blueprism®

ACHIEVING THE TRIFECTA OF CYBERSECURITY GOVERNANCE WITH A HYBRID WORKFORCE

Collaboration with intelligent automation enhances public sector's security posture

Introduction

The pandemic has served as an inflection point for public sector modernization. Across all areas, its organizations have had to innovate and transform at breakneck speed to maintain critical services and continue meeting citizens' demands and expectations. But, at the same time, cybersecurity threats have skyrocketed.

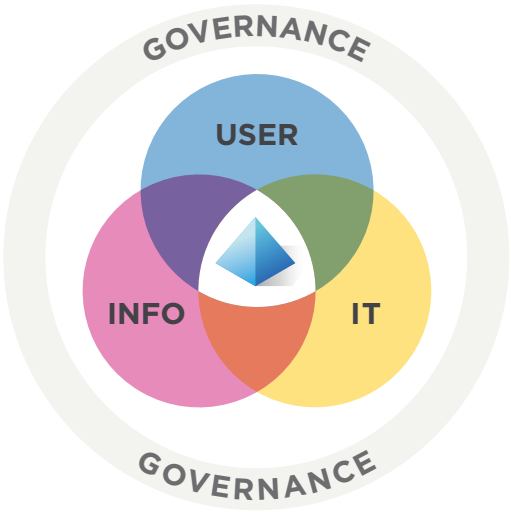
Cybercriminals have looked to exploit new opportunities that have arisen with millions of citizens turning to digital services for the first time, including many without an understanding of what is 'safe' within their digital engagements. Public sector employees have also helped to increase the size of the cyber target for criminals by accessing IT applications and infrastructure remotely and relying on online identity verification checks.

A hybrid workforce of human workers collaborating with intelligent digital workers can provide the resources, skills and robust processes organizations need to counter an ever more fragmented and complex risk landscape.

The scale and sophistication of these threats continue to increase, particularly ransomware attacks. In fact, instances of ransomware have soared to a staggering 288% in the first half of 2021, according to a report from NCC Group's Research Intelligence and Fusion Team (RIFT). Additionally, our partner Deloitte ran an article, Impact of COVID-19 on Cybersecurity, suggesting that CISOs and CIOs must consider a zero-trust "security model where only authenticated and authorized users and devices are permitted access to applications and data" to counter the explosion of cyberattacks.

The Executive Order on Improving the Nation's Cybersecurity was the biggest signal yet that federal government concerns about emerging online risks are increasing, both at home and abroad. It acknowledged the federal government's need to improve and accelerate its efforts to identify, detect, ameliorate, deter and respond to increasingly sophisticated, malicious cyber campaigns. It was also a call to action for stakeholders outside of government to work together to foster a more secure cyberspace. Partnerships between public and private sectors are critical in meeting immediate and future threats.

Across the industry, public sector organizations recognize that the online risk landscape is rapidly evolving, and they simply can't afford any slip-ups in data privacy and security. Hence the massive focus (and huge investment) on to zero-trust initiatives across every corner of the public sector.



But one role that has, until now, been largely overlooked when it comes to cybersecurity responses within the public sector is the one intelligent automation can play. A hybrid workforce of human workers collaborating with intelligent digital workers can provide the resources, skills and robust processes organizations need to counter an ever more fragmented and complex risk landscape.

This paper explores how a hybrid workforce can be implemented by public sector organizations across the Trifecta of Cybersecurity Governance—user, information and IT governance—to identify vulnerabilities, minimize risk and enhance the security posture.

PART ONE

User Governance

How a hybrid workforce can minimize user-initiated risk

For many public sector organizations, user governance is the most difficult area of vulnerability to manage. The sheer number of variables makes it extremely hard to predict and manage the behaviors of an entire workforce. Internal users are typically the root cause of most data breaches; employees fail to manage their accounts properly, whether they're writing down passwords, enabling unauthorized people to access systems or falling victim to phishing attacks.

The scale of the challenge has been exacerbated by the increase in remote access with which organizations have enabled their staff to work from home during the pandemic. It has created vulnerabilities around user identification, access, and management.

Of course, organizations also must deal with more intentional, malicious insider attacks. The Snowden and Manning disclosures exposed the limitations of people-centric approaches to background checks. Rigorous security training, though effective at thwarting some disclosures, is not always enough to prevent determined threat actors from executing an attack.

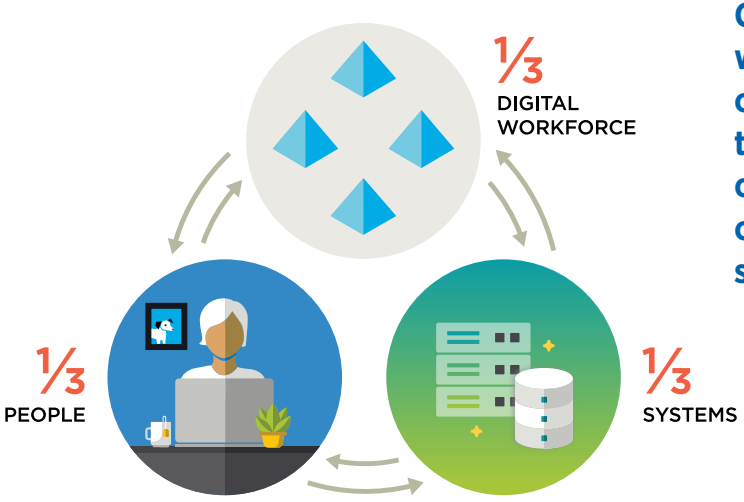
This is why, to fully guard against insider threats, public sector agencies must utilize identity technology solutions rooted in governance. While strong, multi-factor authentication is an essential first step to defending against external actors attempting to steal credentials and gain access to a network, using it as the only aspect of an identity security strategy is insufficient. After all, malicious insiders are already credentialed to act within a network.

A hybrid workforce to tackle "The Five As" in Identity and Access Management

Governance-based Identity and Access Management (IAM) approaches go beyond authentication. Addressing the full lifecycle of IAM lifecycle, viewed through the prism of "The Five As"—Authentication, Authorization, Administration, Analysis and Audit—enables organizations to tackle the full range of identity risks associated with insider threat.

And with intelligent automation, organizations can automate large parts of their user governance processes across these five areas, improving accuracy, efficiency, and speed. Digital workers execute pre-determined tasks and processes, freeing up human workers to focus on decision-making and handling exceptions. Overall, this hybrid model greatly improves the strength and proficiency of the organization's IAM.

Digital workers can also be deployed within teams to streamline and optimize privileged access management (PAM), controlling and monitoring internal employee privileged user activity through additional security steps such as second factor authentication.



Critically, with an intelligent digital workforce on-board, public sector organizations can consistently ensure that users aren't creating the loopholes or vulnerabilities within applications or systems that can so easily lead to serious data breaches.

Fighting phishing with a hybrid workforce

Another major vulnerability for public sector agencies is the growing threat of phishing attacks. Many employees either don't know how to identify a potentially fraudulent email, or they're not aware of the risk at all.

Digital workers, on the other hand, are far less susceptible to trickery from look-alike emails. Organizations can deploy digital workers to monitor a centralized inbox as part of a business process, identifying emails that match a specific subset of messages from a small set of whitelisted email addresses. Only these emails are permitted through to be opened by human workers. Emails that don't match this rigorous set of criteria are rejected by the digital worker from the outset, eliminating any chance that an employee might click on something that he or she shouldn't.

For public sector organizations, this hybrid approach, utilizing the capabilities of both human and digital workers, creates the potential to dramatically reduce the risk of phishing attack, as it has done in industries such as financial services over recent years.

An automated, proactive approach to user governance

From user behavior analytics through to security information and event management, digital workers can deliver real-time analysis of anomalies and security alerts generated by applications and network hardware. They can continuously monitor inventory and make updates when they discover risky areas. Risk classification can also be automated by applying cognitive learning to previously detected data.

Critically, with an intelligent digital workforce on-board, public sector organizations can consistently ensure that users aren't creating the loopholes or vulnerabilities within applications or systems that can so easily lead to serious data breaches.

Another way of thinking about this is that intelligent automation can reinforce and enhance cybersecurity by reducing the number of human touchpoints within applications, particularly in legacy applications that lack modern security capabilities.

For instance, some federal and SLED entities are still deploying legacy mainframe applications, which are notoriously susceptible to modern security threats. However, by automating the interface of these applications and reducing or removing the human element involved, a limited number of touchpoints remain, if any, where malicious insiders or external actors can attempt to probe the system and exploit vulnerabilities.

PART TWO

Information Governance

Driving data security with a hybrid workforce

A key area where digital workers can make a huge impact is in mitigating data privacy risks by efficiently defining, finding, managing and securing files containing sensitive data, across both live and backup data. A digital worker can learn which type of data is sensitive, then scan through millions of files to identify those containing such data. Where an anomaly is detected, the digital worker can also streamline remediation, facilitating decision-making between IT, security teams and data owners to ensure that sensitive data is secured or appropriately deleted.

Critically, by undertaking these tasks, the digital worker can free up IT and security teams from this kind of time-consuming, process-driven work to focus on higher value tasks. Digital workers can perform process-driven tasks faster and more accurately than human workers—but they can't apply creativity and objective problem-solving to tackle business issues. By implementing a hybrid workforce, organizations can point their best IT and security talent towards their biggest strategic priorities. This is particularly important when the federal government struggles to find and retain the very best cybersecurity skills.

Easing the compliance burden on IT and security teams

Public sector entities are finding adherence to the amount of regulation which now applies to data privacy increasingly difficult. Not only must they execute and report on compliance with federal legislation, such as the National Institute of Standards & Technology (NIST) and Cybersecurity Maturity Model Certification (CMMC), but many organizations also need to follow industry-specific regulation, such as Health Insurance Portability and Accountability Act (HIPAA) within the healthcare sector.

But compliance is an area which naturally lends itself to the deployment of a hybrid workforce, thanks to its rule-based nature. Digital workers can be deployed to automate all subprocesses of certification, replacing manual validation checks of precertification data, campaign checks during access certifications and reviews, and certification configuration management. Beyond this, digital workers can automate post-certification reconciliation and reporting, leading to significant reductions in unauthorized access and PII data looting.

Once again, the benefits in terms of information governance are potentially game-changing. Digital workers are able to ensure compliance across multiple sets of regulation, while also minimizing personal data footprints from live and backup data sources.

With digital workers providing real-time, accurate data and insight into current and future risks, IT and security leaders can develop a more agile governance structure across all facets of security, directly aligned with their wider business strategy.

At the same time, existing teams can move away from manually carrying out process-driven tasks and instead focus on addressing anomalies and troubleshooting red flags before they become serious issues.

A proactive approach to risk with a compliant hybrid workforce

Risk assessment and management is another major area of information governance where a hybrid workforce can alleviate much of the pressure on public sector agencies.

Currently, IT and security teams spend a significant proportion of their time analyzing incident logs and reports, trying to identify potential vulnerabilities, loopholes and decipher patterns of suspicious behavior. But even the most diligent team members miss things when manually undertaking this type of fine detail activity.

This is where a digital worker can make all the difference, automating the entire risk identification, analysis, and evaluation process. Digital workers can assess physical, cyber and personnel vulnerabilities from multiple attack scenarios with far greater efficiency and accuracy, eliminating the risk of human error.

This has clear benefits when it comes to mitigating immediate risks but, beyond this, the use of digital workers in this area enables IT and security teams to take a more proactive approach to both enterprise security and compliance.

With digital workers providing real-time, accurate data and insight into current and future risks, IT and security leaders can develop a more agile governance structure across all facets of security, directly aligned with their wider business strategy. This, in turn, can enable them to embed a zero-trust culture and behaviors within their workforces, a shift that every public sector agency needs to instigate urgently.

But to do this, it's vital for public sector agencies to implement an intelligent automation platform. Furthermore, they must provide a full audit trail for digital workers with all relevant legislation to show and report on compliance. The platform should ensure accountability for all digital workers, assigning unique identities to each digital worker and allowing for frequent rotation of security credentials.

With the right platform in place, IT and security leaders can immediately start to reap the benefits of intelligent automation across all areas of information governance. And they can ensure their organizations have the right structures in place to respond to an evolving risk landscape, by harnessing the unique capabilities of an agile, highly skilled hybrid workforce.

PART THREE

IT Governance

According to Gartner, IT governance became the biggest risk for organizations in 2021. The pandemic has given rise to 'new sets of risks while exacerbating long-standing vulnerabilities.'

With entire workforces suddenly forced to work from home, a massive increase in remote access to IT systems and infrastructure has introduced significant vulnerabilities for many public sector organizations. Meanwhile, rapid innovation to develop new digital services to meet dramatic changes in citizen needs during lockdown has led to soaring IT complexity. IT departments are suddenly managing a spiraling IT estate across on-premise, cloud, and hybrid environments, often without unified data and insight.

The risks for public sector organizations are obvious. Any breach in IT security can have enormous repercussions, in terms of citizen data security and privacy, fraud and a decrease in government trust by citizens.

But, as anybody that has worked in public sector IT during the COVID-19 pandemic knows, the sheer complexity and speed at which online security risks are evolving are posing a massive challenge to IT and security leaders. And despite the much-needed coordination of Government and Big Tech in response to these threats, most public sector organizations currently don't have adequate resources and processes to manage IT security and compliance effectively and/or sustainably.

With the volume and sophistication of cyberattacks against critical infrastructure and federal and state government agencies likely to increase further in the months and years ahead, public sector organizations urgently need new solutions to this challenge.

Once again, the introduction of a hybrid workforce offers exactly that. Digital workers provide IT and security leaders with an unlimited pool of resources to handle all process-driven work, identifying and managing risk, testing security policies and processes, and providing real-time data and insight across all aspects of IT security. In turn, the best cybersecurity minds are free to focus on higher value, strategic work which can minimize future risk and deliver better citizen experiences.

Optimizing incident handling and compliance with a hybrid workforce

Incident handling and reporting is one such area where digital workers can deliver significant benefits to IT and security teams. Currently, most agencies rely on a manual response to any suspected security breach. After the breach is identified, a team member must go through multiple logs and reports to decipher what's happened, how and why. Once cause is determined, the IT team can work on remediation. But in a highly complex, fragmented IT environment, the process is long-winded, laborious, and inaccurate.

However, with intelligent automation, an AI-enabled digital worker can immediately detect abnormalities or suspicious events on Security Information and Event Management (SIEM) platforms and extract relevant logs and information from multiple affected systems. The digital worker can then triage the issue, undertaking verification processes, such as online information gathering around suspicious IP addresses, domains, or URLs. It'll aggregate this data and present it to human colleagues for analysis.

Indeed, this is where a hybrid workforce can be so powerful. Rather than spending a large portion of their time carrying out exactly this type of process-driven work, IT and security teams can use their skills to make informed, data-driven decisions in real-time, leading to an improved performance.

And once teams have decided on a course of action, they can hand it back to the digital worker to execute, taking on tasks such as disabling user accounts, disconnecting infected endpoints or adding deny rules to block specific IP addresses in parameter devices. The digital worker will also generate custom reports for management and SOC personnel to demonstrate compliance at every stage.

Again, agencies don't need to use their highly skilled (and costly) human talent to perform routine manual work within incident response such as ticket status follow-ups, password resets and firewall rules housekeeping.

Removing the pain of security policy management and maintenance

A hybrid workforce can also deliver marked improvements in how public sector agencies are able to manage and enforce IT security policies across the organization. Digital workers can work 24/7 to ensure employees' online actions and behaviors are compliant with company security policies and wider industry standards.

So, for instance, digital workers can monitor systems and applications to ensure access is restricted to the right—and right number of—people, where only one person can log in at a time. Similarly, digital workers can enforce policies, such as users changing their password each time they log in to an application or document.

By automating these policies, IT and security teams can eliminate the potential for employees to take advantage of loopholes and thereby bring additional risk into the organization. And they can deliver a far higher level of compliance with security policies consistently.

Digital workers can take penetration testing and ethical hacking to a new level

Perhaps the area where digital workers can deliver the biggest impact on IT governance is within penetration testing and ethical hacking. Today's hackers and fraudsters are utilizing bots to test the defenses of hundreds or thousands of IT systems at any one time, fully unleashing the power of AI and automation for their own gains. However, many organizations, particularly within the public sector, are still relying on manual penetration testing where they test one system at a time. It's simply not a level playing field.

But with intelligent automation, agencies can use digital workers to carry out a massive number of penetration tests at the same time, so that they're able to identify weaknesses more quickly and beat the hackers at their own game. Digital workers can attempt to hack into every corner of IT infrastructure simultaneously, across APIs, networks and frontend and backend servers, to uncover vulnerabilities such as un-sanitized inputs that are susceptible to code injection attacks.

Digital workers can be used across the penetration testing lifecycle, from information gathering and threat modeling, through to vulnerability analysis, exploitation, and reporting. The insights gathered from this comprehensive approach to 'pentests' can then be used by IT and security teams to fine-tune WAF security policies and patch detected vulnerabilities at speed, working one step ahead of the hackers.

With the volume and sophistication of cyberattacks against critical infrastructure and federal and state government agencies likely to increase further in the months and years ahead, public sector organizations urgently need new solutions to this challenge.

Conclusion

Getting on the front foot with a hybrid workforce

With cybersecurity threats evolving and growing by the day, public sector agencies need to be open to new approaches and embrace new technologies to stay ahead. Intelligent automation presents them with an opportunity to achieve marked improvements across the trifecta of cybersecurity governance, providing an unlimited and flexible pool of resources which can be deployed whenever and wherever needed.

Digital workers can operate 24 hours a day, 7 days a week, and they can be taught to undertake a range of different processes. Teams can decide where they are used, depending on business needs.

What's more, because today's digital workers are enabled with AI and machine learning, they learn on the job, so their performance improves over time.

Also, at a time when so many organizations are suffering from a crippling skills shortage in the cybersecurity space, a hybrid workforce allows IT and security leaders to get more out of their teams, enabling their highly skilled professionals to make a real difference. Ultimately, by combining the strengths of human and digital workers, public sector agencies can minimize current and future risk and take a more strategic, proactive approach to cybersecurity governance.

blueprism®

Blue Prism is the global leader in intelligent automation for the enterprise, transforming the way work is done. At Blue Prism, we have users in over 170 countries in more than 2,000 businesses, including Fortune 500 and public sector organizations, that are creating value with new ways of working, unlocking efficiencies, and returning millions of hours of work back into their businesses. Our intelligent digital workforce is smart, secure, scalable and accessible to all; freeing up humans to re-imagine work.

To learn more visit **www.blueprism.com** and follow us on Twitter **@blue_prism** and on **LinkedIn**.