BRIGHT MINDS

Q & A SERIES

OCTOBER 2021

Rushing to Automation

Don Heckman, ICIT Fellow

Defense Cyber Solutions Leader & Director, Cybersecurity Solutions, Guidehouse

ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

ICIT's Bright Minds Q&A Series

Rushing to Automation

With Don Heckman, ICIT Fellow, Defense Cyber Solutions Leader, & Director, Cybersecurity Solutions, Guidehouse

October 2021

About This ICIT Bright Mind Q&A:

In continued support of our mission to cultivate a cybersecurity renaissance that will improve the resiliency of our nation’s 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders, ICIT has embarked on a journey to hold candid interviews with some of the brightest minds in national security, cybersecurity, and technology. Our goal is to share their knowledge and insights with our community to shed light on solutions to the technology, policy, and human challenges facing our community. Our hope is that their words will motivate, educate, and inspire you to take on the challenges facing your organizations.

Robotic Process Automation (RPA) has the potential to improve cybersecurity and cyber-hygiene, lessen the impact of the looming talent shortage, and alleviate the resource burden associated with securing critical systems; however, RPA is often misunderstood, oversimplified, or conflated with traditional automation or artificial intelligence.

In this ICIT Bright Minds Q&A, Don Heckman, ICIT Fellow and Defense Cyber Solutions Leader, & Director, Cybersecurity Solutions, Guidehouse, will clarify the function, role, and benefits of RPA and detail potential implementations and use-cases.

About this Bright Mind:

Donald Heckman is director in the Guidehouse Advanced Solutions Cybersecurity practice. He is a cybersecurity subject matter expert, and brings more than 36 years of experience in government leadership, spearheading cybersecurity and secure information-sharing initiatives across the Department of Defense, Intelligence Community (IC), and national security sectors. He is Guidehouse’s Defense Cyber Solutions leader, as well as leading multiple data protection and privacy offerings for public and commercial sector clients.

ICIT:
What is the difference between intelligent automation, like robotic process automation (RPA), and traditional automation?

Heckman:
Although it is easy to confuse intelligent automation, like RPA, with traditional automation tools, they are very different. Traditional automation tools have been around for decades, focusing on repetitive tasks and usually requiring integration into applications or infrastructure, which can be very time intensive. On the other hand, RPA does not require integration as it sits on top of existing systems. It offers an easy-to-use graphical user interface, placing automation capabilities into the hands of business process owners. This ability mitigates lapses in translation between business user requirements and technical specifications. RPA creates and deploys a software robot, called a "bot," which launches and operates other software. Because of this, RPA has revolutionized computer automation. RPA software enables reusable, scalable, and centrally manageable solutions. Additionally, in complex processes that may include substantially nuanced and complex decision-making, artificial intelligence (AI) can be layered into RPA solutions to produce powerful automation that delivers higher business impact and value.

ICIT:
What do you consider to be the most significant benefit(s) of intelligent automation adoption?

Heckman:
Organizations that implement RPA reap the following benefits:

- Lower costs. RPA simulates the actions of a human worker on a computer, sits on top of existing systems, and works seamlessly with existing infrastructure.
- Reduced errors. Human errors are common in high-volume, repetitive tasks. Automating these processes virtually eliminates human error.
- Empowered workforce. When manual, repetitive processes are transferred to automated bots, human employees are empowered to focus their time and energy on more rewarding, creative tasks and knowledge work.
- Scalability. Due to its rapid processing speed and lack of reliance on costly, time-intensive technology system enhancements, RPA is well-suited to handle seasonal surges in workload.
- Improved Security. Role-based access controls, logging of robot activity, and audit trails are key features of RPA that ensure segregation of duties and subvert fraud attempts and operational error. By running automated processes behind locked screens, automations avoid compromising data privacy.

ICIT:

How can intelligent automation support cybersecurity? What are some typical applications or examples?

Heckman:

Intelligent automation can help address the shortage of skilled cybersecurity professionals while improving the overall cybersecurity posture of organizations. Multiple workforce studies in 2020, including one by ISC2, estimate the cybersecurity skills gap to be between 3 and 4 million professionals. Intelligent automation can perform routine cybersecurity tasks, allowing limited cybersecurity staff to focus on higher-priority complex tasks.

In terms of improving cybersecurity for an organization, intelligent automation can improve the cyber hygiene of an organization by:

- Improving asset visibility
- Ensuring assets are patched and configured correctly
- Verifying the use of strong multifactor authentication
- Detecting and prohibiting weak passwords
- Collecting and reviewing audit logs; and
- Disabling accounts when users leave the organization

Additionally, it can automate cyber intrusion detection and response playbooks by detecting incoming threats, analyzing and prioritizing alerts, and executing remediation actions much faster than humans. Tasks considered for automation solutions are rules-based repetitive processes, such as data management, report creation, and routine email communications. Tasks like these are considered “low-hanging fruit” since they generally take significant time to manually complete and are relatively easy to automate. Since these repetitive tasks are located in many departments throughout an organization, automation can produce substantial time and cost savings with minimal effort.

ICIT:

Are there any potential drawbacks, and, if so, how might those circumstances be mitigated?

Heckman:

Intelligent automation and RPA bots are software that can introduce a new attack surface for threat actors. In RPA, common security concerns are user access management, bot privileges, data security, and security regulatory requirements. RPA bots may need elevated privileges to perform their tasks or their credentials may be static and shared amongst multiple bots. Given these facts, they have the same cybersecurity issues as traditional software applications and need to follow a well-defined cyber security framework and security principles as follows:

- RPA Software Integrity – Ensuring RPA software is up to date, patched, and properly configured.
- User Access Management – Implementing role-based access control supported by strong identity management, including using randomized passwords updated at specific intervals and never stored in plaintext.
- Bot Privileges – Utilizing least privilege and least functionality. In other words, bots should only have the privilege and access to applications needed to perform their tasks.
- Secure Logging and Auditing - Bot activities need to be logged, and those logs should be protected from modification or deletion.
- Data Security - While RPA vendors provide data security features, organizations should use approved encryption standards during the entire data processing lifecycle.

ICIT:
Are there any misconceptions about RPA that you want to address?

Heckman:
As with any new technology, there are misconceptions. Some common misconceptions are:

- RPA replaces humans. Because RPA bots are focused on doing human tasks, some people think they will replace humans and reduce jobs. However, RPA is ideally suited to augment staff, freeing them to work on higher-level activities and tasks requiring cognitive reasoning.
- Bots don't make mistakes. A bot does exactly what it is programmed to do. If you have a flaw in your RPA process and implementation, it will consistently replicate that flaw until someone discovers it.
- We can automate everything. RPA is suitable for a very specific class of tasks, as mentioned previously. They are not good for jobs that require human input or decisions.
- RPA is complex and expensive. As with any technology, companies can start small and scale-up. If you start with simple pilots to automate a few tasks, you can expand as your organization becomes more familiar with the technology.

ICIT:
How would you recommend cybersecurity professionals "sell" intelligent process automation to C-level executives and other organizational stakeholders, both upstream and downstream?

Heckman:
Cybersecurity professionals need to focus on presenting the benefits to both groups of stakeholders. For C-Suite Executives, highlight the impact and value of addressing workforce

shortages, improved data processing, efficiently supporting business intelligence, effectiveness, and growth. For other organizational stakeholders, highlight the fact that intelligent process automation can allow them to be more efficient by handling workloads quickly and with fewer errors. Additionally, the technology also empowers users to work flexibly and agilely by enabling them to focus their time and energy on rewarding, creative tasks without relying on costly or time-intensive technology system enhancement cycles.

ICIT:
Are there any sector or industry-specific considerations when automating? For example, financial and auditing industries currently have a higher adoption rate for automation.

Heckman:
No, there are not any industry-specific considerations when thinking about automation. RPA is currently implemented across various functions and industries, including federal agencies and Fortune 500 companies. It’s about identifying the best candidate applications for automation. In the case of the financial and auditing sectors, they have a lot of repetitive, rules-based processes, such as data management, report creation, and routine email communications, that lend themselves to automation. For example, banking industries use RPA for compliance and credit card processing, while human resources use RPA for payroll and processing employees’ information.

ICIT:
As terms like RPA, automation, and AI become buzzwords, the market becomes saturated with vendor solutions that market the terms without actually delivering on those technological promises. Do you have any recommendations on how to best distinguish between faux and reliable solutions for those looking to adopt automation?

Heckman:
I recommend working with a company with a proven track record of delivering RPA capabilities with industry-specific expertise. They can help drive automation, data-driven decision-making, and assist with identifying candidate applications and processes to automate while keeping in mind your organization’s requirements and regulations. Additionally, it is crucial to find a technology agnostic company that can work with the leading automation products such as UiPath, Blue Prism, Automation Anywhere, and Microsoft Power Automate.

ICIT:
How can automation success be gauged or what are appropriate metrics for automation efficacy?

Heckman:
Companies can use multiple metrics to determine the value of automation. You can measure work hours saved or increased productivity. Alternatively, you could measure improved quality through error reductions or improvements to metrics related to the automated business processes. Businesses can also measure employee satisfaction as they are freed from doing repetitive manual time-consuming tasks.

ICIT:
Please share an example of an automation implementation. What best practices should business leaders learn from this example?

Heckman:
The Office of the Chief Financial Officer within the Department of Housing and Urban Development worked with a major global consulting company to overhaul multiple financial management business processes using RPA. Along with being more efficient and cost-effective, these new processes created a replicable and Federal Accounting Standards Advisory Board-compliant workflow that ensured the accuracy and completeness of the needed financial data. Using RPA, the project delivered new methodologies to:

- Gather and validate data;
- Provide audit-ready packages containing root cause analyses;
- Create remediation approaches;
- Develop training materials;
- Supply additional supporting documentation; and
- Address and rectify the Office of the Inspector General findings.

Best practices include defining and documenting the vision, demonstrating measurable impact for the organization and its employees through a pilot, and establishing an RPA center of excellence to develop in-house RPA programs.

ICIT:
Are there any final thoughts you would like to conclude on?

Heckman:
From simple, repetitive, rules-based tasks to complex, multi-step processes requiring machine learning or AI, RPA can be customized to the unique demands of the business process and the

environment in which it operates. While RPA cannot replicate every nuance of human activity, it can create efficient and reliable solutions that leverage the strengths of both automation and human intelligence. This outcome allows business leaders to better optimize their assets in terms of both data and personnel while creating a significant opportunity for evidence-based decision-making.

In terms of supporting cybersecurity, RPA and intelligent automation can take over for various manual, time-consuming tasks related to good cyber hygiene, such as patching, configuring, and deploying systems. RPA bots can also respond to cyber events and review and analyze audit and SEIM logs, freeing up limited cyber resources to focus on more challenging tasks. In terms of cybersecurity, when implementing RPA technologies, one should use sound cybersecurity principles, including least privilege and least functionality, to accomplish the desired functions. Adopting new and innovative technologies creates new challenges and opportunities. Businesses must effectively manage new solutions with a mission-driven approach to ensure success. Consult with an independent and trusted advisor that combines high-quality thought leadership with deep mission understanding. Experienced partners can help an organization develop an effective, secure, intelligent automation strategy by providing customized organizational analysis and advice on technological tools and skillsets tailored to your specific organizational needs and objectives.