GETTING CLOUD SECURITY READY FOR THE RESPONSIBLE CORPORATE CITIZENS

By Dr Lee Hing-Yan

Executive Vice President APAC of Cloud Security Alliance

With cloud computing fast becoming the IT system of choice, enterprises are reaping the various benefits, such as increased agility and lowered capital investments. What have not sufficiently progressed are relatively outdated mindsets many corporate citizens still have about information systems security. To them, it is still a domain very much the purview of their IT department, although they might not readily admit it. This is despite the numerous cybersecurity educational and awareness programmes that enterprises have been rolling out.

While we were able to get away with such myopic views in the past, corporate citizens need to understand that the business risks of such complacent mindsets are immense. It is no longer an issue of "someone else's problem". According to the National Cyber Security Alliance, 60 percent of small and midsize businesses that were victims of data breaches or hacks went out of business within six months. Even large enterprises that were able to pull through the calamity of a breach or attack were left dealing with repercussions of the incident for months, including paying for potential penalties imposed by data privacy authorities. In the case of data breaches, companies could be fined a staggering 4% of their annual turnover or 20 million Euros under the European Union's General Data Protection Regulation. Security is a business problem with the livelihood of every corporate citizen at stake.

YOU ARE PART OF THE ATTACK SURFACE

Understanding the potential fallout when the enterprise is hit by a cybersecurity-related incident is one side of the awareness coin. Corporate citizens should also be fully aware that every individual in the enterprise forms part of the attack surface and is vulnerable. An attacker will make attempts at an enterprise's key assets by looking for the weakest link, rather than targeting C-level personnel who are usually under closer scrutiny by cyber defenders. The weakest links are often successfully exploited through phishing (tricking victims into sharing sensitive information), spear-phishing (personalised and targeted phishing) and social engineering, which are still very much the primary arsenal used by attackers when targeting the enterprise. According to a data breach report, 80 percent of hacking-related breaches are still tied to compromised and weak credentials. In short, every employee, regardless of seniority, needs to keep in mind that they can be a potential target for attackers to compromise the enterprise.

NECESSARY INCONVENIENCE AND A DOSE OF HEALTHY PARANOIA

In view of the evolving threat landscape, we would even go as far to say that every corporate citizen should have a minimum level of general and basic understanding of information systems and cloud security (as it becomes the default IT system), just like how each employee has a basic understanding of finance, marketing, human resources etc. The ideal outcome is every employee inculcated with a little bit of 'healthy paranoia' to take a pause and think before plugging in that USB stick picked up at the office lobby, before opening the email attachment announcing the annual bonuses, or before entering their credentials into any websites.

WHAT ABOUT CLOUD SECURITY?

As cloud adoption surges ahead in the enterprise, cloud security will increasingly be in the spotlight. This does not mean that the cloud is any less secure than other

outsourced infrastructure or services. You might have anecdotally heard claims such as on-premise or private cloud infrastructures are more secure than public cloud. Or you might have seen irrational procurement processes that impose much stricter requirements on CSPs, sometimes with requirements far exceeding those that the enterprise implements on business-critical systems. Are such biased views of the cloud justified?

Major CSPs operate some of the largest IT infrastructures the world has ever seen, serving millions of customers. It is in their economic best interest to invest substantially in security. Although this does not translate to being infallible (the only secure computer is one that is unplugged and kept in a box), they are definitely running a tighter ship and rival any large enterprise's security teams.

The corporate citizen should recognise that using cloud services is akin to outsourcing, and therefore should exercise the same judgement and prudence as in any outsourcing arrangements when it comes to procuring cloud services.

THE SHARED RESPONSIBILITY MODEL

Cloud users will no longer need to worry about security because they are taken care of by the CSPs? That could not be further from the truth. Any corporate citizen making use of cloud services should have a basic understanding of the Shared Responsibility Model, a fundamental framework for cloud security that determines where the security obligations of the CSP ends and where it starts for the users. Depending on the cloud service model (Infrastructure-as-a-Service, Platform-as-a-Service, or Software-as-a-Service) in use, the enterprise as a cloud user will have differing levels of responsibility. For example, if the enterprise deploys a proprietary messaging software on the public cloud, the CSP will be responsible for ensuring that the underlying infrastructure is secure, whereas the enterprise will be responsible for ensuring that the messaging software is free of vulnerabilities. The detailed responsibilities are typically spelled out in the contractual service level agreements.

HEALTHY PARANOIA

Information systems security is no longer just a concern for the IT departments. It affects each and every corporate citizen to the core. The only way to protect the enterprise from the associated risks is to inculcate security as a culture, mindset, and even a little dose of healthy paranoia. Only by doing so do we have a fighting chance to survive the evolving threat landscape.

TODAY'S IT PERIMETER IS EVER-SHIFTING AND TOUGH-TO-DEFEND

Further adding to the complexity is the ever-shifting and sometimes invisible IT perimeter the modern enterprise struggles to have visibility of and defend. Some statistics extracted from published reports to consider:

94%

Enterprises already use cloud services, and 83 percent of enterprise workloads will be in the cloud by 2020

The average enterprise uses

1,427

distinct cloud services

60%

Workers use a smartphone for work purposes

Shadow or unsanctioned IT makes up

30-40%

IT spending in large enterprises