrictions must be implemented.

**Bringing it Together**

B2B marketers have huge amounts of customer data that needs to be kept secured at all costs. Having data backups, installing anti-malware and firewalls, training employees, and monitoring access control are bare essentials to leverage cybersecurity for protecting data. This is a shared responsibility of everyone in an organization, and all employees should make collective efforts towards it.