Certified Digital Marketing Associate

Challenges and Risks

PRESENTED BY

INSERT NAME

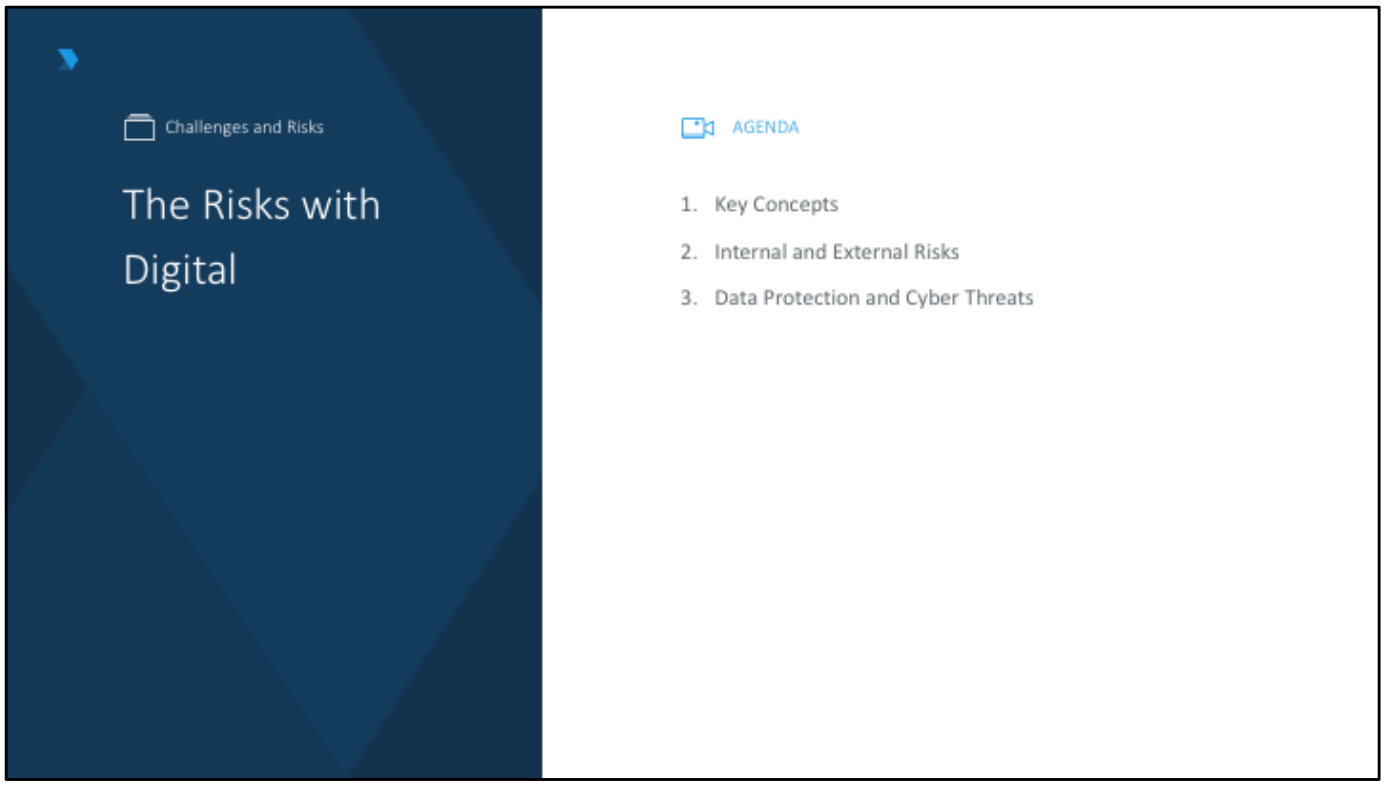
Margaux Denneulin

Customer Support Specialist @ HubSpot

- One year working at Twitter as a Product Marketing Coordinator
- Expertise in Twitter Ads products, content, talking points, and best practices
- Two years' agency experience in creative teams
- Master's Degree in Media Studies, and Bachelor's Degree in Integrated Marketing & Communications

Challenges and Risks

Challenges and Risks



[LECTURER NOTES]
It's important for organizations operating across the digital landscape to be aware of the 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 that can occur when issues sometimes spiral out of control.

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 P&L 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. 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.

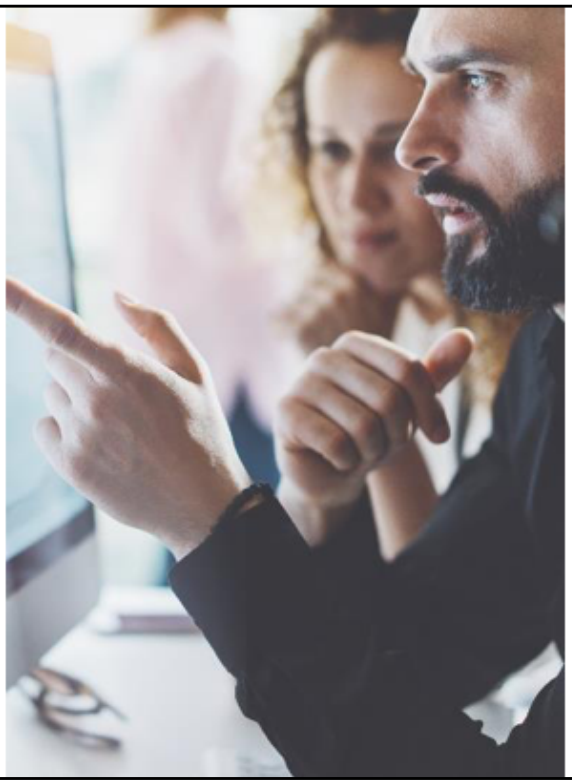
Key Concepts

Risks Expose Businesses to Danger

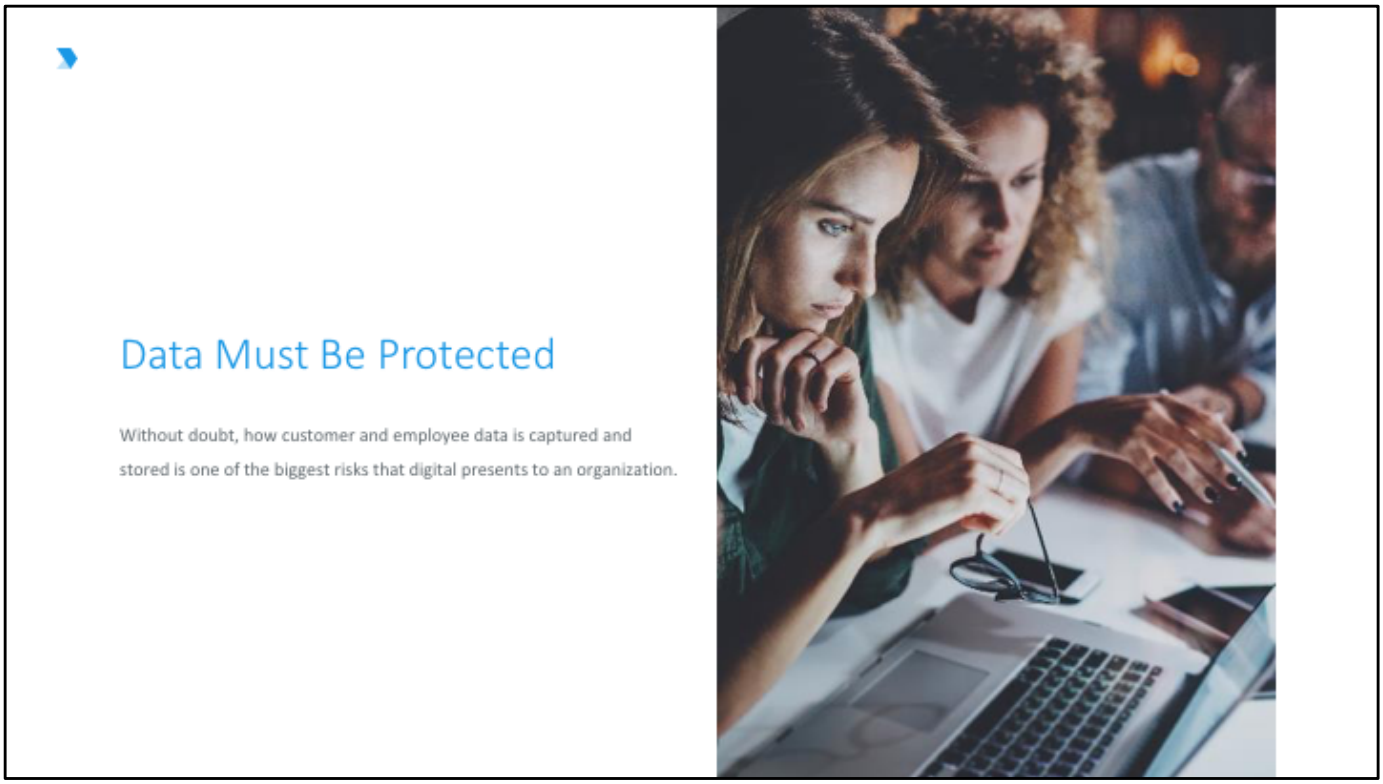
In businesses, risks present both a challenge and a danger to employees, customers, and the wider organization.

Therefore, it's important to recognize:

- What a risk is
- How best to identify risks within the company

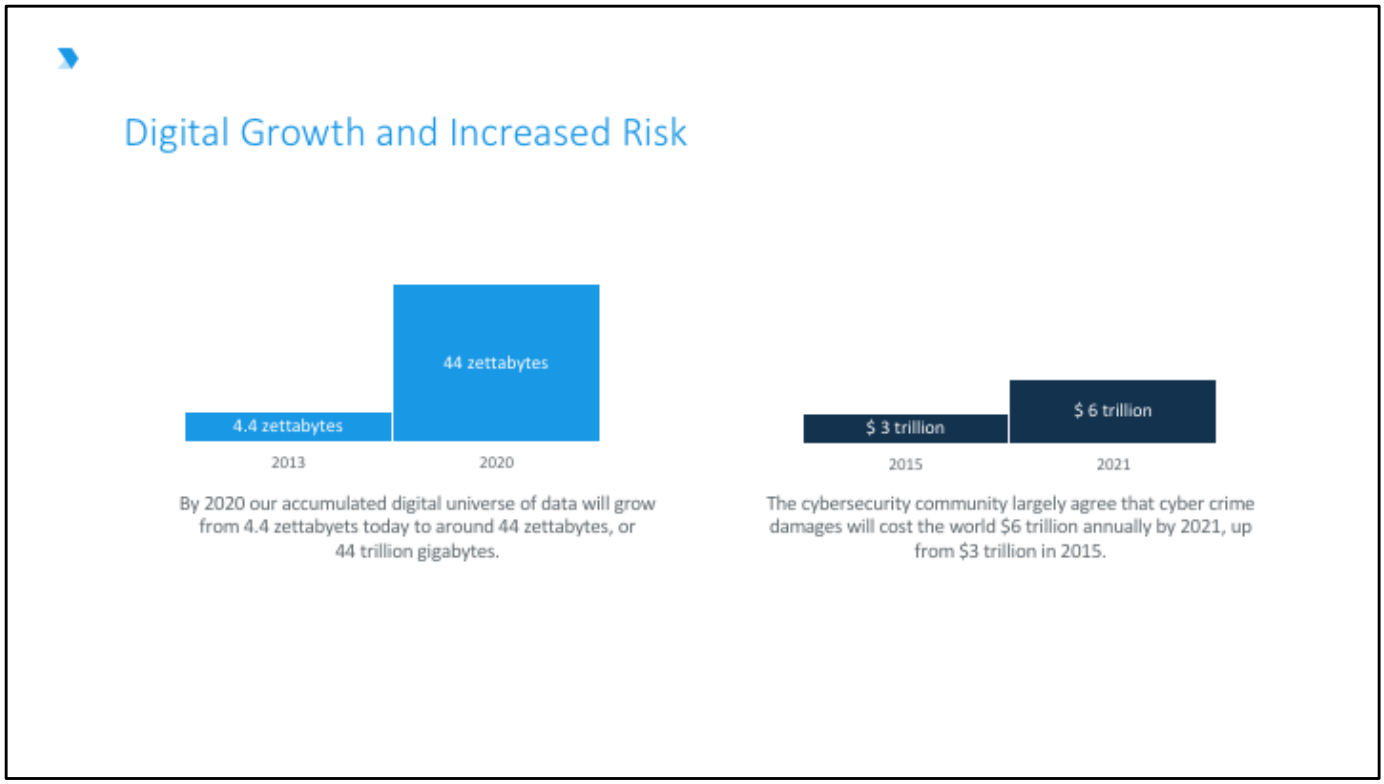


[REF.] 5.1.1.1



[REF.] 5.1.1.2

[LECTURER NOTES]
Without doubt, how customer and employee data is captured and stored is one of the biggest risks that digital presents to an organization. Without protection, your company is vulnerable to data breach. This has significant consequences for the business - not just fines from the supervisory authorities, but also negative impacts on your reputation.



[REF.] 5.1.1.3

[LECTURER NOTES]
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.

[REFERENCES]
https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm

https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Internal and External Risks


Not Every Risk Is an Opportunity!
Some Risks Just Need to Be Protected Against.

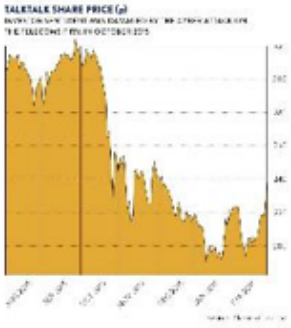
[REF.] 5.1.1.4

Data Breach

TalkTalk

21,000 customers were impacted

€ £400,000 fine for the business

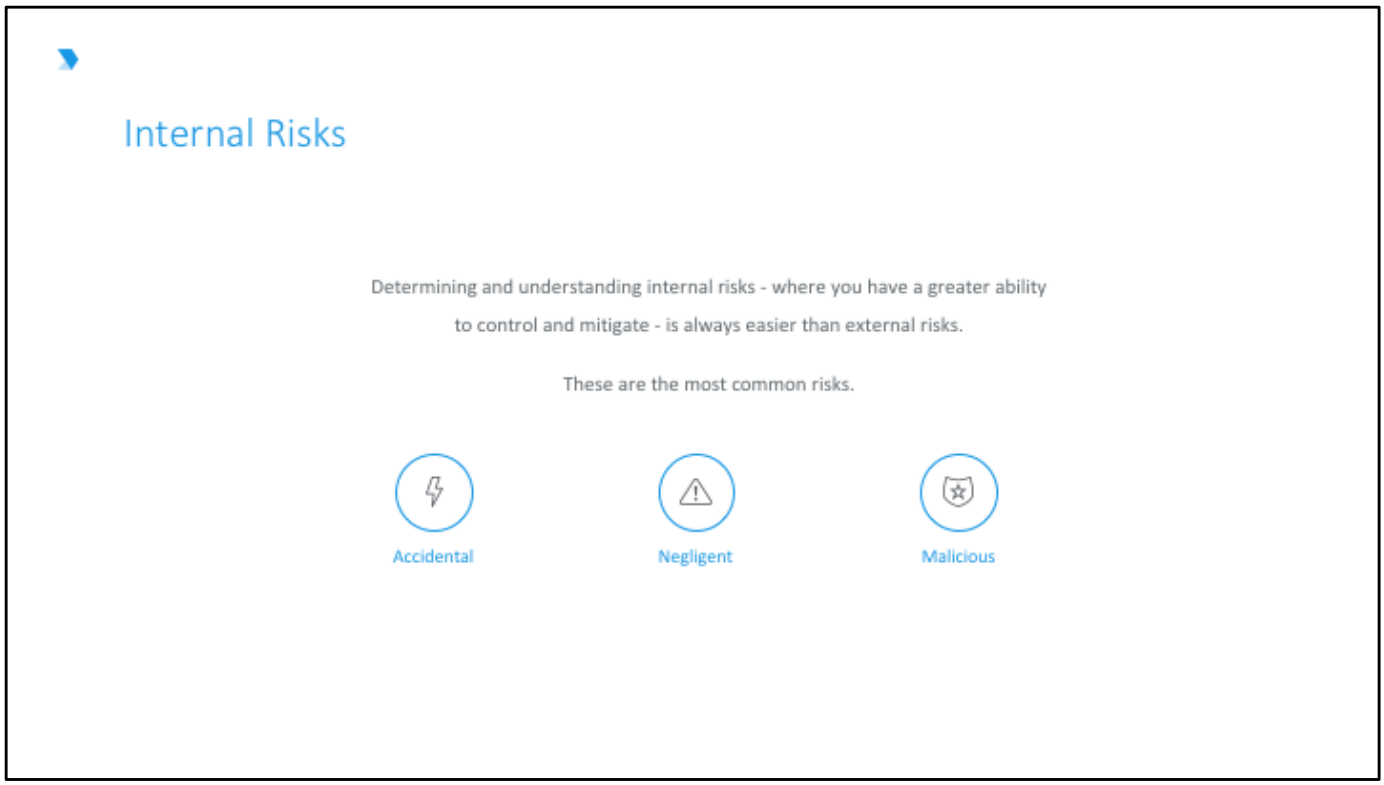


[REF.] 5.1.1.5

[LECTURER NOTES]
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 TalkTalk 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 TalkTalk with their data and therefore would have subsequently chosen to get their broadband services elsewhere.

[REFERENCES]
https://www.raconteur.net/technology/protecting-brand-reputation-in-the-wake-of-a-cyber-attack



[REF.] 5.1.1.6

[LECTURER NOTES]
Determining and understanding internal risks - where you have a greater ability to control and mitigate - is always easier than external risks. Internal risks are those within your own business.

These are the most common internal risks:

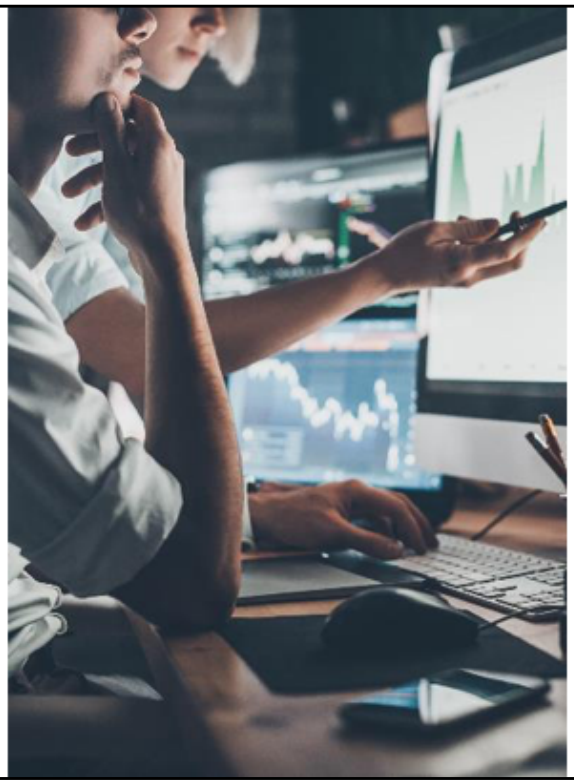
Accidental: Accidental insider risks are when employees and staff don't observe cyber security best practices or aren't aware of these practices. This can be anything from clicking on a link in a phishing email or downloading a program that's actually malware in disguise.

Negligent: Similar to the above, negligent risks are when employees and staff circumvent your security policies. Again, this isn't exactly to be malicious, but in many cases, they are doing it so they can 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 your organization instead of outside. Attacks like these include espionage, financial gain, and even revenge.

External Risks

External risks, while harder to predict and control, are critical to consider. They can lead to greater exposure to customers and employees, and the impact is far higher than if steps are taken to manage the risk.



[REF.] 5.1.1.7

[LECTURER NOTES]
External risks, while harder to predict and control, are critical to consider. They can lead to greater exposure to customers and employees, and the impact is far higher than if steps are taken to manage the risk.

Scenario analysis is a useful tool. It involves considering the external environment for potential risks and determining how best to deal with them if they occur.

Data Protection and Cyber Threats

Key Terms

Cyber Attack

A general term to describe an attempt to damage or destroy a computer network or system. Cyberattacks may have many consequences including: identity theft, fraud, extortion, viruses, theft etc.

Malware

Short for 'malicious software', 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 Privacy

Data privacy is the right to control (your) personal information.

Data Breach

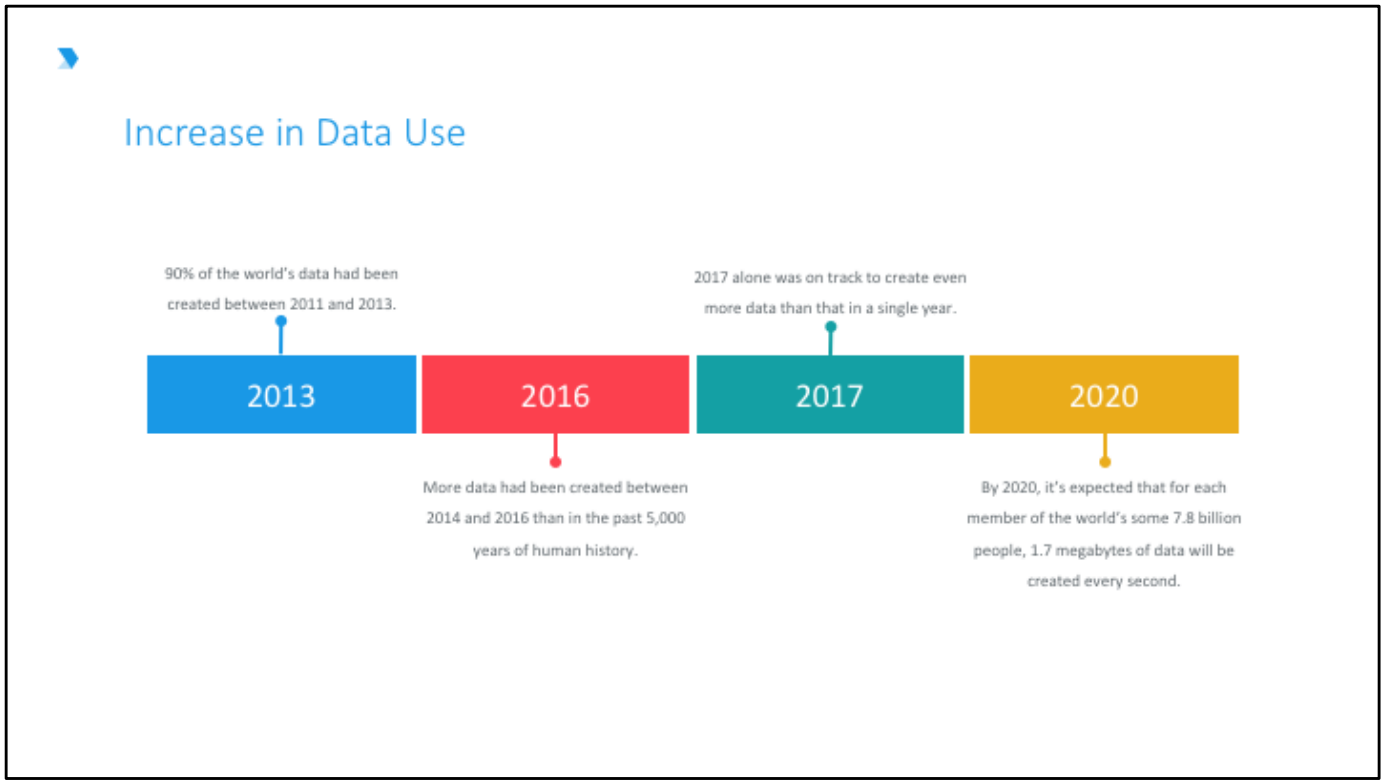
Data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted environment.

[REF.] 5.1.2.1

Trust - An Important Commodity in Modern Business

Trust is the cornerstone of good business. It's important to do all you can to maintain and build your customers' trust. This means protecting your customers' privacy and data, as well as finding new and engaging ways to nurture the relationship.

[REF.] 5.1.2.2

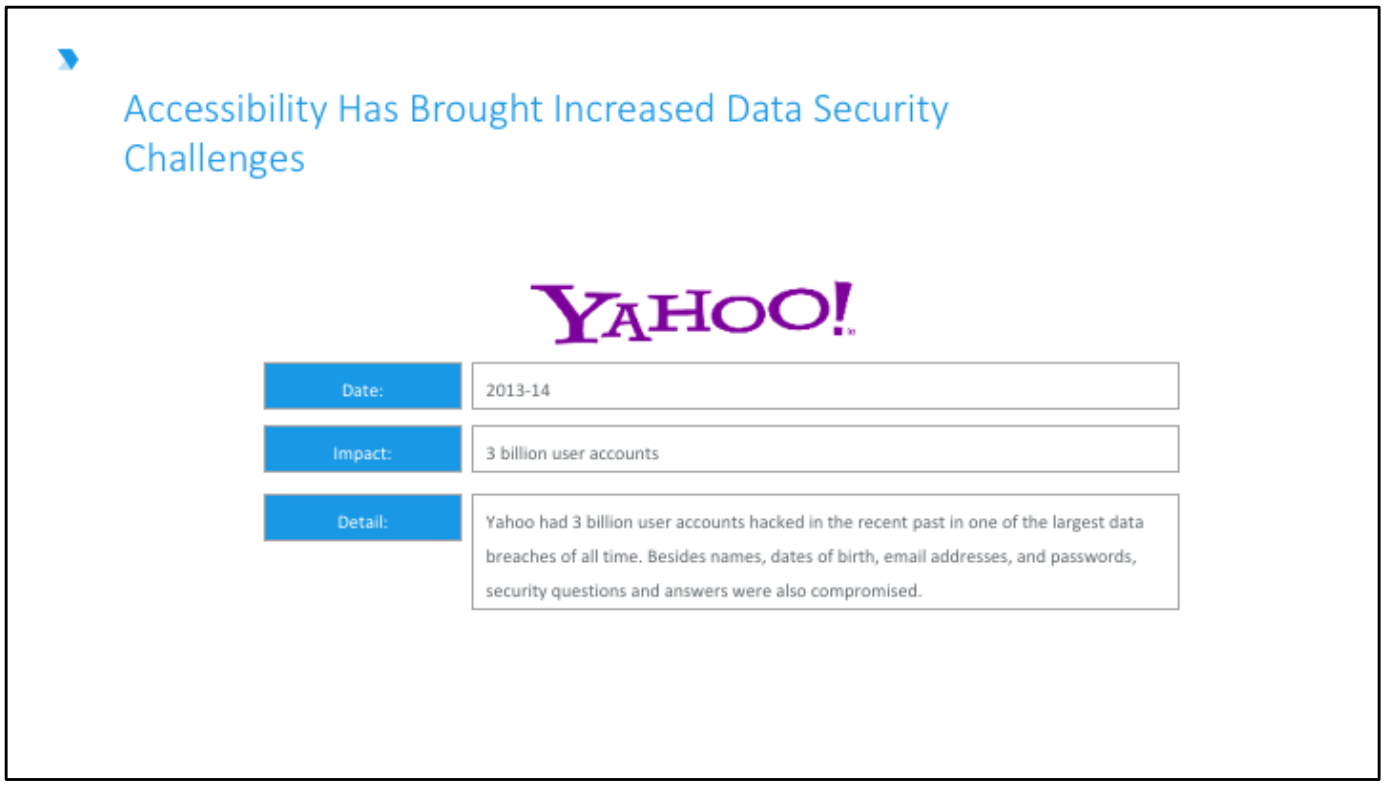


[REF.] 5.1.2.3

[LECTURER NOTES]
As data use increases, more businesses and consumers are interacting online, meaning cyber attacks are a growing threat.

[REFERENCES]

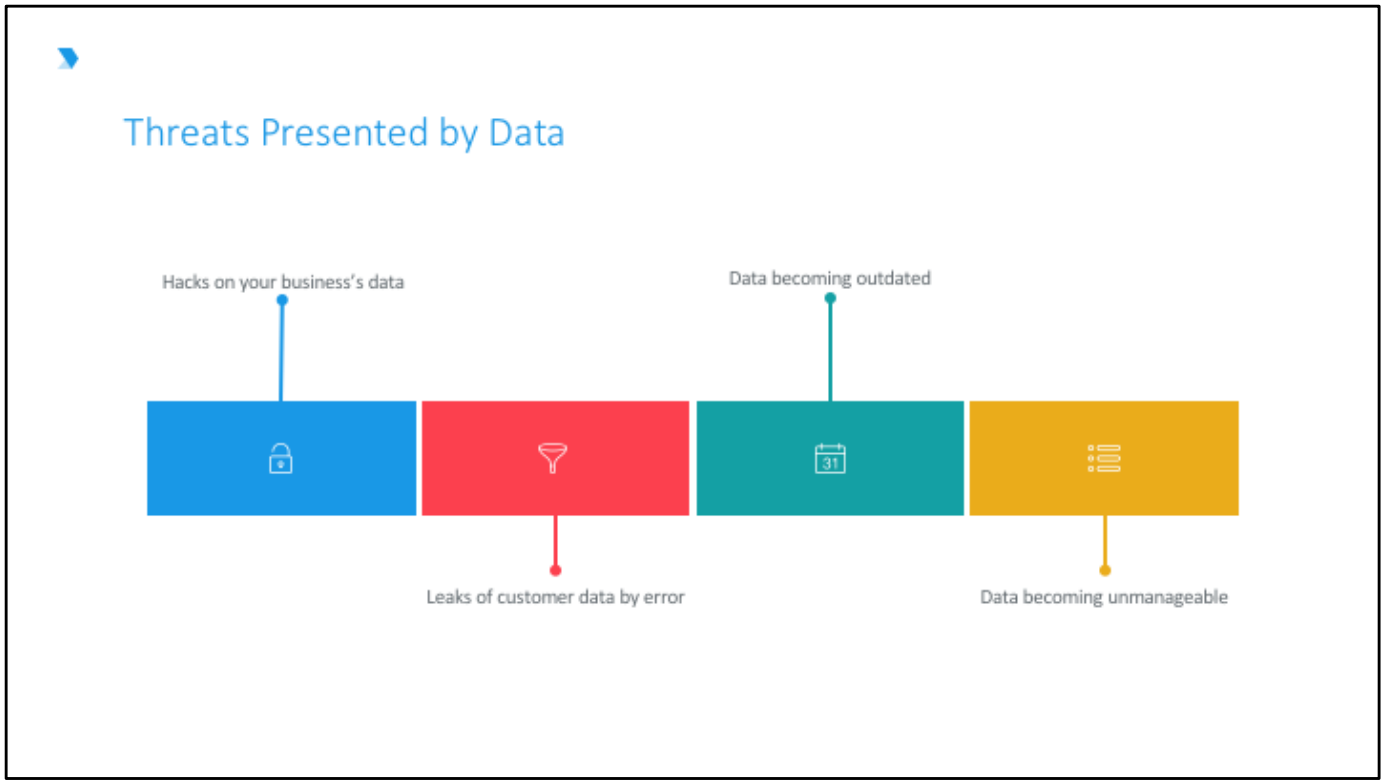
https://digitalmarketinginstitute.com/the-insider/20-02-18-is-the-future-of-digital-transformation-cognitive



[REF.] 5.1.2.4

[LECTURER NOTES]
Mobile devices, outsourcing, and cloud computing have increased accessibility. However, they have also brought increased security challenges. Much of the data used by mobile devices is stored in information servers in the cloud. Services such as Facebook, LinkedIn, and even Google Mail store your information in secure locations around the world.

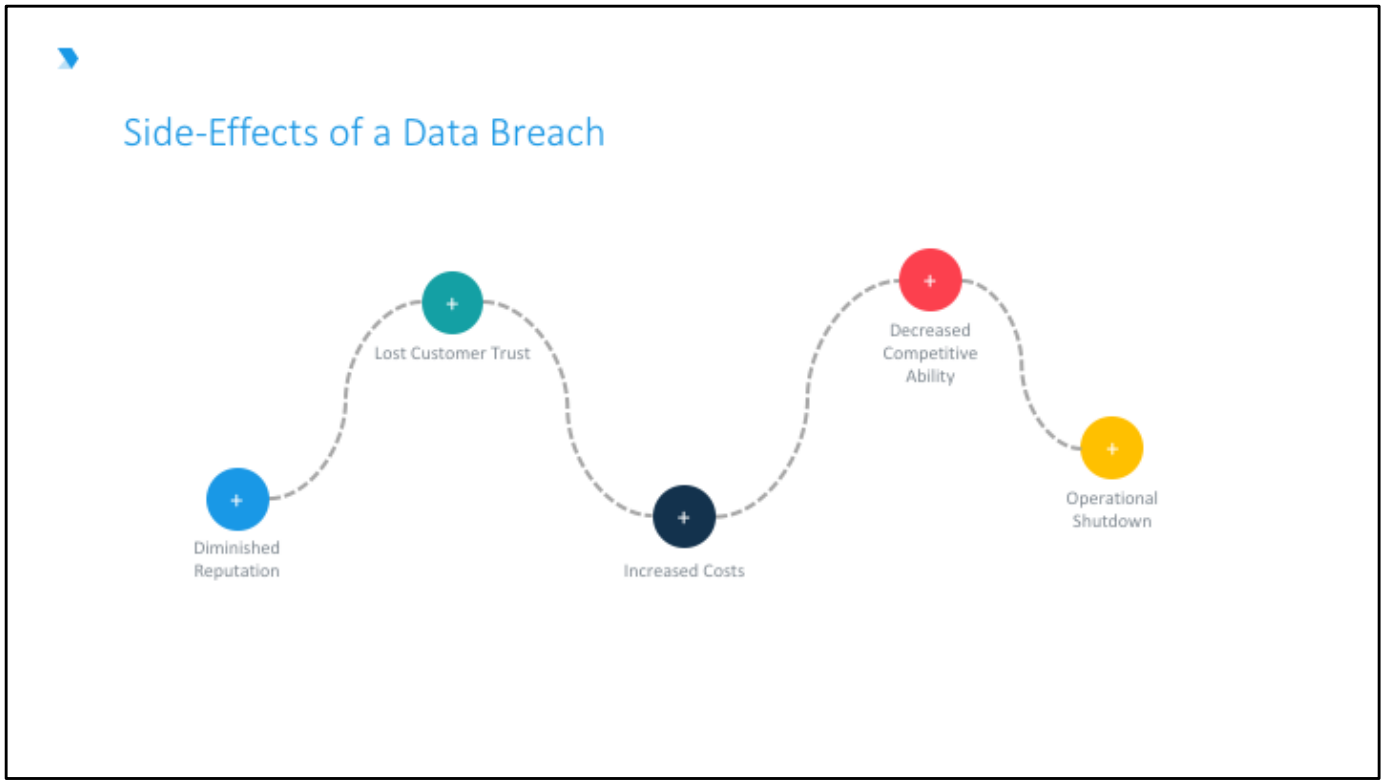
[REFERENCES]
https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html



[REF.] 5.1.2.5

[LECTURER NOTES]
When you think about it, there are many different kinds of threats:

- Your business's data can be hacked.
- Customer data could be leaked through error.
- The data you maintain can quickly become outdated (for example, contact data or payment details for customers).
- The data itself can become unmanageable, as it changes and grows.



[REF.] 5.1.2.6

[LECTURER NOTES]
Let's examine some of the side-effects of a data breach.

Diminished reputation

One compromising episode, such as a data breach, can tarnish even the best of reputations. In fact, 46% of organizations say they suffered damage to their reputation and brand value as a result of a cybersecurity breach.

Lost customer Trust

Clients share their sensitive information with businesses frequently, assuming the companies have the proper security measures in place to protect their data. As soon as a data breach occurs, customers will question the amount of trust they've put into a business. Furthermore, consumers want to believe that enterprises can not only prevent but also properly manage a potential data breach.

Increased costs

There are direct costs associated with a data breach, which can include hiring external data security consultants, purchasing new hardware or security systems, and so on. However, there are also indirect costs to be considered – for example, increased insurance costs.

Decreased competitive ability

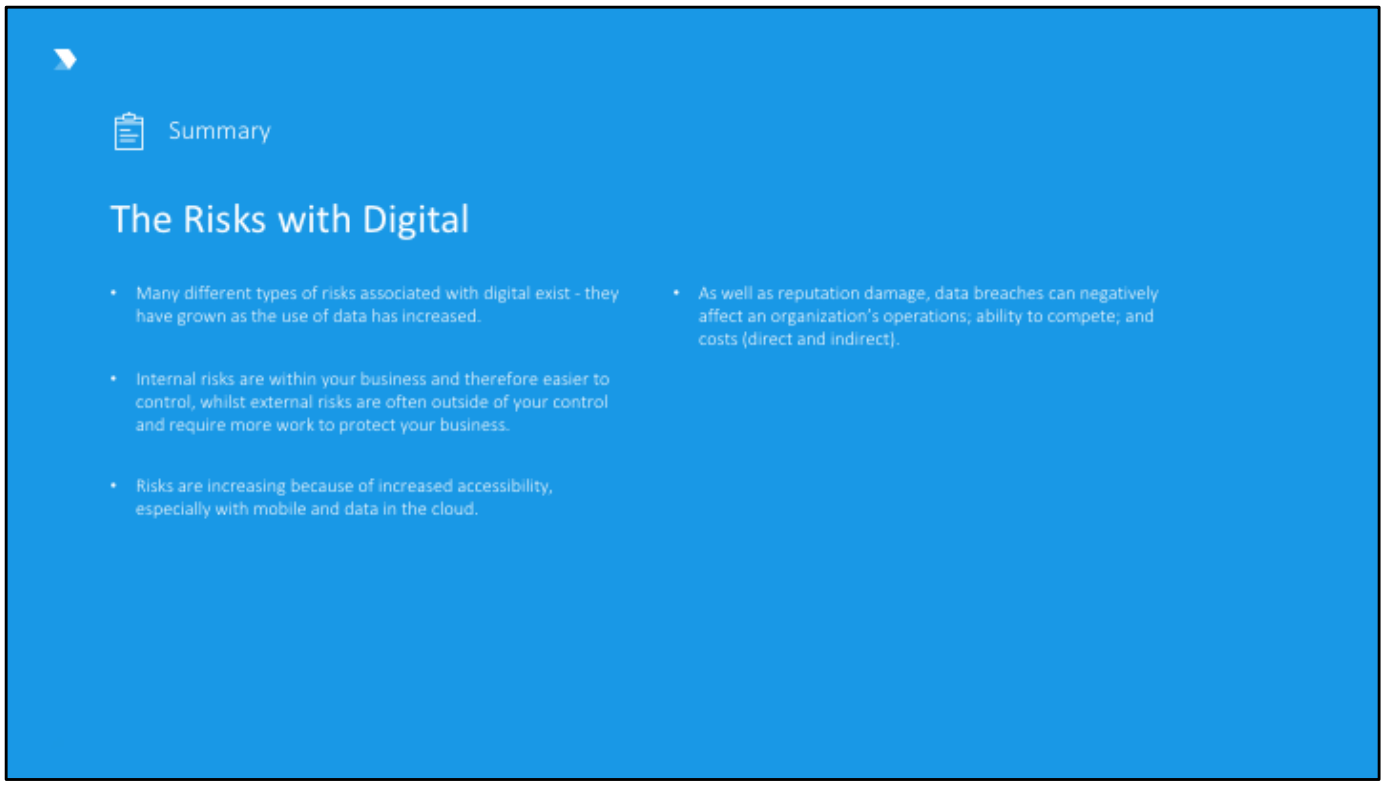
Often, data hackers are interested in a business's proprietary information, including customer lists, pricing strategies, and trade secrets. Once cybercriminals have this information, they can effectively damage a company's competitiveness by providing these materials to industry rivals or by exposing the information to the public. Additionally, a company's competitive ability will decrease following a cyber data breach as customers are likely to look to other sources for making purchases.

Operational shutdown

Once businesses are aware their system has been compromised, the most common course of action is to stop operations until a solution is found. Whilst operational shutdown processes are in effect to eradicate criminal activity, businesses can lose significant revenue streams until the problem is fixed and the system is fully secured.

[REFERENCES]

http://deloitte.wsj.com/riskandcompliance/2017/05/17/seven-hidden-costs-of-a-cyberattack/



[LECTURER NOTES]
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. 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 reputation and to your operations. Your ability to compete can be affected and there are both direct and indirect costs to consider.

Challenges and Risks

[LECTURER NOTES]
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.

Mitigating Risk through Planning

Risk Mitigation Starts inside the Organization

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

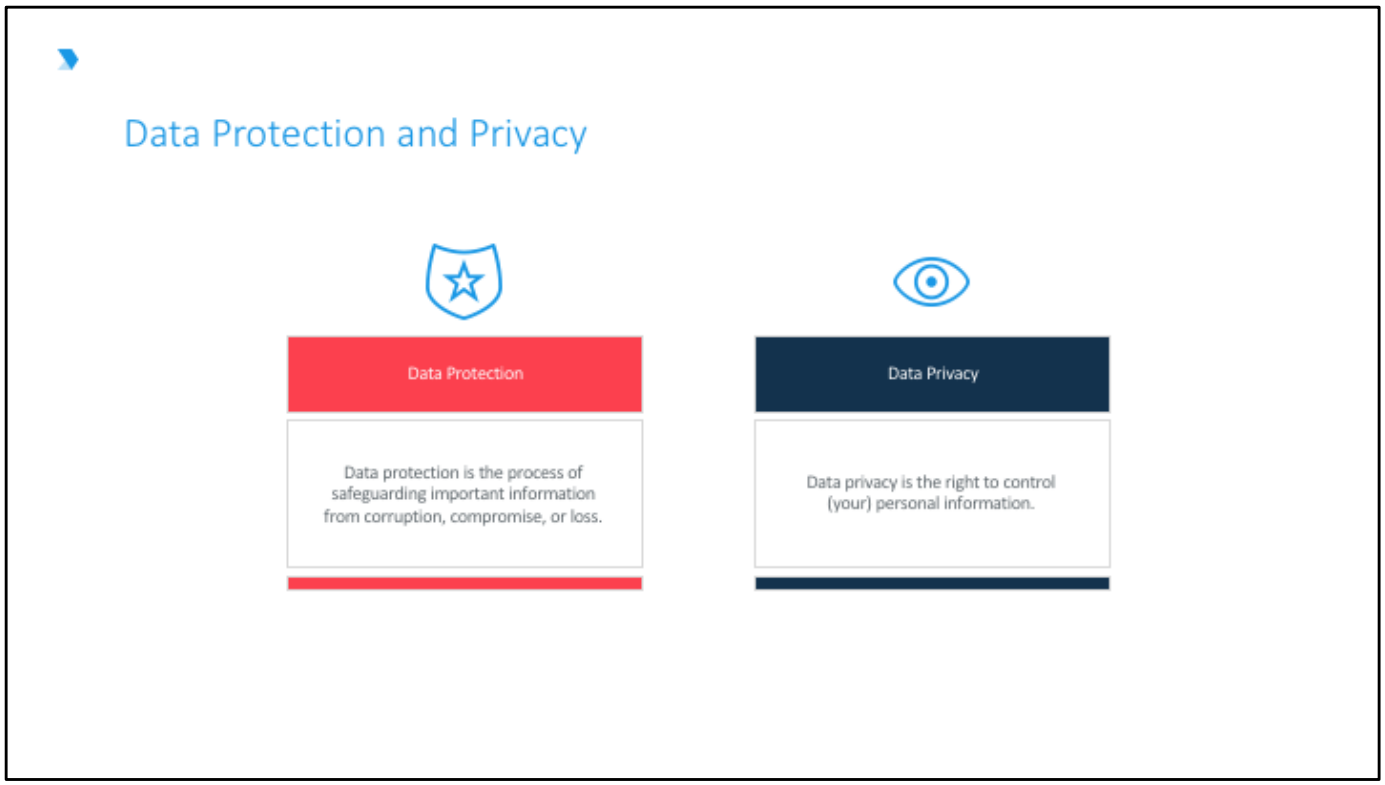
[REF.] 5.2.1.1

Risk Mitigation and Risk Management

It's important to carry out **risk mitigation** as a planning activity before issues occur.

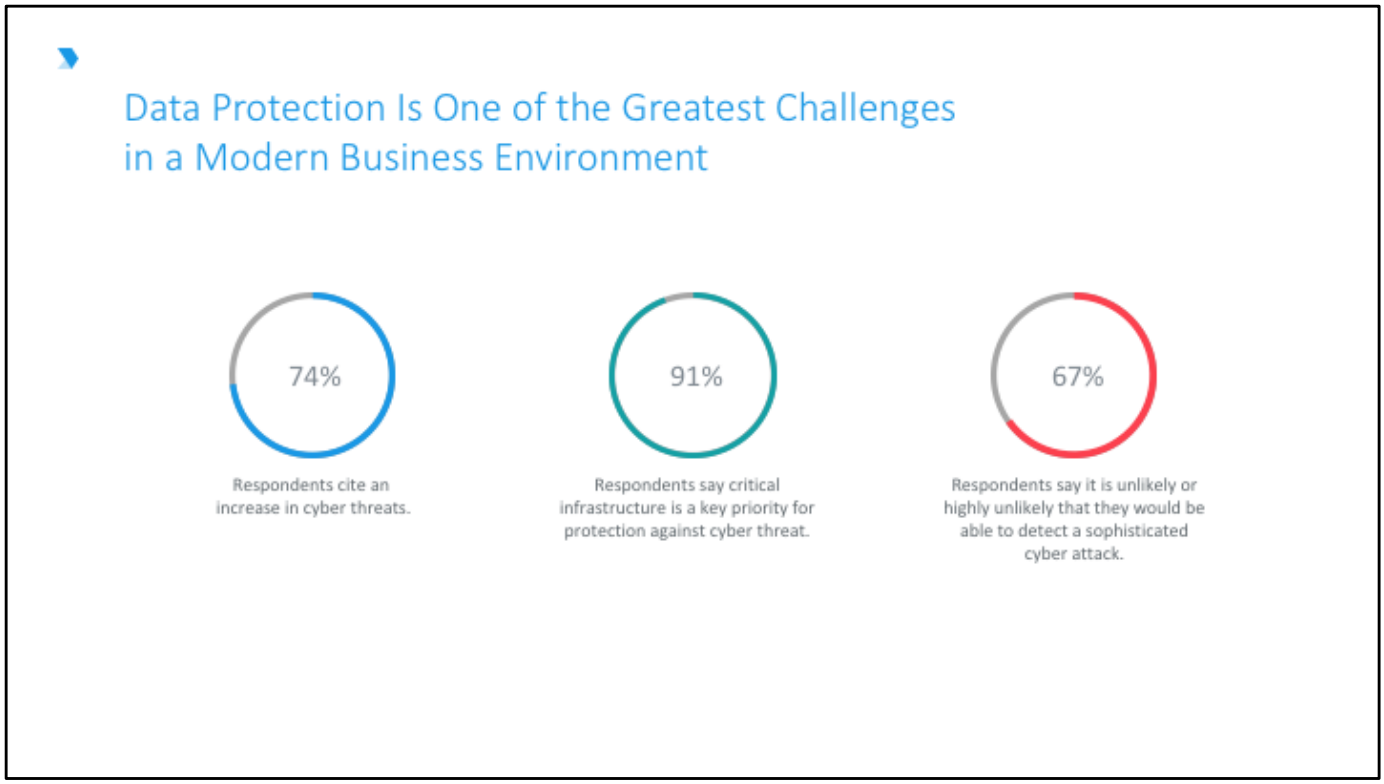
When dealing with the issues in real time, it becomes **risk management**.

[REF.] 5.2.1.1



[REF.] 5.2.1.2

[LECTURER NOTES]
Data protection is more than just protecting data from unauthorized access: it's about ensuring it's used for the sole purpose it was collected, and respecting the privacy of those who own the data.

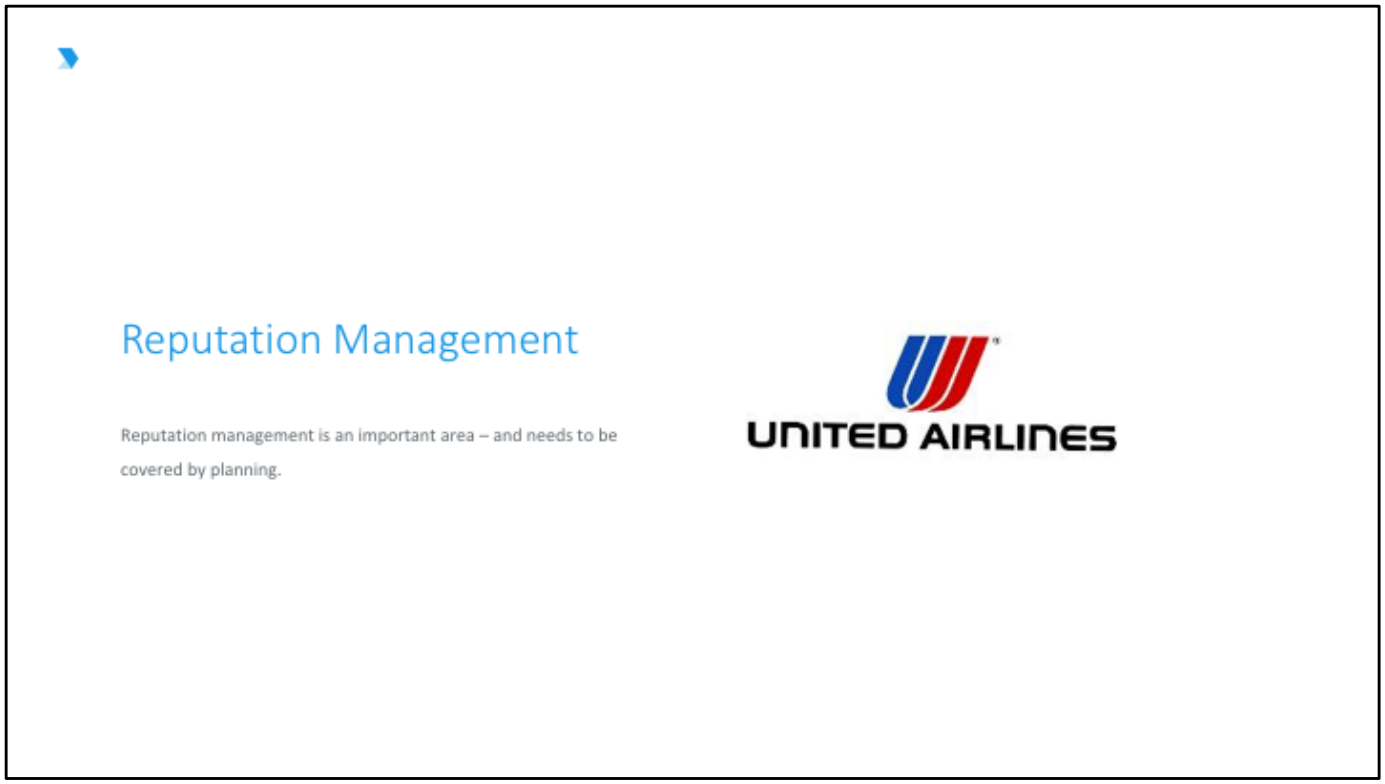


[REF.] 5.2.1.3

[LECTURER NOTES]
There is no doubt that 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.

[REFERENCES]
https://digitalmarketinginstitute.com/the-insider/20-02-18-is-the-future-of-digital-transformation-cognitive

https://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-regained-preparing-to-face-cyber-attacks/$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf



[REF.] 5.2.1.4

[LECTURER NOTES]
Reputation management is an important area that also needs to be covered by planning. Consider some recent high-profile negative publicity that organizations have been involved in. Companies need to be conscious that the smallest of incidents in one part of the world can spread, becoming a major issue with global reach.

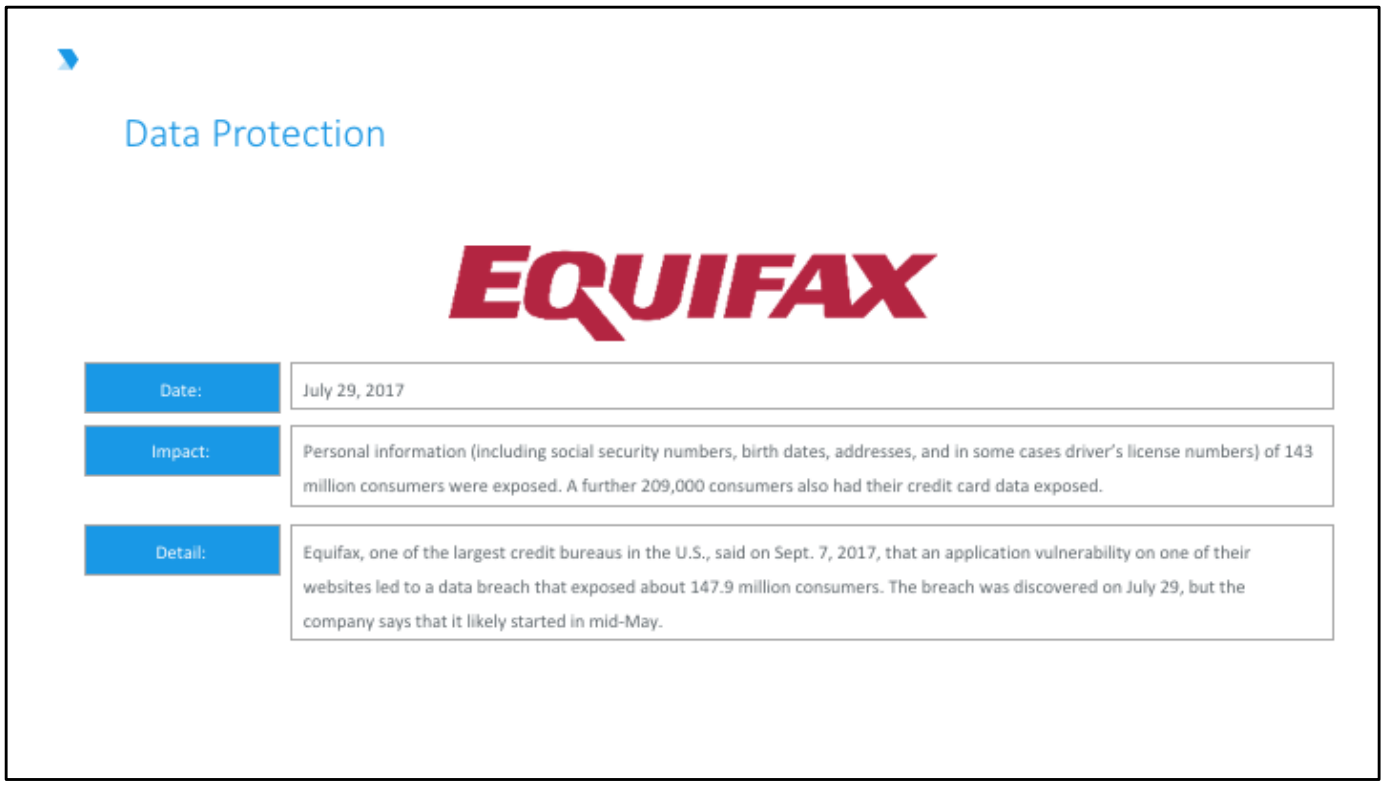
A good example of this is the recent incident with United Airlines when a passenger was abruptly removed from a plane. A global response and discussion erupted with significant reputational consequences for the airline.

According to The Drum *"A social media sentiment analysis by Brandwatch laid bare the depth of the reputational impact the airline had suffered over the incident. Data from the social media monitoring outfit showed the brand's name was mentioned over 762,000 times on Facebook, Instagram and Twitter the day after it went public (April 10, 2017)."*

[REFERENCES]
http://www.thedrum.com/news/2017/04/11/united-airlines-pr-disaster-the-21st-century-every-disgruntled-passenger-potential

https://www.ey.com/Publication/vwLUAssets/ey-tmt-global-information-security-survey-2018/$File/ey-tmt-global-information-security-survey-2018.pdf

Practical Requirements for Mitigating Risks



[REF.] 5.2.2.1

[LECTURER NOTES]
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.

[REFERENCES]
https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

Contingency Planning

Contingency planning is an important element of a business's planning. It involves deciding on the specific actions that need to be taken (and by whom) in the event of situations arising.

[REF.] 5.2.1.5

[LECTURER NOTES]
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 is 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.

Practical Implementation of Policies

Once guidelines and policies are in place, they need to be implemented in a practical way within an organization.

[REF.] 5.2.2.2

[LECTURER NOTES]
For example, social media guidelines which are reviewed by Legal may need to be implemented (and signed off) by HR within employment contracts. Policies that affect the website, such as blog or other content guidelines, need to be easy to implement so that they do not affect the efficiency of your website (and processes).

[REF.] 5.2.2.3

[LECTURER NOTES]
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.

Some subjects can invite a flame war.

"Be careful discussing things where emotions run high (e.g. politics and religion) and show respect for others' opinions."

Don't even think about it…

"Talking about financial information, sales trends, strategies, forecasts, legal issues, future promotional activities. Giving out personal information about customers or employees. Posting confidential or non-public information. Responding to an offensive or

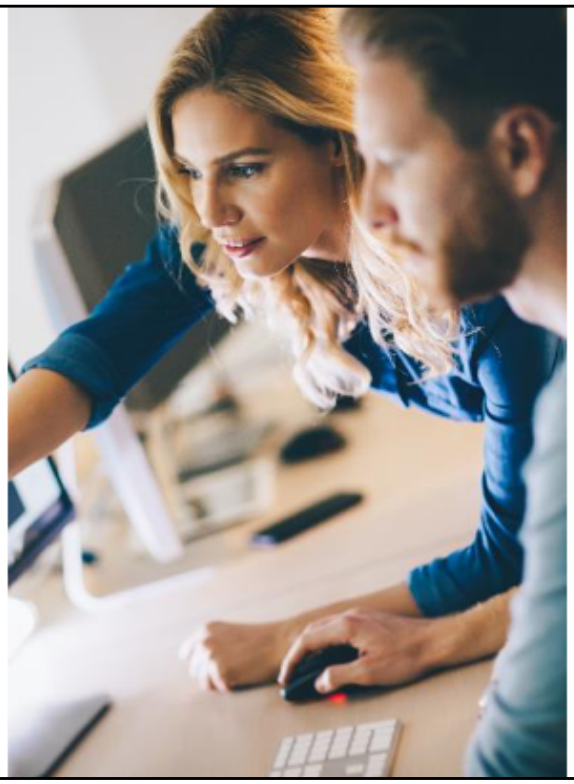
negative post by a customer. There's no winner in that game."

[REFERENCES]

http://blog.hirerabbit.com/5-terrific-examples-of-company-social-media-policies/

IT Processes

Strong IT processes are a key element of risk mitigation for data. That includes training of staff (password policy; equipment and portable devices, such as USBs; email and opening attachments; and so on), employee access control, and up-to-date security software (to cater for malware).



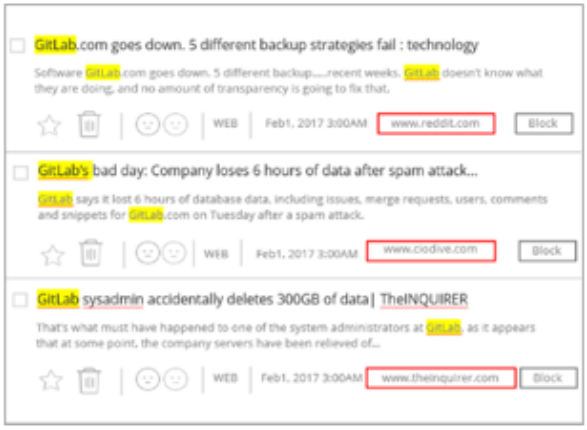
[REF.] 5.2.2.4

[LECTURER NOTES]
A key element of risk mitigation for data in any business is also your IT processes. The human element is often the weakest link when it comes to protecting your data, so training on password policy, security of portable devices such as 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.

Managing Live Issues
with Processes

Social Listening

What can organizations do to mitigate against external issues that arise?



[REF.] 5.2.3.1

[LECTURER NOTES]
One good practice is social listening, which involves listening out for key words, such as the organization's name, online. Organizations immediately become aware of what communities are saying about them, which helps them to mitigate against issues that arise before they get blown out of proportion.

[REFERENCES]
https://www.semrush.com/blog/social-listening-in-practice-big-brand-examples/

Quick Response

With social listening, because you have real-time information on conversations, your company can respond in short order, if required.

[REF.] 5.2.3.2

[LECTURER NOTES]
With social listening, because you have real-time information on conversations, your company can respond in short order, if required.

Social media has enabled customers to have an open dialog 24/7. That means some companies will respond to serious issues within minutes. However, there's also a cost to provide cover, ensuring there is always a response capability for serious issues.

[REFERENCES]
http://www.adweek.com/creativity/best-corporate-apology-ever-posted-twitter-140815/

PR Strategy

It's important to have a crisis PR strategy for risks.

Buffer, an online social media scheduling site, was recently hacked.

[REF.] 5.2.3.3

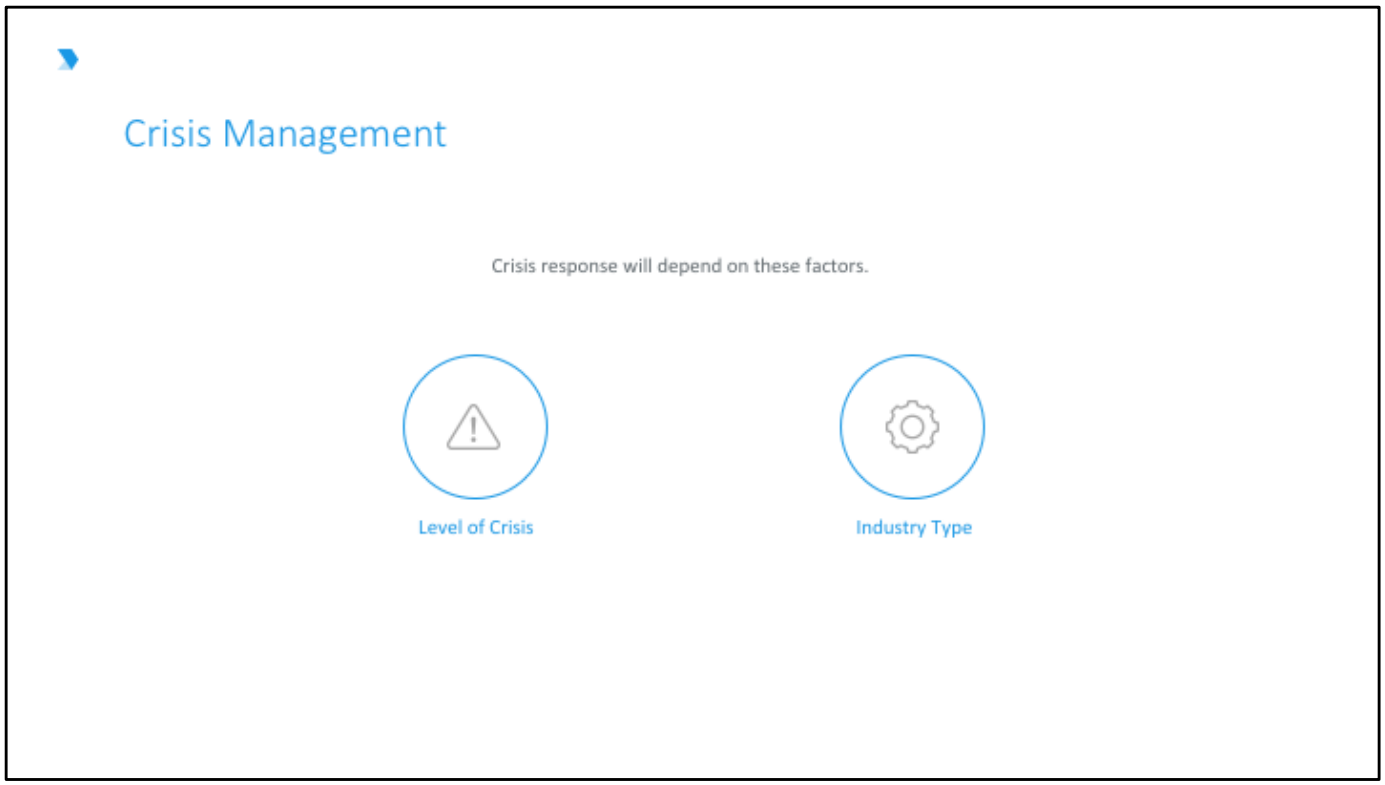
[LECTURER NOTES]

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'd been an attack.

[REFERENCES]

https://www.socialmediaexaminer.com/defend-your-social-media-reputation/



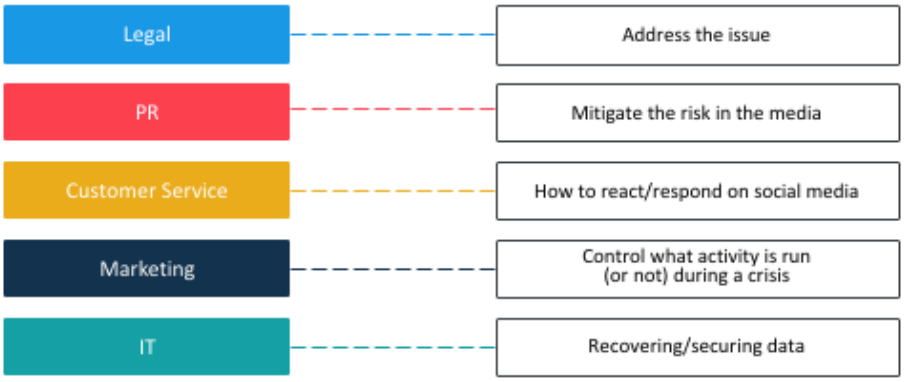
[REF.] 5.2.3.4, 5.2.3.5

[LECTURER NOTES]
Your response will depend on two factors:

Level of crises
It's important to decide on the criteria for the level of seriousness of the crisis to put in place an appropriate response. For example, a serious issue might involve a customer's banking personal details being hacked.

Industry type
Crisis response for a large pharma company would be a lot different than that for a financial institution.

Crisis Management



[REF.] 5.2.3.6

[LECTURER NOTES]

As we've seen, 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.

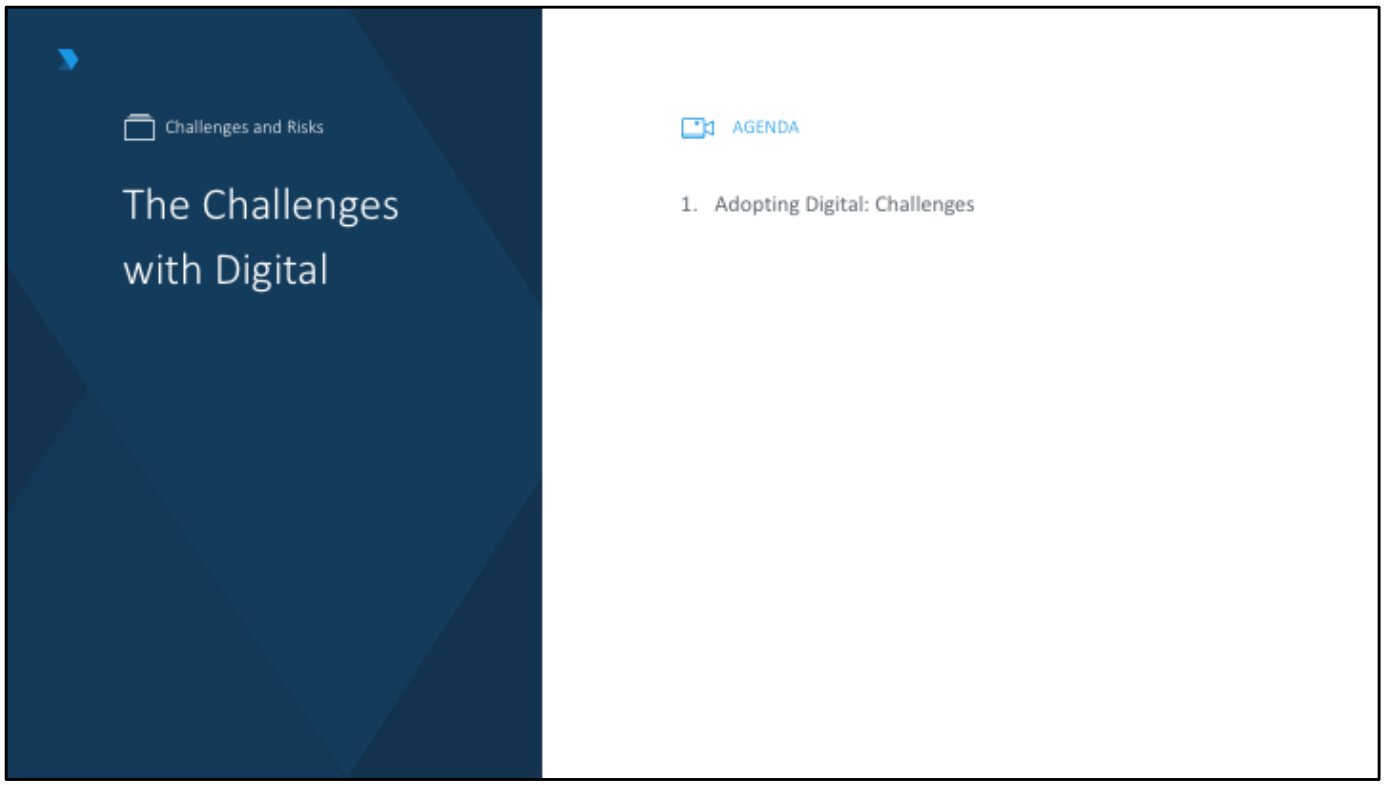
[LECTURER NOTES]
To summarize, in this section, we learnt that risk mitigation should take place as a planning activity before issues occur, while Risk Management is dealing with the issues in real-time when they occur.

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 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.

Challenges and Risks

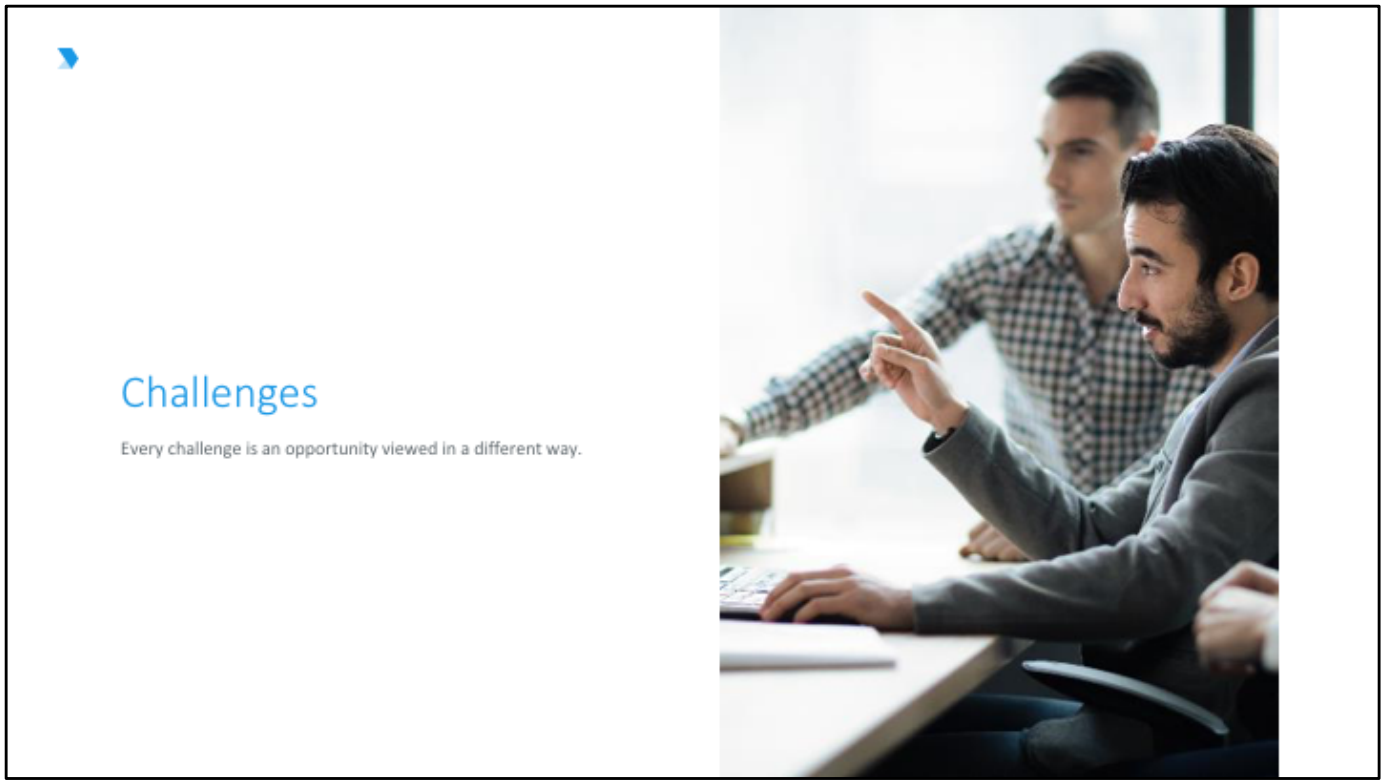


[LECTURER NOTES]
Next, we're going to look at the challenges that organizations might face when implementing a digital strategy. As we'll see, there are a number of areas that might not be obvious to think about – such as your organizational structure or whether you have the digital skills within your business to be successful. We'll think about what those specific skills are and how they impact the business.

As we'll see also, it 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.

Adopting Digital: Challenges



[REF.] 5.3.1.1

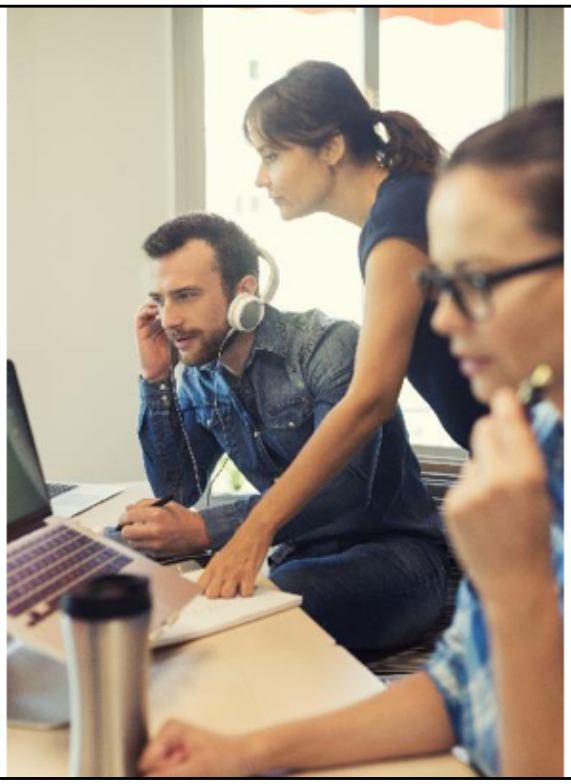
[LECTURER NOTES]

Every challenge is an opportunity viewed in a different way.

For example, most businesses experience a lack of resources - whether it's internal staff, external resources, 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.

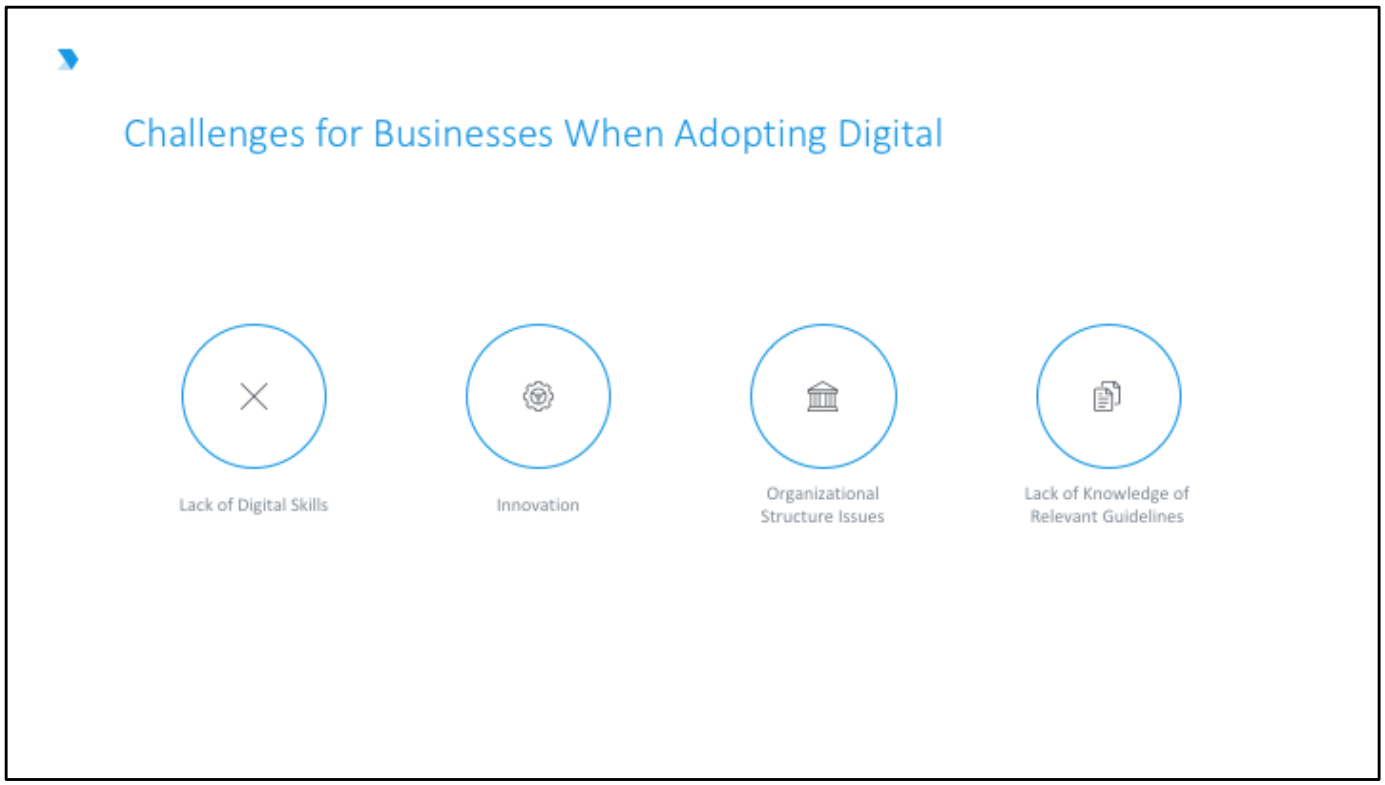


[REF.] 5.3.1.2

[LECTURER NOTES]

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".



[REF.] 5.3.1.3

[LECTURER NOTES]
What challenges might you encounter when adopting digital?

Lack of digital skills
The digital skills gap has been widely publicized, with the following percentages of marketers perceiving themselves as “very” or “fairly” competent in digital marketing:

- USA: 59%
- UK: 47%
- Ireland: 51%.

However, the actual level of their skills is equally low across all three countries (38% on average).

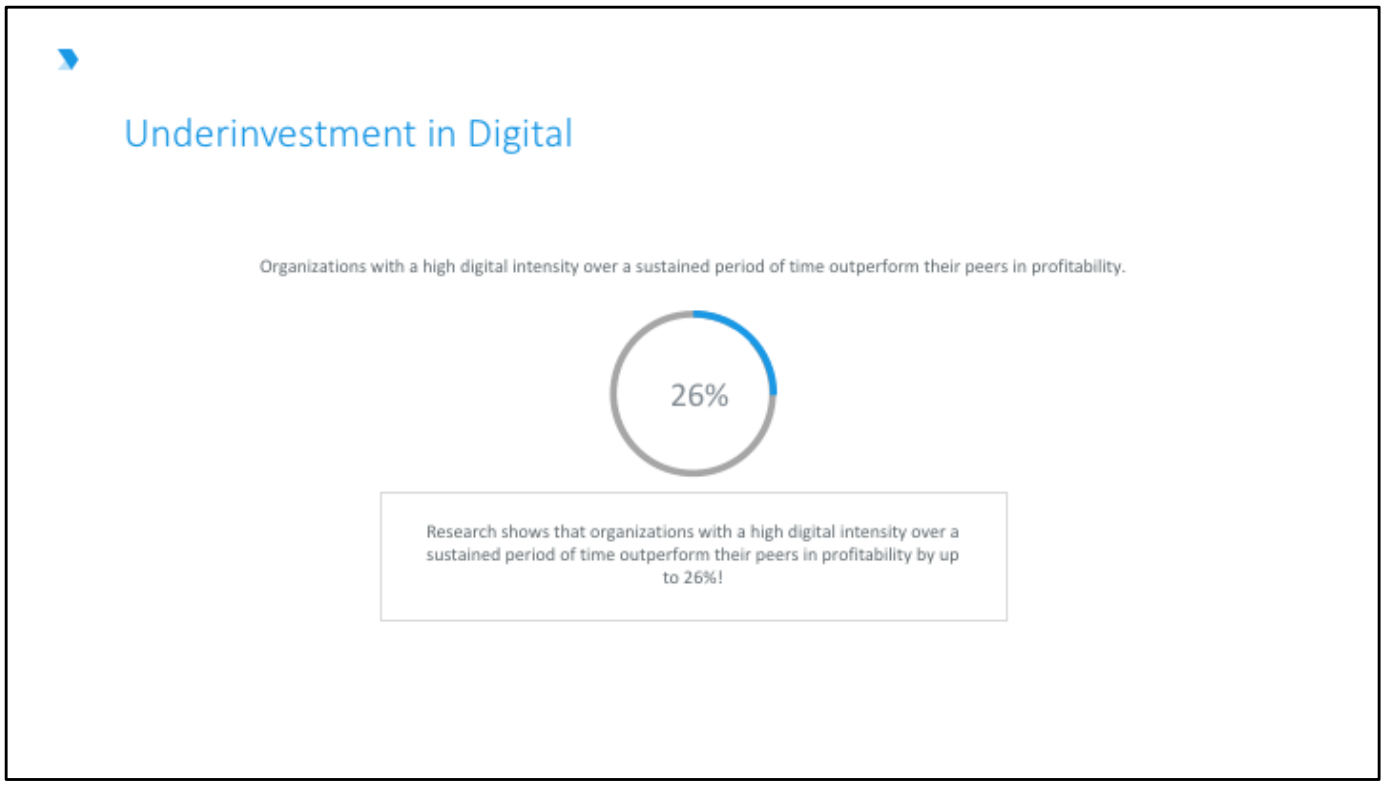
Innovation
Innovation is key to growth within a business. Being able to come up with innovative ways for your business to move forward through digital is a skill that is often in short supply in an organization.

Organizational structure issues
It’s less costly to build business operations around digital technology - the cost per transaction is lower.

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. In a world of open communications, employees are now the voice of the organization as well as company communications.

[REFERENCES]

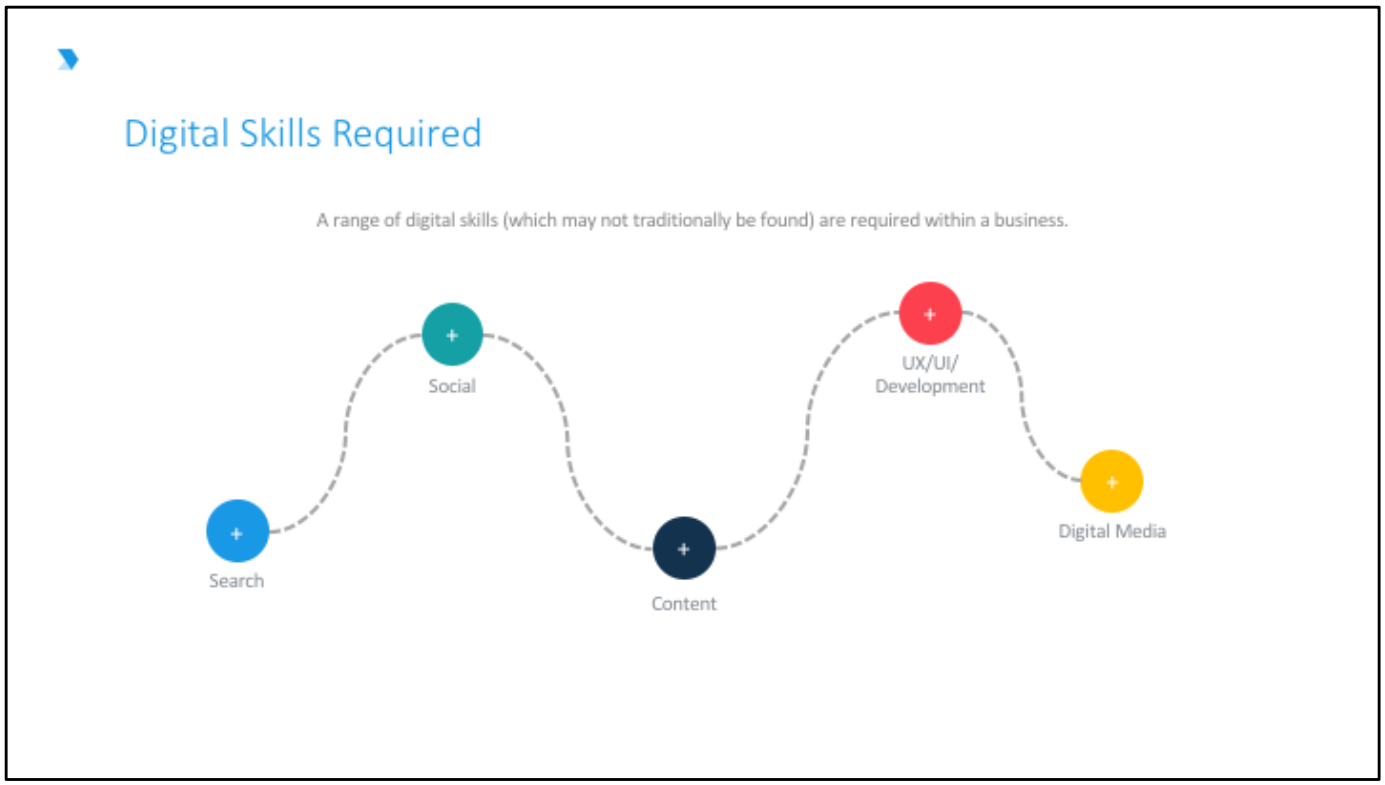
https://digitalmarketinginstitute.com/en-gb/the-insider/missing-the-mark-the-digital-marketing-skills-gap-in-the-usa-uk-ireland



[REF.] 5.3.1.4

[LECTURER NOTES]
Organizations with a high digital intensity over a sustained period of time outperform their peers in profitability. Consequently, underinvestment in digital over time can negatively affect the commercial performance of a business.

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



[REF.] 5.3.1.5

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 brand's products/services.

UX/UI/Development: The creation of engaging, intuitive and brand consistent designs through digital assets.

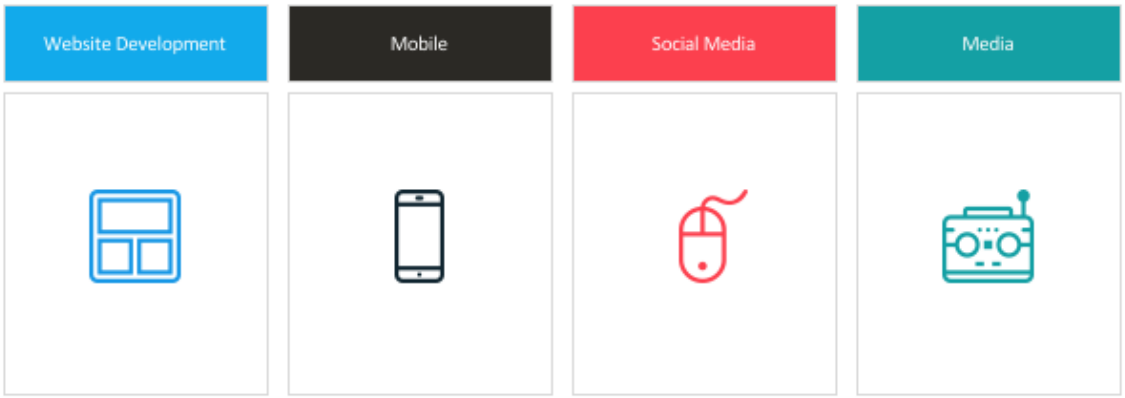
Digital Media: Digitized content for distribution online (including text, audio, video, and graphics).

Employee Voice

Be mindful that, in a world of open communications, employees are also the **voice of the organization** (in addition to the company communications). This presents its own challenges.

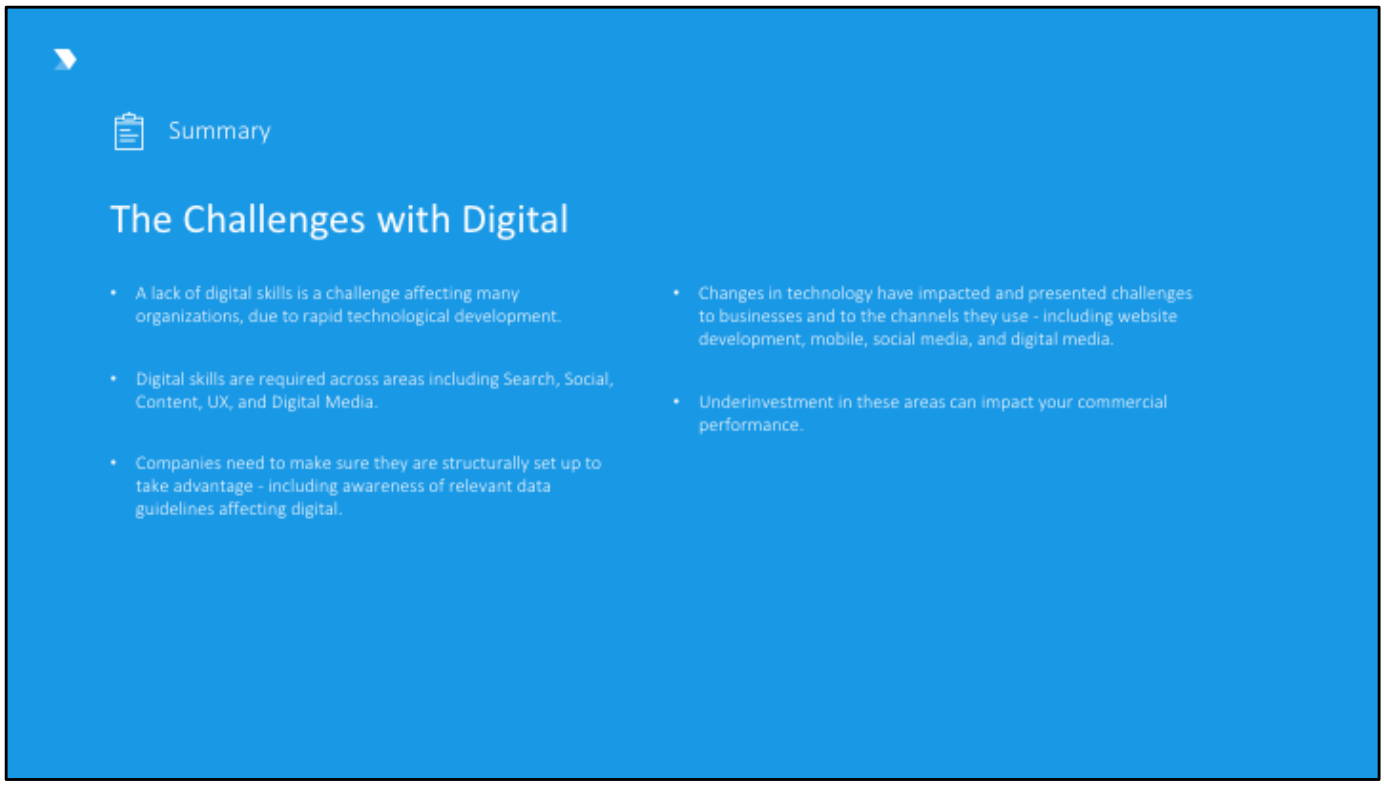
[REF.] 5.3.1.6

Technological Change – Key Areas of Impact



[REF.] 5.3.1.7

[LETURER NOTES]
Here are 4 specific areas of digital where technology change is impacting businesses and therefore presenting challenges.

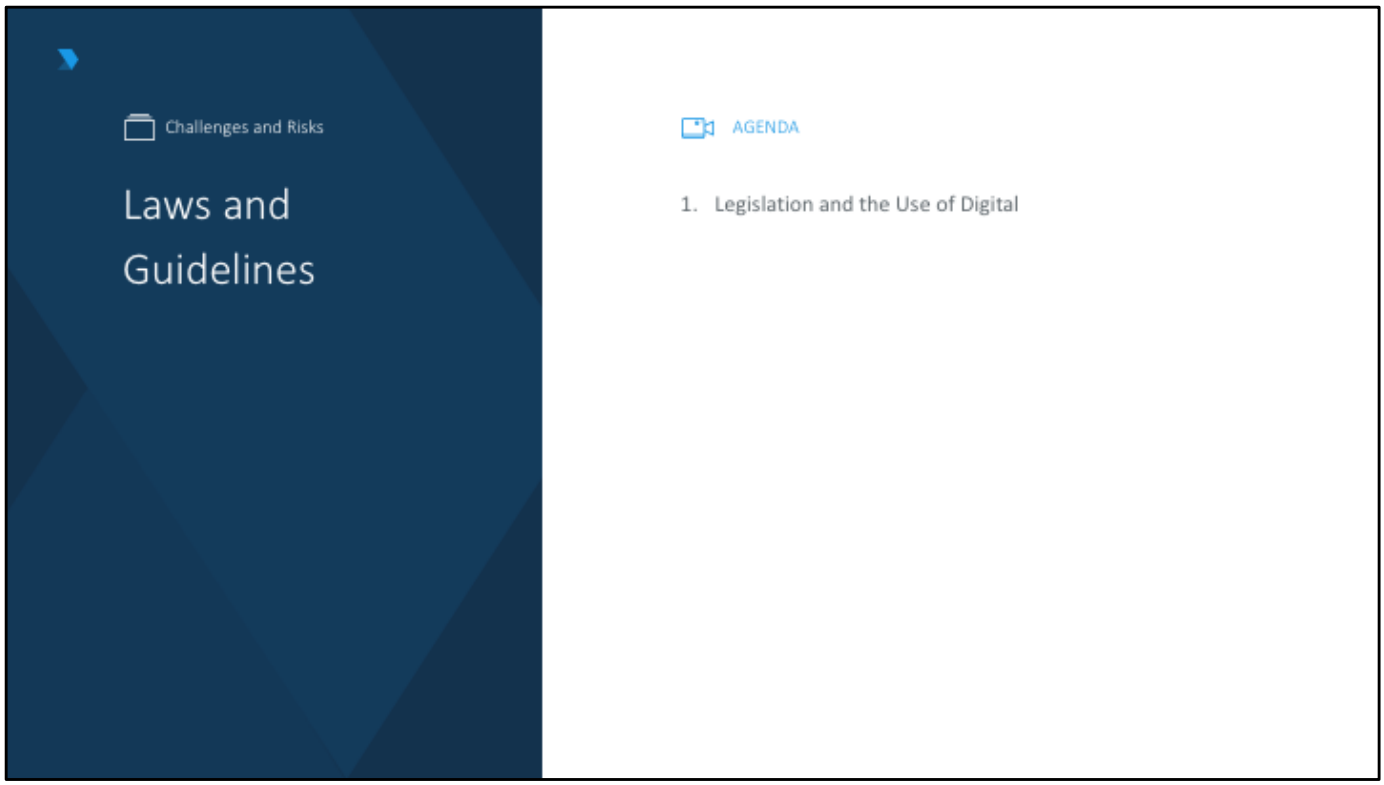


[LECTURER NOTES]
So hopefully you now have an insight into the challenges associated with digital for businesses. Because of advances in technology, the lack of digital skills is a challenge affecting many organizations. Digital skills are required across areas including Search, Social, Content, UX, 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, there are specific areas where changes in technology have both impacted and presented challenges to businesses and to the channels they use. These include website development, mobile, social media, and digital media. The reality is that underinvestment in these areas can impact your commercial performance.

Challenges and Risks



[LECTURER NOTES]
In 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 alike.

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

Legislation and the Use of Digital

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.

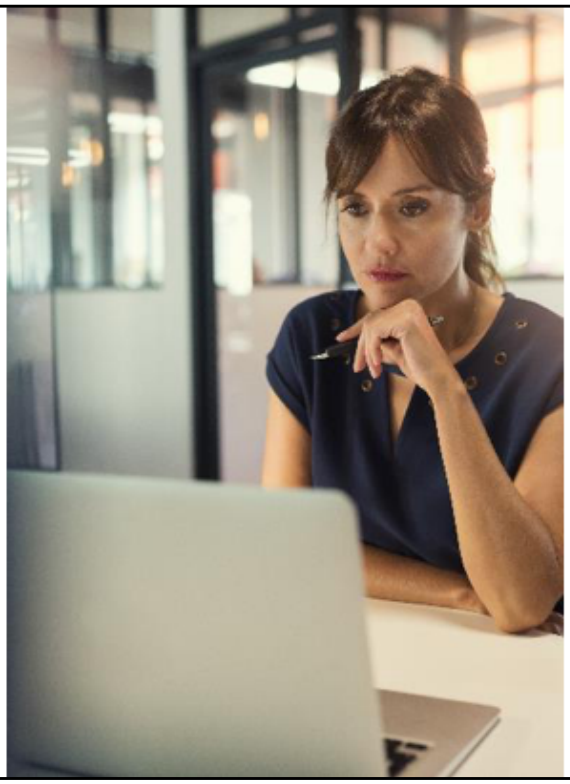
Data Retention
Also called records retention, it is the continued storage of an organization's data for compliance or business reasons.

Cookie
A small piece of data that is stored on a user's computer. Often used to track the websites user's visit.

Legislation Depends on Your Market

Most legislation is dependent on the market that your business is operating in.

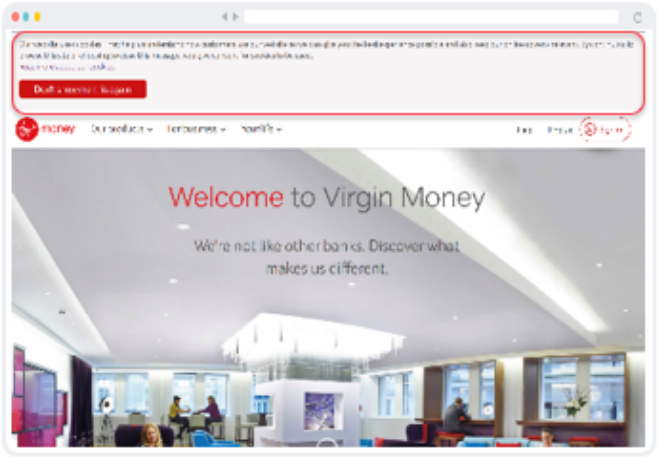
Therefore, it's important to be aware of the legislation in both your home market, as well as all other markets that you operate in.



[REF.] 5.4.1.1

The EU Cookie Directive

All businesses in the EU need to comply with the Cookie Directive, which is designed to protect consumers online privacy.



[REF.] 5.4.1.2

[LECTURER NOTES]
All businesses in the EU need to comply with the Cookie Directive, (also known as the Cookie Law), 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 Information Commissioner's Office (ICO) has powers to force websites to change or it can impose a fine of up to £500,000 in the most serious cases.

[REFERENCES]

https://uk.virginmoney.com/virgin/

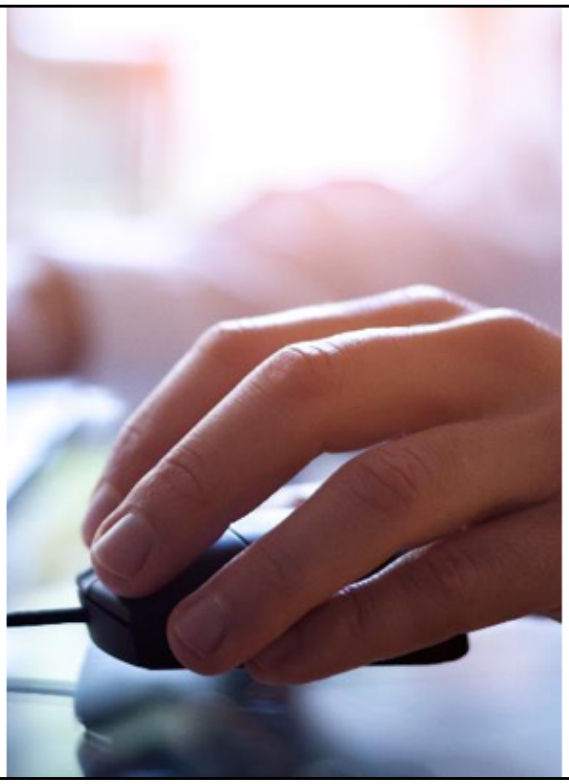
[REF.] 5.4.1.3

[LECTURER NOTES]
The Cookie Directive 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.

Data Guidelines

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



[REF.] 5.4.1.4

[REF.] 5.4.1.5, 5.4.1.6

[LECTURER NOTES]
The General Data Protection Regulation (GDPR) came into effect from May 25th 2018 across the European Union. It strengthens data protection for all individuals within the EU and poses significant fines for organizations that fail to meet its new high standards. It also addresses the export of personal data outside the EU.

[REFERENCES]
https://www.eugdpr.org

[REF.] 5.4.1.7

[LECTURER NOTES]
Data consent refers to collecting personal data about leads and prospects via your organization's various digital marketing channels, and gaining their explicit and unambiguous consent to opt-in to hearing from your organization.

Data processing refers to how your organization uses that collected data, and whether the leads, prospects and customers understand why it needs to be processed that way.

Data retention refers to how long your organization retains personal data, and the business reasons for doing so.

Data transfer refers to the transfer of the personal data of European Union citizens outside of the EU for legitimate business purposes.

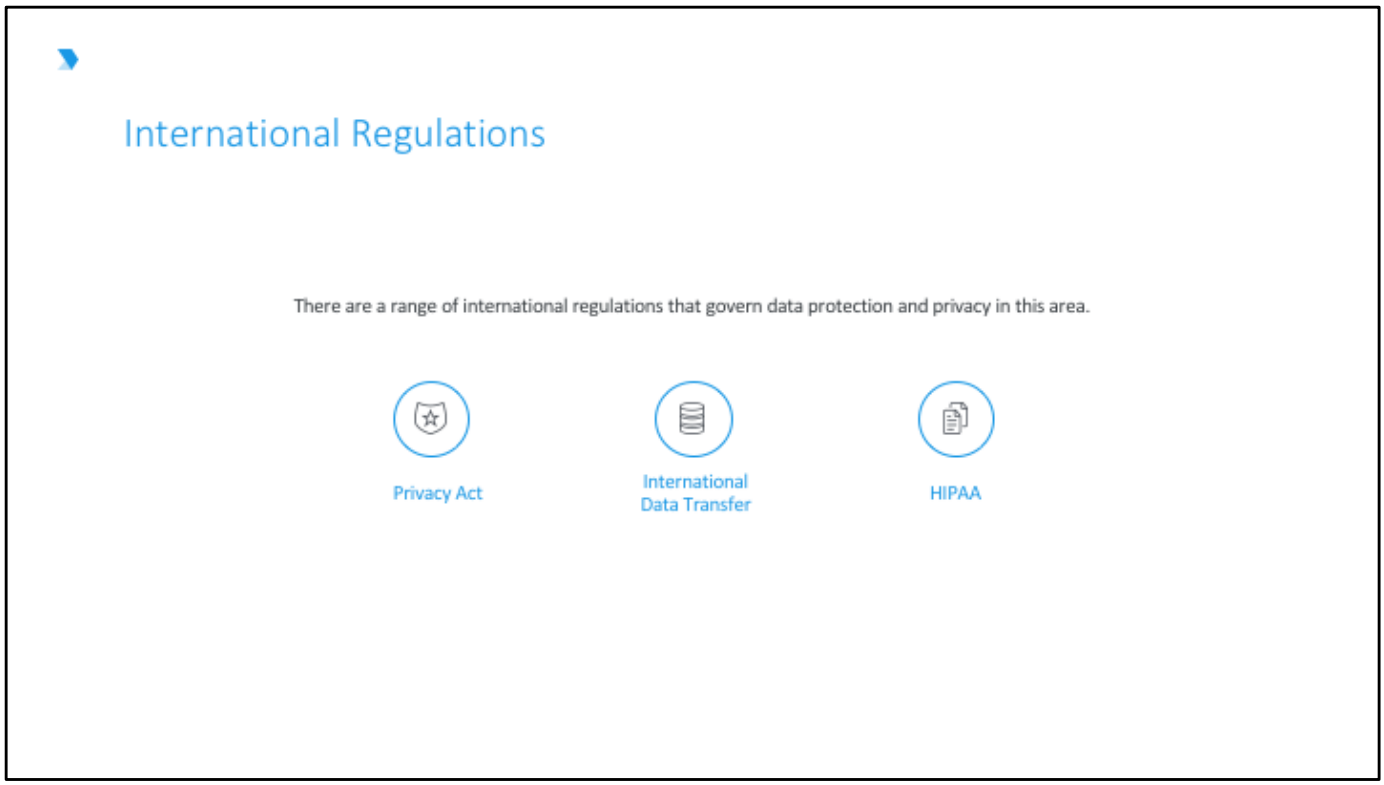
Data deletion refers to when and how personal data is permanently removed from your organization's systems.

GDPR and other Data Privacy Standards in the EU

- GDPR is a regulation which will be enforced.
- The existing Data Protection Directive (DPD) served more as a guideline for best practices.
- GDPR supersedes DPD.

[REF.] 5.4.1.8

[LECTURER NOTES]
It's also very important to consider brand reputation and not just regulation when thinking about compliance with the GDPR. Central to this is ensuring that personal data processing doesn't cause harm or damage to the individual.
In a nutshell, it's all about being fully transparent and accountable for the processing of personal data and putting control over back into the hands of the individual – the customer, client, supporter and employee.



[REF.] 5.4.1.9

[LECTURER NOTES]
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.

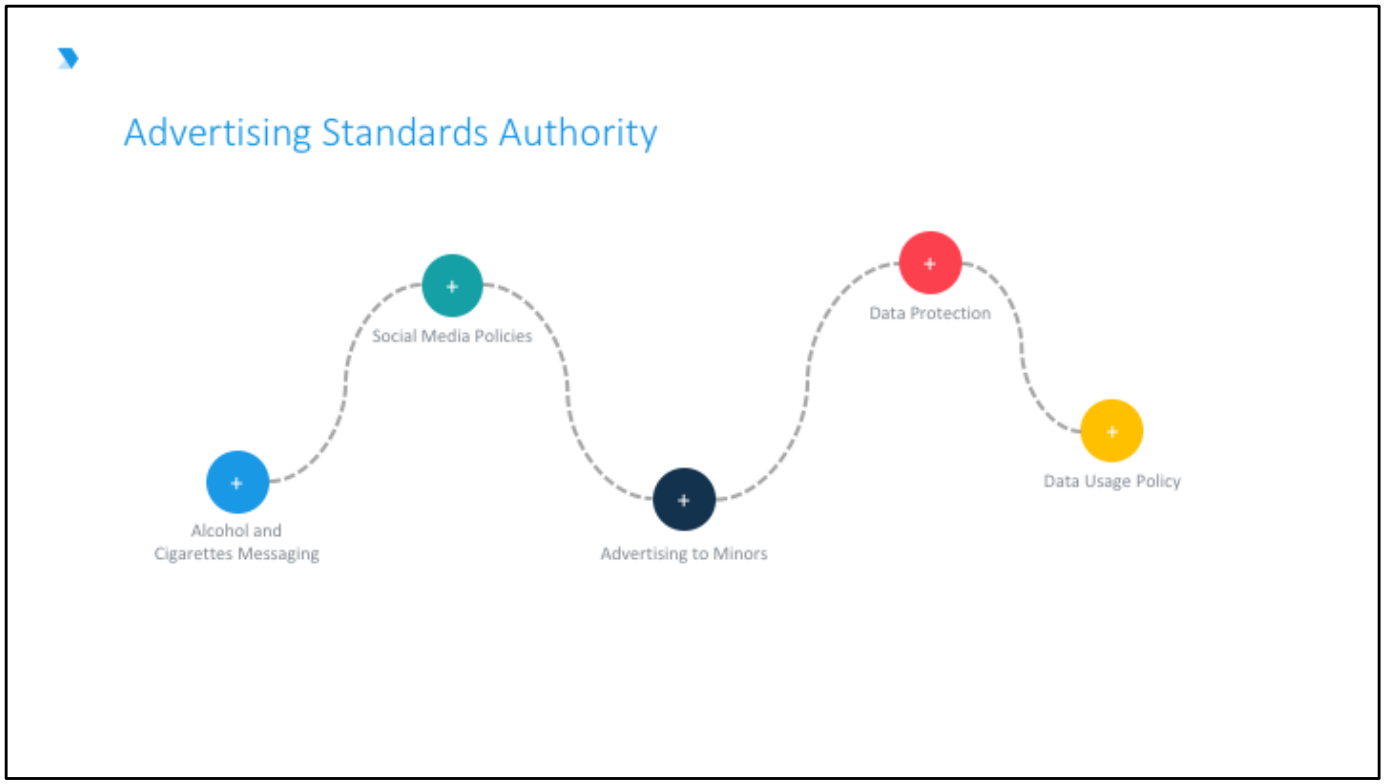
Privacy Act
The Electronic Communications Privacy Act and the Computer Fraud and Abuse Act regulate the interception of electronic communications and computer tampering, respectively. The Electronic Communications Privacy Act of 1986 protects the privacy and security of the content of certain electronic 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.

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 Harbour programme, using European Commission-approved model contracts. In October 2015, Europe's highest

court struck down the established Safe Harbour 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 healthcare 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”.

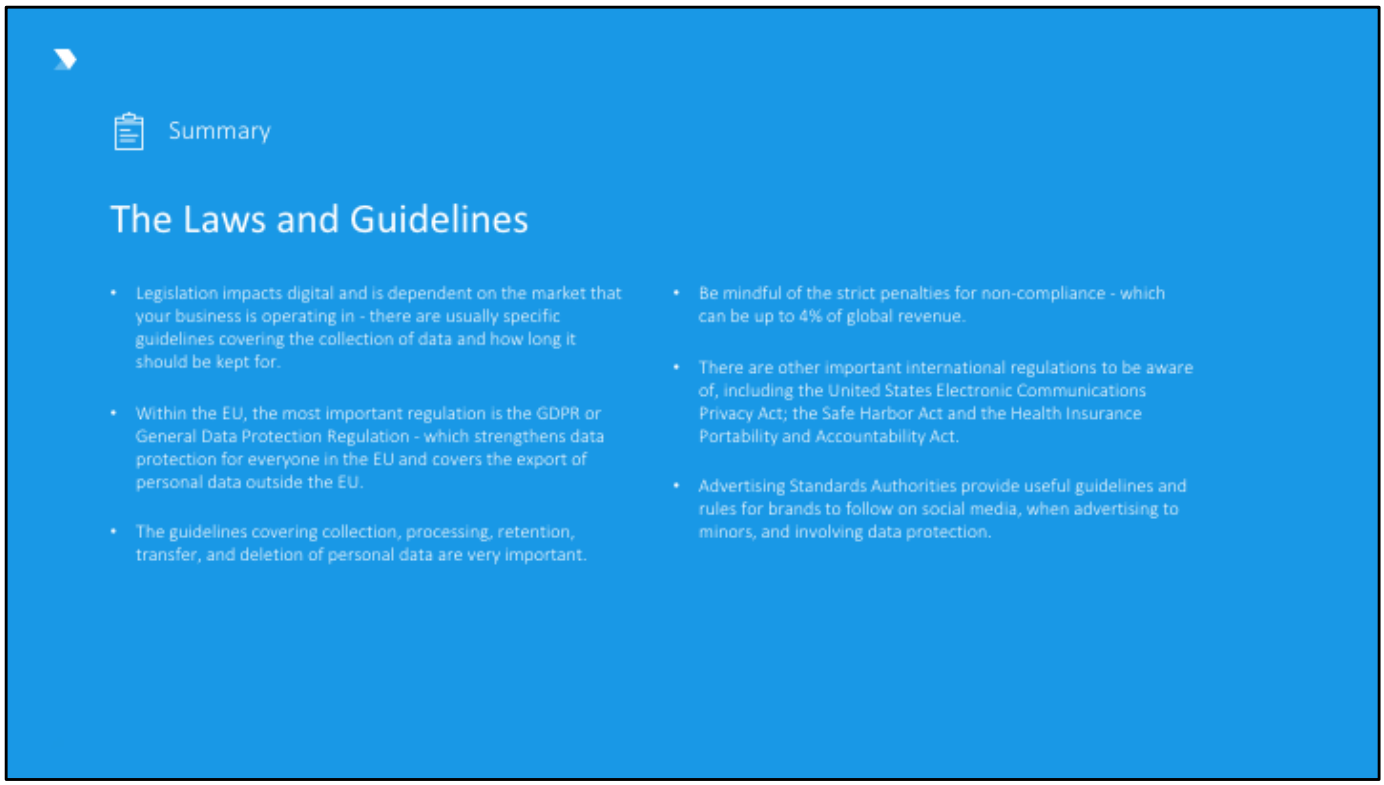


[REF.] 5.4.1.10

[LECTURER NOTES]
In most regions (for example, the UK and Ireland), there is an Advertising Standards Authority, which is an independent body that provides guidelines and rules for brands to follow the areas listed below:

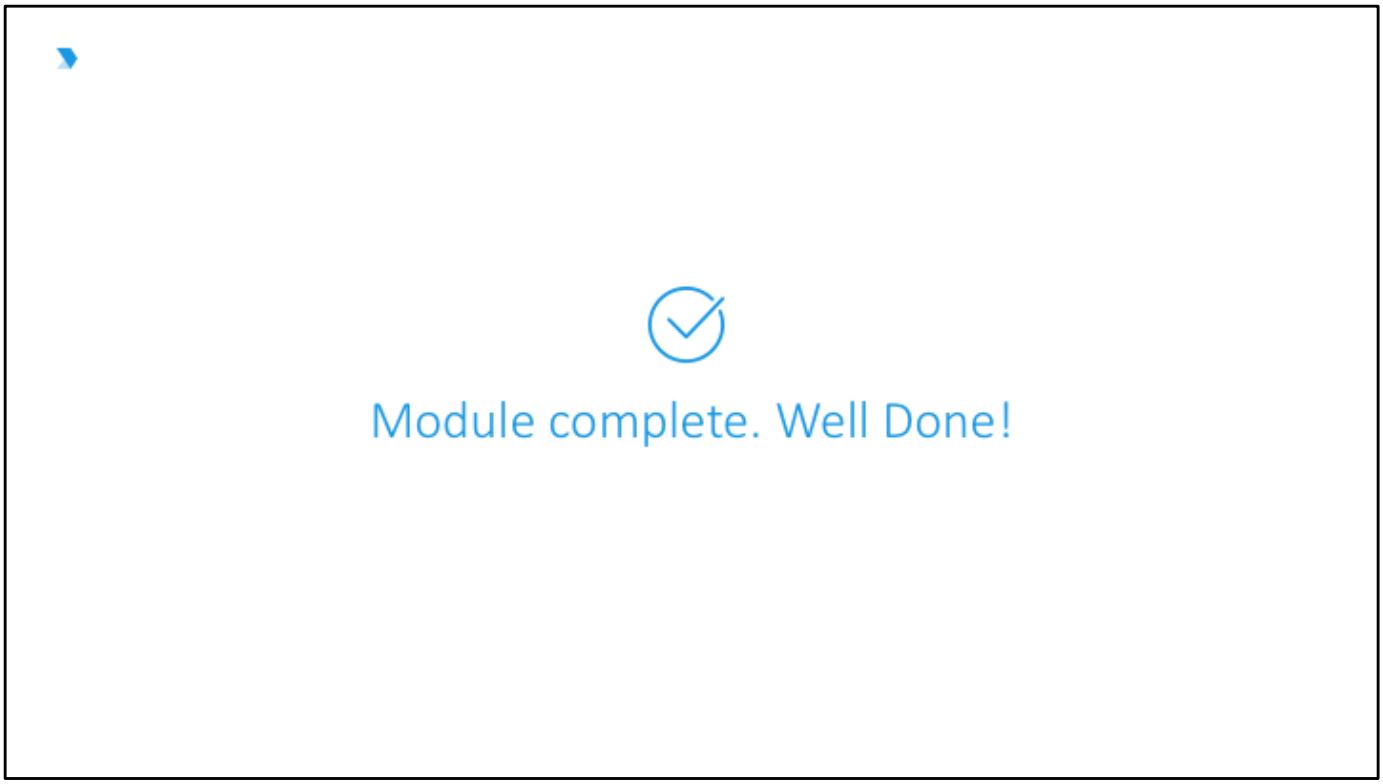
- Alcohol and Cigarettes
- Social Media Policies
- Advertising to Minors
- Data Protection
- Data Usage Policy

[REFERENCES]
https://www.asa.org.uk/



[LECTURER NOTES]
We've covered a lot of ground in this module, which hopefully has been useful in highlighting the risks and challenges, as well as the opportunities, that the digital environment presents to organizations. In particular, if organizations plan and put steps in place to reduce the risks to both customers and employees, then they will see a significant up-side. That said, there are a range of additional risks that must be considered and carefully planned for in order to protect customer data and the reputation of organizations. It's all too easy in today's social media-driven environment for a small incident to become a much larger global issue.

Finally, as we 've seen, there is an increasing role for regulation in the area. But, it's important to remember that these are largely market driven and that organizations need to develop their own strategies to deal with them in the markets that they operate in.


Module complete. Well Done!


digital
marketing
institute