RSM PARTNERS

MAINFRAME

EXECUTIVE BRIEFING

Digital Transformation, Cybersecurity, IoT and You

Securing your mainframe systems and your business in a connected world

Mark Wilson, Technical & Security Director, RSM Partners Ltd

Executive summary

Digital transformation brings unprecedented opportunities to improve business agility, drive innovation and enhance performance. But its downside is **cybersecurity,** which needs to be treated as a fundamental element of any digital transformation strategy. Indeed, cybersecurity will only grow in importance as consumer technology and a connected world bring both disruption **and** opportunity: a Bring Your Own Device (BYOD) and Internet of Things (IoT) world with more than 50 billion devices connected to the Internet by 2025. Businesses need to ensure they have appropriate and robust cybersecurity practices to make their transformation a success and to underpin their digital future – including mainframe systems.

This paper describes the impact of digital transformation and the cyber threat landscape. It discusses the IoT megatrend and its implications for your mainframe and business. It then suggests next steps to start planning your own response, including educating consumers: to embed robust cybersecurity measures and approaches in your mainframe systems, wider business strategy and working environment.

RSM PARTNERS
MAINFRAME

Contents

About the author: a global thought leader in mainframe technology and security issues, Mark Wilson heads RSM Partners' Technical and Security teams. Drawing on more than 30 years' experience in z Systems in diverse sectors and environments, in both hands-on technical and strategic roles, his insight and solutions-driven approach mean he is highly valued by RSM clients, IBM and third party technology partners, and is much in demand as a speaker on the international circuit. Mark is Chair of the Guide Share Europe Large Systems Working Group and Technical Co-Coordinator of the GSE Enterprise Security Working Group.

Introduction: is your business prepared?

Digital transformation offers organizations unprecedented opportunities to increase agility, drive innovation and achieve growth. That **transformative** element suggests not only enhancing and supporting more 'traditional' ways of working but actively enabling brand new types of business innovation and creativity. This is a connected Bring Your Own Device (BYOD) world. IBM talks about an age of "widespread digital reinvention" characterised by, for example, opportunities to completely re-imagine customer experiences, and to offer new mobile experiences that transform "both customer interactions and how employees work", bridging the gap between the physical and the digital.

The dark side of this transformative environment is, of course, **cybersecurity.** As the risk landscape evolves and the threats to IT and business escalate, appropriate cybersecurity practices have to be considered as a fundamental aspect of any organization's digital transformation strategy, particularly as the Internet of Things (IoT) fuels rapid growth in the number of devices connected to the Internet.

Whatever online, broadcast or print media you follow, it's unusual for a day to pass without seeing a story on hacking or some other security breach. The list of companies and organizations affected is large and constantly growing: TalkTalk, Sony PlayStation Network, T-Mobile, Adobe, Yahoo, Home Depot, VISA, MasterCard and national governments. In February 2017, the head of the UK's National Cyber Security Centre (NCSC) reported that the UK had experienced 188 "high level" cyber attacks in just three months. Across the world, company assets are being accessed and stolen on a regular basis, and in some cases the leaks or breaches remain undiscovered for years. The reality is that, in this new world, cybersecurity is not only a technical issue - and it will only assume even greater importance as consumer-driven and people-driven experiences and connected technology proliferate. So, what steps can an organization take to help secure and protect their essential mainframe systems and, by extension, their business?

> **Only those who will risk going too far can possibly find out how far it is possible to go.**
>
> T.S Eliot

What is Digital Transformation?

A buzz phrase that's been around for a while, **digital transformation** has been defined as the changes associated with applying new and emerging digital technologies in all aspects of society. It's a term that you've probably heard many times over the years - but I'm unsure that it's properly understood. From my own research, **digital** is a synonym for the pace of change driven by the rapid adoption of new technology. That also means client engagement is changing, along with the ways that we create new and sustain competitive advantage.

There appears to be two main types of organization now: those just 'doing' digital, and the Digital Innovators such as Amazon, Apple, Airbnb and Uber. Innovators like these are winning: disrupting every conceivable marketplace, fuelled by the rapid adoption of new technology. In this world, one of the biggest mistakes to make is simply **digitising** existing services. Adding technology to an existing service is simply **not** Digital Transformation. So, what does digital transformation look like?

- It's a **journey** of planned strategic change
- That journey starts by **empowering** teams with new methods and creating highly responsive data-driven strategies
- It also demands a **fearless** culture of innovation
- You can only create genuinely highly performing innovative organizations through **true leadership.**

Transforming is the most important concept, not the technology being applied, when redefining your organization's innovation, teams and culture for a new era. And with opportunity comes risk: but as the old saying goes...

> **Opportunity dances with those on the dance floor.**

Cybersecurity: the new threat landscape

Cybersecurity can be defined as the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorised access. In a computing context, the term security implies **cybersecurity.**

If you follow any IT media, analysts and research reports, you'll already know that cybersecurity poses huge risks to business. In recent times, specific threats have included **malware** (malicious software used to disrupt operations and harvest sensitive or private data), criminal gangs making use of **ramsomware** to covertly install and execute cryptovirology attacks on a victim's device, and continued evolution of **hacking,** including its more recent variation of 'hacktivism' to leak confidential or sensitive data or conduct a Distributed Denial of Service (DDoS) attack against perceived enemies.

At the beginning of 2017 in an article on tech trends, **BBC News** commented that "Cybersecurity will undoubtedly be the dominant theme" and that "all tech innovations could be undermined by data thefts, fraud and cyber propaganda. The chair of the National Cyber Management Centre was reported saying "a major bank will fail as a result of a cyber-attack in 2017" resulting in "a loss of confidence and a run on that bank." In 2016, hackers stole £2.5m from thousands of customers from a bank in an attack described as unprecedented by the UK Financial Conduct Authority. With the connected world now promised by the IoT and IIoT (Industrial Internet of Things) the opportunities for criminality and attacks can only increase.

The Internet of Things (IoT) is here to stay

IoT refers to the interconnection or internetworking of physical devices, everyday objects and vehicles, via the Internet, so they can send and receive data.
You'll also come across the terms **connected devices** and **smart devices.** The Industrial Internet of Things (IIoT) refers the use IoT technologies in manufacturing and other industrial processes. What is clear is that the IoT is here to stay: from smart homes (e.g. home controls, home monitoring, entertainment, appliance control, landscape control) to connected cars (e.g. traffic and weather services, navigation, driverless/ automation, fuel tracking maintenance, remote track and lock, entertainment). A study conducted some time ago by industry analysts Gartner, Inc. reported 6.4 billion IoT connected devices in 2016, an increase from more than 4.9 billion in 2015 – and more than 20 billion IoT connected devices anticipated by 2020. The majority will be in the hands of consumers.
A **Cisco** report conducted way back in 2011 predicted **50 billion** IoT connected devices in 2020.

> IoT security has been described as...
>
> **hilariously broken and getting worse**

So, what's the problem?

In a word: **security.** IoT security has been described as "hilariously broken and getting worse". Fashionable devices, like smart TVs, are produced to appeal to today's more technically savvy consumers.
But manufacturers of IoT devices don't really have security in mind. Some devices such as routers have the firmware customised by the Internet Service Providers (ISP): they don't allow firmware updates directly from the manufacturer, and don't provide customised updated versions of the firmware.
We should be worried. A year or so ago, an IoT search engine introduced a section for users to browse vulnerable webcams. As was reported, "The feed includes images of marijuana plantations, back rooms of banks, children, kitchens, living rooms, garages, front gardens, back gardens, ski slopes, swimming pools, colleges and schools, laboratories, and cash register cameras in retail stores..." Scary stuff.
The cameras were vulnerable because they used the Real Time Streaming Protocol to share video - but have no password authentication in place.

How to hack

Potential back doors to supposedly secure systems are opening at an alarming rate. So, could a fridge be used by a cybercriminal to hack your mainframe? Hacking isn't terribly difficult. Indeed, cybercriminals and would-be hackers can look to multiple information sites and other resources on the Internet and dark web: from dedicated web sites, blogs and forums to specific software tools, scripts, vulnerabilities and specialized search engines. The wherewithal is out there; have a look. Given this new IoT connected world, the conclusion must be that cybersecurity is not just a technical problem: it's as much a **human behaviour** and **business culture** problem.

Cybersecurity: not just a technical issue

Security is a technical and a human problem; organizations are being challenged by cyber risks at both a technical and a human level.

On the **technical** side, network security has become extremely complex because networks and applications are themselves far more complex today. To be effective, business operations have come to depend on advanced network architecture and infrastructure. Maintaining and securing this type of infrastructure, architecture and capability is, frankly, out of reach for most small to mid-sized businesses - and poses major challenges to even the largest enterprises. On the **human** side: governance, processes, skills and judgement need to come together to ensure the best (cyber, risk, security) decisions are made and that operations can remain secure and protected. And of course, external threats are just one side of the coin. Organizations need to remain vigilant against unauthorised internal activities and access, whether malicious or accidental. Exercising good judgement and informed decision-making are critical components in maintaining security.

Human + Technical

In my experience, the best outcomes arise when these human and technical aspects are working together to compound the security challenges. For example, many companies prefer to use on-premises applications and systems rather than cloud-based solutions because they feel more comfortable controlling their own security than outsourcing it to a cloud provider. So, what are the next steps? What can you start to do today, in terms of your own cybersecurity, if you haven't done so already?

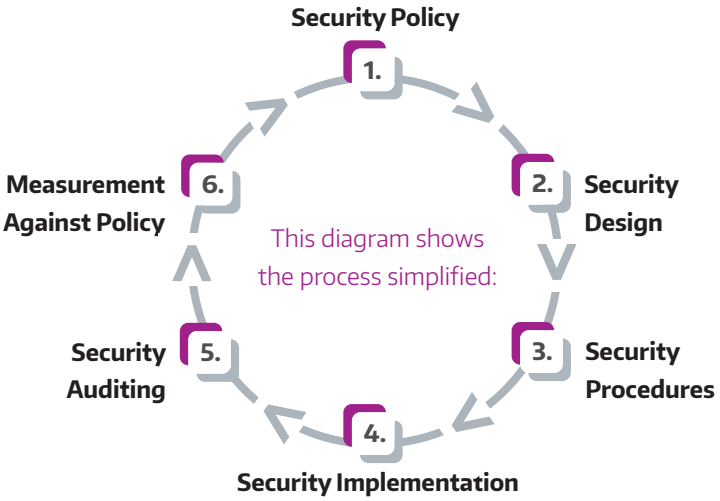
Security: devising a plan

In a recent blog post, the author came up with 10 basic things that we **must** do in terms of cybersecurity. The list contained all the usual suspects:

1. Secure your web presence/applications
2. Secure your endpoints
3. Secure your people from phishing baits
4. Secure software by timely patching
5. Manage users via an Identity Access Management (IAM) solution
6. Effective Password Policy
7. Secure Mobile, cloud and IoT
8. Protect Sensitive Data
9. Backup Your Data
10. Prepare for the worst incident and test the process

While this list is good, I think it does give a slightly false impression of priorities. This is my advice:

It's important for everyone in the business to have at least a vague understanding of why you're adding a defence, otherwise they may manage to find a way to do it, yet still not protect your critical assets. So, take a good look at your most critical assets and figure out the best ways to protect them: whether that's through Data Loss Prevention (DLP), encryption, access controls, or something else. Then build the required processes and procedures, using appropriate technology to govern it.



> **Focusing on your assets and prioritising defences is a better strategy than blindly doing everything on the list. Data is usually, but not always, the most valuable asset that your organization is responsible for.**

A continuous process

The approach I'm describing can make all the difference, and should be treated as a continuous process.

- **Discover** - start thinking like the bad people out there, and like typical consumers using their own devices for work
- **Education** - security awareness training is fundamental to success: not only for leaders but for the entire business
- **Knowledge** - put what you and your teams learn to practical day-to-day use
- **Attack** - penetration testing (pen testing) is a given: use your own teams or bring in outside expertise
- **Success?** Use all the findings and evidence that you gather to your benefit, to further enhance your security posture

Taking people with you

It's extremely important, as part of this, to 'educate the consumer' and take your people with you. Remember, this is as much a human issue as it is a technical problem. As industry professionals, we should have moved beyond **PEBKAC - Problem Exists Between Keyboard and Chair.**
Old assumptions no longer hold. On the other hand, it should not become **PEBDAA - Problem Exists Between Device and Application.**

Summary

Four main takeaways:

1. Digital transformation is a must for most organizations today if they want to grow - or even survive.
2. An effective well thought-out cybersecurity programme is essential to any digital transformation journey.
3. In an IoT and BYOD world, security is not just an IT problem, it's a human, cultural and business issue too.
4. When you get the balance right, you can achieve greater business agility (better, faster, stronger) and an improved customer experience - and do so without **reckless abandon.**

RSM PARTNERS
MAINFRAME

Why RSM?

RSM Partners is a globally recognized specialist in IBM mainframe security - providing both consultancy services and niche software tools. Working with some of the world's largest organizations - no other partner offers the same depth of knowledge and experience in ensuring mainframe security.

From specialist penetration testing and vulnerability assessments, to software tools greatly enhancing security management of the platform, clients know they can rely on RSM for quality, flexibility, and value.

Business Partner IBM

Business Partner IBM
Ready for Security Intelligence

To find out more about RSM Partners solutions,
email **info@rsmpartners.com,** call **+44 (0) 1527 837767**
or visit **www.rsmpartners.com**

RSM PARTNERS
MAINFRAME

T +44 (0) 1527 837767
E info@rsmpartners.com
www.rsmpartners.com

The Courtyard, Buntsford Dr, Stoke Pound, Bromsgrove, B60 3DJ, UK

17_0060 - 22/02/17 V01