第四周词汇理解作业 （2016 年 12 月真题）

①The ocean is heating up. That's the conclusion of a new study that finds that Earth's oceans now___1___ heat at twice the rate they did 18 years ago. Around half of ocean heat intake since 1865 has taken place since 1997, researchers report online in Nature Climate Change.

②Warming waters are known to___2___to coral bleaching（珊瑚白化） and they take up more space than cooler waters, raising sea___3___While the top of the ocean is well studied, its depths are more difficult to___4___The researchers gathered 150 years of ocean temperature data in order to get a better___5___of heat absorption from surface to seabed. They gathered together temperature readings collected by everything from a 19th century___6___of British naval ships to modem automated ocean probes. The extensive data sources,___7___with computer simulations （计算机模拟）, created a timeline of ocean temperature changes, including cooling from volcanic outbreaks and warming from fossil fuel___8___.

③About 35 percent of the heat taken in by the oceans during the industrial era now resides at a___9___of more than 700 meters, the researchers found. They say they're___10____whether the deep-sea warming canceled out warming at the sea's surface.

A. absorb	**B.** combined	C. contribute	D. depth
E. emissions	F. excursion	G. explore	H. floor
I. heights	J. indifferent	K. levels	L. mixed
M. picture	N.unsure	O. voyage	

第四周长篇阅读作业 （2016 年 12 月真题）

Can Burglars Jam Your Wireless Security System?

[A]Any product that promises to protect your home deserves careful examination. So it isn't surprising that you'll find plenty of strong opinions about the potential vulnerabilities of popular home-security systems.

[B]The most likely type of burglary（入室盗窃）by far is the unsophisticated crime of opportunity, usually involving a broken window or some forced entry. According to the FBI, crimes like these accounted roughly two-thirds of all household burglaries in the US in 2013.The wide majority of the rest were illegal, unforced entries that resulted from something like a window being left open. The odds of a criminal using technical means to bypass a security system are so small that the FBI doesn't even track those statistics.

[C]One of the main theoretical home-security concerns is whether or not a given system is vulnerable to being blocked from working altogether. With wired setups, the fear is that a burglar（入室盗贼）might be able to shut your system down simply by cutting the right cable. With a wireless setup, you stick battery-powered sensors up around your home that keep an eye on windows, doors, motion, and more. If they detect something wrong while the system is armed, they'll transmit a wireless alert signal to a base station that will then raise the alarm. That approach will eliminate most cord-cutting concerns—but what about their wireless equivalent, jamming? With the right device tuned to the right frequency, what's to stop a thief from jamming your setup and blocking that alert signal from ever reaching the base station?

[D]Jamming concerns are nothing new, and they're not unique to security systems. Any device that's built to receive a wireless signal at a specific frequency can be overwhelmed by a stronger signal coming in on the same frequency. For comparison, let's say you wanted to “jam” a conversation between two people—all you'd need to do is yell in the listener's ear.

[E] Security devices are required to list the frequencies they broadcast on—that means that a potential thief can find what they need to know with minimal Googling. They will, however, need so know what system they're looking for. If you have a sign in your yard declaring what setup you use, that'd point them in the right direction, though at that point, we're talking about a highly targeted, semi-sophisticated attack, and not the sort forced-entry attack that makes up the majority of burglaries. It's easier to find and acquire jamming equipment for some frequencies than it is for others.

[F] Wireless security providers will often take steps to help combat the threat of jamming attacks. SimpliSafe, winner of our Editor's Choice distinction, utilizes a special system that's capable of separating incidental RF interference from targeted jamming attacks. When the system thinks it's being jammed, it'll notify you via push alert（推送警报）. From there, it's up to you to sound the alarm manually.

[G] SimpliSafe was singled out in one recent article on jamming, complete with a video showing the entire system being effectively bypassed with handheld jamming equipment. After taking appropriate measures to contain the RF interference to our test lab, we tested the attack out for ourselves, and were able to verify that it's possible with the right equipment. However, we also verified that SimpliSafe's anti-jamming system works. It caught us in the act, sent an alert to my smartphone, and also listed our RF interference on the system's event log. The team behind the article and video in question make no mention of the system, or whether or not in detected them.

[H]We like the unique nature of that software. It means that a thief likely wouldn't be able to Google how the system works, then figure out a way around it. Even if they could, SimpliSafe claims that its system is always evolving, and that it varies slightly from system to system, which means there wouldn't be a universal magic formula for cracking it. Other systems also seem confident on the subject of jamming. The team at Frontpoint addresses the issue in a blog on its site, citing their own jam protection software and claiming that there aren't any documented cases of successful jam attack since the company began offering wireless security sensors in the 1980s.

[I] Jamming attacks are absolutely possible. As said before, with the right equipment and the right know-how, it's possible to jam any wireless transmission. But how probable is it that someone will successfully jam their way into your home and steal your stuff?

[J] Let's imagine that you live in a small home with a wireless security setup that offers a functional anti-jamming system. First, a thief is going to need to target your home, specifically. Then, he's going to need to know the technical details of your system and acquire the specific equipment necessary for jamming your specific setup. Presumably, you keep your doors locked at night and while you're away. So the thief will still need to break in. That means defeating the lock somehow, or breaking a window. He'll need to be jamming you at this point, as a broken window or opened door would normally release the alarm. So, too, would the motion detectors in your home, so the thief will need to continue jamming once he's inside and searching for things to steal. However, he'll need to do so without tripping the anti-jamming system, the details of which he almost certainly does now have access to.

[K]At the end of the day, these kinds of systems are primarily designed to protect against the sort of opportunistic smash-and-grab attack that makes up the majority of burglaries. They're also only a single layer in what should ideally be a many-sided approach to securing your home, one that includes common sense things like sound locks and proper exterior lighting at night. No system is impenetrable, and none can promise to eliminate the worst case completely. Every one of them has vulnerabilities that a knowledgeable thief could theoretically exploit. A good system is one that keeps that worst-case setting as improbable as possible while also offering strong protection in the event of a less-extraordinary attack.

36. It is possible for burglars to make jamming attacks with the necessary equipment and skill.

37. Interfering with a wireless security system is similar to interfering with a conversation.

38. A burglar has to continuously jam the wireless security device to avoid triggering the alarm, both inside and outside the house.

39. SimpliSafe provides devices that are able to distinguish incidental radio interference from targeted jamming attacks.

40. Only a very small proportion of burglaries are committed by technical means.

41. It is difficult to crack SimpliSafe as its system keeps changing.

42. Wireless devices will transmit signals so as to activate the alarm once something wrong is detected.

43. Different measures should be taken to protect one's home from burglary in addition to the wireless security system.

44. SimpliSafe's device can send a warning to the house owner's cellphone.

45. Burglars can easily get a security device's frequency by Internet search.

第四周长篇阅读作业 （2016 年 12 月真题）

①Recently I attended several meetings where we talked about ways to retain students and keep younger faculty members from going elsewhere.

②It seems higher education has become an industry of meeting-holders whose task it is to "solve" problems—real or imagined. And in my position as a professor at three different colleges, the actual problems in educating our young people and older students have deepened, while the number of people hired—not to teach but to hold meetings—has increased significantly. Every new problem creates a new job for an administrative fixer. Take our Center for Teaching Excellence. Contrary to its title, the center is a clearing house（信息交流中心）for using technology in classrooms and in online courses. It's an administrative sham（欺诈）of the kind that has multiplied over the last 30 years.

③I offer a simple proposition in response: Many of our problems—class attendance, educational success, student happiness and well-being—might be improved by cutting down the bureaucratic（官僚的）mechanisms and meetings and instead hiring an army of good teachers. If we replaced half of our administrative staff with classroom teachers, we might actually get a majority of our classes back to 20 or fewer students per teacher. This would be an environment in which teachers and students actually knew each other.

④The teachers must be free to teach in their own way—the curriculum should be flexible enough so that they can use their individual talents to achieve the goals of the course. Additionally, they should be allowed to teach, and be rewarded for doing it well. Teachers are not people who are great at and consumed by research and happen to appear in a classroom. Good teaching and research are not exclusive, but they are also not automatic companions. Teaching is an art and a craft, talent and practice; it is not something that just anyone can be good at. It is utterly confusing to me that people do not recognize this, despite the fact that pretty much anyone who has been a student can tell the difference between their best and worst teachers.

46.What does the author say about present-day universities?

A)They are effectively tackling real or imagined problems.

B)They often fail to combine teaching with research.

C)They are over-burdened with administrative staff.

D)They lack talent to fix their deepening problems.

47.According to the author, what kind of people do universities lack most?

A)Good classroom teachers.

B)Efficient administrators.

C) Talented researchers.

D) Motivated students.

48.What does the author imply about the classes at present?

A)They facilitate students' independent learning.

B)They help students form closer relationships.

C)They have more older students than before.

D)They are much bigger than is desirable.

49.What does the author think of teaching ability?

A)It requires talent and practice.

B)It is closely related to research.

C)It is a chief factor affecting students' learning.

D)It can be acquired through persistent practice.

50.What is the author's suggestion for improving university teaching?

A)Creating an environment for teachers to share their teaching experiences.

B)Hiring more classroom teachers and allowing them to teach in their own way.

C)Using high technology in classrooms and promoting exchange of information.

D)Cutting down meetings and encouraging administrative staff to go to classrooms.