HOW CAN YOUR FIRM TACKLE THEM?

1 COMMUNICATING IN THE DIGITAL AGE

As digital technology becomes ever-more pervasive throughout all aspects of everyday life, more and more of our activities will rely on these solutions, both at home and in the office. And one of the key uses for the latest developments will be to help people keep in touch with colleagues, partners and friends.

Whether it is via email, instant message or mobile app, it's now hard to imagine working without the benefit of digital solutions. Since the first email was sent in 1971 by computer engineer Ray Tomlinson, the number of messages sent has moved into the realm of hundreds of billions every day.

And the demand for fast, effective digital communications has been heightened by the emergence of new technologies, with mobile and social tools now forming an integral part of how we stay in touch. Technology research group International Data Corporation names these developments as two of the keystones of the so-called 'third platform' that will transform the business IT landscape.

In 2015, the company expects these solutions - which also include cloud computing and big data - to account for almost all technology spending increases in the enterprise[1]. For instance, IDC predicted that sales of smartphones and tablets will reach $484 billion, accounting for 40 per cent of all IT spending growth.

Despite these advances, many firms continue to rely heavily on legacy tools for their digital communications. This may be because they are comfortable using a familiar technology, are concerned about the cost of a migration, or even do not recognise the risks they are taking - either because they believe they have never had a security breach, or do not even know all the solutions that are actually used, or how insecure their solutions really are.

But whatever the reason for continuing to persist with legacy technology, it comes with a range of challenges and problems. These include effectively transferring these operations to a more mobile environment and the matter of security. There is also the matter of usability, as many of these outdated tools are unintuitive and difficult to manage, with user interfaces that make it difficult to send data efficiently and subsequently drive workers to easier-to-use - but less secure - alternatives.

Protecting highly-sensitive data from prying eyes is a particular worry in the current environment, where hacking attacks and data breaches have become an everyday fact of life for many businesses. And it is not just criminals out for personal gain that are engaging in this, as snooping and cyberespionage by governments is also an issue that needs to be considered - as the revelations regarding the NSA's PRISM programme illustrated very publicly in 2013.

"Targeted operations could mean disaster for the victim: resulting in the leak of sensitive information such as intellectual property, compromised corporate networks, interrupted business processes, and the wiping of data. There are tens of scenarios that all end up with the same impact: the loss of influence, reputation and money."

- Alex Gostev, chief security expert, Global Research and Analysis Team, Kaspersky Lab[2]

1. IDC http://www.idc.com/getdoc.jsp?containerId=prUS25285614
2. Kaspersky Lab http://www.kaspersky.com/about/news/virus/2014/Kaspersky-Lab-number-of-corporate-sector-targets-in-2014-has-more-than-doubled-since-2013

2 OLD SOLUTIONS FOR NEW PROBLEMS

Despite the rise of new alternatives for digital communications, traditional methods of keeping in touch and sharing vital information are not going away any time soon. While in the consumer space, email is facing fierce competition from options such as instant messages, for businesses, email is still very much the number one choice.

In 2015, it is estimated there will be 4.3 billion email accounts in use around the world, with consistent annual growth of six per cent seeing this rise to 5.2 billion by 2018[3]. And the majority of email activity is set to come from the business world. This accounted for more than 108.7 billion emails every day in 2014, with the average user sending or receiving 121 emails a day. By 2018, this figure will have increased to 140 emails per day. At the same time, FTP servers remain one of the most common ways of transferring files.

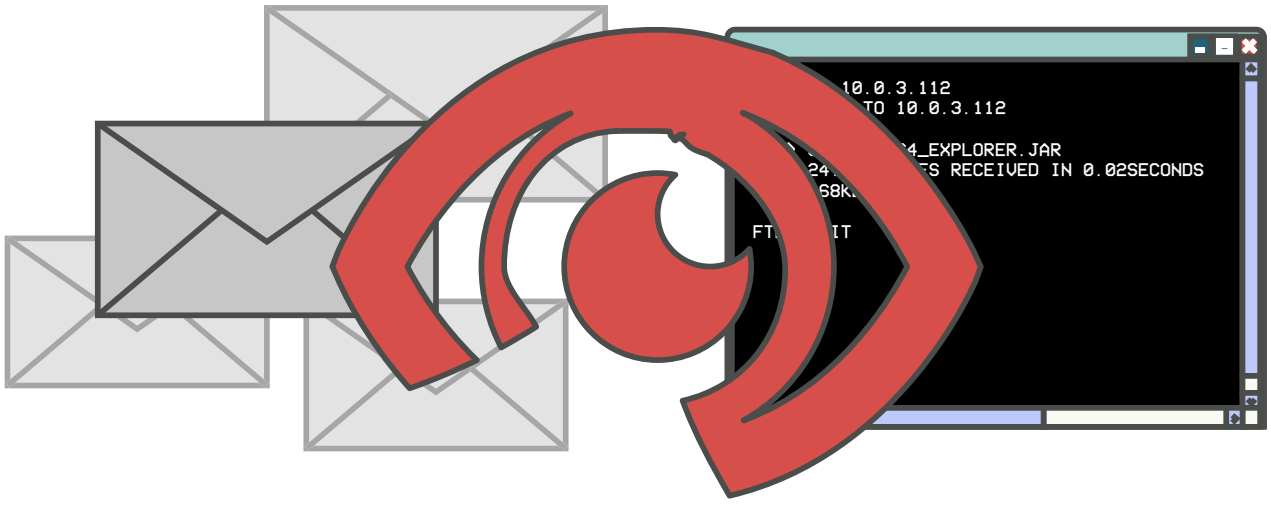
Both these technologies have been in operations since the 1970s, with few changes in that time. And both have a range of issues that pose significant challenges to enterprises. With email, for instance, security and privacy are among the key issues, unless companies seek to add additional encryption.

For FTP, standard security protections are also poor, but it has the added challenge of usability, which is well below the capabilities businesses expect nowadays. FTP makes users wait in order to receive their files, is hard to manage and lacks basic tracking and accountability features.

As a result of this, these communication methods can present a tempting target for hackers and other snoopers. Whether the goal is to steal corporate secrets such as intellectual property or simply embarrass the company, records often prove to be easy to access and highly damaging.

One example of this came at the end of 2014 with the problems faced by Sony Pictures, following the theft and publication of thousands of internal messages between executives at the movie studio. These were pored over by the press, with revelations of gender pay gaps and the disparaging of Hollywood's biggest names among the most well-reported - though the hack also saw personal and financial details of many employees stolen.

Indeed, one newspaper described the incident as a "PR car crash from which the studio might never recover"[4]. It should therefore be a clear warning to any other firm of the perils of persisting with legacy communications in an era in which hackers have become much more sophisticated.



3. The Radicati Group http://www.radicati.com/wp/wp-content/uploads/2014/01/Email-Statistics-Report-2014-2018-Executive-Summary.pdf
4. The Observer http://www.theguardian.com/technology/2014/dec/14/sony-pictures-hack-pr-car-crash

3 THE CHALLENGES OF 21ST CENTURY COMMUNICATIONS

Security will therefore be one of the major concerns for businesses when seeking to share information in today's environment, with the costs for this potentially huge, both in financial and reputational terms.

According to PwC, the average financial losses due to security incidents for large companies in 2014 was $5.9 million - up from $3.9 million the previous year[5]. It also estimated that the cost of lost trade secrets around the world could be anywhere between $749 billion and $2.2 trillion a year.

With the number of threats on the rise, these numbers are only likely to increase. In 2013, Kaspersky identified around 5.2 billion malicious attacks on user computers and mobile devices. But in 2014, this increased to 6.2 billion[6]. The company also revealed almost four out of ten user computers (38 per cent) were subject to at least one attack last year.

As the volume of communications across all channels is on the rise, and a large number of these are taking place via unsecure connections, this often leaves businesses vulnerable to data breaches. And in many cases, the problems could be exacerbated if administrators do not have full visibility or control over their networks.

For instance, one issue that could affect many companies is unmonitored and untracked communications. Not only does this mean businesses will not be aware of exactly what data is being sent in and out of the company when it occurs, it can result in vital auditing activities ending up being inaccurate.

Figures from AttachMate reveal 56 per cent of IT decision-makers worry about their ability to comply with audit requirements[7], and as communications channels become more diversified and less centralised, this is a problem that may only get worse.

Another factor that's important to consider is usability. If a system is too complex to be understood by employees, or requires a great deal of extra time and effort to implement, frustrated users will find ways to bypass it - thus rendering the entire operation useless.

One result of relying on tools with poor usability is workers will look to one of the wide range of free and cheap consumer tools that are now on offer. The likes of DropBox or iCloud may be highly attractive to workers who have used them in their personal lives and appreciate the fact they are straightforward to use. But their security measures will not have been tested by IT departments and will often be found to be short of enterprise requirements.

To prevent users turning to insecure solutions, enterprises need to look for options that can fit seamlessly into workers' everyday activities and do not require extra steps or training to use. The best approach to this is to look for transparent solutions that end-users will not even notice.

5. PwC http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml#
6. Kaspersky Lab http://www.kaspersky.com/about/news/virus/2014/Kaspersky-Lab-counts-up-this-years-cyber-threats
7. AttachMate https://www.attachmate.com/blogs/datainmotion/new-infographic-files-and-tribulations-the-importance-of-managed-file-transfer/

4 A MORE MOBILE WORLD

Businesses are also dealing with the fact that a growing proportion of communications no longer involves a desktop PC, as smartphones and tablets become more ubiquitous in businesses around the world. In today's environment, many workers will not only expect to be able to connect via mobile devices, but use their own personal gadgets to do so, rather than being constrained by what their employer can offer.

According to Gartner, sales of traditional PCs (both desktops and notebooks) in 2015 are expected to total 261.6 million units[8]. However, this year will see sales of tablet devices overtake PCs for the first time. Some 320.9 million tablets will be sold in 2015, along with 1.95 billion mobile phones, and many of these will end up in the hands of business users.

By 2017, it is expected that 90 per cent of organisations will support some form of bring your own device (BYOD) solution, where employees are encouraged to use their personal mobile gadgets for work[9]. Reasons for this may include making it easier for employees to work remotely, boosting productivity and motivating a workforce, as employees who can work in the manner of their choosing and on the device they are most comfortable with are likely to feel more positive about their job.

But this brings with it a whole new set of challenges when it comes to securing and controlling enterprise communications. First and foremost, businesses will need to make sure their solutions are compatible with multiple platforms, as what may be designed and optimised for one mobile operating system may not have the same functionality on another.

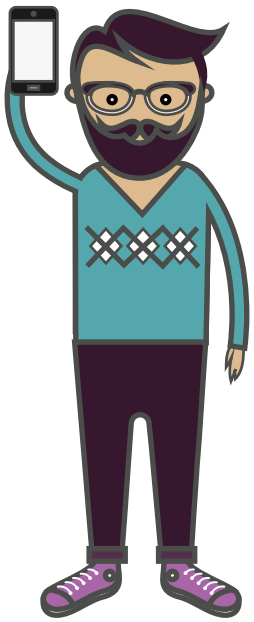
In many cases, there could be cost benefits to embraced BYOD, as well as the productivity gains associated with allowing employees the opportunity to choose how they work. However, this will depend on the approach firms take and how far they commit to full freedom of device choice, as although reduced expenditure is often possible, this is dependent on numerous factors, such as the type of devices used.

> **"Without a stipend, direct costs of user-owned tablets are 64 per cent lower [than enterprise-owned tablets]. When organisations have several users who want a tablet as a device of convenience, offering a BYOD option is the best alternative to limit cost and broaden access."**
>
> - Federica Troni, research director, Gartner9

Finding the right balance between giving your employees the freedom to work in the way that best suits them and retaining security can be a struggle, so it is important businesses recognise the additional risks of adding new channels to their communications mix and take the appropriate steps to secure them.

If firms opt for a completely open BYOD approach, they may find employees will want to use numerous platforms, such as iOS, Android, Windows and BlackBerry. Ensuring full support and interoperability for all of these can be an extremely costly and time-consuming experience.

Therefore, enterprises will need to weigh up the pros and cons of this and consider limiting their employees to only one or two approved options in order to ensure tighter control of their communications.



8. Gartner http://www.gartner.com/newsroom/id/2791017
9. Gartner http://www.gartner.com/newsroom/id/2909217

5 A SECURE SOLUTION

Therefore, in such an environment, where various competing requirements need to be weighed up and security is such a crucial part of many digital communications, the importance of having a robust solution businesses can rely on to protect their most precious assets cannot be understated. But what should firms be looking for in order to make sure they end up with a system that meets high expectations?

Businesses will require tools that meet the three key requirements for enterprise communications - security, usability and mobility. These areas each bring their own challenges that firms need to address.

For instance, strong encryption is only one aspect of a highly-secure solution. Tools that offer a high level of automation are also vital, as this can ensure encryption is always applied and removes the human factor. Such solutions do not rely on workers understanding and remembering the need for protection, and as they work transparently, they do not affect a solution's usability.

As more business activities shift to smartphones and tablets, security tools must also be mobile-enabled and protect information from end-to-end in order to be effective. This will require them to support multiple operating systems without the need for additional client components that will add cost and complexity to an organisation.

Such extra components for mobiles can harm a solution's effectiveness and make it less convenient. Instead of being able to rely on the smartphone's native apps, a worker would need to install additional apps in order to communicate securely. Given that research has indicated there is an "upper limit" to the number of apps people are prepared to download and use[10], anything that adds to this may not be well-received by end-users.

In today's environment, there is also a high need for accountability - which demands that communications systems be auditable and compliant with all relevant standards. Depending on where a firm is located and the industry it operates in, it may need to meet a variety of standards, such as PCI, HIPAA, SOX or the EU Data Protection Directive. These will typically require businesses to maintain a full record of communications in the form of audit logs that can be provided on-demand.

totemo's solutions can assist with meeting all these demands, providing businesses open standards-based offerings that are secure, reliable, user-friendly and fully auditable, as well as being completely mobile-enabled.

10. Nielsen http://www.nielsen.com/us/en/insights/news/2014/smartphones-so-many-apps--so-much-time.html

totemo ag
Freihofstrasse 22
CH-8700 Kusnacht

Phone: +41 44 914 99 00
Fax: +41 44 914 99 99
Mail: info@totemo.com

totemo®
securing data in motion