Econ 4.0

BY **RAJU CHELLAM**

Is robotic process automation for you?

Here's a serious software story: A team of programmers is tasked with developing a sophisticated software package using the latest tools and technologies on a substantial budget. The team hires a hot-shot artificial intelligence (AI) programmer who labours diligently and completes the project to the satisfaction of senior management.

"Great job, bro," the team leader congratulates the AI programmer. "Can you conduct a training session to show us how your code works?

The AI programmer looks up at the sky in despair.

"When I wrote this AI code, only me and God knew how it works," he frowns in frustration. "Now, only God knows ... ."

If that story made you ponder, the following points should make you wonder: The market for automating repetitive tasks is ready to boom. Called robotic process automation (RPA), it is software that mimics the activity of humans in carrying out a task within a process. RPA can do repetitive tasks more quickly, accurately and tirelessly than humans, freeing employees to do other tasks that require human abilities such as emotional intelligence, reasoning, and judgment and interacting with customers.

How is RPA different from cognitive intelligence?

"RPA deals with simpler types of tasks," Leslie Willcocks, professor of technology, work and globalisation at the London School of Economics (LSE) informs McKinsey in an interview. "RPA mainly carries out physical tasks that don't need knowledge, understanding or insight — or tasks that can be done by codifying rules and instructing the computer or the software to act."

Companies in highly regulated industries such as insurance and banking find that RPA is a cheap and fast way of applying superior capability to the problem of compliance.

"You also get better customer service because you've got more power in the process," Willcocks says. "A company that receives lots of customer inquiries, for example, can free staff to deal with more complex questions and issues."

RPA AND ROI

What's the major benefit? In 16 case studies done at the LSE in 2016, RPA provided an ROI (return on investment) between 30% and 200% in the first year itself.

"However, it's wrong to look just at the short-term financial gains, particularly if those are simply a result of labour savings," Willcocks advises. "That approach does not do justice to the power of the software, because there are multiple business benefits."

One of the Big Four accounting firms, PwC (PricewaterhouseCoopers), estimates that 45% of workforce tasks can be automated. This could save an estimated US$2 trillion (RM9 trillion) in global workforce costs.

"Software robots are easy to configure and do not require extensive IT knowledge," PwC says. "Organisations can use RPA to automate manual tasks, such as copying and pasting data between applications or reconciling and cross-referencing data."

For internal audit, RPA presents both opportunity and responsibility.

"By helping organisations understand and control RPA risks and identifying opportunities to embrace RPA within their organisations, internal audit can position itself as a trusted adviser," PwC notes. "Understanding how an organisation is using RPA and its impact on its risk profile is crucial for internal audit professionals."

Management consulting company Gartner, Inc says end-user organisations globally may spend US$2.9 billion on RPA solutions this year, up 19.5% over 2021.

"By achieving a growth rate of 31% in 2021, the RPA market grew well above the average global software market growth rate of 16%," says Cathy Tornbohm, an analyst at Gartner. "Organisations are leveraging RPA to accelerate business process automation initiatives and digital transformation (DX) plans — linking their legacy nightmares to their digital dreams — to improve operational efficiency."

By end-2024, the drive towards a state of hyper-automation will drive organisations to adopt at least three out of the 20 process-agnostic types of software that enable hyper-automation.

"North America, Western Europe and Japan together are on pace to account for 77% of global RPA end-user spending in 2022," Tornbohm says. "North America will have the largest share at 48.5%, followed by Western Europe at 19% and Japan at 10%."

What about the rest of Asia-Pacific? The surge in demand comes from financial services.

"Spending by the financial services sector in the Asia-Pacific region ex-Japan may grow at a CAGR (compound annual growth rate) of 35.8% to reach US$271 million in 2024," says Ashutosh Bisht, a senior research manager at global market intelligence firm IDC (International Data Corp). "The financial services sector in 2024 might represent over 31% of the total RPA spending in this region."

Although the growth rate took a slight dip in 2020, IDC estimates RPA spend will grow at a year-on-year rate of 34.4% to cross US$103 million in 2021.

"Leading organisations are doubling down on tech investments, such as automation, AI and cloud, and are identifying opportunities to survive and thrive in the next normal," Ashutosh says. "As the CEO's agenda develops to support digital initiatives, automation is fast becoming one cornerstone of the future enterprise."

An example would be Singtel subsidiary NCS (the National Computer Systems Group), which is an early adopter and implementer of RPA for many of the largest public and private sector organisations.

"We have implemented more than 500 RPA processes in finance, HR, IT, operations, procurement and sales," says Sam Liew, managing partner of NCS' government strategic business group. "We have deployed RPA platforms from different vendors, enabled programmes for companies to create 'citizen developers' and set up ROCs (robotic operating centres) as a managed service for customers."

RPA RISKS

Is RPA foolproof ?

"Like all other tech, RPA is not foolproof," says Liew, who is also president of the Singapore Computer Society (SCS). "RPA is an orchestration layer that mimics human actions across a diverse range of infrastructure, apps, networks and cybersecurity. A security breach at an application, infrastructure or network layer will inadvertently affect the security of RPA. We start by adding security features at the bot scripting layer itself. NCS has also built its own version of AI operations — called iQOPS — with self-healing bots to secure RPA operations at the apps, infra and network layers."

The bright side is clear: RPA promises efficiency, simplifies compliance, reduces cost and mitigates operational risks.

But what about the flip side? Can it offer a tool for fraudsters to automate attacks?

"It could, all the more so since the pandemic began and forced hundreds of millions of consumers to go online from their home Wi-Fi networks," says Rajat Maheshwari, Mastercard's vice president of digital identity and cybersecurity for the Asia-Pacific region. "This trend has led to fraudsters creating fake accounts to victimise retailers and consumers."

Fraudsters typically begin with small RPA programmes and move to more sophisticated ones. "Mastercard's fraud and analytics network detected that 50% of cyberattacks are sophisticated attacks," Rajat says. "Sophisticated bot attacks that use RPA could have a success rate 10 times higher than a basic attack. A sophisticated RPA-based attack can even bypass basic bot detection and other cybersecurity tools and firewalls in most cases."

How does it work in reality? "For example, in an e-commerce webpage, attacks could begin at the account creation stage itself," Rajat adds. "Fraudsters could use RPA to probe the environment and check for vulnerabilities in the security systems. It is therefore crucial to detect and sew up all the vulnerability points — from login to transaction completion — to foil sophisticated RPA-initiated cyberattacks."

Also, as companies adopt massive data analytics, they must determine how to identify risks created by datasets that integrate many types of sensitive customer information. It would be ideal to collaborate with infrastructure and architecture teams to build crucial security services into standardised solutions for analytics and RPA.

"Teams must also incorporate security controls into analytics solutions that may not use a formal software development methodology," global management consulting firm McKinsey notes. "As companies apply RPA, they must manage bot credentials effectively and make sure that boundary cases — ones with unexpected or unusual factors or inputs that are outside normal limits — do not introduce security risks."

How should one get teams involved? Start small and identify use cases for automation that your company needs to generate business value. While it is prudent to implement integrated corporate security architecture, keep it simple and do not over-engineer solutions, advises KPMG, another of the Big Four accounting firms. However, the fear of missing out on the latest trends may prod companies to go on a buying spree and acquire tools that often go unused for lack of knowledgeable employees.

"Leverage your current technology stack first," KPMG says. "There is an enormous amount of advanced automation capabilities that exist within current tooling; it is not necessary to look outside the organisation. Find colleagues with existing automation experience and make them part of the cyber team. It's easier to take staff with previous experience using RPA in other areas of the business or with a previous employer and teach them how to apply RPA within cyber, than to take someone with basic cyber credentials and try to teach them RPA."

Since we started with a software story, let's end with another. When I first learnt software programming, I was worried about errors in my code and why something I wrote so rigorously wasn't working. One day, I ran into a veteran programmer.

"Why are you looking so dejected, bro?" he asked me.

I explained my frustration to him.

"Don't worry if it doesn't work right," he laughed. "If everything worked perfectly, you'd be out of a job." E

Raju Chellam is vice president of new technologies at Fusionex International, Asia's leading big data analytics company