4-2017

Cybersecurity in the 21st century

Singapore Management University

Citation

Singapore Management University. Cybersecurity in the 21st century. (2017).
Available at: https://ink.library.smu.edu.sg/pers/335

CYBERSECURITY IN THE 21ST CENTURY

Published:
28 Apr 2017

Increased awareness is necessary in fending off data theft and cyber attacks, and it is not just the CIO's job to do so

Cyber attacks have become an inescapable feature of 21st century life: Amidst accusations of Russian interference in the U.S. Presidential election, reports of similar attempts to influence the French presidential race have surfaced earlier this month; Yahoo! disclosed in 2016 two hacks (in 2013 and 2014) that compromised over a billion users, which bought back into focus the infamous leak of stolen pictures of Hollywood stars at around the same time.

Given the troubling frequency of such reports and the consequences of security lapses, why are people so cavalier about cyber security?

"We polled Singaporeans - about 2000 of them, and we found that 70 percent of them feel that everyone has a role to play in cybersecurity," relates **David Koh**, Chief Executive of the island state's Cyber Security Agency. "However, only one in three actually manage their passwords well or, for that matter, have antivirus on their cellphones. We're not doing enough.

"The reality is that the attacker has the advantage when it comes to cybersecurity. The defender has to get it right every time, all the time. The attacker only has to succeed once. And that's the real challenge that we're facing."

CYBERSECURITY OR CYBER COMPLACENCY?

Individual users were not the only ones guilty of cyber complacency. According to a poll done by professional services consultancy Accenture, 77 percent of 2500 senior executives surveyed felt good about the cybersecurity posture their organisation has taken. Yet, one in four cyber attacks have gotten through in organisations.

"I think cybersecurity is everyone's problem," states **Joshua Kennedy-White**, Accenture's Managing Director - Accenture Security Lead, APAC. "The research we've conducted reveals that the focus is on the external threat [focused on] the idea of a hacker scheming away trying to get into an organisation.

“The reality [is] less dramatic – [it’s mostly] the inadvertent error of users inside [an organisation]. This tells me that, as an organisation, we need [the entire company] to understand the threat and not just…the IT department. And a great statistic in that is that a majority 60-plus percent of incidents in organisations are reported by everyday employees, not by the CIOs.”

With regard to organisations’ cybersecurity challenges, **Robert Deng**, SMU Professor of Information Systems & Director of the Secure Mobile Centre, expanded on the asymmetric nature of cybersecurity.

“The asymmetrical war is because of three factors,” Deng explains. “One of them is that the systems today are so complicated. Nobody knows what is going on in the systems. If we take commercial operating systems for example, one operating system has tens of millions lines of code. Based on our experience, we know that the number of vulnerabilities is in proportion to the square of the number of lines of code.

“The second factor is we have so many legacy systems which were not designed for security. It’s nobody’s fault but that is part of history and those systems introduce a lot of loopholes. The third one is even though that the companies have the intention to make the systems secure, they do not have enough qualified security professionals to [do so].”

Koh, Kennedy-White and Deng made those comments as members of the panel discussion “Cybersecurity: Enhancing Safety Online” for Singapore-based station Channel NewsAsia’s Perspectives programme. They were joined by **George Loh**, Director of Programmes at the National Research Foundation in Singapore, who drew the analogy of staying safe physically.

“If you [think about] physical security, you will not go to dark places,” Loh explains. “You would take precautions if you’re going to certain places, you go with friends [instead of] going alone. You leave your house, you will lock up the doors.

“But when it comes to cybersecurity, a lot of the time we are too careless. We think that cyberspace is safe. It gives us a false sense of security because it is easy to get in.”

Citing the example of the leaked pictures of Hollywood stars, Deng explains how a lack of cybersecurity awareness led to the whole episode.

“Number one: They are not even aware that the devices can take a photo and upload automatically onto the cloud. The second one point is the system design, in when they upload the data, the hackers exploited a certain authentication weakness. For example, they know the user name, and [they activate the] password reset feature. To reset the password, the server will ask you a certain secret question. What the secret question is is in the social network. They just go to celebrity’s network and get the answers to the secret question.

“So, authentication must be strong. The third one is when you upload your data, you better encrypt your data. We are doing a lot of research on how to do the data encryption.”

A TRADEOFF BETWEEN SECURITY, CONVENIENCE, AND COST

The leaked Hollywood pictures, while embarrassing and caused professional damage, left victims unharmed. With an increasing number of internet-connected devices that make up the Internet of things (IoT), from fridges to toasters to self-driving cars, hackers could set off explosions or hijack control of cars to cause physical hurt.

If that happens, who is responsible? Are the necessary laws in place to address such an eventuality?

“Attribution is always difficult.” Loh explains. “If I buy an IoT device, let’s say I have an IP camera, I install in my home because I want to monitor my house [and] some hackers go through the IP camera and hack not my house nor my systems, and does not steal any data from me, but they get into the telco, or the larger eco-system.

“Who is responsible? Is it me, the consumer? Is it the manufacturer of the IP camera? Or is it the telco themselves because they need to protect the infrastructure too? So it’s a difficult question and it’s very difficult to pinpoint.”

Given the complex and multidimensional nature of the issue, can there be a guarantee for online security?

“It’s a 3 sided tradeoff between security, convenience, and cost, so there’s no such thing as absolute security,” says Koh, who continues by saying, “If you want absolute security, the most secure computer is the one that’s still in the box. The moment you take it out, connect it, you’re taking on risks.

“So it’s a balance between the kind of risk that you accept for the purpose of convenience, and the cost which you are prepared to pay for new developments. You have to balance between trying to facilitate innovation, new things like autonomous vehicles…If you want to implement cybersecurity decisions, requirements from the onset, you probably snuff out the innovation.”