HERBERT SMITH FREEHILLS

ZERO-DAY ATTACKS, RED TEAMING AND OTHER CYBER CONCERNS

02 July 2019 | Australia
Legal Briefings – By **Kwok Tang**

There are a myriad cybersecurity issues that legal departments must concern themselves with, with proactivity being key to the safety of a business's information.

Speaking recently on a live webcast hosted by Lawyers Weekly — Security breaches: is your firm protected? — Telstra security consultant Keith Kerr said zero-day attacks refer to instances where legal teams discover vulnerabilities that haven't before been apparent.

> *"Every day up to that day, that vulnerability is a zero day, which can be used to exploit that system or service or software. To what extent depends on the zero day itself, but for example, say it was something which could compromise the latest version of Windows, or a particular service running within that," he explained.*
>
> *"Depending who discovers this zero day, if it's a researcher they would tend to go through what we call a bug benefit program where they're given compensation from a vendor for their finding, and the vendor then works on a patch and fixes that up so it's no longer an issue. Or, in the worst-case scenario, it could be someone who's a black hat hacker, who's actually using it for malicious means for [themselves], to either extract data or harm a company or an individual.*
>
> *"Or, more likely, go through a broker on the black market and sell that vulnerability to absolutely anybody for however much they're willing to pay and set claim or whatever they'd like to pay."*

Also discussed during the webcast was the issue of red teaming, which Herbert Smith Freehills partner Kwok Tang explained refers to going in and attacking and testing the capabilities of legal teams. This, he said, requires a proactive approach by those in charge.

> *"Most data breaches arise from, really, human error. A large part of the protection around that is really cyber resistance training or awareness. Giving training and when you're onboarding give the training to all your staff, not just necessarily give it to the legal staff, just all staff should have cyber awareness training and then to frequently test that," he said.*
>
> *"[We had a phishing exercise] at my firm, maybe a couple of month's back, where they sent a funny-looking email and you look at it and in the back of your mind you treat it as, this doesn't quite look right, and then we have a mechanism where you could press a button to notify and trigger that this is potentially a phishing exercise.*
>
> *"That, it was a test from the firm, from our IT department, testing us. No, we have onboard training but also just frequent reminders and real-life examples of testing to make sure that your staff is aware that's an issue."*

Mr Kerr added: *"That behavioural element, when combined with awareness training, [has] certainly much more of an impact, because if you think about it, a lot of organisations have awareness training which is essentially click-through, people are given it when they're busy, so they'll click through to get to the end of it, and it doesn't really sink in.*

> *"If you're being tested through things like phishing emails, and you're starting to build a habit of clicking on that report button, or it may be a case of raising your hand to your IT guy, so if it's a small company and they're just sitting across the room from you, flicking it through in an email, or just shouting across the room, that's changing your behaviour and that takes the onus off you to make a decision.*
>
> *"By doing that you're empowering the user to say, 'Okay, I don't need to understand the extent of this email, whether it's malicious or not; what I need to do, I think, is, could this be a malicious email? If it could, what action do I take?' You need to facilitate users with an action to take, and that's part of the process."*

This article was written by Jerome Doraisamy, and featured exclusively in Lawyers Weekly.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

KWOK TANG
PARTNER, SYDNEY

+61 2 9225 5569
Kwok.Tang@hsf.com

LEGAL NOTICE