BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF COMMERCE

DEPARTMENT OF MARKETING

E-MARKETING 2 MKT 513

JUN 2025

TIME: 3 HOURS

INSTRUCTIONS TO CANDIDATES

1. Answer questions number one and any other three.
2. Start each question on a fresh page.
3. No cell Phones are allowed in the Examination Room.

QUESTION ONE

Read the case study below and answer the questions that follow:

Case Study: Low-Risk, High-Profit Opportunities Drive Up Cybercrime

Costs for victims jump as cyber-attacks target government sites

Washington - it does not cost much to become a cybercriminal

A $500 investment buys MPack, software developed by Russian hackers, allowing users to steal credit card data or retail vouchers. Renting software robots known as bonnets, which spew out spam (unsolicited commercial or bulk e-mail), can generate $7,700 in net weekly profits, according to Peter Guerra of Black Hat, a digital security company.

Cybercriminals can profit from their activities because inadequate national and global legal frameworks make it difficult for law enforcement authorities to catch them. The ever-increasing reliance of businesses, governments and individuals on computer networks creates more opportunities for cybercrime, and its low-risk/high-profit nature attracts an increasing number of cybergangs, according to Karthik Kannan of Purdue University's Krannert School of Management.

Complaints of online crime hit a record high of more than 27,000 in United States in 2008, according to the internet Crime Complaint Centre, a public-private research group. The centre estimates that Internet fraud reached $265 million that year.

"If we want to make progress against cybercrime, we need to change the economics of cyber security" Kannan said. This means raising the cost and risk for criminals while making defences cheaper, a task that he said is not easy.

THE PRICE OF CYBER-ATTACKS

Many corporate executives do not truly appreciate the gravity of cyber threats, according to experts. Laws, regulation and policies have lagged behind increasing crime as the use of the Internet has grown exponentially, several studies say.

In developed countries, companies may strengthen cyber defences only when relevant regulations are introduced, according to a 2009 study commissioned by MacAfee Inc., a computer software security developer. Fewer than a third of U.S companies are committed to adopt the best cyber practices because most companies fail to see the link between cyber security and good management, according to the annual industry survey conducted by PricewaterhouseCoopers LLP. Half the U.S executives surveyed did not even know how much money their firms had lost through attacks, the survey said.

Nailing down the scope of financial losses is difficult. Bruce Schneier, Founder and Chief Technology Officer of Counterpane, a computer security company, said a modest infection by malicious software could cost a small company $83,000 a year. "The larger a company is, and the deeper an infection goes, the higher the costs", he wrote in a 2005 report.

On average, cybercrime costs a company more than $500,000 a year, according to Kevin Coleman, Management Consultant. A 2007 Government Accountability Office report estimates the total U.S. business losses due to cyber-attacks exceed $117.5 billion per year. This may be just the tip of the iceberg, many analysts say.

Scott Borg, who established and runs the U.S. Cyber Consequences unit, an independent research group, said the economic impact of essential corporate information lost to cyber thieves "is much bigger ... than credit card fraud, which is pretty big", on the other hand, he said, many claims about the costs of cyber-attacks, particularly denial-of-service attacks, are wildly inflated.

Cybercrime also causes intangible losses such as tarnished reputations and lost customer trust. Some cyber-incidents go unnoticed for months and, even when detected, may be coerced up by technical staff or executives to avoid liability issues. As attackers become more business savvy, they steal information essential to companies' competitive positions.

The international consulting firm Delloitte & Touche LLP estimates the global private-sector losses in intellectual property due to cybercrime at around $1 trillion. The Mcfee report noted how difficult it is to measure the impact of a weakened company's competitive position because a reduced market share may only manifest itself after several years.

STRENGTHENING CYBERDEFENSES

Cyberdefenses need not be expensive. The Central intelligent Agency's chief of information assurance, Robert Bigman, told an October 2008 conference that between 80 and 90 percent of attacks could be prevented through "due diligence".

Trying to fashion an effective response to attacks has become more challenging as increasing numbers of government computer systems are infected with malicious software. The Department of Homeland and Security logged 5,499 such incidents in 2008- a 40 percent increase over the previous year. Deputy Defense Secretary William Lynn says this department spent more than $100 million defending its networks during the first six months of 2008.

Attacks on critical infrastructure are another huge concern. A cyber-attack on the electricity grid, which could cut the power supply to one-third for the country for three months, would generate losses to $800 billion, according to Borg. But the total expenditures necessary to recover from these losses, including the costs of restoring, restarting, and making up lost production, would be much greater - around $3 trillion, he added.

The global economic crisis could weaken existing defences. Spending and staff cuts could lead to more porous defences and increased opportunities for cybercrime that may attract laid off software engineers, Borg said.

(a) Outline the impact of cybercrime on e-marketing. **[10 marks]**

(b) Examine how an organisation can minimise customers' fears of transacting online. Motivate your answer. **[10 marks]**

(c) State and explain five (5) different cybercrimes that have negatively impacted on e-marketing. **[10 marks]**

(d) Explain at least five (5) different measures that can be implemented by an organisation to protect its computer system from cybercrime. **[10 marks]**

QUESTION TWO

Explain the strategies that can be adopted by online book sellers to increase their sales giving examples. **[20 Marks]**

QUESTION THREE

Examine the aspects that determine the quality of a good website using the 7Cs framework. **[20 Marks]**

QUESTION FOUR

Discuss different forms of marketing communications offered by the Internet. **[20 Marks]**

QUESTION FIVE

Analyse the main benefits and challenges of establishing intranets and extranets in an organization like BUSE **[20 Marks]**

QUESTION SIX

Discuss how Customer Relationships can be established online. **[20 Marks]**