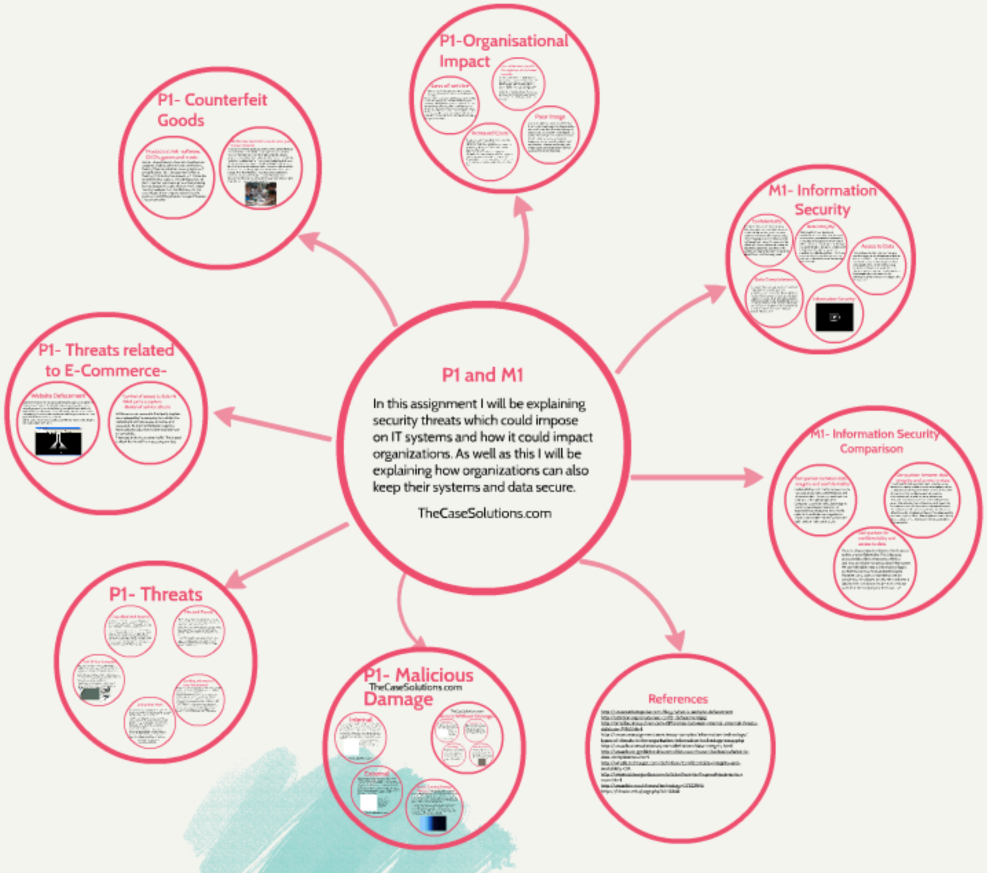


P1 and M1

In this assignment I will be explaining security threats which could impose on IT systems and how it could impact organizations. As well as this I will be explaining how organizations can also keep their systems and data secure.

P1-Organisational Impact

P1- Counterfeit Goods

M1- Information Security

P1- Threats related to E-Commerce-

M1- Information Security Comparison

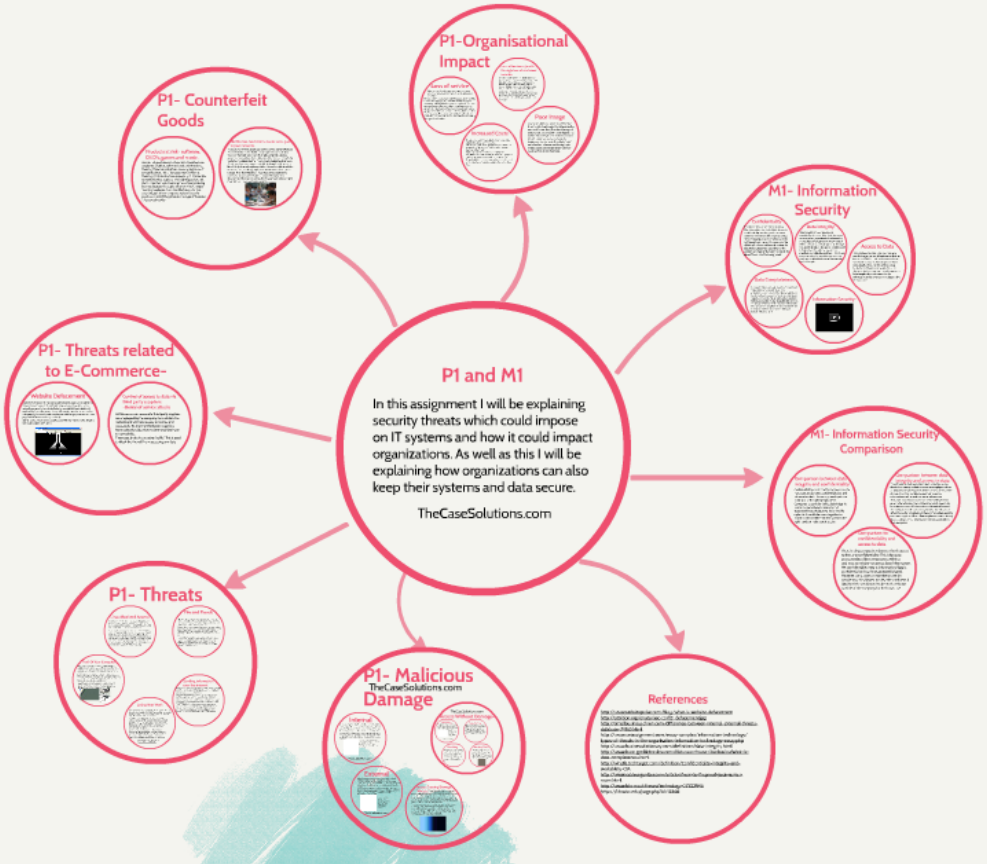
P1- Threats

P1- Malicious Damage

References

WHAT A DIFFERENCE A WORD MAKES: UNDERSTANDING THREATS TO PERFORMANCE IN A VUCA WORLD

TheCaseSolutions.com



P1 and M1

In this assignment I will be explaining security threats which could impose on IT systems and how it could impact organizations. As well as this I will be explaining how organizations can also keep their systems and data secure.

TheCaseSolutions.com

P1-Organisational Impact

P1- Counterfeit Goods

M1- Information Security

P1- Threats related to E-Commerce-

M1- Information Security Comparison

P1- Threats

P1- Malicious Damage

TheCaseSolutions.com

References

WHAT A DIFFERENCE A WORD MAKES: UNDERSTANDING THREATS TO PERFORMANCE IN A VUCA WORLD

P1 and M1

In this assignment I will be explaining security threats which could impose on IT systems and how it could impact organizations. As well as this I will be explaining how organizations can also keep their systems and data secure.

P1- Malicious Damage

Internal

Internal malicious damage can be both from accidents and attacks. Internal malicious damages happen within the business/company. Internal accidents that could occur could be employees within an E-Commerce site copying important information from a database table into an email for troubleshooting purposes and accidentally include external email addresses in the recipient list. To support this a 2012 study has showed that 51% of employees duplicate confidential information with a company printer.

However, sometimes employees don't make a mistake. Employees use their access and privilege to damage their company they work within, they often can sell the information on the black market to infiltrators who work for outside intelligence.

This is a news article which shows how a Starbucks employee takes advantage of personal customer information. She uses the advantage to make a copy of a customers card which she later on uses to buy groceries.

Access Without Damage-

Phisihing

Phishing is where someone tries to obtain another persons personal information such as website details, bank details and many more. Users are likely to get an email in their junk mail asking for bank details which users should not give out. Because these emails look like legitimate company emails users are likely to trust them and enter their personal information.

This is an example of a phishing email, it shows how the 'bank' requires some personal information from the user in order to continue with their bank account.

http://[illegible]/phishing/[illegible] example.gif

Piggy Backing

Piggy backing is the name used for when an intruder tries to use someone's wireless without them knowing. If a users wireless is secured with a weak password it is very likely and easy to break into. From this it slows down a users internet and the person 'piggy backing' on the wireless can download illegal software so that it cannot be traced back to them.

Hacking

Hacking is where a person is able to break codes and passwords to gain unauthorised entry to computer systems. A lot of hacking cases have no specific fraudulent intent yet just enjoy the challenge. Yet a lot of hackers do have the intent to commit fraud, steal personal data/ information.

Passwords are a popular way to prevent any hacking. Companies should make sure that their staff have their own User ID and Password to gain access to the system. This reduces the risk of outsiders being able to get into the system and damage any data. It also allows different employees to access different data.

Firewalls are also designed to prevent hackers from intruding onto a computer system. They work by controlling the data which is sent on a computer ingoing and outgoing based on a set of rules.

Identity Theft

Identity theft is where a person steals another persons personal information and uses it. For example they could obtain someones home address, name, phone number to be able to do multiple things such as open bank accounts etc. In big companies it is very important to lock all the doors where the servers are stored to prevent intruders from accessing the servers and causing damage to it.

Identity theft is tackled under a number of related acts. These are; Theft Act 1968 such as a property, Data Protection Act 1998 which protects personal data, Identity Cards Act 2006 which describes identity theft crimes and identity fraud relating to ID cards and the Fraud Act 2006 which makes it illegal to assume another persons identity.

External

External malicious damage can also be both from accidents and attacks. External damage happens outside of the business/company.

An example of an external accident is a power cut of a server that stores software licenses for other servers. Without licenses, data backup software may not function at is scheduled time meaning the database open to irreversible corruption

The most common and worst external attack is from skilled hackers. Computer hackers are able to find network vulnerabilities or socially manipulate insiders to get past a number of outer network defenses. Once they get past the network defenses hackers are able to steal important information which makes the business lose information and data.

Hackers steal 1.3 million Orange customers' personal data

This is an example of an external malicious damage. Hackers were able to gain access within the phone company Orange and steal 1.3 million of orange customers personal mobile data.

Access Causing Damage- Viruses

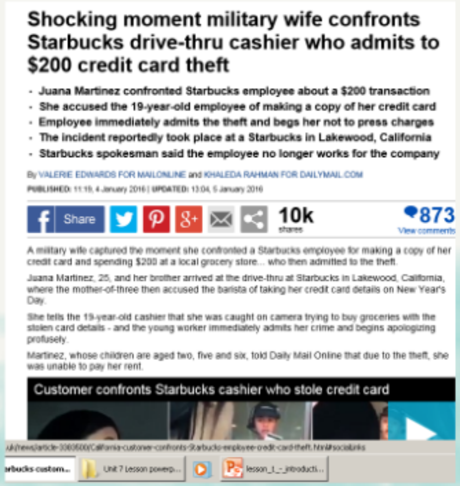
Access causing damage is where a computer virus has been targeted at specific computer programs. Because it has targeted specific programs this prevents them from downloading/opening up and it sometimes even directs a user to another service. This type of attack is commonly done on users internet browsers.

The most common way to prevent a virus is using an anti-virus software. These are used to find any viruses and try to get rid of them. Before doing this. the software tries to detect if there any there first. if the software does find one it will notify the user to ask what you would want to happen to it. It is important for users to keep updating and checking for viruses because they could occur very quickly.

Internal

Internal malicious damage can be both from accidents and attacks. Internal malicious damages happen within the business/company. Internal accidents that could occur could be employees within an E-Commerce site copying important information from a database table into an email for troubleshooting purposes and accidentally include external email addresses in the recipient list. To support this a 2012 study has showed that 51% of employees duplicate confidential information with a company printer.

However, sometimes employees don't make a mistake. Employees use their access and privilege to damage their company they work within, they often can sell the information on the black market to infiltrators who work for outside intelligence.



Shocking moment military wife confronts Starbucks drive-thru cashier who admits to $200 credit card theft

- Juana Martinez confronted Starbucks employee about a $200 transaction
- She accused the 19-year-old employee of making a copy of her credit card
- Employee immediately admits the theft and begs her not to press charges
- The incident reportedly took place at a Starbucks in Lakewood, California
- Starbucks spokesman said the employee no longer works for the company

By VALERIE EDWARDS FOR MAILONLINE and KHALEDA RAHMAN FOR DAILYMAIL.COM

PUBLISHED: 11:19, 4 January 2016 | UPDATED: 13:04, 5 January 2016

A military wife captured the moment she confronted a Starbucks employee for making a copy of her credit card and spending $200 at a local grocery store... who then admitted to the theft.

Juana Martinez, 25, and her brother arrived at the drive-thru at Starbucks in Lakewood, California, where the mother-of-three then accused the barista of taking her credit card details on New Year's Day.

She tells the 19-year-old cashier that she was caught on camera trying to buy groceries with the stolen card details - and the young worker immediately admits her crime and begins apologizing profusely.

Martinez, whose children are aged two, five and six, told Daily Mail Online that due to the theft, she was unable to pay her rent.

Customer confronts Starbucks cashier who stole credit card

Share
10k
shares
873
View comments
uk/news/article-3380600/California-customer-confronts-Starbucks-employee-credit-card-theft.html#socialinks
arbucks-custom...
Unit 7 Lesson powerp...
lesson_1_-_introducti...

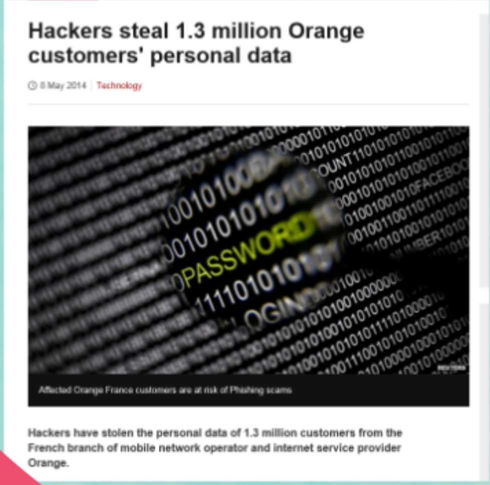
This is a news article which shows how a Starbucks employee takes advantage of personal customer information. She uses the advantage to make a copy of a customers card which she later on uses to buy groceries.

External

External malicious damage can also be both from accidents and attacks. External damage happens outside of the business/company.

An example of an external accident is a power cut of a server that stores software licenses for other servers. Without licenses, data backup software may not function at is scheduled time meaning the database open to irreversible corruption.

The most common and worst external attack is from skilled hackers. Computer hackers are able to find network vulnerabilities or socially manipulate insiders to get past a number of outer network defenses. Once they get past the network defenses hackers are able to steal important information which makes the business lose information and data.



Hackers steal 1.3 million Orange customers' personal data

8 May 2014 | Technology

Affected Orange France customers are at risk of Phishing scams

Hackers have stolen the personal data of 1.3 million customers from the French branch of mobile network operator and internet service provider Orange.

This is an example of an external malicious damage. Hackers were able to gain access within the phone company Orange and steal 1.3 million of orange customers personal mobile data.

Ac
at
pr
sc
is

Th
Th
do
sc
to
fo

ks.

res
tware may
ersible

Computer
insiders to
network
s the

Access Causing Damage-Viruses

Access causing damage is where a computer virus has been targeted at specific computer programs. Because it has targeted specific programs this prevents them from downloading/opening up and it sometimes even directs a user to another service. This type of attack is commonly done on users internet browsers.

The most common way to prevent a virus is using an anti-virus software. These are used to find any viruses and try to get rid of them. Before doing this, the software tries to detect if there any there first, if the software does find one it will notify the user to ask what you would want to happen to it. It is important for users to keep updating and checking for viruses because they could occur very quickly.

err_write ,("ERROR: unable to
malicious virus; Install;
,("Boot sector was successful
ScanObjReq SCAN
ScanObjRep SC
SCAN_REQ STR
; binder
55

ge

Access Without Damage–

Phisihing

Phishing is where someone tries to obtain another persons personal information such as website details, bank details and many more. Users are likely to get an email in their junk mail asking for bank details which users should not give out. Because these emails look like legitimate company emails users are likely to trust them and enter their personal information.

This is an example of a phishing email, it shows how the 'bank' requires some personal information from the user in order to continue with their bank account.

http:/www.freecomputerzone.com/phishing/hsbcphsishing-example1.gif

Piggy Backing

Piggy backing is the name used for when an intruder tries to use someone's wireless without them knowing. If a users wireless is secured with a weak password it is very likely and easy to break into. From this it slows down a users internet and the person 'piggy backing' on the wireless can download illegal software so that it cannot be traced back to them.

Hacking

Hacking is where a person is able to break codes and passwords to gain unauthorized entry to computer systems. A lot of hacking cases have no specific fraudulent intent yet just enjoy the challenge. Yet, a lot of hackers do have the intent to commit fraud, steal personal data/ information.

Passwords are a popular way to prevent any hacking. Companies should make sure that their staff have their own User ID and Password to gain access to the system. This reduces the risk of outsiders being able to get onto the system and damage any data. It also allow different employees to access different data.

Firewalls are also designed to prevent hackers from intruding onto a computer system. They work by controlling the data which is run on a computer ingoing and outgoing network based on a set of rules.

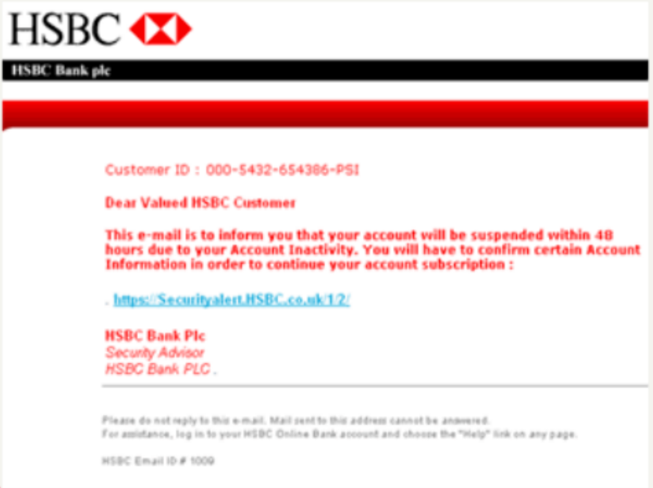
Identity Theft

Identity theft is where a person steals another persons personal information and uses it. For example they could obtain someones home address, name, phone number to be able to do multiple things such as open bank accounts etc. In big companies it is very important to lock all the doors where the servers are stored to prevent intruders from accessing the server and causing damage to it.

Identify theft is tackled under a number of related act. These are; Theft Act 1968 such as a property, Data Protection Act 1998 which protects personal data, Identity Cards Act 2006 which describes identity theft crimes and identity fraud relating to ID cards and the Fraud Act 2006 which makes it illegal to assume another persons identity.

Phisihing

Phishing is where someone tries to obtain another persons personal information such as website details, bank details and many more. Users are likely to get an email in their junk mail asking for bank details which users should not give out. Because these emails look like legitimate company emails users are likely to trust them and enter their personal information.



HSBC

HSBC Bank plc

Customer ID : 000-5432-654386-PSI

Dear Valued HSBC Customer

This e-mail is to inform you that your account will be suspended within 48 hours due to your Account Inactivity. You will have to confirm certain Account Information in order to continue your account subscription :

. https://Securityalert.HSBC.co.uk/1/2/

HSBC Bank Plc
Security Advisor
HSBC Bank PLC .

Please do not reply to this e-mail. Mail sent to this address cannot be answered.
For assistance, log in to your HSBC Online Bank account and choose the "Help" link on any page.

HSBC Email ID # 1009

This is an example of a phishing email, it shows how the 'bank' requires some personal information from the user in order to continue with their bank account.

http:/www.freecomputerzone.com/phishing/hsbcphsishing-example1.gif