Business: LogMeIn Talks About the Future of Business Risk

Created by esldebates.com

Warmer questions

1. From what you can remember what have been the largest business failures over the last 5 years?
2. What might a company do to lower its exposure to risk?
3. Can risk ever be reduced?

Created by esldebates.com

Introduction

Business risk refers to a company's or organization's exposure to factors that could reduce profitability or cause it to fail. A business risk is anything that jeopardises a company's capacity to meet its financial objectives. There are a number of things that might come together to produce business risk. It is sometimes a firm's senior leadership or management that puts the organisation in a position where it is more vulnerable to danger.

However, the source of risk can occasionally be found outside of a corporation. As a result, it is impossible for a business to totally eliminate risk. However, there are ways to reduce the total hazards of running a business, and most organisations do so by implementing a risk management strategy.

Reading 1/4

Effective security and intelligence structures to prevent remote attacks are a challenge that governments and businesses around the world are becoming increasingly alive too. Technology has changed the way we have traditionally thought about our world's borders. Threats to computer security are increasingly organised and multinational, with no respect for geographical precincts. The pressing need to invest in the right technology and equipment is now crucial for national security, development, and privacy worldwide.

In a computing context, security comprises cybersecurity and physical security. Cybersecurity issues are becoming a day-to-day struggle for businesses. Trends indicate a vast increase in hacked and breached data from mobile and IoT devices. Additionally, recent research suggests that most companies have unprotected data and weak cybersecurity practices in place, making them vulnerable to data loss or misuse.

Created by esldebates.com

Reading 2/4

Cybersecurity is the protection of internet-connected systems –including hardware, software, and data– from cyberattacks. They are both used to protect against unauthorised access to data centers and other computerised systems. Information security, which is designed to maintain the confidentiality, integrity, and availability of data, is a subset of cybersecurity.

Experts say that over the last year, the severity of malicious cyber activity has significantly increased worldwide.

Reading 3/4

While in negotiations to sell itself to Verizon in September 2016, the once leading Internet titan, Yahoo, announced it had been the victim of the biggest data breach in history in 2014. The attack compromised the real names, addresses, email, dates of birth, and telephone numbers of 500 million users. The company said most of the passwords involved had been compromised using the bcrypt algorithm. In October of 2017, Yahoo announced that all 3 billion user accounts had been compromised.

Created by esldebates.com

Reading 4/4

Most of the passwords were protected by the SHA-1 hashing algorithm. The company said hackers got into the company network using the credentials of three corporate employees, and had full inside access for 229 days, during which time they were able to collect 20 years of data.

In the UK, the impact of major cyber security incidents, such as the WannaCry attack, affected 48 NHS Trusts. To meet this challenge in the UK, the government has put in place its National Cyber Security Strategy 2016-2021, supported by £1.9bn of investment.

Created by esldebates.com

Questions from the reading section:

1. The regular salary for a cybersecurity professional is £5,000 more than the average technology job (CW). But, are there enough qualified people to fill these roles?
2. Data breaches happen daily, in too many places at once to keep count. If this pace persists, who will protect our digital assets from cyberattacks?
3. Impact can determine what constitutes a huge breach versus a small one. Can nuclear weapons be hacked?

Created by esldebates.com

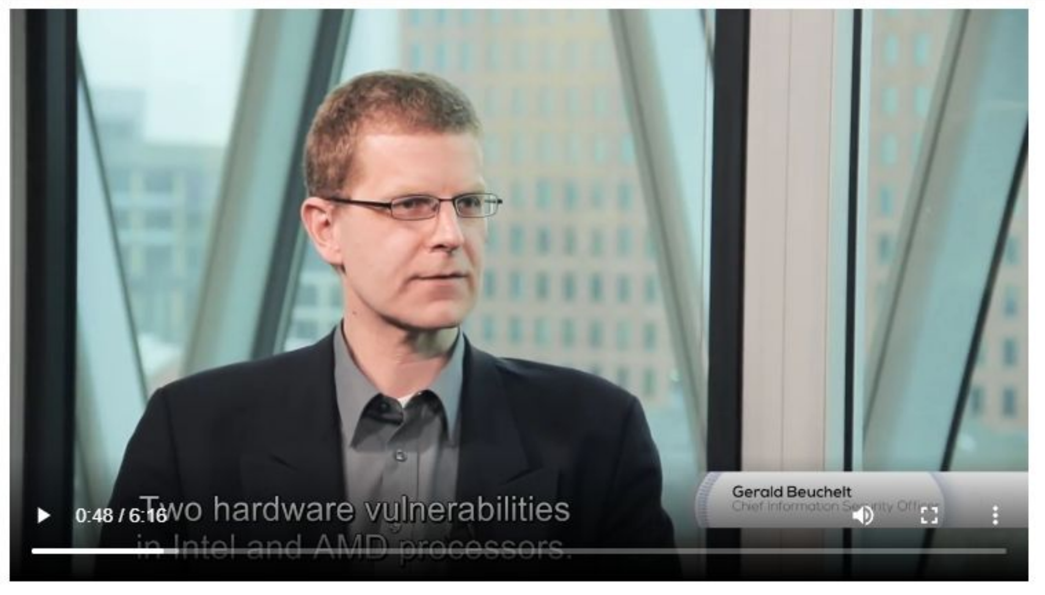
Vocabulary matching: Match the vocab on the left with the correct definitions on the right.

Vocabulary	Meaning
Crosshairs	costing a lot; expensive.
Vulnerability	inexpensive; reasonably priced.
Sensitive data	a written ordinance of Congress, or another legislative body; a statute.
Industrial espionage	“he was suspected of passing sensitive information to other countries”.
Awareness	spying is directed toward discovering the secrets of a rival manufacturer or other industrial company.
Costly	refers to steps that computer users can take to improve their cybersecurity and better protect themselves online.
SMEs	the quality or state of being exposed to the possibility of being attacked or harmed, either physically or emotionally
Affordable	to swear that something is completely truthful, genuine, or sincere.
Cyber hygiene	“The category of micro, small and medium: sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding 50 million euro, and/or an annual balance sheet total not exceeding 43 million euro.”
Act	the quality or state of being aware: knowledge and understanding that something is happening or exists.
Hand on heart	a person or thing likely to cause damage or danger
Threat	a fine wire or thread in the focus of the eyepiece of an optical instrument used as a reference line in the field or for marking the instrumental axis: used figuratively to describe someone or something being targeted as if through an aiming device having crosshairs: … in the crosshairs this political season.

Created by esldebates.com

Video: LogMeIn talks about the Future of Business Risk

“Anyone who fails to protect their corporate networks shouldn’t be surprised if they lose sensitive data”, says Gerald Beuchelt, Chief Information Security Officer of LogMeIn, a software company, which, as well as online collaboration and remote maintenance solutions, also specialises in password and identity management.



Two hardware vulnerabilities in Intel and AMD processors.

Video Link: https://esldebates.com/business-logmein-talks-about-the-future-of-business-risk/

Created by esldebates.com

Video: LogMeIn talks about the Future of Business Risk

Watch the video and then answer the questions below:

1. What does the acronym GDPR stand for?
2. Has 2018 been a dangerous cyber year?
3. Where has artificial intelligence been used?
4. Who is in the crosshairs of these attacks?
5. Why do companies need to protect themselves?
6. How well are companies' defenses set up?
7. Can large companies protect themselves better than SMEs?
8. To set up protection systems: What does it mean for SMEs?
9. Who is Gerald Beuchelt?

Created by esldebates.com

Benefits of cyber protection

1. It protects users −individuals, business and government− against data theft.
2. It protects systems against viruses, worms, spyware and other unwanted programs.
3. It guards computers and portable devices from being hacked.
4. Cyber protection minimises devices’ freezing and crashes.

Disadvantages of cyber protection

1. Software installation and maintenance could be costly for the average user and SMEs.
2. Firewalls can be difficult to configure correctly.
3. Firewalls configured incorrectly may block users from performing certain activities on the Internet.
4. Cyber protection software may need constant updating.

Created by esldebates.com

Potential debating topics

1. Viruses, worms, spyware and other unwanted programs are developed by the cyber security companies in order to have users buy their products.
2. Cybercrimes are a real threat. We need cyber protection companies to keep us safe from hackers.
3. Security software updates are a waste of time and money. Updates bring no additions to software and do not help prevent or fix any problems.
4. Keeping our security software updated is a must. Updates protect users from unwanted breaches and enhance the computing experience.
5. Cyber security professionals wage an ongoing war of intelligence and wits against hackers. Cyber-attack risk on nuclear weapons systems is now relatively high.
6. There is no realistic way to hack a weapon of massive destruction. Nuclear weapons are not connected to the Internet for security reasons. It requires physical access and deactivating multiple independent safety systems to launch a missile, for example.

Created by esldebates.com

Conclusion

Due to the growth in Internet use, the number of cyber security breaches experienced by businesses and individuals has increased rapidly in recent years. Both businesses and users have adopted relaxed security practices that offer hackers the perfect occasion to launch their attacks. Unscrupulous scammers and hackers have, as a result, plenty of opportunities to intercept and misuse the information. Business leaders and individuals need to recognise the various threats involved in the Internet and establish cyber security policies and procedures to minimise their risks.

Created by esldebates.com

Answers

Answers: Vocab section

Vocabulary	Meaning
Crosshairs	a fine wire or thread in the focus of the eyepiece of an optical instrument used as a reference line in the field or for marking the instrumental axis: used figuratively to describe someone or something being targeted as if through an aiming device having crosshairs: … in the crosshairs this political season.
Vulnerability	the quality or state of being exposed to the possibility of being attacked or harmed, either physically or emotionally
Sensitive data	“he was suspected of passing sensitive information to other countries”.
Industrial espionage	spying is directed toward discovering the secrets of a rival manufacturer or other industrial company.
Awareness	the quality or state of being aware: knowledge and understanding that something is happening or exists.
Costly	costing a lot; expensive.
SMEs	“The category of micro, small and medium: sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding 50 million euro, and/or an annual balance sheet total not exceeding 43 million euro.”
Affordable	inexpensive; reasonably priced.
Cyber hygiene	refers to steps that computer users can take to improve their cybersecurity and better protect themselves online.
Act	a written ordinance of Congress, or another legislative body; a statute.
Hand on heart	to swear that something is completely truthful, genuine, or sincere.
Threat	a person or thing likely to cause damage or danger

Created by esldebates.com

Video section answers

1. The acronym GDPR stands for European General Data Protection Regulation.
2. Yes, it has. At the beginning of the year, Spectre and Meltdown faced some issues and there were two hardware vulnerabilities in Intel and AMD.
3. Artificial intelligence has been used in the criminal field.
4. We all are. We all have personal or financial data that could be of interest to cyber-criminals or other attackers.
5. Companies need to protect themselves because they have very sensitive data (and company secrets) that could be of interest for industrial espionage.
6. In the last few years the attacks have become public and have led to a new level of awareness in terms of cyber security in companies.
7. Yes, they can. Large companies have the means to protect themselves better, to detect attacks and to react appropriately. Protection systems or processes are too costly for the small and medium-sized enterprises (SMEs) to afford.
8. SMEs have to create a clear security concept which meets their requirements but is still affordable.
9. He is Chief Information Security Officer of LogMeIn.