Cyber Security: Case Study

Chatter - Activity Pack

pwc

Table of Contents

Overview

Company Overview

Fledgling social media platform, 'Chatter' launched in September 2017. Its main users are 13-21 year olds. Users can:

- Share photos and post status updates
- Send messages via a private chat
- Play games with other users, and make in-app purchases

Their head office is in Birmingham, and they employ 30 people. All staff members have a staff pass to enter the building, and have a company iPhone and laptop. All staff have received an email outlining the best practice for cyber security but this was not read by everyone and staff have not undertaken any mandatory training.

Your Challenge

Recently, Chatter had a minor cyber security threat. They are therefore looking to improve their cyber security and are looking for a cyber security specialist to help. PwC are in competition with other firms to be selected by Chatter to help them. You are part of the PwC Cyber Team who will have to pitch our proposal to Chatter for how we could resolve their cyber security threats.

In your teams, you will have to **prepare a pitch** to Chatter that outlines:

1. **Chatter's cyber risks - which one of these do you think Chatter should focus on first?**

2. **Which team you think Chatter needs to help them improve their Cyber Security and why.**

"For companies, successful cyber attacks could result in material fines, legal actions, operational outages, and adverse impact on stakeholders. Individuals need to be confident that vast amounts of personal data submitted to organisations is safe and that the digital services on which they increasingly depend are reliable."

Dr Richard Horne, PwC Specialist Partner for Cyber Security

Research and Background Information

Chatter's recent cyber security incident

A staff member left their laptop on the train while commuting home. The laptop was picked up by someone and they were able to gain access to it. Fortunately, the member of staff had reported it missing and the laptop was remotely wiped. Chatter cannot be sure if any data was accessed before the laptop was remotely wiped.

Important Government Regulations

GDPR - General Data Protection Regulation

As of Spring 2018, changes to GDPR came into force, designed to better protect consumer and personal data. Any organisation holding data must:

- Gain consent from the consumer to process their data

- Anonymise the data collected to protect privacy

- Provide data breach notifications

- Safely handle the transfer of data across borders. Transferring data outside Europe. The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third-party countries or international organisations, to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

- Require certain companies to appoint a data protection officer to oversee GDPR compliance

If these rules are not followed, then companies face hefty fines of up to €20million.
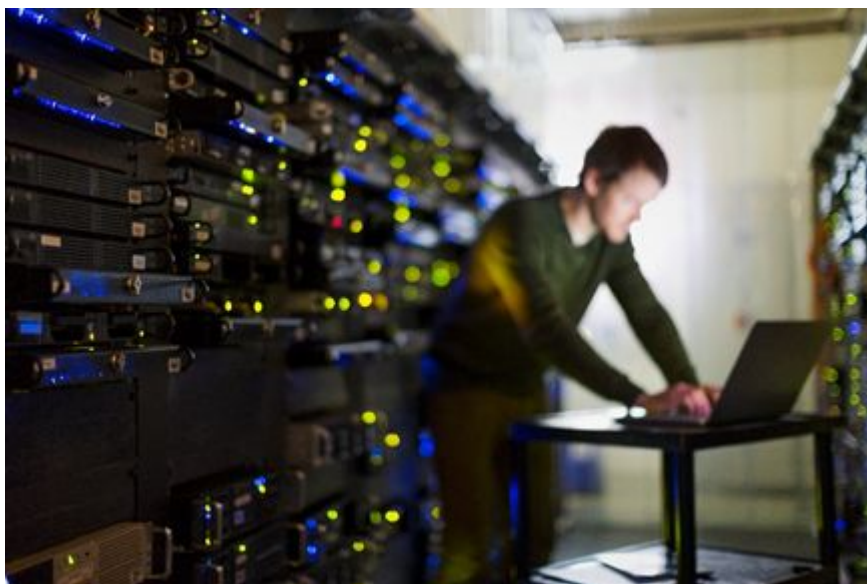
PwC's Cyber Security Teams

Core Advisory

We help organisations from all sectors **operate securely in the digital world.** Our expertise enables clients to **resist, detect and respond to cyber-attacks**. Our Core Advisory team, works globally to support clients across the public, private and financial sectors, helping them to understand and reduce their cyber risks.

Some of the services offered to clients include:

- Assessing and measuring their exposure to cyber security risk

- Developing a strategy and vision for tackling cyber security

- Designing and implementing the secure IT systems a client needs to be secure

- Designing and putting in place security training and awareness programmes

- Gaining experience of security operations and incident response

Ethical Hackers

The ethical hacking team will work within the boundaries defined to **legally penetrate the company with their permission**. This exercise is designed to **help companies understand their technical security weaknesses, to provide specific recommendations** to clients to help them keep hackers out.

- Ethical hacking to expose vulnerabilities in client IT systems

- Identifying and monitoring malicious activity on client networks

- Actively tracking and disrupting cyber threat actors and seeking out new ones

- Investigating networks which attackers have compromised and removing threat actors.

Crisis Team

Cyber crisis team help companies **prepare for, respond to and recover from a cyber-security crisis**. A crisis may include events that prevent the business from operating. This team works with their people, to define these plans or understand what work has already been done to prepare for these types of events. The team also **facilitate exercises to help companies test their approach**, helping the team **to practise for real events** and can turn up to help you 'steady the ship' when under attack.

Benefits of this service include:

- Help companies consider what they would do when under attack. The team may help simulate this and ensure non-technical members of staff know how to respond.
- Help companies to understand and develop key access controls to their critical systems and assets during a crisis or active cyber threat.
- Helping the company to 'steady the ship' when under attack.

Cyber Threat Team

This team **tracks and gathers information on cyber threats across the globe that could target the industry or type of company**. The team uses various methods to gain a well-rounded view of the company's threat landscape, and can help them to understand those that could be motivated to attack the company.

- Threat intelligence - look into political situations and try and detect threat actors e.g. hacking groups.
- Track and gather intelligence to share with companies.
- Analyse the virus and malware used for information.

**Identity and Access Management**

Companies often grant access to information and assets to staff even if it is not relevant to that member of staff's role. **It is important for companies to follow the principle of least privilege - only granting access to the systems necessary for each member of staff's role.** This helps to reduce the risk of attackers gaining access to critical systems by compromising a less protected user account used in another area in the business. If all user accounts only have access to what they need, this should help contain compromises to their area of origin, to help prevent them from spreading throughout the business.

- Help companies to understand who in their company has access to what information
- Help them to improve their governance and management of their access granted throughout the business.

Recent News Articles

Could a similar attempt be made to access Chatter's customer base?
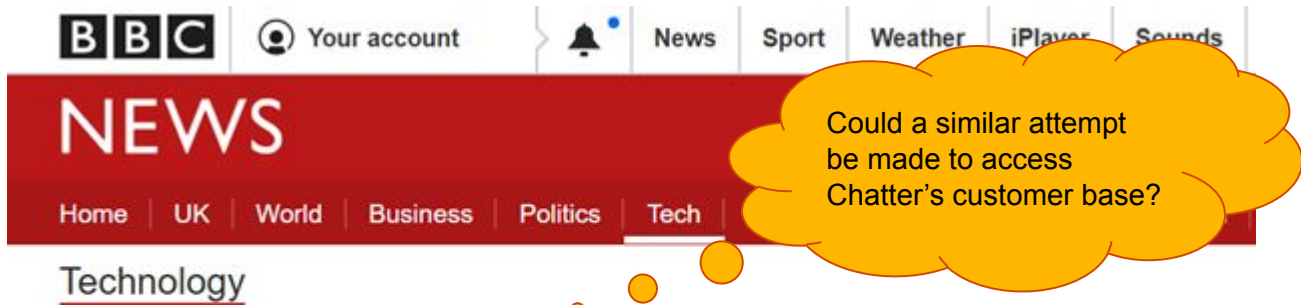
Facebook security breach: Up to 50m accounts attacked

Facebook says almost 50 million of its users were left exposed by a security flaw.

The company said attackers were able to exploit a vulnerability in a feature known as "View As" to gain control of people's accounts. The breach was discovered on Tuesday, Facebook said, and it has informed police. Users that had potentially been affected were prompted to re-log-in on Friday.

The flaw has been fixed, wrote the firm's vice-president of product management, Guy Rosen, adding all affected accounts had been reset, as well as another 40 million "as a precautionary step". Facebook - which saw its share price drop more than 3% on Friday - has more than two billion active monthly users.

The company has confirmed to reporters that the breach would allow hackers to log in to other accounts that use Facebook's system, of which there are many. This means other major sites, such as AirBnB and Tinder, may also be affected. The firm would not say where in the world the 50 million users are, but it has informed Irish data regulators, where Facebook's European subsidiary is based. The company said the users prompted to log-in again did not have to change their passwords. "Since we've only just started our investigation, we have yet to determine whether these accounts were misused or any information accessed. We also don't know who's behind these attacks or where they're based. He added: "People's privacy and security is incredibly important, and we're sorry this happened." The company has confirmed that Facebook founder Mark Zuckerberg and its chief operating officer Sheryl Sandberg were among the 50 million accounts affected.

Web Link to full article: https://www.bbc.co.uk/news/technology-45686890

News   **Opinion**   **Sport**   **Culture**   **Lifestyle**   More ⌄

UK World Business Football UK politics Environment Education Society Science **Tech** Global development Cities Obituaries

Hacking

⊘ This article is more than **4 years old**

Xbox live and Playstation attack: Christmas ruined for millions of gamers

Sony and Microsoft networks suffering outages after an apparent denial of service attack that rendered them useless for millions

What is the level of risk of attack from a hacking group for Chatter?

Millions of people could not use their games consoles for a second day as disruption on the Xbox Live and Sony Playstation networks continued after an apparent cyber-attack.

A group calling itself Lizard Squad claimed responsibility for bringing down both networks on Christmas Eve, which could have affected nearly 160 million gamers.

Even an intervention by eccentric internet entrepreneur Kim Dotcom, who offered the hackers free lifetime use of his file storage service, does not appear to have ended the attack. Known as a distributed denial of service, or DDOS, the attack is overloading the systems of both services by generating fake access requests…..

….Sony has not responded to requests for comment. Its official Twitter account repeatedly responded to users' complaints with the same message, but did not acknowledge an attack: "We are aware that some users are unable to access at the moment. Our technicians are working to fix this issue." The official PSN status was listed as "offline" at the time of writing, while Xbox Live is "limited".

Microsoft would not comment on the cause of network problems but a spokesman told the Guardian: "We are aware some users are unable to sign in to Xbox Live. Our teams are working to resolve the issue. Visitxbox.com/support for status updates."

The news is damaging for Microsoft but particularly for Sony, which suffered a high profile hack in early December by a group called Guardians of Peace. Stolen emails were leaked and published, revealing embarrassing exchanges between executives and celebrities, while stolen files and even film scripts left the company so exposed it has reportedly reverted to using fax machines and paper in its offices….

Web Link to the full article:
https://www.theguardian.com/technology/2014/dec/26/xbox-live-and-psn-attack-christmas-ruined-for-millions-of-gamers

Support The Guardian
Available for everyone, funded by readers
Contribute → Subscribe →

Search jobs   Dating   🔒 Sign in   🔍 Search ∨

The Guardian

UK edition ∨

News   **Opinion**   **Sport**   **Culture**   **Lifestyle**   More ∨

Retail industry   ● This article is more than 9 months old

Superdrug targeted by hackers who claim to have 20,000 customer details

Health and beauty retailer advises online customers to change their passwords

What are the issues with hackers gaining personal details?

Superdrug has advised its online customers to change their passwords after the high street chain was targeted by hackers claiming to have stolen the personal details of thousands of people.

The health and beauty retailer told customers it had been contacted by a group on Monday evening claiming to have obtained the details of 20,000 customers, including names, addresses, dates of birth and phone numbers.

Superdrug said in the email to customers the company had only seen evidence so far that 386 of the accounts had been compromised.
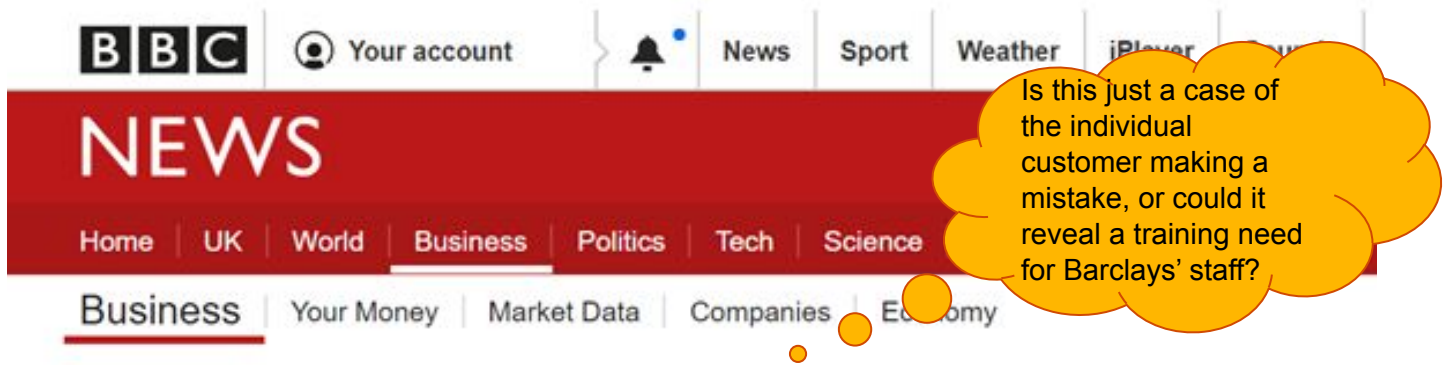
A spokeswoman said: "The hacker shared a number of details with us to try to prove he had customer information – we were then able to verify they were Superdrug customers from their email and log-in."...

...Superdrug is the latest high street retailer to report a data breach. Last month Dixons Carphone said personal data belonging to 10 million customers may have been accessed illegally last year, nearly 10 times as many as the firm initially thought.

The electronics retailer had estimated the attack – one of the biggest-ever data breaches – involved 1.2m personal records when it first reported the breach in June.

Web Link to the full article:
https://www.theguardian.com/business/2018/aug/22/superdrug-targeted-by-hackers-who-claim-to-have-20000-customer-details

BBC | Your account | News | Sport | Weather | iPlayer

NEWS

Home | UK | World | Business | Politics | Tech | Science

Business | Your Money | Market Data | Companies | Economy

Is this just a case of the individual customer making a mistake, or could it reveal a training need for Barclays' staff?

'Fraudsters exploited my angry tweet' By Kevin Peachey. 28 November 2018

A bank customer was tricked into transferring money by fraudsters who pretended to be responding to his angry Twitter post about poor service. Writer Mike Tinmouth was furious with the process and time taken to open a business account with Barclays. He expressed his frustration in a public tweet - which was seized on by fraudsters who posed as the bank in an attempt to trick him out of £8,000. Fraud experts say con-artists are becoming skilled at impersonation…

... [In the Twitter post] he even posted an email that he received from the bank which he felt was unprofessional and had to confirm was genuine. The bank urged him to delete this public post. All this information, together with some personal details that were already available about him online, was enough for fraudsters to mimic the bank and appear to know details of the case.

Soon after the Twitter exchange, he received another email apologising for the poor service and offering to deal with his case. This time the message was from a fraudster posing as his bank.

After various exchanges, he was provided with details of his "new" account, and he started to transfer money from his personal current account with a different bank. The transfer was blocked, saving Mr Tinmouth from losing the £8,000 he intended to move between the two accounts. Barclays said that customers should always be careful about posting details in public, and that it had a system of ensuring customers dealt with the bank's social media teams on private channels. No-one should transfer money to a new account without having all the relevant paperwork and full control of the account…

Web Link to the full article:
https://www.bbc.co.uk/news/business-46309561

Mike Tinmouth @michaeltinmouth (Follow)

@BarclaysBizChat your help team are utterly incompetent. Trying to set up a business account is proving impossible when your staff are initially vague, then don't reply to emails and then refuse to assist.

9:26 AM - 16 Oct 2018

Barclays UK Help @BarclaysUKHelp · Oct 16
Replying to @michaeltinmouth
Hi Mike, could you tell me a little more about what has happened? Corrina

Pitch Planning

On an individual level, cyber security is about the individual users' personal protection. For example, sharing and tagging pictures is a personal cyber risk for an individual as they are revealing personal information. These are important to consider as individual users, however, for this task, bear in mind that PwC is advising Chatter on risks to its business. This could certainly be influenced by user's personal cyber security risks but try to consider the risks to the business' security as a whole such as the personal data Chatter collects and how they store it is. Keep this in your mind throughout the task.

1) **What are the company's key assets?** What do they need to protect? (An asset is an item of property owned by a person or company. These could be physical assets or information they hold).

Physical assets	Potential cyber security threats to assess
1) Company iPhones for all staff members	
2) Staff and their awareness of cyber security (this is known as their cyber security culture).	
3)	
4)	
5)	

Informational assets	Potential cyber security threats to assess
1) Users must give their bank details when signing up to pay in-app games.	
2)	
3)	

2) **How have other companies been affected by cyber security attacks?** What can Chatter **learn** from these experiences?

Company Name	Description of their cyber security attack	How might this be a risk for Chatter?

3) From your tables of assets and examples of other companies who have been affected by cyber security, what do you think are the **two main areas of cyber security improvements** that Chatter should consider?

4) **Which one of the PwC Cyber teams do you think can help them?** If you think multiple teams could help, pick the one that you think they should prioritise and use first.

Presentation Structure

Introduction: Introduce your team and what you are presenting about

Main body:

1. Outline Chatter's cyber risks, which one of these do you think chatter should focus on first?
2. Which team do you think Chatter needs to help them improve their cyber security and why?
3. How will you persuade the client to invest in PwC's service?

Conclusion: Summarise the biggest risk and how you intend to help

Glossary

Cyber security: are the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation (such as to access or destroy sensitive data or steal money).

Individual cyber security risk: the individual users' personal protection. For example, sharing and tagging pictures is a personal cyber risk for an individual as they are revealing personal information.

Business level cyber security risk: concerned with the risks to things the business has responsibility for i.e. their assets. For example, businesses should ensure the security of the personal data they collect, how they store it, who has access to it and who/how they share it.

GDPR (General Data Protection Regulation): a regulation in EU law on data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas.

Asset: an asset is an item of property owned by a person or company. These could be physical assets or information they hold.

Cyber Security Case Study