Device Management in our Digital World

A Whitepaper on how businesses can commit to and benefit from the World Economic Forum's 'Great Reset'

Max Sherwood

Abstract

The Great Reset

The World Economic Forum launched 'The Great Reset', an initiative in which they established a number of critical focus areas aimed at not only addressing the results of Covid 19 but, also, how business can work towards improving the state of the world.

A key initiative addressed how businesses can contribute to this initiative and how they can make the most positive impact, defining a framework for sustainable performance and influence on stakeholders.

Introduction

The COVID-19 pandemic has led to increased pressure on the businesses fundamentally altering the way they do business and provide services. The main catalysts for change during the pandemic have been the escalation of the digital economy, the increasing necessity for and drive towards the hybrid working model, and has paved the way for a greater number and increasing sophistication of cyber security threat vectors.

This has driven a need to optimise processes, embed strong and ethical working practices into business philosophy, and ultimately to achieve better and more efficient patient outcomes.

But making the necessary adaptations in order to achieve these changes is progressively more challenging. This is exacerbated by the organic growth of the Internet of Things (IoT), an increasingly interconnected framework of hardware, software and associated services that facilitates all kinds of functions and services across the industry.

The benefits of the IoT and those that rely on it are vast. The ecosystem allows for the automation of processes and savings on resource, time and budget. The ever increasing need to demonstrate green credentials means businesses can reduce waste, improve service delivery and deliver goods, whilst providing transparency to customers.

Yet as its scale increases, the potential for vulnerability points, transparency, regulatory breaches, and speed of response are potentially impacted negatively.

In this whitepaper, we discuss and analyse how businesses can build strong foundations that support the World Economic Forum's COVID-19 recovery initiative known as 'The Great Reset'. By defining a clear framework for sustainable business performance.

Background

The need to reimagine how they work has become a dominant theme for businesses everywhere. As the COVID-19 pandemic begins to settle all over the world, the focus has begun to shift from the immediate provision of "business as usual" to evaluating performance and using this to shape the future business landscape.

With this assessment and the manner in which the IoT continues to develop, advances such as virtually enabled working and the increasingly sophisticated data-enablement systems that support them will take on greater importance. While the focus during the pandemic was on adapting to remote working, the post-pandemic landscape will shift more towards a hybrid approach, preparedness and the ongoing digitalisation the working environment.

With data-enabled systems containing highly sensitive data and personal information providing the bedrock on which commerce revolves, the need to protect it with best-in-class device management that includes cyber security, is becoming all the more acute.

Visibility

Data underpins the huge gains businesses achieve through automation, interconnected working and delivery of digital outcomes. And unlike pre-IoT times, the modern ecosystem draws its strength and value from its ability to collect data from a large number of relevant sources.

The more devices and systems that are incorporated into the connected environment, the richer and more valuable the pool of data becomes that can be used to improve operational efficiency, economies of scale and deliver more positive patient outcomes. So securing this data is key, and strong security requires visibility.

In the digital economy, it is just impossible to protect what cannot be seen. And with cyber threats increasing in both quantity and quality, being aware of their presence is an essential for preventing them and limiting the damage that occurs as a result.

Artificial Intelligence (AI) can be harnessed to detect the behaviour of potential attackers. This approach serves to secure all the potential entry points of malicious threat vectors – which are becoming more and more numerous even since the onset of the COVID-19 pandemic.

Modern cyber attacks have been known to exploit a variety of hosts and users both inside and outside the perimeter of corporate firewalls. This makes it all the more vital for healthcare organisations to holistically consider all possible entry points in their security framework. This landscape includes user devices and IoMT-connected devices and associated services and software platforms, enterprise networks, data centre infrastructure, and even data hosted in cloud applications.

The ability to stay one step ahead of cyber attackers is therefore vital. By automating security using AI and algorithmic models that predict and fend off the most complex and innovative threat attempts, it is possible to create a cybersecurity ecosystem that

holds a distinct advantage over attackers. With automated detection, clustering and prioritising attacks in order to anticipate as or before they strike, AI-powered visibility is as powerful a tool for the healthcare industry as the sophisticated interconnected systems it protects.

Validation

Change is a constant in the digital, post-pandemic environment. For businesses, this means that equipping with the right tools to fend off cyber threats, continuing to innovate, learn from their findings, and push through barriers to growth.

To stay on top of this constant change, organisations need to find an effective means of knowing the true cyber risk that they carry. Without this knowledge, there is no way of understanding which vulnerabilities have the highest potential for negative business and operational impact.

Governance and Control

Responsibility, accountability and trust are all essential pillars in the digital economy. Ensuring they remain a positive power for good and not a constraint on growth is a delicate balance organisations have to juggle. Having the right tools and architecture in place to do so is essential to achieving this balance.

One of the core aspects of good governance and control for businesses is having the ability to control access to the data that is so integral to the integrity and optimal functioning. Implemented correctly, this control involves the ability to proactively revoke inappropriate access to data, enforce security policy, and detecting advanced incoming threats.

To be effective, governance and control of an organisation's vast infrastructure, a multilevel security architecture provides defence for data stored in the cloud, in transit in the network, and on endpoint devices. For complex and multi-site organisations, the implementation of simplified, centrally controlled security management systems is essential to ensure robust adherence to the values of governance and control.

Response

The ongoing and increasingly rapid digitalisation of industries presents the opportunity to drive higher standards, and manage change and process improvement.

This change also presents greater levels of opportunities and potential access points for cyber criminals. Having a robust protocol for acting on these threats can be achieved through the ability to identify, pinpoint and respond to malicious operations with precision.

By deploying an operation-centric response system to tackle malicious operations from their root cause to every affected endpoint device, healthcare organisations can benefit from holistic details of all incoming attacks. As a result, attacks can be fended off simply and automatically before they even take hold.

Conclusion

As a greater number and quality of digital technologies are used by enterprises operational efficiencies are greatly enhanced. With this, the IoT continuously incorporates new devices, software and data points into its ecosystem.

Yet as the size of this data pool and the access points that feed it grows, so do the opportunities for malicious actors to gain access and take advantage. Standing up to the security challenge is therefore a critical priority across the businesses to ensure that the interconnected ecosystem remains secure – and that its potential and benefits continue to far outweigh the potential cybersecurity risks it creates.

Adopting the principles of 'The Great Reset' and creating a tangible and robust security architecture based around the pillars of visibility, validation, governance and response ensures that businesses are perfectly placed to secure data and infrastructure.

About the Author:

With a background in retail advertising and marketing, Max Sherwood is a results driven business strategist who recognises the impact the digital economy will have on us all.

Having experienced first hand the transition from traditional 'bricks & mortar' retailing to online, Max can speak with experience about transformation and the need to think beyond just process automation.