Virtual Work Experience

Info Security Task 1 Answers

Scenario	Confidentialty? Integrity? Availability?	Who would this impact?	Why?
Your employees can't log into the quote system on Monday morning.	Availability	Customers, the business, our profits, reputation	We don't know why the systems are down so only the availability is impacted at the moment. This means we are paying staff although they aren't working, we're not getting any new customers in or dealing with existing customers, and so it is hitting our profits and also our reputation.
A member of your quote team is desperate to finish early for the day. They notice some information is missing from the last caller which means they can't finish the quote process. They are due to finish so rather than spend time calling up the customer to confirm the details, they guess the answers and fill in the quote themselves.	Confidentiality	Customers, the business, our profits, reputation	Mistakes happen but they can be costly. A data breach like this could end up costing us in fines and compensation. This will hit our reputation which will likely impact the business. We also have a duty to inform our customers of the breach. They will likely be upset by the breach and will be concerned about whose hands their details might have fallen into – making them vulnerable to future scams.
Yesterday there was a lightning storm, and the office is unable to get electricity to their building.	Availability	Customers, the business, our profits, reputation	Even though the weather is out of our hands we will still feel the financial and reputational impact of not being able to serve our customers. Good security should account for backup plans in instances such as this, for example, enabling people to work from home.
Someone has clicked the wrong button and now all the customer data you have is posted as a spreadsheet on an online forum for everyone to see. This includes names, addresses, and policy details but no card details.	Confidentiality	Customers, the business, our profits, reputation	Mistakes happen but they can be costly. A data breach like this could end up costing us in fines and compensation. This will hit our reputation which will likely impact the business. We also have a duty to inform our customers of the breach. They will likely be upset by the breach and will be concerned about whose hands their details might have fallen into – making them vulnerable to future scams.
A hacker has managed to get into your network, they are able to view documents and send them to their own computer.	Confidentiality (Integrity, Availability, potentially)	Customers, the business, our profits, reputation	If an unauthorised person can access your documents, then this is a breach of confidentiality. If the hacker then went on to change the details of these documents, then it would be an integrity issue also. If they then took down the system remotely, it would also be an availability issue. Note, hackers are not necessarily out to bring systems down. Sometimes they want to quietly steal information without the company knowing to sell on or use at a later date.

Virtual Work Experience

Info Security Task 1 Answers

Scenario	Confidentialty? Integrity? Availability?	Who would this impact?	Why?
A customer has managed to gain access into our backend system which has all their account and home insurance details in it. They change their contents policy to include a Tesla, a Banksy and 10 blue French Bull dogs – none of which exist. Our system does not track changes, so we have no record these items have only just been added. The next day they call to say that all of these items have been stolen and they wish to claim….	Integrity, Confidentiality	Customers, Our reputation, Profits, The Business	Changing details, even your own, without consent, is a breach of integrity. It is vital that the data we hold is accurate and true so we can act accordingly. It is also a breach of confidentiality because the customer may be able to see other people's data but also how our quote system works.
The CEO has clicked on an email – Uh Oh! It's ransomware! They are saying you need to pay up to gain access to your system again and to stop them releasing all your data on the internet.	Availability, Confidentiality	Customers, Our reputation, Profits, The Business	Ransomware is a very popular and effective way for criminals to make money because it involves the human element – one single click. Criminals will always aim to get into a system from the easiest point of entry which tends to be us! It is rare for ransomware criminals to want to change the data so it is not usually an integrity (but that doesn't mean never) issue. Ransomware is also usually a very public breach and many companies who have impacted have actually found out about the hack from staff posting images on social media before calling the IT department.
You previously operated a very open policy which meant everyone, regardless of the job they did, could access and edit customer data; from the cleaner right to the CEO, to save time on people always having to ask for access permissions.	Confidentiality, Integrity	Customers, Our reputation, Profits, The Business	Companies should operate on a premise of 'least privilege.' This is a bit like being on a 'need to know' basis. Do you need to know about a customer's dog if you handle the marketing of the company? No. So by the means of least privilege, you would not have access to those systems. This keeps the business and our customers safe as only those who need to know certain information, have access to it. We don't want to risk people disclosing private information or changing things either on purpose or accidently.
A rival company don't like how successful you've become so they've set so much traffic to your website that your system can't cope and it crashes! None of your customers can access your website and it's been down for an hour now.	Availability	Customers, Our reputation, Profits, The Business	Rival businesses have been known to cause disruption to their competition by paying criminals (or sometimes doing it themselves) to takedown another business' website. This is known as a DDoS attack, or Distributed Denial of Service. This involves sending packets of information to the target which causes the system to be overloaded and crash. The impact of a site being down can run into millions and is often a very public even, causing reputational damage.