So you think you know security

1 **Canadian firms are less confident this year in their firm's IT security posture than in 2006.** True or false?

2 **The majority of data breaches can be traced back to:**
- **A** Malicious insider threats
- **B** Innocent insider threats
- **C** Outside online fraudsters
- **D** Angry consumers

3 **A business development organization has engaged the in-house IT department to develop a custom application for their external clients. The IT department in turn has outsourced the creation of the application to a third party. Which group has the authority to determine the level of access privileges to the application?**
- **A** The application/business owners
- **B** The IT department
- **C** The outsourcing third party
- **D** The board of directors

4 **Which of the following are not Canadian Privacy regulations?**
- **A** PIPEDA
- **B** PHIPA
- **C** HIPAA
- **D** FIPPA

5 **An enterprise information security strategy cannot be successfully implemented without the following stakeholders' involvement and buy in?**
- **A** The IT department
- **B** Senior management
- **C** The business owners
- **D** All of the above

6 **According to industry research, who places the highest priority on IT security in Canadian firms?**
- **A** The CEO and other business executives
- **B** The CIO and other IT executives
- **C** IT managers
- **D** IT practitioners

7 **Which of the following elements is not key to quantifying risk?**
- **A** Severity of impact
- **B** Likelihood of occurrence
- **C** Breadth of threat landscape

8 **What risk factors face CIOs of the 21st Century?**
- **A** Regulatory compliance
- **B** Outsourcing and off-shoring
- **C** Growing merger and acquisition activity
- **D** All of the above

9 **Not only is the number of data thefts and losses due to security breaches continuing to grow at an alarming rate, but the resulting monetary impact of these losses is also skyrocketing. So-called 'enterprise data loss' cost businesses how much last year? (all figures in US dollars)**
- **A** $20 billion
- **B** $50 billion
- **C** $100 billion
- **D** $200 billion

10 **According to some estimates, 90% of companies that lose their data due to improper information data storage and insufficient information-recovery mechanisms go out of business within:**
- **A** 2 years
- **B** 4 years
- **C** 6 years
- **D** No direct correlation to a company's demise

11 **Which of the following specifications or protocols is most closely associated with federated identity services?**
- **A** Security Assertion Markup Language (SAML)
- **B** Lightweight Directory Authentication Protocol (LDAP)
- **C** Multiple Input Multiple Output (MIMO)
- **D** IEEE 802.13

12 **Insider data breaches alone cost businesses an average of how much per company each year?**
- **A** $500,000
- **B** $1.2 million
- **C** $3.4 million
- **D** $6.8 million

13 **The PCI Data Security Standard centres around six high-level control objectives – essentially, targets for security that bolster the protection of credit card information. Broad security requirements support each control objective. Which of the following is NOT a correct requirement?**
- **A** Use vendor-supplied defaults for system passwords and other security parameters on your network
- **B** Encrypt transmission of cardholder data across open, public networks
- **C** Assign a unique ID to each person with computer access
- **D** Track and monitor all access to network resources and cardholder data

14 **What is the average cost for a help desk to perform a simple password reset for users?**
- **A** $10
- **B** $18
- **C** $38
- **D** $58

15 **Most hackers will go to great lengths to avoid detection. Some will go as far as patching and maintaining systems for you to keep them healthy so you don't do any investigation**

that may catch them. True or false?

16 It is easier than the IT department often leads users to believe to remove 'Administrator' privileges from end users. True or false?

17 Antivirus is effective at stopping nearly all malware. True or false?

18 With a victim population of 10 million, identity theft is now the fastest growing crime in North America. True or false?

19 What percentage of all data loss results from unprotected lost or stolen computers?

A 25 or less
B 25-55
C 55-75
D 75+

20 What is the estimated average cost to an organization of a security breach?

A $10,000
B $50,000
C $150,000
D $200,000+

21. According to Ekos Research Associates, less than a third of Canadian businesses are either still in the process of complying with PIPEDA or have yet to begin. True or false?

22 Since its creation by the FBI in 2000, roughly how many complaints has the the Internet Crime Complaint Center logged?

A 100,000
B 500,000
C 1,000,000
D 2,000,000+

23 Which of the following can drastically reduce the incidence of online identity theft and other online fraud?

A Username and password
B Two-factor authentication
C Trojan authentication
D Anti-virus software

24 Which of the following is NOT true about NAC (Network Access Control)?

A Stops unauthorized, guest or non-compliant systems accessing your network
B Ensures all computers conform to a defined security policy
C Virtually eliminates backdoors that can be exploited by hackers
D Protects against threats posed by unauthorized, unknown, compromised, or misconfigured computers

25 Which has been identified as the top country hosting malware-infected Web pages?

A China
B United States
C Canada
D Russia

26 Which of the following file types is not a virus carrier?

A EXE
B PDF
C COM
D BAT

27 What makes Behavioral Genotyping technology an important part of a security infrastructure?

A It identifies programs that will behave maliciously before they execute
B It prevents users from opening an email if it contains malicious programs
C It blocks spyware, viruses, malware and unwanted applications at the gateway
D It monitors and controls what Web sites users access through the network

28 Which of the following is not a negative effect resulting from the growth of Web 2.0?

A Infected sites
B Identity theft
C Lack of productivity
D Infected email attachments

29 Which of the following is not a recommended action for companies to take to protect themselves from being infected by a zero-day attack?

A Deploy intrusion detection/intrusion prevention systems and regularly update antivirus software
B Ensure that security patches are up to date and that they are applied to all vulnerable applications in a timely manner
C Limit the amount of time Internet access is permitted, thereby reducing the chances of threat exposure
D Use an Internet security solution that combines antivirus, firewall, intrusion detection, and vulnerability management for maximum protection

30 Which of the following threats is the most difficult for security solutions to detect and eliminate?

A Polymorphic virus
B Macro virus
C Trojan horse
D Malware

31 Security risks, such as spyware and adware, are complex problems that require a multipronged security strategy in order to maximize the effectiveness of the security solution. Which of the following should an effective antispyware solution encompass to protect IT infrastructures?

A Breadth of detection
B Thoroughness of removal
C Proactive prevention
D All of the above

32 One way to ensure your company's endpoint is protected is to validate every endpoint that attaches to the corporate network to determine if access should be granted? True or false?

33 What percentage of devices on a typical company network are unmanaged?

A 0-10%
B 11-20%
C 21-30%
D More than 3

34 Which of the following is not an important element of an effective data loss prevention plan:

A Protect against the loss of sensitive, proprietary or regulated content by real-time filtering of messages
B Enable endpoint users to save mission critical information to personal data storage devices, like

flash/jump drives, MP3 players, or SD cards

C Monitor and alert communications which violate content sharing

D Audit and provide discovery capabilities against a comprehensive archive

35 In which location should most corporations NOT have sensitive data stored?

A Data centre or third-party hosting site

B Branch office

C Employees laptops

D None of the above

36 Fibre optic cable does not lend itself to secure communications systems because it is fairly easy to tap. True or false?

37 Tape back-up and real-time data mirroring are key components of a secure disaster recovery plan. True or false?

38 What caused the great Northeast blackout of 2003?

A Lightning striking a power plant in Northern New York

B Failure to trim trees near power lines in Ohio

C A small outage in Michigan, cascading from there throughout the Northeast

D Faulty power lines in New Jersey

39 Which of the following regulations about personal information is not mandatory under PIPEDA?

A Information must be collected with consent and for a reasonable purpose

B Information must be used and disclosed for the limited purpose for which it was collected

C Information must be accessible for inspection and correction

D Information is not required to be stored securely so long as it is compliant

This article is provided by IT World Canada. Please visit us at www.itworldcanada.com

SECURITY TEST ANSWERS:

**IT practitioners recently edged out CIOs and other IT executives in the priority that they assign to security. CEOs place security quite low on their priority stack.*

1.	FALSE	9.	C	17.	FALSE	25.	A
2.	A	10.	A	18.	TRUE	26.	B
3.	A	11.	A	19.	D	27.	A
4.	C	12.	B	20.	D	28.	D
5.	D	13.	A	21.	TRUE	29.	C
6.	C*	14.	D	22.	C	30.	A
7.	C	15.	TRUE	23.	B	31.	D
8.	D	16.	TRUE	24.	C	32.	TRUE

33.	D
34.	B
35.	D
36.	FALSE
37.	TRUE
38.	B
39.	D

RATING:

35-39 correct	head of the class; apply now for the top job at CSIS
25-34 correct	good showing; you've earned your security stripes
15-24 correct	a passing grade, but you could use a refresher
5-14 correct	in need of remediation; beg the CISO for some tutoring
0-4 correct	there's an opening for you at Tim Horton's

SECURITY TEST CONTRIBUTORS

CIO Canada would like to thank the following individuals and organizations for contributing the questions and answers to the National CIO Security Test. We have relied on these contributors for the validity of their answers.

- CMS Consulting, Brian Bourne
- Computer Associates, Sumner
- Blount
- CRYPTOCard
- Deloitte Canada
- IDC Canada, David Senf
- Fusepoint
- Juniper
- Microsoft Canada, Bruce Cowper
- Novell Canada, Ross Chevalier
- RSA, The Security Division of EMC
- Sophos
- Symantec
- Toronto Hydro Telecom, David Dobbin
- WhiteHat Inc., Tom Slodichak