As a B2B digital marketer, you may consider cybersecurity as something only technical guys in your company’s IT department need to worry about. However, that’s not how it is. In fact, cybersecurity is the responsibility of every department and individual in the organization. A breach of sensitive data can be a result of ignorance from an employee in any department.

So, what should be a B2B marketer’s concern regarding cybersecurity? The good news is, that with basic security practices in place, it’s not that difficult to keep cybercriminals at bay. Let’s look at some common cybersecurity concerns from a B2B marketer’s perspective.

**Securing Network Traffic**

If your network traffic is not secured from hackers, they may redirect users to themselves. In other words, by hijacking your software programs, computer systems, or network communications, an attacker tricks search engines into directing your traffic to their URL.

This can have severe consequences for the victim, such as harming your brand image in particular. Not only does one lose control of the brand messaging sinch the website URL is not under your control, you will also face channel conflict between your Search Engine Marketing team and automated campaign software. Moreover, since search engines only allow one advertiser for a single display URL, you will not be visible in search results. This means losing out on website traffic, clicks and click-through rate. For an [ecommerce](http://www.cardzgroup.com/ContactSmartCard.html%20or%20http:/www.cardzgroup.com/ScratchCard.html) business, it means customers being redirected to a fake website and conducting transactions there.

**Brand Impersonation on Social Media and Peer Review Sites**

B2B marketers are well aware of the importance and effectiveness of social media marketing. However, the same can be used to their disadvantage, since social media accounts are easy target of hackers – where they not only steal personal information but can also damage your brand reputation by posting offensive material – unless they are paid to stop.

This can be a serious threat for marketing teams as most of the times there are multiple members that use a company’s social media account. Even if your official account is not hacked, anyone can still create a page in your company’s name with same logo and setup, making it difficult for visitors to recognize your brand’s original page. For example, on Facebook, a cybercriminal may comment on a brand’s real page and answer customer queries. This may trick the users into believing that it is the actual page that is responding. Similarly, on Twitter, a fake account can tweet while impersonating as the real brand account and also use brand-related hashtags. As feeds move very fast on social media, they might rarely have time to verify the authenticity of the account and believe in the fake tweet itself.

Similarly, on product review websites, a competitor may pose as a customer and post fake negative reviews about your product or service. This may cause you to lose customers and create a negative image of your brand.

**Identifying and looking out for Threats**

It is important that your marketing team is able to recognize and look out for all threats that can harm their brand. Just as employees should be able to identify phishing scam emails that trick users into sharing their sensitive information, they can also use social media such as Instagram, Twitter or Facebook to attack your systems. Your social media team should be active and vigilant to look out for any fake accounts and report them in case they are there. Moreover, your presence is also important in all review websites to be aware of any fake reviews you may be receiving from your competitors.

**Dealing with the Threats**

Once identified, as a marketer you need to ensure that all these threats are dealt with some basic but important security measures.

To deal with web hijacking, there should be an automated monitoring and reporting system. It should be able to crawl through ads to identify affiliate links, landing pages, and redirect links – and compare them to authorized links to isolate hijackers from real advertisers. A request can then be submitted to search engines to take down fake ads and URLs.

For minimizing the risk of your social media accounts getting hacked, always ask all your social media team members to use a password manager to keep their credentials unique and secure. Furthermore, major social media platforms have reporting tools for counterfeit pages. It is important to use them as a tool to get all fake pages removed.

**Data Privacy and Managing Customer Relations**

Apart from your brand image and reputation, you are also liable to keep your customer data secure from cyber criminals. If you don’t take necessary steps to protect your customer’s data, your company will be vulnerable to hacking threats, leading to loss of customers, potential lawsuits, and fines. Then there are also certain regulations, such as California Consumer Privacy Act (CCPA) and General Data Protection Regulations (GDPR), that require you to protect your consumer data.

To keep their customer data secure, B2B marketers need to ensure that they only collect vital data from their clients or customers. This will not only decrease the associated risks; it will also increase your customer’s confidence in you. For a business that only requires collecting email addresses, you don’t need to collect the names, location, household income, or phone numbers of customers. Moreover, not everyone in the marketing team needs to access that data to perform their job duties. Hence, it is important to put access control in place and only allow relevant members to utilize the data. This can help avoid a breach resulting from a disgruntled or negligent employee behavior.

You also need to use marketing tools that follow minimum security standards to the least. Make sure to use tools that comply with ISO27001 or SOC 2, standards that comply companies to monitor their data security protocols regularly.