

Robotic Process Automation Security

How to Ensure Your BOT Doesn't Go Terminator

For many enterprises considering robotic process automation, concerns around security are preventing action. More often than not, it's the IT department that is slamming on the brakes, concerned about the potential scenario of dozens of robots running amok across its systems. What's real and what's not when it comes to RPA security concerns?

While robotic process automation (RPA) is currently one of the most popular enablers of services, there is still plenty of mistrust, and sometimes fear, around the idea of unleashing an army of robots on enterprise systems. In many cases it is the IT department – often for the right reasons – that presents the main hurdle. While an often touted ‘benefit’ of RPA is that the business itself can implement robotic solutions, with little input required from IT, the truth of the matter is that you’ll need IT’s engagement in design and deployment if you need them to partner on a solution, when things go wrong.

Despite these concerns, the market for RPA is undoubtedly growing. The danger is that in the current feeding frenzy, it's tempting for firms to build a ‘quick and dirty’ robotic capability that lacks security, scalability, and sustainability. While there may be cost benefits in the short term, there’s a good chance the company will pay for it in risk and scale, in the long run.

Content curated by: Barbara Hodge, Editor, SSON

Robotics as Drivers of Survival and Success

The agility that RPA offers can make the difference between surviving or not. Enterprises like the UK's Lloyds Bank have recognized this and are jumping at the opportunity to reinvent themselves for the Millennial age and the growing Millennial customer base. Lloyds is not simply tweaking itself to present a more modern face to the market, but is rebuilding itself as a true digital bank with highly automated processes that attract the Millennial generation.

"Opting out really isn't an option," says Scott Furlong, a service delivery consultant from ISG, who references Blockbuster and Kodak as examples of what happens when organizations fall behind and their more innovative competitors take the lead.

While robotics is still primarily driving cost savings, the potential for shifting into an integrated, digital ecosystem driven by automated processes is enormous. Consider Disney's Magic band – it's a room key, a security device, a payment system, a GPS and a channel for cross selling. "The Internet of Things presents a vast opportunity, and robotics is absolutely key to leveraging it," Furlong says.

Safer than humans?

But first: how much is robotic automation exposing your processes to risk? RPA vendors and consultants point out that, contrary to general concerns, robotic processes tend to be far more secure than human-run processes. After all, robotics operates strictly within the regulatory and security parameters of the humans they replace. And, unlike humans, robots following a clearly programmed, automated, sequence of events are unlikely to err. They don't get distracted halfway through a project, or respond to rogue emails, leave a screen unlocked that contains sensitive information while they get coffee, or allow themselves to be derailed from the current task.

"Realistically, your processes probably couldn't be more secure than in a robotically automated environment," Furlong says. He points out that in the late nineties, the idea of moving shared services captives offshore resulted in similar denials around the impossibility of serving multiple languages from distant locations, processing non-paper documents out of country, etc. Furlong insists the biggest problem around security tends to be convincing IT that there is none. "As long as things are done right!"

"A robot is just another piece of software," he says. "It does what it is told to do. So, as long as you test the code rigidly and lock it up, no one else can tamper with it." The key, Furlong says, is to maintain strict controls and testing on development and maintenance throughout the life cycle.

Valid Concerns (but manageable)

One of the first firms to develop RPA solutions was Blue Prism, which initially introduced robotics to its banking clients back in 2008. CMO Pat Geary agrees that the concerns around RPA security are entirely valid, but can easily be mitigated, "as long as companies take a thorough approach to implementation and partner with a reputable firm."

To understand the reality of security issues within RPA, we need look no further than the most regulated industry of our time: banking and financial services, many of whom are now entrusting their core operational data centers to robotic processing.

Geary believes the key security determinant is getting IT involved from the start and ensuring they are on board. One of the selling points of RPA has been the ease with which it can be implemented by the business line, 'without the involvement of IT.' On closer inspection, many of these broad statements are more of a marketing gimmick than a real strategy, warns Geary.

Your Bot is Visible, Traceable and Secure – So What is Missing?

Automated logins are entirely traceable. The challenge arises where one part of the process is administered by humans, then handed over to robots, then back to humans. Geary points out the problem here is really about simplification, and lack of straight-through processing or integration, where a single sign on allows continuous workflows without the stop-start that characterizes handovers.

What it usually comes down to is the more homework and preparation done, the more robust and secure the solution. Today, recognizing the enormous opportunity of RPA, the market is exploding with providers who profess to offer quick and easy (and cheap) solutions to processing challenges. As always, if it sounds too good to be true it may just be that, at least in the long term – which is where you may run into trouble as you post patches or upgrades that could possibly destabilize your operations.

"Everything we do is based on central control via secure servers," Geary explains. "And while that may mean it takes a bit longer and it costs a bit more, you'll never find yourself on the wrong side of the security fence".

Bot 'Personification' Misleading

One reason there is still so much resistance to RPA might be the personification that has evolved around robotic processing, which opened up the specter of robot armies taking over the enterprise. "It's led to a kind of paranoia that is hard to reason with," explains Neil Kinson, chief of staff, at Redwood Software. "In truth, and despite rare, but high profile, attacks on payment portals, notably the Bangladesh Bank heist, the bulk of the real risk exposure comes from the people in your organization. It's silly things like Post-it notes with passwords sticking on a monitor, or shortcuts people take to ease their daily workload, or the malware they inadvertently install... There is plenty of risk associated with humans, which robotics removes from the equation."

Locking in System Weakness

While it's true the rigor of robotics removes a lot of process risk, ironically, the more user interface-focused the solution, the greater the exposure to another kind of risk.

The reasoning is quite simple: desktop, or user interface-based robotic process automation (also called swivel chair robotics), effectively emulates the behavior of a human, just faster and more rigidly. This does mean, however, that you are effectively locking in legacy technologies. Kinson warns the perpetuating of legacy systems, which by definition are more prone to vulnerabilities, represents one of the key risks of RPA. In addition, once organizations robotically automate a process, many take their 'foot off the pedal' and don't modernize the underlying systems, because they've been 'fixed' through robotics. "The real danger, then, is whether the next security patch might 'break' the robot," says Kinson.

"While it's true the rigor of robotics removes a lot of process risk, ironically, the more user interface-focused the solution, the greater the exposure to another kind of risk."

Regression Testing

One of the questions right now is the extent to which providers are supporting regression testing to ensure that the bots won't break as updates occur.

This is a key concern for Christina Critzer, SVP of ECM, BPM, Automation & EIS Delivery Tools at SunTrust Bank. Her team provides technology solution implementation services across the enterprise and has actively been promoting document imaging, workflow, and, more recently, robotics.

One of the questions Critzer's team is seeking answers to, right now, is the extent to which providers are supporting regression testing to ensure that the bots won't break as updates occur. "We use the same robotics components across multiple processes, so we want to be sure that as we update the workflow, or change one of the applications, we only need to make one adjustment, which is automatically pushed across all iterations," she says. The question is, therefore, how will providers

handle configuration management and how will they adjust as a workflow is redesigned, so as to minimize risk exposure? “It would be highly inefficient if we had to make changes at individual process levels, considering the volumes we work with,” Critzer says. “What we are finding, though, is that each provider has a different answer”.

Starting Point: Architecture and Authentication

To tackle security concerns in RPA head on, everything must be built solidly and securely from the ground up, says Geary. And that starts with the architecture. Attention to detail is crucial. It’s this approach, Geary believes, that has gained Blue Prism more than 140 high-performing F500 clients to date, including IBM, Accenture, and EY.

One area Geary warns about is ‘individual authentication’, where robots use employee log-ons and it becomes difficult to distinguish human activities from those of the bot. Instead, he believes, companies should opt for a tried-and-tested enterprise model that takes work off the desktop and onto virtual machines that are locked down. In this scenario, Geary explains, robotic authentication takes place in the data center, complete with their own access rights and controls. “It’s completely different from the shadowing that goes on with user IDs,” he says.

Security is given a boost when each robot is given its own individual logon, and its own permissions from the system. The architectural-design philosophy behind high-security RPA implementations stands head and shoulders apart from desktop-driven RPA, Geary emphasizes – and it removes the fear of ‘script-ageddon’, where work is thrown onto hundreds of desktops without the strict controls that need to be in place.

There are plenty of examples of what can go wrong. Local script-driven automations are vulnerable to power outages that result in script failures, and tapping IT for help won’t help either, unless IT has ownership over the software and has signed off on security installations. In addition, the potential of having open scripts running on a user’s desktop while that person steps away for coffee would expose an organization to extreme risk.

“An enterprise or platform approach takes longer,” Geary concedes, “but if you want to build a tall building you need to build on a solid structure.”

IT: Your Partner If (When) Things Go Wrong

Most practitioners cite ‘getting IT on board’ as their main challenge, and it’s a significant one, given that RPA marks the first time many business lines or Shared Services Centers are driving technology solutions themselves, instead of relying on IT to take the lead. IT is often seen as a ‘blocker’ to RPA, often suggesting ‘the next version of SAP’ as the better solution to a problem. But waiting simply isn’t an option for organizations that needs to reap a competitive advantage in every area of operations – and that includes support services.

To tackle security concerns in RPA head on, everything must be built solidly and securely from the ground up.

Christina Critzer represents the forward-looking face of IT that organizations need to harness if they are going to shift beyond ad hoc RPA fixes, and develop an operational capability to drive performance. “In the early days, businesses underestimated how important it was to get IT involved. Today we are partnering to build a forward, unified vision,” she explains.

At SunTrust, the business led early robotic processing implementations, and Critzer has now been tasked with assessing how best to operationalize this capability across the enterprise, building a Center of Excellence. “To a certain extent there’s a panic now,” she says, as the enterprise realizes that we need to catch-up and get that solid foundation in place.

“Robotics works great the first time, but the moment you start upgrading the parts there is the risk of breaking the bot. If IT has not been engaged up to that point, it’s going to be difficult to get them in to help at that critical stage. Right now, we’re slowing down to go faster, and building in robust governance to ensure success.”

In preparing, Critzer is planning for “the unhappy path”, not the happy path that most functional leaders like to focus on. “From an IT perspective, we need to figure out how to support this application across the enterprise and impose the same disciplines we are already committed to onto this new solution.”

RPA Beats EUC, But...

While actually committing to RPA is still a big step, most companies have been undertaking automations using various tools for many years, says Simen Munter, Global Head of ANZ’s Shared Services Organization, and passionate RPA advocate. “And they have an established in-use approach to End User Computing (EUC).” There are key issues that distinguish RPA from these EUC tools, he says, and which work in RPA’s favor, including a detailed audit trail, centralized user management and scheduling management.

On the other hand, all software solutions have future support and migration issues, Munter warns. For example, the people that created them may have moved on. “This is an increased risk when you are deploying tools that are not maintained by your own technology function, but by a provider,” he says. In addition, as these tools can be developed by business resources that do not have IT programming experience, there’s also the risk of logic errors creeping in, which could compromise the accuracy of processing or information used to make decisions that have an adverse financial, reputational or regulatory impact.

“Given the ease with which these solutions can be developed, there is also a risk that teams fail in standard release management, or in executing the proper segregation of duties in the development and support phases,” Munter says. “In addition, it’s important to ensure that you have the right skills sets within your IT group, as many IT teams don’t know how to manage these tools and, as a result, are coming up with rules that make it impossible to meaningfully implement RPA.”

Some of the other risks Munter lists include:

1. *Compliance risk through extracting or processing data outside of core systems, which can cause regulatory intervention and fines. (Regulations typically do not discourage the use of Automations, however require businesses to ensure that data controls created in one applications are not overridden elsewhere – including through the use of RPA.)*

2. *Accuracy of RPA coding that may result in financial loss or reputational damage. (Logic errors; incorrect process logic; risk of replication of transactions; scripts facilitating fraud, information leakage or damaging information held in systems; failure to trap, return or handle errors and thereby bring them to human attention when an unexpected event occurs in logic conditions; inaccurate or unexpected input data; assumptions that all input data is clean and accurate.)*

3. *Exposure of confidential or restricted customer and company data. (RPA Automations that are used to collect confidential or restricted information may not have the same level of protection controls as technology supported applications, or as required by company standards for information handling, regulatory or industry bodies.)*

4. *Availability of critical business processes. (Whilst improving BCP for a normal outage, malfunctions in automation tools may have an impact on a critical business function which would not be able to operate manually post RPA; risk of not enough FTEs to compensate manually if RPA is unavailable; missing documentation may affect service restoration time as it may require skilled persons or time to understand the logic within the tool to correct the bug(s) which caused defect(s); key person risk – staff who have developed applications may no longer be available to support the automations.)*

Given the ease with which these solutions can be developed, there is also a risk that teams fail in standard release management, or in executing the proper segregation of duties in the development and support phases.

Loss of Process Intimacy Impacts Continuous Improvement

While the user-interface approach is quick, easy, and effective, it can be inherently risky. Desktop robotics is about eliminating a discrete set of topics, explains Redwood's Neil Kinson. This translates well to transactional work that takes up a lot of man hours, but has the downside of eventually hitting a glass ceiling of sorts, where you max out the ability of interconnected micro-tasks to interact. Another limitation is that robots, unlike people, cannot identify which parts of the process are a waste of time. So, when it comes to continuous improvement, the loss of 'process intimacy' also means the loss of the innovation driver that humans bring to the table.

"The risk is that you hold onto a lot of inefficiency because it's now embedded in robotics and you don't have the context that an output-oriented solution would give you," says Kinson.

Published Interfaces Provide Robust Basis

One solution providers like Redwood or Blue Prism are promoting is to work through published interfaces that connect directly with enterprise applications, instead of desktop interfaces. This approach effectively ‘reengineers’ the way the process is done, says Kinson: “Instead of emulating how humans connect systems, via various steps, you start with the desired outcome and work towards getting to the same solution – but via a different route.” The added comfort, he says, is that by definition these published interfaces represent higher levels of stability and protection because they are core to the ERP architecture.

Next Up: Artificial Intelligence – Where Will It Take Us?

AI is often thrown into the same mix as RPA without enough practical proof of their connection or even applicability. “Right now, artificial intelligence is being overstated, at least in terms of its practical implementations in support services to date,” says Kinson. “In truth most of the automation today is not yet about intelligence, but what you might term ‘automated stupidity’ – it’s the dull and mindless work that’s been automated so that humans are freed up to leverage their intelligence.”

The real wins of AI right now are in crunching large volumes of data for analytics and trends. As far as financial processing or other functions are concerned, AI is still more of a philosophical debate, believes Kinson. “AI is about the ability to find patterns in enormous volumes of data and to identify these patterns for decision-makers. We can certainly see the applicability for connecting with robotics, but we are not yet at the stage where we would want robotic software to draw conclusions about financial data and redesign itself without human intervention or governance.”

“Intelligent Automation (IA), on the other hand, is something developers are wrapping their minds around. That is really about intelligent insights into executions that drive intelligent improvements – but again, it’s based on AI’s ability to analyze large volumes of data.”

SUMMARY

Any innovations, whether in technology or travel, push the envelope. Early adopters run the risks but also reap the rewards. The promise of RPA’s impact on service performance simply cannot be overlooked, but organizations need to take a holistic approach, ideally from the start, in setting up a strong platform to leverage the benefits of RPA across the enterprise.

While most companies so far have started small and local – may, indeed, carry on starting that way – getting IT to the table early on will safeguard your investment and support scalability.

Robotic Process Automation at SS&O Week...

ATTEND THESE SESSIONS:

RPA TRACK

A range of practical case studies and panel discussions on RPA for the finance and HR processes. Topics discussed include: Practical Implementation Guides, Intelligent Automation Security Governance (How to Ensure Your BOT Doesn't Go Terminator) and AI within Shared Services.

Hosted by  **ANYWHERE**
Intelligent Automation



RPA INTERACTIVE DISCUSSION GROUPS

Sign up and reserve your place on one of our RPA interactive discussions: The Truth (And Myth) behind Robotics Process Automation or Removing Manual Activities from your Period-End Close via Enterprise Robotics.


PRE-CONFERENCE RPA MASTER CLASS - OPERATIONALIZING RPA - TOP 10 CHALLENGES (AND HOW TO OVERCOME THEM!)

Using a variety of case studies this master-class focuses on; a) collaboration with IT on architecture, infrastructure, security and change management, b) communication planning, stakeholder management and organizational redesign, c) governance, compliance, controls, audit and measuring success and d) RPA COE organizational structure.

Hosted by  **ALSBRIIDGE**
Challenging the Future

SITE TOUR AND ROBOTICS HOW TO GUIDE

See first hand the impact of PWCs robotics process automation pilot in their Finance, HR and Procurement functions, and understand how, as one of the US's biggest recruiters, RPA had a significant impact on their hiring process.

Hosted by  **pwc**

HR AND ROBOTICS

Explore Walgreens' recent RPA transformation within its HR function and understand how you can use Robotics for recruiting, payroll, scheduling, talent management and much more.



KEYNOTE PRESENTATION, THE RISE OF THE ROBOTS, MARTIN FORD

Futurist, New York Times Bestselling Author, Speaker and Silicon Valley Entrepreneur



**FOR MORE INFORMATION OR TO REGISTER,
VISIT WWW.SHAREDSERVICESWEEK.COM
OR EMAIL ENQUIRY@IQPC.COM**