Progress® MOVEit®

# Future Cybersecurity Challenges and the Role of Managed File Transfer

WHITEPAPER

# Welcome to the Information Age

You may have noticed that cybersecurity risks are continuously growing. You might also have observed that cybersecurity itself is becoming increasingly complex. There is a simple reason for this. It's because we are now living and working in the Information Age, an age which is very different from the Industrial Age we inherited and even more dissimilar from its predecessor the Agricultural Age. The characteristics of these earlier ages still persist of course, though in smaller pockets and with dwindling influence.

This important distinction and its epoch-making implications for business, society and warfare were first pointed out by the futurists Alvin and Heidi Toffler in a series of groundbreaking books in the 1980s and 1990s. [1] Their work caught my attention in the early 1990s when I was astounded to read an Alvin Toffler quote that "The 21st Century will be dominated by information wars and increased economic and financial espionage." [2]

On reading this, I immediately began to assess the impact of the Information Age on what we now call cybersecurity. It struck me that these threats would become greater as knowledge, networking and the storage and movement of money in the form of data all continued to grow. I also realized that our vulnerability to these threats would also increase with the proliferation and networking of our IT systems and infrastructure. And it seemed clear also that the impact of incidents would increase with growing business dependence on technology and the increasing value of the data stored and transmitted.

This continuous growth in all dimensions of risk is now familiar to everyone who has encountered this phenomenon over the last three decades. But there are also several subtle, less evident changes that accompany the proliferation of digital networks, including continuing trends such as growth in the scale, complexity and externalization of business systems, data flows and network entry points.

**This paper explains the implications of these important changes for business processes, information systems, data and cybersecurity. It also shows how Managed File Transfer (MFT) can be a powerful tool in helping to manage the major challenges presented by these unavoidable paradigm shifts.**

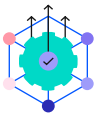
# Continuous Growth in Scale

Computers and networks are the key drivers of the Information Age. Networks are in fact a quintessential game-changer, playing a similar role to the proliferation of factories at the outset of the Industrial Age, enabling spectacular growth in the scale and speed of manufacturing and transforming the balance of power in business and society.

We are living and working through no less than a revolution in our lifestyles and work styles. We have business and social networks of unprecedented scale and complexity. And even greater change will come. We have only scratched the surface of what can and what will be achieved. Scale is an inevitable issue when networks are deployed. Applications that were once restricted to local usage are now global in reach and extending to suppliers, partners, customers, citizens and enemies. This trend will continue as endpoints become increasingly smaller and cheaper. We should anticipate accelerating growth, diversity and change in every dimension of our infrastructure.

Virtualization of platforms using cloud services is an obvious, essential starting point in managing scalability. But there are other useful measures, such as standardization, automation and smart load balancing, fallback and database scaling, as well as simpler measures such as verifying that database fields are the maximum allowable size.

**Managed File Transfer is a technology that standardizes, automates and simplifies the management of data transfers and offers unlimited scalability.**



# Growing Complexity

Computers and networks also amplify complexity. [3] This fact has been known since the 1950s, when cybernetics, artificial intelligence and systems theory were fashionable sciences. As life becomes increasingly complex, we instinctively seek simple solutions to manage these situations. Simplicity is an obvious and laudable goal but the truth is that correctness and completeness are much more important. And unfortunately, it is an absolute fact that simple control mechanisms cannot control complex situations.

There is a formal, mathematical law that states that if we wish to control a system or situation, we need to have the same number of states (termed “variety”) in our controlling mechanisms as there exist in the system we are trying to control. Otherwise, that system will be unstable and out of control. This is the so-called First Law of Cybernetics, otherwise

known as Ashby's Law of Requisite Variety, named after the eminent British operational researcher W. Ross Ashby.[4] It is a proven law that cannot be avoided, unlike Occam's razor (a medieval tenet in praise of simplicity) or its modern maxim "Keep it simple, stupid."

The consequence of Ashby's Law is that a simple control mechanism cannot control a complex situation. This might at first sight seem surprising, as not all of our increasingly complex business processes and information systems are out of control. So how do we manage to control them in practice? The answer is simple and twofold. Firstly, we instinctively use a number of techniques to reduce the variety (number of states) in the system we wish to control. And, secondly, we can use technology to amplify the variety in our control mechanisms.

Let's consider the first approach. The number of allowable states in a system can be substantially reduced by techniques such as standardization, centralization, categorization, incorporating limits or filters, using a Controlled Natural Language (CNL) or a standardized data model and resisting unnecessary changes. [5] These methods are rarely recognized or taught but many are often stumbled upon by smart managers and administrators.

You may have noticed for example that improvisation and diversity of thinking are rarely tolerated in large organizations. Everyone is encouraged to share the same culture and strictly adhere to business processes, though this is counter to the true spirit of empowerment enabled by the Information Age and is more akin to the mass production philosophy of the Industrial Age. [6]

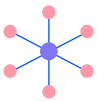
The second approach, which is to scale up the number of states in the controlling mechanism using technology, is equally and potentially even more powerful. In fact, the fundamental reason why complexity is increasing in our applications, databases and infrastructures is because they are formed of computers and networks. This is an important point to note because computers and networks are so-called variety amplifiers. Computers enable an almost unlimited number of records to be kept to monitor the individual states of a system, infrastructure or environment. And networks enable a single endpoint to harness the power of an entire network. Consider the power of a botnet for example.

Artificial intelligence (AI) might appear to present a smart solution to the challenge of managing complexity. These technologies, however, have limitations and they must be used in the correct way to manage complex situations. We can easily envisage that an AI model that has been extensively trained on very large sets of data will offer a powerful means of consolidating the rules governing a large number of possible system states. On the other hand, a lightly trained model will be incapable of dealing effectively with a highly complex problem space.

This is the reason why the most effective AI systems are those trained on massive amounts of data, such as Clearview AI's facial recognition system or ChatGPT's large language models (LLMs). These models deliver spectacular results because they were extensively trained using public data gleaned from the entire internet. Many AI systems, however, have an unfortunately high degree of entropy (uncertainty) because of inadequate or unsuitable training, for example by not correctly balancing the risks of overfitting and underfitting, which can result in excessive numbers of false positive or false negative matches when deployed on a large scale. [7]

AI offers great potential in control mechanisms if deployed with the correct choice and combination of ML technologies, supported by sufficient and carefully selected training data. Inadequate attention to these points, however, will result in the user being swamped with excessive amounts of false positive reports, as can be regularly experienced today in the Security Operation Centers (SOCs) of large international companies.

**Managed File Transfer is a technology that encourages standardization, improves quality and reduces the complexity and associated high management costs of proliferating data transfers.**



# The Curse of Fragmentation

Alongside increasing complexity comes growing fragmentation. This is a curse of society, academia and business. Most people like to break large things down into smaller pieces, while losing sight of the bigger picture. This makes things difficult and expensive to manage. That is why the introduction of Business Process Reengineering (BPR) in the 1990s was so successful in helping to streamline business activities, speed up activities, cut jobs and save money. As IT governance and cybersecurity management become increasingly complex, there is a danger of focusing too much on individual components such as platforms and firewalls in isolation rather than how the components work together as a whole.

As the US theoretic physicist David Bohm (who worked with Einstein and the Manhattan Project) correctly put it: "Wholeness is what is real and fragmentation is the response of this whole to man's action, guided by illusory perception shaped by fragmentary thought." He clearly understood that at the atomic level everything is a single sea of interacting particles, not a collection of separate objects.

David Bohm's point is well made. We concentrate far too much on the individual components in our infrastructure rather than the processes that connect them. To manage complexity, we need to focus on the activities that connect the numerous objects and participants in our organizations and not the objects themselves. From an ontological perspective, activities are the most powerful entities in our architectures and data models as they are composed of numerous participants in specific roles and create all of the changes experienced by other entities.

IT and cybersecurity architects should set out to simplify rather than complicate our view of the enterprise. Architects should start with the activities, not the individual objects, attributes or roles, as these are the entities that bring together all of the individual components within the organization.

**Managed File Transfer is a technology that avoids the increased expense and management overhead of fragmentation as it focuses on the process of data transfer rather than on the management of individual data sets and endpoints.**

## Increasing Externalization and Citizen Power

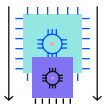
Digital networks are the powerhouses of the Information Age. They transform the volume, direction and content of our information flows, disrupting every aspect of society, whether public, private or business. Scalability and complexity of control mechanisms have already been discussed regarding the issues of dealing with rapid growth in applications infrastructures and information flows. A further issue, however, is the shift in the direction of information flows from a mostly vertical direction up and down the organization to a horizontal direction sideways to colleagues, business partners and customers, both internal and external.

We generally imagine that power lies with people who have greater strength, status or money. These are powerful factors. But power over people is less about who or what you are and more about how other people respond to you. Social networks have transformed the perception of the masses. They increasingly empower staff, customers and citizens. Social networks resist dominance and will progressively erode the traditional, hierarchical power bases within organizations, weakening the influence of corporate policy within organizations and that of public policy in society.

The result will be that staff are likely to be less inclined to adhere to organizational policies and guidance and more likely to align with what their colleagues and friends are thinking, saying or doing. We should not, therefore, rely completely on employees to fully understand and implement our policies and rules. Such guidance is only effective for those staff who choose to obey it. We must, therefore, expect an increasing number of mistakes and security breaches as procedures become increasingly faster and more complex.

Security education is a powerful tool for incident reduction. But however often and strongly it is enforced, it cannot completely eliminate mistakes and breaches. The real solution lies in greater automation of business and administration processes, which is more reliable and can detect and respond to oversights and miscalculations far quicker than any human can.

**Managed File Transfer is a technology that flourishes in an increasingly externalized environment. It also minimizes the risk of user mistakes and breaches that will inevitably continue to increase.**



# Progressive Miniaturization of Technology

One trend that is likely to continue is the progressive miniaturization of technology. We started out with a single computer that filled an entire room. We then created mainframe computers, then minicomputers, then microcomputers, then laptops, then smart phones, then wearable devices, then smart sensors. Where will it end? Smart dust perhaps? [8]

For each new generation of technology, the processors at our disposal become more numerous and connected. Even supercomputers are now assembled from large numbers of smaller processors. The challenge for cybersecurity is that each new generation of technology initially lacks adequate security and the security technology developed for previous generations is unlikely to fit into a smaller technology space. Fixing this problem requires no less than a paradigm shift in thinking and engineering.

The Internet of Things (IoT) is a contemporary example of this phenomenon. Today's endpoint security technologies will not fit into a sensor. New thinking is needed to respond to this challenge. And it is not that difficult. There is, in fact, a simple, perfect solution: migrate the security to the Data Link level in the OSI protocol stack. This is a brilliant

solution with huge benefits. Yet, despite promoting this approach for a decade, not a single vendor, government or standards body has considered this solution because it's either not-done-here or not traditional or because it's simply not believed to be possible as it's outside the education and experience of the practitioners.

**Managed File Transfer is a technology that can quickly adapt to changes in each new generation of technology, as it is agnostic to specific platforms, applications and protocols.**

# Faster Processes and Quicker Responses

Have you noticed how everything in business gets faster and faster? Unfortunately for us overworked employees, this is a permanent trend, though one that has nothing to do with the Information Age. It's simply the result of the fact that the faster you go in business, the more money you make. Workaholics and business owners may welcome this possibility, though most humans prefer an easier life and would rather lie stationary on a beach for several hours than work fast and long in order to enrich their employer.

System development used to be a long, slow process until business managers paid more attention to information systems and began to demand faster and faster changes. Cybersecurity, however, remains painfully slow as there is, as yet, relatively little business interest. Instead, it is driven largely by auditors who allow security deficiencies to be mitigated over months, even years. Some security authorities even promote the use of painfully slow cycle such as the Deming Quality Cycle of "Plan, Do, Check, Act," which was designed to churn out identical widgets each day, rather than to help safeguard intellectual assets and adapt in real time to new threats and opportunities. [9]

Meanwhile, business continues to proceed at an accelerating rate, creating changes, mergers and acquisitions far faster than traditional cybersecurity is able to respond to. Hackers have no bureaucracy to slow them down. But cybersecurity needs time to prepare a business case and justify a future budget for any improvements. Chief Information Security Officers need a fast-track process to find and fix vulnerabilities before hackers can. Real-time visibility of events and transactions is essential to pinpoint and respond to possible incidents.

We also need a portfolio of solutions that are quick to install and readily extendable without the need for a fresh business case. Automation of installation and administration is also a key requirement as products that require additional support staff to implement and manage will involve further delays and expense.

**Managed File Transfer is a technology that supports accelerating business change. It is quick to implement, automated and extendable and it rapidly corrects failed transactions and delivers real-time visibility and auditing of events.**

## Summary

So, we have seen that Information Age presents many challenges and paradigm shifts. Most of these are created by the emergence of digital technologies. Others by manufacturing trend such as the progressive miniaturization of technologies or because technology enables faster business processes and changes.

IT governance and cybersecurity are highly challenged today, not only by the growing risks they face but also by the legacy of the slow, manual and error-prone solutions they have inherited. No less than a paradigm shift is needed to transform our defences into the smart, automated, standardized, scalable, extendable, interrogatable and easy-to-implement solutions that are needed to manage a future business environment and infrastructure that is accelerating in speed, complexity, vulnerability and externalization.

**I am a strong supporter of Managed File Transfer because it ticks all of my boxes for an Information Age solution. It enables standardization, automation, externalization, extendibility, real-time recovery and monitoring (to regulatory compliance standards) of transactions. These are the features we need and should look for in IT and cybersecurity solutions. MFT is a true Information Age product.**

# About David Lacey

David Lacey is a highly experienced CISO and Cybersecurity thought leader. He founded and led functions for the UK Foreign & Commonwealth Office, Shell International and the British Royal Mail Group. During this time, he developed the set of controls that became the basis of the International Standard ISO/IEC 27001/2 and achieved the world's first and largest accredited certification. He also founded the Jericho Forum (part of the Open Group) to develop the principles and architecture for a De-Perimiterised network environment, the concept for which was subsequently adapted by Forrester Research as Zero Trust.

David has written five books and numerous papers on Cybersecurity and is a keen futurist, having been the first CISO to recognise and articulate the impact of the Information Age on Cybersecurity. He is also a long-standing member of the Infosecurity Europe Hall of Fame.

---

[1] For example, read "The Third Wave" by Alvin Toffler (ISBN 0-553-24698-4).

[2] The first person to coin the phrases "Information Warfare" and "The Electronic Pearl Harbour" was the extraordinary Winn Schwartau, Cybersecurity author and former lead sound engineer for Led Zeppelin. He was immediately raided by the FBI who wanted to know from whom he got these ideas. He told them he had simply invented them.

[3] I accept the typical dictionary definition of complexity: "The state of having many parts and being difficult to understand." And I measure complexity in terms of the number of states a system can be in.

[4] For the mathematically minded, Ashby's law can be seen as a generalization of Shannon's tenth information theorem, which indicates that the level of redundancy required to overcome a noisy communication channel must be equal to or greater than the noise that is corrupting the channel. If you are really clever, you might even trace this logic back to Alan Turing.

[5] A Controlled Natural Language (CNL) is simply a subset of a natural language that is designed to reduce ambiguity and complexity by discouraging alternative words to describe things. It can be implemented for example by using drop-down menus to force users to choose from an approved set of options rather than insert their own descriptions.

[6] Read "The Stupidity Paradox – The Power and Pitfalls of Functional Stupidity at Work" by Professors Mats Alvesson and André Spicer (ISBN-13 978-1781255414) for a good account of the reasons for and pros and cons of thoughtless conformity.

[7]Overfitting occurs when the model is complex and fits the training data very closely, resulting in poor generalization of the model. The model may perform well on training data but not for new, unseen data. Underfitting occurs when a model is too simple and is unable to properly capture patterns and relationships in the data.

[8]When I visited MIT Media Lab some 25 years ago, they were discussing the implications of smart dust.

[9]I have long advocated that cybersecurity should consider adopting the military Boyd loop, of "Observe, Orient, Decide, Act" which is designed to kill and survive in fast-moving situations such as aerial dog fighting and those encountered by special forces.

**Would you like to discuss these insights with an expert? Contact our team.**

## About Progress

Progress Software (Nasdaq: PRGS) empowers organizations to achieve transformational success in the face of disruptive change. Our software enables our customers to develop, deploy and manage responsible AI-powered applications and digital experiences with agility and ease. Customers get a trusted provider in Progress, with the products, expertise and vision they need to succeed. Over 4 million developers and technologists at hundreds of thousands of enterprises depend on Progress. Learn more at www.progress.com



## Worldwide Headquarters

Progress Software Corporation
15 Wayside Rd, Suite 400, Burlington, MA 01803, USA
Tel: +1-800-477-6473

facebook.com/progresssw
twitter.com/progresssw
youtube.com/progresssw
linkedin.com/company/progress-software
progress_sw_

Progress