FT Business School Concern

Respond to hacker attacks from the MBA

The lack of network security experts in the business world is not news. Not so well known is that companies also lack the technical knowledge to deal with hacker attacks on the executives.

Collection

Updated April 24, 2017 06:56 The Financial Times **de la Bradshaw**

When Nuno Sebastião went to the London Business School (LBS) MBA program, his eyes were beyond the traditional career of consulting and investment banking. In fact, he decided to fight against hackers.

This is not for purely ideological reasons. He has witnessed a hacker attack on the computer network where his former employer, the European Space Agency, has trained him to discover a profitable niche market: getting people with business and communication skills into cybersecurity This technical field.

He said: "(even) in 2009, for me, there is obviously a problem to be solved."

After graduation, he created a company that identified fraudulent payment transactions, Feedzai, who was the same as his two engineers from Portugal. "My mission is to identify business issues," he said, adding that his company is headquartered in California and has 150 employees and plans to increase to 300 this year.

Sebastian is far from the only MBA student or graduate who has found opportunities in the field of cybercrime. Many people are becoming interested in mastering the skills needed by future leaders to combat hacking, and some colleges incorporate cybersecurity into their MBA programs.

It is recognized that there is a lack of technical level of network security experts. However, a less well-known problem is the lack of management who has the technical knowledge to be able to deal with hacker attacks.
Gianluca D'Antonio, chairman of the FCC Group's chief information officer and president of the Spanish Association for Information Advancement for Information, said: "When a company employs a network of security workers, their technical ability is strong, but the lack of soft skills and business intelligence.
He said that those who work in the field of cybersecurity can not introduce the relevant risks to the board. "It's about communication, about management, and everyone is talking about the incredible numbers of the future, but nobody is right to discuss digital risk.

Guard against future hacking
José Esteves, a professor of information systems at the IE Business School in Madrid, teaches digital students an innovative course to MBA students who invade students in the classroom and demonstrate how easy it is to them. This year in October, the business school will also be the future of business leaders to launch a master's degree in network security courses.
At the same time, the Iese Business School in Barcelona invited Deloitte to help provide a network security course in one of the MBA electives.
"(Cyber security) can not be commissioned, it is about corporate security and reputation," said Javier Zamora, senior lecturer at the IESE Business School Information System.
Even the safest networks are vulnerable to cyber attacks, as Yahoo and Sony data leaks show. According to Grant Thornton, 2016, hacker attacks resulted in global corporate losses of $ 280 billion, and the

company described reputation damage as a major risk to the company.

Stuart Madnick, professor of IT and engineering systems at the MIT Sloan School of Management, says the high-level consequences of cyber attacks mean that they must be handled by executives who direct the company's strategy, rather than to the technical staff.
Madnick taught network security in the college's MBA program, saying that companies need extremely flexible management thinking because hackers may be more unpredictable than natural disasters.
"The hurricane will not change the direction because you know you are coming, but the network attacker can."

David Upton, a professor of operations management at Saïd Business School at Oxford University, says that a large part of the problem for managers is the complexity of the problem.
He added that cyber attacks include acts of various acts, from government-supported espionage, to trivial acts aimed at obtaining monetary benefits.
However, he added that for many business leaders, the prevention of catastrophic negative events is "fundamentally unattractive." "When you mention this problem, managers are often at a loss."
However, he said that the risk must be addressed at the board level and include all corporate departments.

The duties of the board of directors
Professor Upton helped design executive-level executive courses and coached a compulsory course at the Saide Business School MBA

program. "There is a global industry that is working on it, and some of our managers are sleeping."

Prof. Zamora of the IESE Business School also believes that with the spread of technology, cybersecurity issues will penetrate all aspects of a company from human resources to insurance risks.

At present, security is often reduced to an afterthought, the latest product to market speed into a priority task. "Every time you design a product or service, you have to build a network security at the beginning," the professor said. "It's an integral part of the design."

At the Harvard Business School, Associate Professor Ben Edelman defended the scholars' reluctance to discuss these issues because the technical level was incompatible with the overall management strategy. But that did not stop him. He said: "I think these issues are really important, so threw himself."

In Edelman's lesson, he presented a hypothetical case where a company's system was hacked and students had to make a decision as to how managers should respond. This case involves a core ethical issue: should the administrator shut down the company's network to prevent further incursions, or would he hope to be resolved behind the scenes without telling the client?

"Obviously, these questions are hard to answer, but that does not mean we should not solve it," said Professor Edelman.

Sebastian compared this to the 2008 financial crisis. "No one was interested, and then the whole world collapsed, and then people had set up various mechanisms to guard against the outbreak of the crisis, which was exactly the same as cyber security.

Translator / Liang Yan Sang

From http://www.ftchinese.com/story/001072309

FT商学院 关注

应对黑客攻击从MBA抓起

企业界缺乏网络安全专家并非新闻。 不那么为人所知的是，企业还缺乏拥有技术知识、能够对付黑客攻击的高管。

收藏

更新于2017年4月24日06:56 英国《金融时报》 德拉●布拉德肖

1 全文

他补充称，网络攻击包括各种行为，从政府支持的间谍活动，到旨在获得金钱好处的琐碎犯罪行为。

然而，他补充称，对于很多企业领袖而言，防范灾难性负面事件"从根本上说是没有吸引力的"。"在你提到这个问题时，管理者往往神情茫然。"

然而，他表示，这种风险必须在董事会层面得到应对，并包括所有公司部门。

董事会的职责

厄普顿教授帮助设计了董事会层面的高管课程，并在萨伊德商学院MBA课程中执教一门必修课程。 他说："有一个全球性行业正致力于此，而我们有些管理者却在昏睡。"

IESE商学院的萨莫拉教授还认为，随着技术的传播，网络安全问题将渗透到一家公司的方方面面，从人力资源到保险风险。

目前，安全往往沦为一个事后的想法，将最新产品推向市场的速度变成优先任务。"每当你设计产品或服务，一开始就必须构建网络安全，"教授表示，"这是设计方面不可或缺的一部分。"

在哈佛商学院(Harvard Business School)，副教授本•埃德尔曼(Ben Edelman)为学者们不愿讨论这些问题做出辩护，因为技术层面与总体管理策略格格不入。 但这并未阻止他。 他表示："我认为这些问题确实很重要，于是全身心投入了。"

在埃德尔曼的授课中，他提出了一个假想案例，一家公司的系统遭到黑客攻击，学生们不得不就管理者应该如何回应做出决定。 这个案例涉及到一个核心的道德问

题：管理者是应该关闭公司网络阻止进一步入侵，还是希望在不告知客户的情况下在幕后解决？

埃德尔曼教授表示："显然，这些问题回答起来很难，但这并不意味着我们不应解决。"

塞巴斯蒂昂将这种情况比作2008年金融危机之前。"没有人感兴趣，接着整个世界坍塌了，后来人们设立了各种机制以防范危机再次爆发。这与网络安全一模一样。"

译者/梁艳裳

FT商学院 关注

应对黑客攻击从MBA抓起

企业界缺乏网络安全专家并非新闻。 不那么为人所知的是，企业还缺乏拥有技术知识、能够对付黑客攻击的高管。

收藏

更新于2017年4月24日06:56 英国《金融时报》 德拉●布拉德肖

1 全文

他补充称，网络攻击包括各种行为，从政府支持的间谍活动，到旨在获得金钱好处的琐碎犯罪行为。

然而，他补充称，对于很多企业领袖而言，防范灾难性负面事件"从根本上说是没有吸引力的"。"在你提到这个问题时，管理者往往神情茫然。"

然而，他表示，这种风险必须在董事会层面得到应对，并包括所有公司部门。

董事会的职责

厄普顿教授帮助设计了董事会层面的高管课程，并在萨伊德商学院MBA课程中执教一门必修课程。 他说："有一个全球性行业正致力于此，而我们有些管理者却在昏睡。"

IESE商学院的萨莫拉教授还认为，随着技术的传播，网络安全问题将渗透到一家公司的方方面面，从人力资源到保险风险。

目前，安全往往沦为一个事后的想法，将最新产品推向市场的速度变成优先任务。“每当你设计产品或服务，一开始就必须构建网络安全，”教授表示，“这是设计方面不可或缺的一部分。”

在哈佛商学院(Harvard Business School)，副教授本•埃德尔曼(Ben Edelman)为学者们不愿讨论这些问题做出辩护，因为技术层面与总体管理策略格格不入。 但这并未阻止他。 他表示：“我认为这些问题确实很重要，于是全身心投入了。”

在埃德尔曼的授课中，他提出了一个假想案例，一家公司的系统遭到黑客攻击，学生们不得不就管理者应该如何回应做出决定。 这个案例涉及到一个核心的道德问题：管理者是应该关闭公司网络阻止进一步入侵，还是希望在不告知客户的情况下在幕后解决？

埃德尔曼教授表示：“显然，这些问题回答起来很难，但这并不意味着我们不应解决。”

塞巴斯蒂昂将这种情况比作2008年金融危机之前。“没有人感兴趣，接着整个世界坍塌了，后来人们设立了各种机制以防范危机再次爆发。这与网络安全一模一样。”

译者/梁艳裳