Stuart Madnick of MIT: 'The Hacker has more Advantages in a Cyber Attack

Stuart Madnick

Working Paper CISL# 2019-16

June 2019

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

FROM https://epoca.globo.com/stuart-madnick-do-mit-hacker-tem-mais-vantagens-num-ataque-virtual-23725987

STUART MADNICK OF MIT: 'THE HACKER HAS MORE ADVANTAGES IN A CYBER ATTACK'

One of the world's leading specialists in combating cybercrime, the Massachusetts Institute of Technology professor says companies are poorly prepared to fight hackers

White Leo

08/06/2019 - 3:00 p.m.

Stuart Madnick Photo: WS / WS

Professor Stuart Madnick, 74, is probably the world's leading expert on the effects of cyber crimes on business. Madnick researches the mishaps of technology since joining the prestigious Massachusetts Institute of Technology (MIT) as a student in 1972. Five decades later, Madnick heads a university department - the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity (or Interdisciplinary Consortium for Improving Cyber Security Critical Infrastructure)

dedicated to studying strategies for companies to create defenses against hackers.

Customers include large businesses such as the Nasdaq stock exchange, technology giants IBM and Phillips, and mining company Vale. In five decades, he has published more than 380 books and has run a half-world as a guest lecturer at universities such as Harvard, Nanyang (Singapore), Newcastle (UK), Technion (Israel) and Victoria (New Zealand) to address the cyber risks inherent in business. For the expert, how companies are idealized to succeed, and be functional to their customers, little organization time is dedicated to what may not work - like a successful hacker attack. So more than investing in new anti-virus software, Madnick advocates a change in the mental model of companies.

In the following interview, given during a visit to Sao Paulo where he spoke at the headquarters of the recently launched digital bank C6, which has been using the Madnick department to build systems that are resistant to cyber attacks from the beginning, the expert tells why change internal cultures of an organization more difficult than investing in systems.

What does the department do at MIT?

We usually do not worry about searching for new hardware or software and firewalls, since many companies are already researching this subject. The reality is that 70-90% of cyber attacks are made by people of the company itself. Usually unintentionally. For example, an employee who forgets his password writes it on paper and leaves it somewhere. This employee is not a bad person, but gave a bad person the opportunity to access important information in your company. The focus of my study is the corporate management strategy to combat cybercrime. Few people pay attention to them, but they are the most important.

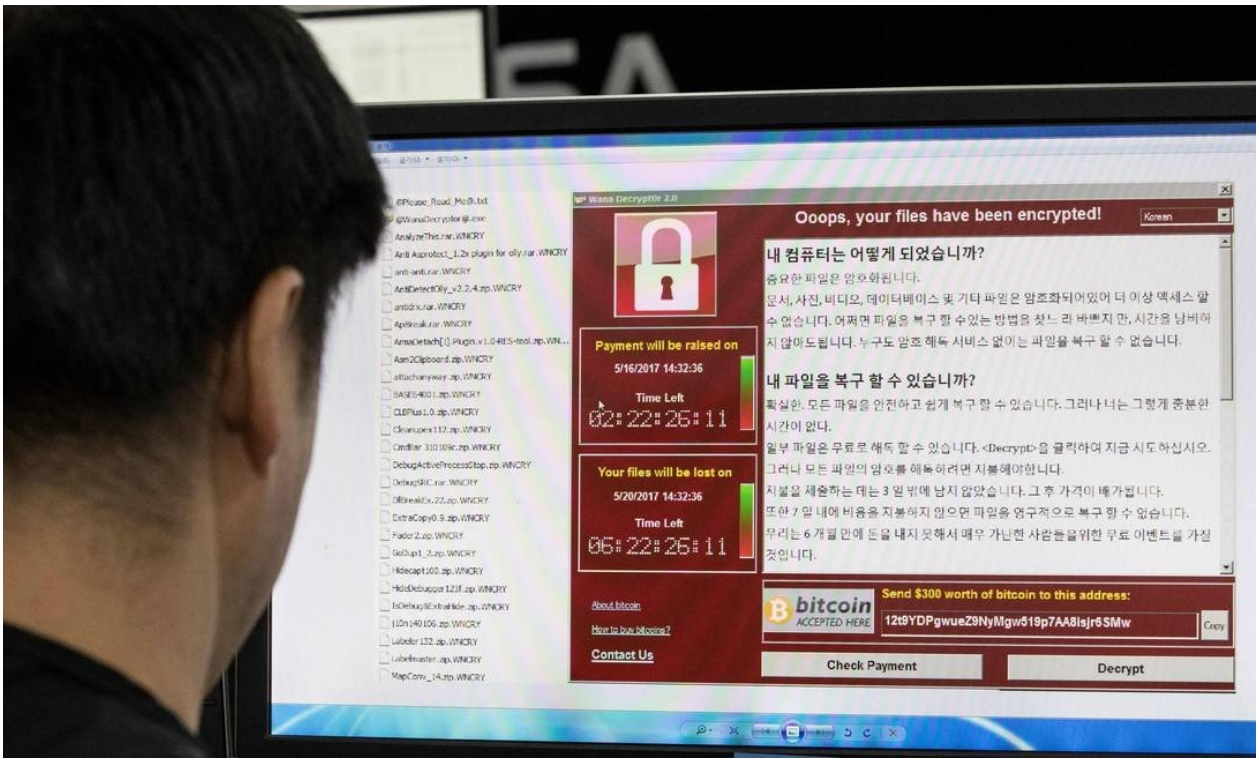
Why do not people pay attention to these strategies?

Ordinary people have many conceptions of their own when it comes to cyber security. I call these conceptions myths because they are not correct. A lot of people thinking of a cyber security problem remember credit card data being stolen. In the United States, you are responsible

for the first 50 dollars spent on a card. If they were improperly spent, the fact that someone runs the risk of losing that money causes people to worry about reporting potential data thefts. But that's not the main problem in cyber security.

What is the main cyber threat these days?

They are what we call 'ransom' attacks, in which nothing is stolen from you. What happens is that the software of a hacker enters your computer and locks your computer so that the real owner of it does not have access to the information inside. More importantly: it picks up the data and shuffles it completely. Nothing is stolen, everything is there, but you can not do anything with what is there. In 2017 such an attack blocked 80% of the computers of Telefonica (Spanish telephone operator). What can be done? Close a whole company for a whole day? These are very large events, much larger than a person having a stolen credit card, but no one is aware, unfortunately. Because? Because the companies attacked have no interest in demonstrating their weaknesses.



Monitor displays WannaCry virus blocking message at the South Korea Internet & Security Agency (KISA) Photo: Yonhap / AFP

But ransom attacks are one of many attack cases that companies do not want to talk about. The first reason is their reputation. It does not seem good to close your company because of such fragility. In addition, encourage other people to make the same attack against you. If another criminal looks at this, he thinks: "Telefonica is not safe, I'm going to attack too." A still the legal consequences: a cyber attack gives reason to think that executives of a company do not know how to manage it properly. This leaves room for legal action against the company, which will cause it to lose a few million dollars more. For many reasons, companies are always eager to avoid exposure to these attack cases. That is why, when these cases end up being made public, companies still deny that they have suffered this type of attack. And so ordinary people know nothing about this kind of attack.

Why are companies attacked?

That's a big question. Let me make an analogy: if you own a castle, and need to defend it, you need to make sure that all the castle gates are closed. If you're on the hacker side, you just need to find a gate that's open. This is what we call an asymmetric war. The hacker has many more advantages in the fight against the defender of a system. In addition, software is increasingly complex - it is very close to the complexities of humans, to be honest. Type software has hundreds of millions of lines of code. It is entirely possible that one of these lines is not well written. But the problem does not stop there.

There is a mental model problem. When a person is assembling something, be it a building or a software, that person thinks about how this structure should be used for good and not all the ways in which this structure can be misused. But hackers only think about it: how to use a framework for evil. Normal people would think about seeing something wrong: "ok, this should not be happening." For a hacker only works that way.

We put within our software some preconditions for using these same systems without thinking that a hacker will use this software in ways that normal people would never have thought of before. And with consequences never thought before. No one in general designs a system, such as software for example, with the intention of seeing it violated. But in fact, one of the reasons I'm working with the C6 bank is that 15 or 20

years ago hardly anyone knew what cyber security was. I've been talking about it since 1979, when I wrote a book about it. That is, it was not something invisible. But what we've been seeing over the past 10 or 20 years is that people continue to design software without paying proper attention to these "unusual" behaviors on the part of hackers.

Companies need to give security to procedures and diffuse a "culture of ethics" Photo: Pixabay

Where do so many vulnerabilities come from?

Much of this comes from the fact that Microsoft, which designed the foundation of current computing with Windows 30 years ago, also did not think about these vulnerabilities. Or, to go to something more fundamental: the internet was created in the late 60's initially for universities to collaborate with each other. Can you imagine that a university would mount a cyber attack on you or someone else? Probably not. That is, the assumptions about how the internet would be misused were not a priority of those who created the internet back there. Who created the internet lived in an American university world, in those communities where it is possible to leave the door open and no one is going to steal your things. There was trust in one another. No one imagined that the internet could be used to do evil or to break someone's trust.

The cyber security logic that many companies are thinking nowadays, and the C6 is thinking already since the creation of systems, happened relatively late in the companies in general. And then the result is that they need to analyze millions of lines of code 20 or 30 years after they've been drawn. It is an action that demands tremendous effort in companies. We want to design with C6 a system protected from hacker attacks already from the beginning.

How to draw systems totally immune to attacks - or at least very close to it?

There are more and more devices connected to the internet, called the internet of things. My wife, for example, already has a smart toothbrush. She can be connected to the internet and it tells the dentist if she is brushing properly or not. Well, I doubt that anyone who created the smart toothbrush thought about how this brush can be attacked by a hacker. Probably did not even think that about the man who created it.

Another example is the smart refrigerator. They leave the factory with internal cameras to notify the owner, through a mobile application, of the missing products at home. All of this is processed by computers shipped inside the refrigerator. Well, I've seen cases of hacked smart fridges in which the computer, which should be managing the ice level or the temperature of the freezer, is actually sending pornographic messages on the internet. So, in addition to thinking about how they are making ice or keeping the correct temperature, the designer of the smart refrigerator needs to think: how to protect the device from a hacker attack? The problem is that our mental model is not prepared for bizarre uses of the structures we have created.

Hacker attack Photo: Kacper Pempel / Reuters

Is it possible to track vulnerabilities?

I firmly believe that companies are already designing more secure systems. I make the analogy with civil construction. Let's remember that the construction of the Empire State Building, one of the largest buildings in the world in the 1920s, killed 120 workers. People did not think safety at work was important. That was 90 years ago. Since then, due to pressure from society and public opinion, companies have started to worry about safety at a construction site. This has resulted in positive changes over the years. It is very common to see signs on construction sites around the world today with the words: "we are 100 days without accidents and please do not be the person who will turn this counter to zero". People are forced to do good service and work safely. It took some time to happen on real-world production lines. And it's that kind of mental template adaptation that we're trying to instill in companies with respect to protecting them from cyber-security.

How is it possible to change this mental model?

What we try to understand is what could be the best techniques yet to be invented to prevent problems in physical structures? And secondly, we

want to understand: how to adapt the same logic to cyber attacks? That is, how to make our cyber networks secure in the same way that we make our factories safer? We are applying a technique developed by one of our researchers at MIT's Aeronautics Department. She spent 20 years researching ways to reduce air crashes. We are adapting her techniques for cyber security. This method involves two key steps.

The first is relatively simple, but little remembered: it has clarity of what is important in your company. You can ask your boss: what is the most important thing in your organization. I bet he'll say hundreds of things. Few people care to understand what is really important. Most executives never thought about it very well. If you cannot focus on what's really important you cannot really protect yourself. It sounds simple but it is extremely difficult for most executives, many of them trained to think otherwise.

This is relatively obvious to the aviation industry: the top priority is the plane does not fall. The onboard television does not work as well, this is certainly annoying but the priority is the plane not crashing. Having this focus is important about what needs to be protected.

The second part is where engineering actually begins. Everything that happens inside a company is part of an internal process. Doing an interview, for example, is a process. Each process, in general, has some sort of monitoring or control. Your boss seeing the interview results might think: did he do a good job? If not, what kind of training does he need to have to do a good job? But then your boss also suffers some kind of control. In many companies there are hierarchies with many levels of control. And that's a problem.

Because?

There are very common problems in designing the controls of these processes. Many of the vulnerabilities of systems detected by those at the bottom end up not even reaching the level of top management, which has the power to make the right decisions to increase the security of a system. The reason: People do not talk to each other within a company.

WHY I'M WORRIED ABOUT GOOGLE

HOW THE GROUP WOMEN AGAINST BOLSONARO WAS HACKED ON FACEBOOK

HOW THE LARGEST HATE-PROPAGATION GROUP ON THE INTERNET WORKS, WHICH PROFITS FROM MISOGYNY, RACISM AND HOMOPHOBIA

Big tech companies like Google, Facebook and Amazon are already born in a digital world and have management structures considered modern. Do they also suffer from these problems?

Yes, because they came up 15 or 20 years ago, and although they have made changes to perfect their systems, they are companies that have grown very, very fast. In addition, they were created under the logic of a friendly world and in which this huge amount of cyber attacks did not exist. But there is one more dangerous thing behind the expansion of social networks and sites that collect our data.

Because of the sharing of this information, it is relatively easy to create cyber scams with money requests today. If, in the past, such fanciful emails were commonplace as "a prince from Nigeria would like to send you some money but for this you need your credit card", it is now possible for a coup writer to put together a fairly credible email only tracking all kinds of information that people post online. Artificial intelligence today already allows you to crawl all of this information to allow for highly personalized punch emails. About 70% of such attacks are successful.

And what should people do? Turn off your social networks?

Well, at the age of the caves, no one suffered from cyber attacks, but I do not imagine people wanting to go back to that reality just to get rid of the dangers online. It's a big challenge because everything in life is a risk. Getting out of bed is a risk: you can slip on the floor of the room, get hit by a car when leaving the house and so on. You have to judge: it is clear that digital life brings risks but you have to judge the possible benefits with technology. The logic here has to be: how to maximize benefits and reduce risks?

But within a company, how do you do that?

The vast majority of enterprise security flaws occur in inter-departmental interconnections. That is, you know your work, but the editor from another area does not know what you do. He's focused on his work. Few people in the companies can make the relationship about how the two jobs are correlated. In addition, there is a risk of data exposure to a third party outside the organization. The magazine that you work for may have the best cyber security in the world. But the printer who prints the newspaper or the magazine may not have it. These structures are connected. The hacker can come through the printer and attack the magazine. This is not something that companies usually pay attention to and also requires a great change of culture.

But, back to the beginning of the conversation: how many people die today in most developed countries in the construction of buildings? Little or almost nothing, a big change from what they died at the time of the construction of the Empire State Building. If you can change the way you think and act on a particular problem, the transition may be easier. The same change may take ten or more years to occur in cyber security. In any case, it could allow us to build systems that are much safer than the ones we have today.