digital marketing institute

Certified Digital Marketing Associate

Challenges & Risks – Transcript
Version 1.0

CERTIFIED DIGITAL MARKETING ASSOCIATE

Copyright © 2018 digitalmarketinginstiute.com

Copyright © 2018 digitalmarketinginstiute.com

Copyright © 2018 digitalmarketinginstiute.com

Module Overview

Copyright © 2018 digitalmarketinginstiute.com

INTRODUCTION

It’s important for organizations operating across the digital landscape to be aware of the risks and challenges as well as the opportunities presented by embracing a digital approach. This is particularly the case when you consider social media and the damage which can occur when issues sometimes spiral out of control.

Hi, I'm Jeremy Spiller, and I've been helping companies develop digital strategy and online presence for the past 15 years. I'm also an international speaker and adjunct professor at Rutgers University and Hull International Business School.

In this module, we’ll go into detail about the risks that affect organizations, as well as ways to manage and mitigate against them.

We will also explore how, without careful management, risks can easily get out of hand resulting in a range of negative consequences – both to a company’s profit and loss and its long-term reputation. We’ll take a look at the impact of various risks (such as data breach) on the customer and see how planning is the best way to prevent them from happening.

As mentioned, a key consideration is also how, in this social media driven world, small events can sometimes quickly become a global issue for a company. Therefore, they need to be treated with care, using pre-defined guidelines that we’ve created. We will look at some examples where this wasn’t the case and the consequences for all concerned.

Finally, we will look at the evolving regulation in this area and how to make sure your digital approach is aligned with local market requirements.

Copyright © 2018 digitalmarketinginstiute.com

Section 1:

The Risks with Digital

Copyright © 2018 digitalmarketinginstiute.com

INTRODUCTION

Next, we'll look at the different kinds of risks that businesses face as digital becomes more dominant in today's world. The key and most important risk that needs to be managed is the breach of data – not only customer-related data, but also employee data and other stakeholders that the business uses.

We'll also see that risks come from both internal and external environments, and while it may be easier to identify internal risks, you cannot ignore external ones.

We'll also consider where data is stored and a range of ways in which it can be vulnerable. In doing so, it will become clear that companies need to constantly up their game to stay one step ahead.

RISKS EXPOSE BUSINESSES TO DANGER

In any business there are a range of risks that present a challenge or danger to employees, customers and the wider organization. So, at the outset, it's important to recognize what a risk is and how best to go about identifying risks within the company.

DATA MUST BE PROTECTED

One of the biggest risks that digital presents to an organization is how customer and employee data is captured, stored and retained within the business. It must be protected, otherwise your company is vulnerable and exposed to data breaches or cyber-attacks. This will have significant consequences for the business – not just leading to fines from the supervisory authorities, but also negatively impacting your reputation.

DIGITAL GROWTH AND INCREASED RISK

As we know, digital as a channel has had exponential growth over the last number of years. Although, this means greater access and convenience for customers, it has also led to an increase in the number of risks to both the business and its customers.

DATA BREACH

Over the last number of years, there have been a range of well-publicized data breaches that have occurred in Europe and beyond. One notable example is that of Talk Talk in the UK, where 21,000 customers were impacted. This led to a £400,000 fine for the business; however, what perhaps was more damaging was the reputational impact on the brand. This meant that many customers didn't trust them with their data and therefore would have subsequently chosen to get their broadband services elsewhere.

Copyright © 2018 digitalmarketinginstiute.com

INTERNAL RISKS

As the saying goes, “we only know what we know” and therefore determining and understanding internal risks will be an easier task, where you have a greater ability to control and mitigate over external risks. The most common internal risks are:

- **Accidental**: Accidental insider risks are when employees and staff don’t observe cyber security best practices or aren’t aware of these practices. This can be anything from clicking on a link in a phishing email or downloading a program that’s actually malware in disguise.
- **Negligent**: Similar to accidental risks, negligent risks are when employees and staff circumvent your security policies. Again, this is Isn't exactly to be malicious, but in many cases it so they are able to use programs that might be prohibited from your offices. This often includes social networking platforms or unsecured cloud applications, both of which can open your business up to cyber security risks.
- **Malicious**: These attacks we are all familiar with from news coverage. However, they might be happening inside of your organization instead of outside. Attacks like these can include espionage, financial gain and even revenge.

EXTERNAL RISKS

On the flip side, external risks (despite being harder to predict and control) must also be considered. If not, it can lead to greater exposure than necessary on your customers, employees and business, and the impact is far higher than if steps are taken to manage the risk. One useful tool is scenario analysis. This involves considering the external environment for potential risks and determining how best to deal with each if they occur. As Benjamin Franklin said, “By failing to prepare, you are preparing to fail”.

KEY TERMS

Here we take a look at some of the key terms relating to data protection and information security.

- **Cyber-attack**: A general term to describe an attempt to damage or destroy a computer network or system. Cyber-attacks may have many consequences including: identity theft, fraud, extortion, viruses, theft, etc.
- **Malware**: Short for ‘malicious software’, this is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware and other intentionally harmful programs.
- **Data breach**: The intentional or unintentional release of secure or private/confidential information to an untrusted environment.
- **Data privacy**: The right to control (your) personal information.

Copyright © 2018 digitalmarketinginstiute.com

TRUST – AN IMPORTANT COMMODITY IN MODERN BUSINESS

Trust is at the cornerstone of good business. If you lose a customer's trust, it's unlikely they'll do business with you again. Therefore, it's important that you do all you can to maintain and build trust. In a digital context, this means protecting your customer's data, as well as finding new and engaging ways to nurture the relationship.

INCREASE IN DATA USE

As data use increases, more businesses and consumers are interacting online, meaning cyber-attacks are a growing threat.

- **2013**: 90% of the world's data had been created between 2011 and 2013.
- **2016**: More data had been created between 2014 and 2016 than in the past 5,000 years of human history.
- **2017**: 2017 alone was on track to create even more data than the three previous years.
- **2020**: By 2020, it's expected that for each member of the world's some 7.8 billion people, 1.7 megabytes of data will be created every second.

ACCESSIBILITY HAS BROUGHT INCREASED DATA SECURITY CHALLENGES

Much of the data used by mobile devices comes from information servers in the cloud. Services such as Facebook, LinkedIn and even Google Mail store your information in secure locations around the world, with stringent privacy policies and safeguards to make sure they are protected. However, there have been a number of well documented attack, even to the most secure of organizations.

For example, Yahoo had 3 billion accounts hacked in the recent past in one of the largest data breaches of all time. Besides names, dates of birth, email addresses and passwords, security questions and answers were also compromised. This shows that no organization is immune, and companies are having to continually up-skill their own security to remain one step ahead.

THREATS PRESENTED BY DATA

When you think about it, there are many different kinds of threats that are presented – your businesses' data can be hacked…Customer data could also be leaked through error…. the data you maintain can quickly become outdated (for example contact data or payment details for customers) …and finally, the data itself can become unmanageable, as it changes and grows.

SIDE EFFECTS OF A DATA BREACH

Of course there can be a lot of damage to a business when there is a data breach – the costs can be both direct and indirect.

There is **diminished reputation** – when the breach is communicated to whoever is affected.

Copyright © 2018 digitalmarketinginstiute.com

It can result in **operational shutdown** or delays until resolved.

There is the danger of **increased competition** when your data falls into others' hands.

There can be **legal costs** to pay.

And finally, the direct **financial costs** of fixing the problem and potential increased **insurance costs**.

SUMMARY

In this section, we've seen that there are many different types of risks associated with digital and that the risks have grown as the use of data has increased.

We've also seen that there are both external and internal risks – that internal risks are within your business and therefore easier to control, whereas external risks are often outside of your control and require more work to protect your business.

We've also covered some of the key terms associated with data protection and learned that the risks are increasing because of increased accessibility, with mobile and data in the cloud.

Finally, it's important to be aware of the kinds of damage that can occur to an organization as a result of a data breach – including to your reputation, your operations and your ability to compete; there are also both direct and indirect costs to consider.

Copyright © 2018 digitalmarketinginstiute.com

Section 2: Managing the Risks with Digital

Copyright © 2018 digitalmarketinginstiute.com

INTRODUCTION

In this section, we'll take a look at how businesses can manage the risks associated with digital using a range of tools and techniques. We'll consider the importance of planning for issues that may arise within both internally and externally, as well as the importance of being proactive to deal with issues before they arise. After all, prevention is better than a cure.

We'll explore a number of ways we can mitigate against risks within the digital environment. We'll start by looking at internal risks and the importance of doing a risk assessment on how data is collected and stored; before moving onto looking at the online conversation. How we adopt a proactive approach and look at social media policy guidelines as a key tool to provide your company with a robust framework.

Then we'll consider the role of social listening and what we need to do to avoid a local, isolated event from going viral. And finally, we will look at the importance of scenario planning and how each department has a role to play in mitigating against reputational risks.

RISK MITIGATION STARTS INSIDE THE ORGANIZATION

Risk prevention starts internally within the company. This involves looking at how data is collected and managed within the organization. However, it also involves considering how the online conversation with customers is managed.

RISK MITIGATION AND RISK MANAGEMENT

Coming up with a risk prevention strategy needs to start as a planning activity, before issues occur. When dealing with issues in real-time it becomes risk management.

DATA PROTECTION AND PRIVACY

One of the biggest risks that digital presents to an organization is how customer and employee data is captured, stored and retained within the business. It must be protected, otherwise your company is vulnerable and exposed to data breaches or cyber-attacks. This will have significant consequences for the business – not just leading to fines from the supervisory authorities, but also negatively impacting your reputation.

- **Data Protection**: The process of safeguarding important information from corruption, compromise or loss. Data protection is more than just protecting data from the unauthorized; it's about ensuring that it's used for the sole purpose it was collected, and respecting the privacy of those whose data it belongs to.
- **Data Privacy**: The right to control (your) personal information.

DATA PROTECTION IS ONE OF THE GREATEST CHALLENGES IN A MODERN BUSINESS ENVIRONMENT

There is no doubt the protecting data is one of the greatest risks and challenges in the modern business environment. And with the role of digital ever-increasing, this risk will grow if not managed carefully. According to a recent survey:

Copyright © 2018 digitalmarketinginstiute.com

- 74% of respondents cite an increase in cyber threats.
- 91% say critical infrastructure is a key priority for protection against cyber threat.
- 67% say it in unlikely that they would be able to detect a sophisticated cyber-attack.

REPUTATION MANAGEMENT

Consider some of the recent high profile negative publicity that organizations have recently been involved in. In many cases, the issues either started or went viral on social media. Companies need to be conscious that the smallest of isolated incidents in one part of the world can spread quickly, becoming a major issue with global reach.

A good example of this is the recent event with United Airlines when a passenger was abruptly removed from a plane. A global response and discussion erupted with significant reputational consequences for the airline.

CONTINGENCY PLANNING

It's also important to consider contingencies as part of planning to deal with risks. For example, how will you continue to do business if your payment system or website are compromised? It involves deciding on the specific actions that need to be taken and by whom in a situation so that you can keep your business up and running.

DATA PROTECTION

It is important to have the right data protection processes, policies and technology (including information security) in place to protect your data – to mitigate risks both externally and internally.

Equifax, one of the largest credit bureaus in the U.S., said on Sept. 7, 2017 that an application vulnerability on one of their websites led to a data breach that exposed about 147.9 million consumers. The breach was discovered on July 29, but the company says that it likely started in mid-May.

Personal information (including Social Security Numbers, birth dates, addresses, and in some cases drivers' license numbers) of 143 million consumers were exposed. A further 209,000 consumers also had their credit card data exposed.

PRACTICAL IMPLEMENTATION OF POLICIES

Once the guidelines and policies are in place however, they need to be implemented in a practical way within an organization. For example, social media guidelines which are reviewed by Legal, may need to be implemented (and signed off) by HR within employment contracts. Policies which affect the website, such as your blog or other content guidelines, need to be easy to implement so that they do not affect the efficiency of your website (and processes). All affected employees need to be aware of these as well.

Copyright © 2018 digitalmarketinginstiute.com

SOCIAL MEDIA POLICY

As many organizations are turning to social media, not only as a marketing tool, but increasingly for customer service, it's important to have easy-to-understand guidelines. This comes in the form of a 'social media policy guide' and presents a clear path on what individuals are allowed to say and how they should represent the brand.

GAP recognizes the need to moderate the use of social media amongst their employees within the work place. At a company conference last year, GAP handed out brochures to its employees depicting proper guidelines and decorum that had to be satisfied when partaking in social media. It was an interesting approach, as the brochure's content was very conversational, but very straight-forward as well.

IT PROCESSES

A key element of risk mitigation for data in any business is also your IT process. The human element is often the weakest link when it comes to protecting your data, so training on password policy, security of portable devices like laptops or USBs, and not opening unknown email attachments is paramount. Similarly, making sure the right employees have the right access to data and keeping your security software up to date is important.

SOCIAL LISTENING

So, what else can organizations practically do to mitigate against some of the external issues that can arise?

One good practice is social listening, which involves listening out for keywords, such as the organizations name on social media. Organizations can immediately become aware of what their customers and the wider community are saying about them. This can help to mitigate against any issues that arise before they get blown out of proportion.

QUICK RESPONSE

Because social listening provides real-time information on conversations relevant to your organization, companies have the opportunity to respond promptly. One of the key things that social media has enabled is that customers expect to have an open dialog with companies 24/7. That means that some companies will respond to serious issues (which can affect reputation) within minutes; for example, a negative Tweet being posted by one of their customers. However, this also places a burden on companies to provide cover on their social media customer service desk, ensuring that there is always a response capability for serious issues.

PR STRATEGY

It's important to have a crisis PR strategy for risks. Buffer, an online social media scheduling site, was recently hacked. Buffer became aware of the problem very rapidly and took immediate action to handle it. They informed their customers of the problem and explained what they were doing to fix it before most of their customers were even aware there had been an attack.

Copyright © 2018 digitalmarketinginstiute.com

CRISIS MANAGEMENT

Generally speaking, the response to any crisis depends on the seriousness – in terms of how quickly you respond and the resources involved. For example, a serious issue for a financial institution might involve customers' details being hacked. But the key thing is that your organization must decide in advance during planning what level each potential issue is.

MATCH THE DEPARTMENT RESPONSIBLE FOR HANDLING RESPECTIVE CRISIS

Scenario planning is an important technique for preparing for crises. Each part of the business affected needs to play a role. Here is an example of the responsibilities each department might have within an organization in handling a serious issue that may arise.

- **Legal**: Address the issue.
- **PR**: Mitigate the risk in the media.
- **Customer service**: How to react/respond on social media.
- **Marketing**: Control what activity is run or not during a crisis.
- **IT**: Recovering/securing data.

SUMMARY

In this section, we learned that risk mitigation should take place as a planning activity before issues occur, while Risk Management is dealing with the issues in real-time when they occur.

We've also seen that data protection is a key element of risk mitigation and also one of the biggest challenges for modern businesses. Businesses need to also consider contingencies before issues occur – what is the contingency plan if there is a problem with one part of our infrastructure. Putting in place the right processes and technology to protect your data needs to be resourced, and of course it also needs to be done in a practical way. Key elements in this include both strong IT processes and policies covering social media.

We also looked at how businesses manage issues by developing processes to deal with them when they occur. We've seen that it's important to respond quickly to issues to prevent escalation and that tools like social listening are very useful.

When a crisis does occur, the response depends on the level of crisis – the particular response will also of course depend on the industry involved.

And finally, it's also important that it's clear who is responsible for handling each part of the response – and that may include your company's PR strategy, IT, Marketing, Customer Service, Legal and more.

Copyright © 2018 digitalmarketinginstiute.com

Section 3:

The Challenges with Digital

Copyright © 2018 digitalmarketinginstiute.com

INTRODUCTION

Next, we're going to look at the challenges organizations face when implementing a digital strategy. As we'll see, there are a number of areas that might not be obvious to think about. These may include your organizational structure or whether you have the digital skills within your business to be successful.

We'll think about what those specific skills are, and how they impact the business.

As we'll see also, this presents a good opportunity for the companies that get it right, not only in being able to delight customers, but also in generating increased profitability.

Finally, we'll also explore the ways that technology is playing a significant role in up-lifting the expectations of customers, and that it's imperative for organizations to keep up.

CHALLENGES

Every challenge is an opportunity viewed in a different way.

For example, most businesses experience a lack of resources – whether its internal staff, external or budget. In the case of digital content (for a website or other campaign) you can often repurpose content to get more bang for your buck or use external resources to help.

TECHNOLOGY

Technology has completely changed the way consumers want to interact with organizations. They want convenient access to a company, 24/7, and want to be able to do so on the move. This poses a threat to companies that do not keep up with these trends (they will lose business). However, this presents a significant opportunity for the companies that embrace this shift and deliver their customers' digital needs.

CHALLENGES FOR BUSINESSES WHEN ADOPTING DIGITAL

Let's look at some of the challenges a business can face using digital.

- **Lack of Digital Skills**: The digital skills gap has been widely publicized. While 59% of marketers in the USA, 47% in the UK, and 51% Ireland perceived themselves as very or fairly competent in digital marketing, the actual level of their skills is equally low across all three countries (38% on average).[1]
- **Innovation**: Innovation is key to growth within a business. Being able to come up with new and innovative ways for your business to move forward through digital is a skill that is often in short supply in an organization.

[1] https://digitalmarketinginstitute.com/business/digital-skills-report

Copyright © 2018 digitalmarketinginstiute.com

- **Organizational structure issues**: Having a structure that's very hierarchical or creates silos is a sure way to prevent digital creativity. Collaboration is key, and a structure must enable (not detract) from this.
- **Lack of knowledge of relevant guidelines**: Not understanding the relevant guidelines is a challenge for businesses as it can cause individuals to go against company policy.

UNDERINVESTMENT IN DIGITAL

Research shows that organizations with a high digital intensity over a sustained period of time outperform their peers in profitability by up to 26%[2].

The flip side of this is that underinvestment in digital negatively affects the commercial performance of a business. Therefore it's important to demonstrate the return on investment from digital to support continued investment.

DIGITAL SKILLS REQUIRED

There are a range of digital skills required within a business.

- **Search**: SEO increases the visibility of your website in search engine results.
- **Social**: Social channels used to promote a product or service and interact with customers**.**
- **Content**: Creating and sharing online material to generate interest in your brands products/services**.**
- **UX/UI/Development**: The creation of engaging, intuitive and brand consistent designs through digital assets.
- **Digital Media**: Digitized content for distribution online (including text, audio, video and graphics).

PAID SOCIAL CAMPAIGN BENEFITS

- Website development
- Mobile
- Social media
- Media

[2] https://www.capgemini.com/wp-content/uploads/2017/07/The_Digital_Advantage__How_Digital_Leaders_Outperform_their_Peers_in_Every_Industry.pdf

Copyright © 2018 digitalmarketinginstiute.com

SUMMARY

So hopefully you now have an insight into the challenges associated with digital for businesses – because of advances in technology, the lack of digital skills is a challenge affecting many organizations.

Digital skills are required across areas including search, social, content, UX and digital media.

In addition, companies need to make sure they are structurally set up to take advantage – and that includes being aware of relevant data guidelines affecting digital.

And finally, as we've seen, specific areas where technology change has impacted and present challenges to businesses include website development, mobile, social media and digital media. The reality is that underinvestment in these areas can impact your commercial performance.

Copyright © 2018 digitalmarketinginstiute.com

Section 4:

Laws and Guidelines

Copyright © 2018 digitalmarketinginstiute.com

INTRODUCTION

Within this last section, we will take a close look at the laws and guidelines associated with digital for a business. First, we'll look at how legislation impacts the use of digital and its consequences. Thereafter, we'll look at the changes that have taken place over time which add additional layers of protection for the consumer *and* organizations.

In particular we will discuss an important new regulation called the General Data Protection Regulation (GDPR) that came into effect across the European Union and also some of the regulations in place in the US.

KEY TERMS

- **Password Attack**: When someone tries to steal your password through hacking or manipulation.
- **Hacking**: When someone gains unauthorized access to data in a system or computer.
- **Denial of Service**: An interruption in an authorized user's access to a computer network, typically one caused with malicious intent.
- **Identity Theft**: The deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name.
- **Data Retention**: Also called records retention, it is the continued storage of an organization's data for compliance or business reasons.
- **Cookie**: A small piece of data which is stored on a user's computer. Often used to track the websites users visit.

LEGISLATION DEPENDS ON YOUR MARKET

It's important to note that there is a wide variety of legislation that is largely dependent on the market and geographic location. It's important therefore to be aware of the legislation in both your home market, as well as other markets that you operate within.

THE EU COOKIE DIRECTIVE

All businesses in the EU need to comply with the Cookie Directive, which is designed to protect consumers online privacy. This requires websites to get consent from visitors to store or retrieve information on a computer, smartphone or tablet. Non-compliant websites are open to enforcement action. In the UK, for example, the ICO has powers to force websites to change or it can impose a fine of up to £500,000 in the most serious cases.

IMPLICATIONS OF THE EU COOKIE DIRECTIVE

The Cookie Law is a piece of privacy legislation that requires websites to get consent from visitors to store or retrieve information on a computer, smartphone or tablet. It was designed to protect online privacy by making consumers aware of how information about them is collected and used online, and give them a choice to allow it or not. It is practically implemented by asking users and providing a link to the cookie policy that details which information is stored.

Copyright © 2018 digitalmarketinginstiute.com

- **Consent**: Websites must first ask users if they agree to allow the site to store/access cookies.
- **Cookie Policies**: Websites have a cookie policy explaining what information is stored in cookies and why.

DATA GUIDELINES

In most regions globally there are specific guidelines covering the collection of data (permissions, privacy, etc.) and how long data should be kept for (data retention).

GENERAL DATA PROTECTION REGULATION

On the 25th May 2018, the General Data Protection Regulation (GDPR) came into effect across the European Union. It harmonizes a range of the data protection laws from across the EU member states and poses significant fines on organizations that fail to meet its new high standards.

There is strict compliance for companies with penalties up to 20 million Euros, or 4% of global annual turnover, whichever is greater.

Although it is an EU regulation, it has wide reaching effects for organizations with global operations.

GDPR has specific guidelines covering the collection (including consent), processing, retention, transfer and deletion of data that companies need to be aware of.

GDPR AND OTHER DATA PRIVACY STANDARDS IN THE EU

GDPR is a regulation which will be enforced, whereas the existing Data Protection Directive served more as a guideline for best practices; GDPR supersedes DPD.

INTERNATIONAL REGULATIONS

There are a range of international regulations that govern data protection and privacy in this area. We have detailed some of the main regulations here.

Privacy Act

The Electronic Communications Privacy Act and the Computer Fraud and Abuse Act regulate the interception of electronic communications and computer tampering, respectively. The Electronic Communications Privacy Act of 1986 protects the privacy and security of the content of certain electronic communications and related records. The Computer Fraud and Abuse Act prohibits hacking and other forms of harmful and unauthorized access or trespass to computer systems, and can often be invoked against disloyal insiders or cybercriminals who attempt to steal trade secrets or otherwise misappropriate valuable corporate information contained on corporate computer networks.

Copyright © 2018 digitalmarketinginstiute.com

International Data Transfer

For years, many US companies engaging in cross-border transfers of personal data between Europe and the US had relied on the EU-US Safe Harbor program, using European Commission-approved model contracts. In October 2015, Europe's highest court struck down the established Safe Harbor framework in its Schrems v. Facebook ruling. In light of the ruling, companies could no longer rely on self-certification to establish compliance with EU privacy laws. European and American regulators scrambled to find an alternative framework for trans-Atlantic data transfers and in February 2016, the US Department of Commerce and the European Commission released a new 'Privacy Shield' framework, for more robust, enforceable rights protecting data transfers. Although the EU expressed concerns, the European Commission adopted the EU-US Privacy Shield on 12 July 2016. The Privacy Shield imposes strong obligations on companies handling data; clear safeguards and transparency obligations on US government access; effective protection of individual rights; and an annual joint review mechanism.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) regulates medical information. It can apply broadly to health care providers, data processors, pharmacies and other entities that come into contact with medical information. The Standards for Privacy of Individually Identifiable Health Information (HIPAA Privacy Rule) (45 C.F.R. Parts 160 and 164) apply to the collection and use of protected health information (PHI). The Security Standards for the Protection of Electronic Protected Health Information (HIPAA Security Rule) (45 C.F.R. 160 and 164) provides standards for protecting medical data. The Standards for Electronic Transactions (HIPAA Transactions Rule) (45 C.F.R. 160 and 162) applies to the electronic transmission of medical data. These HIPAA rules were revised in early 2013 under the HIPAA 'Omnibus Rule'.

ADVERTISING STANDARDS AUTHORITY

In most regions there is an Advertising Standards Authority (for example, UK, Ireland) which is an independent body that provides guidelines and rules for brands to follow in a number of areas:

- Alcohol and cigarettes messaging
- Social media policies
- Advertising to minors
- Data protection
- Data usage policy

SUMMARY

In this section, we looked at the legislation which impacts digital and saw that it depends on the market in which your business is operating. In most regions globally, there are specific guidelines covering the collection of data and how long it should be kept for.

Copyright © 2018 digitalmarketinginstiute.com

Within the EU, the most important regulation is the General Data Protection Regulation, or GDPR, which strengthens data protection for everyone in the EU. It also covers the export of personal data outside the EU. For businesses, what's important is the guidelines covering collection, processing, retention, transfer and deletion of personal data. And remember that there are strict penalties for non-compliance – which can be up to 4% of global revenue.

And there are other important international regulations to be aware of including in the United States the Privacy Act, the Safe Harbor Act and the Health Insurance Portability and Accountability Act.

Finally, in many regions, for example the UK and Ireland, there are Advertising Standards Authorities which provide useful guidelines and rules for brands to follow on social media, advertising to minors and data protection.

.

Copyright © 2018 digitalmarketinginstiute.com

Copyright © 2018 digitalmarketinginstiute.com