WELCOMING OUR ROBOTIC SECURITY UNDERLINGS

Author:

Fred McClimans, HfS Research
February 2016

Introduction

Security breaches are not restricted to the cyber-realm, and often include an element of physical/human involvement. New technologies, such as Robotic Process Automation, may hold a key to improving digital trust and removing a human element of insider risk.

TalkTalk Telecom Group plc, a major telecom provider in the UK, has become a poster-child for improved security operations. In October 2015, in a clear case of cyber security influencing brand trust, TalkTalk suffered a major data breach involving 157,000 customer records, which impacted consumer trust and resulted in the loss of 100,000 customers (according to the company).

Its most recent breach, however, is perhaps more telling to the industry at large—it involved a small group of insider contractors who leveraged their positions in a service provider's delivery center to conduct unauthorized activities. This issue was only uncovered as a result of an internal forensic audit, conducted by BAE Systems, triggered by the earlier (2015) breach.

The call center breach exposed a significant weakness common to many organizations: unpredictable or rogue insider behavior that tests—and breaks—the traditional technical approach to cyber security (Edward Snowden v NSA incident being perhaps the most notable case in recent years). Contract workers had direct access to data via onsite computers and took advantage of the situation.

How do you counter this type of insider behavior? One increasingly viable approach is through software robots.

The Promise of Intelligent Automation

Outsourcing has played a key role in the evolving value proposition of business process and IT delivery. But the idea of creating business value by shifting processes outside of the control of the enterprise has come with real risks. Too much of the workload that has been outsourced in recent years has included the input and management of data (e.g., consumer support calls, paper documents, etc.) that contains sensitive information often manually handled by human agents.

To help mitigate risk, service providers and enterprises tried to impose security processes, such as physically limiting access to computer/PC workstations, restricting access to USB/drive devices, leveraging desktop applications to limit exposure to sensitive (or not-required) data, and the implementation of scripts that, when activated by the worker, would initiate a preset activity. But risk remains because computers and scripts (which often store customer or credential data) are still under the control of a user, and desktop apps themselves can be easily corrupted or exploited.

With the advent of the online and social revolutions, both customer contact and back-office operations have shifted to digital (many industries now focus on online customer self-service, creating a customer support infrastructure that is entirely digital). The significance here is the elimination of, or diminishing need for, human involvement at both the customer and back-office levels. That helps to address some of the concerns of the more analog-era process delivery under outsourcing but there is still too much access control in the hands of humans to be entirely secure.

The need to remove humans, and the risks related to data management and control, from process tasks is now being addressed by the availability of Robotic Process Automation (RPA) tools and the deployment of dynamic software robots. Deployed properly, RPA and software robots can eliminate the need for human agents to interact with many systems of record and systems of engagement in the enterprise by conducting the same task steps using auditable, managed bots following pre-determined business rules. This eliminates some of the fundamental security risks associated with outsourcing or even the use of remote internal shared service or global business services centers in the enterprise–a point particularly important in highly regulated industries such as financial services or healthcare where the risks associated with data leakage can be extreme compared to those in other industries.

The emergence of today's RPA tools addresses several key business and security requirements:

- **Capacity:** the need for software and automation tools that can handle extremely high/variable work-loads
- **Flexibility**: the requirement to adapt quickly to changes in content or context (flexible rules)
- **Awareness:** maintaining a stateful status that is aware of both workload and workflow (mimicking human behavior, which allows for transactions to slow or roll-back in the event of an error)
- **Risk Mitigation**: removing much of the human interaction with desktops (including virtual desktops) and applications to minimize security risks
- **Audit Trails**: having complete end-to-end verification and auditing mechanisms to eliminate errors, data corruption, and fraud

This isn't to say that all RPA tools are created equally when it comes to security. Just creating an individual desktop software bot that has recorded the tasks of a human and then runs them automatically doesn't necessarily create an entirely more secure environment. The software bots themselves need to be managed and watched to monitor behavior and ensure that the robots are carrying out the rules of the processes as defined and the automated task delivery is as secure as possible. In fact, security requirements and the regulatory environment in which an enterprise operates are major evaluation criteria for both service providers and the enterprise when it comes to selecting which of today's many different tools for RPA make sense for a given process or enterprise.

What to Watch

This is a rapidly evolving space. Increasingly, all RPA tool vendors and service providers are aware of both the security advantages their tools bring over manual human activities as well as the mounting security concerns that the software needs to address. HfS has seen some very interesting approaches to software robots and RPA that have both business process and security/risk management value. Blue Prism, for example, has adopted an approach to implementing RPA that is very similar to what we see in cloud computing, with the ability to spin up/tear down an RPA ecosystem to meet changes in need and provide a high level of flexibility. A single robot can run, and maintain an audit trail for, any number of different processes based on real-time demand.

There is also an inherent level of security associated with robotic automation, as software robots can be essentially "virtual" and torn down upon task completion (you can't hack a resource that no longer exists). Data can also be co-located with the software robots—eliminating a significant risk associated with the transfer of enterprise or consumer data between data and processing centers.

From a digital trust perspective, we see high potential value in the use of RPA to eliminate process-oriented risks and security threats, ultimately resulting in a digital ecosystem that is both reliable and trusted. In that way, RPA software bots have the potential to become our security conscious underlings, delivering rules based processes in a controlled environment that is more aligned to addressing the security concerns of the enterprise today.

About the Author

Fred McClimans

As EVP of Strategy & Research Managing Director, Fred McClimans helps lead the strategic direction of the firm as well as leads our research coverage in the area of digital trust and security.

Fred is a seasoned technology and analyst veteran, having founded two analyst firms, including Current Analysis, a global competitive intelligence and market advisory firm that pioneered the use of real-time market analysis coupled with social SaaS tools to help business and brands monetize changes in global markets. Current Analysis was acquired by Progressive Digital Media (UK) in 2014.

Previously, Fred co-founded Decisys, an analytical consultancy, which was acquired by the Burton Group, and later by Gartner (in 2009). In addition to his years as an analyst at Gartner, Fred's experience includes helping Newbridge Networks (now Alcatel) stand up their Advanced Technology Group, serving as the Chief Information Officer at DTECH LABS (a secure mobile communications provider, now part of Cubic Corporation), and Ernst & Young, were he was a Manager in the Technology Consulting Practice.

Fred lives outside of Washington, DC with his wife and family. An avid competitor, Fred has logged his time as an amateur hockey coach and martial arts instructor.

Fred can be reached at fred.mcclimans@hfsresearch.com and followed on Twitter at @fredmcclimans

About HfS Research

We coined the As-a-Service Economy term because we see a profound change under way that is more all-encompassing than a simple business model or product line. It's a global shift that will leave few sectors of business or society untouched.

To help our clients and the market get to the As-a-Service Economy, we serve the strategy needs of business operations and IT leaders across finance, supply chain, human resources, marketing, and core industry functions in organizations around the world. HfS provides insightful and meaningful analyst coverage of best business practices and innovations that impact successful business outcomes, such as the digital transformation of operations, cloud-based business platforms, services talent development strategies, process automation and outsourcing, mobility, analytics and social collaboration. HfS applies its acclaimed Blueprint Methodology to evaluate the performance of service and technology in terms of innovating and executing against those business outcomes.

HfS educates and facilitates discussions among the world's largest knowledge community of enterprise services professionals, currently comprising 100,000+ subscribers and members. HfS Research facilitates the HfS Sourcing Executive Council, the acclaimed elite group of sourcing practitioners from leading organizations that meets bi-annually to share the future direction of the global services industry and to discuss the future enterprise operations framework. HfS provides sourcing executive council members with the HfS Governance Academy and Certification Program to help its clients improve the governance of their global business services and vendor relationships.

HfS trail blazed the freemium research model. More than 75% of our published research requires just a few check boxes in our simple registration to download—no subscription, no hassles.

See how we're revolutionizing the research business with the Four Pillars of HfS Research—our guiding principles.

Learn more about our services.