The most secure collaboration platform

THE FUTURE OF WORK

The evolution of workplace communications and what it means for enterprise security.

With a majority of companies relying on collaboration and communication tools to connect their workforce, protecting digital assets has become a top concern and security a top priority for organizations worldwide.

The ways in which we work have changed, along with the behaviors, processes, and technologies that underpin the modern business.

The existing changes have been accelerated by the COVID-19 crisis, which forced companies to quickly digitize their ways of working. Remote working and collaboration in the forms of messaging and video conferencing have now become the de facto forms of communication.

However, for companies it's not just about being prepared for a global pandemic. It's about readiness for the future – creating a secure work environment, regardless of the employees' location to prevent data breaches and protect intellectual property.

CHANGE OF THE DECADE 2

FUTURE OF WORK 2.0 2

MOBILITY OF THE WORKFORCE 3

THE VALUE OF DATA 4

SECURITY AT THE GOVERNMENT LEVEL 4

CONCLUSION 5

> The COVID-19 crisis is a wakeup call to ensure enterprise and government organizations not only have the infrastructure to support secure remote work, but equally that they prepared for the Future of Work.
>
> Wire™ CEO Morten Brøgger, speaking to The Daily Telegraph

KEY TAKEAWAYS

- **Adapting to the rising security threats of a decentralized workforce**
- **The increasing value of an organization's digital assets and how to protect them**
- **The security implications of popular communication and collaboration tools**

CHANGE OF THE DECADE

In this new era of work, a company's most valuable assets are its intellectual property and proprietary data. We transmit this data every day throughout the course of business with systems becoming more interconnected, and workforce habits increasingly decentralizing.

Unfortunately, this also means that cyber threats are on the rise as bad actors become more sophisticated in capitalizing on security weaknesses.

A recent report projected that by 2021, the global economy will lose out on **$6 trillion a year**, in order to mitigate the damage inflicted by cybercrime.

The first step towards finding a solution is to move away from viewing data protection as a perimeter issue, but rather look at how we protect the value of data as an asset that exists outside of the company's firewalls. Organizations must ensure an increased security threshold when it comes working remotely.

Secure communication is already undergoing a dramatic change as you read this. Traditional communication vendors are currently under scrutiny for not delivering the security needed by large enterprises and government organizations because they suffer from "man-in-the-middle vulnerability", meaning that they technically can read all content shared and listen in on all calls.

The landscape is changing dramatically and now more than ever, we are steadfast that the Future of Work belongs to tools that have eliminated this vulnerability by delivering both mobility and security.

FUTURE OF WORK 2.0

Just ten years ago, the workplace was very different from what it is today. Back in 2010, email was the primary form of communication, both internally and externally. Employees sent numerous emails daily, clogging up bandwidth and keeping IT teams constantly on their toes due to the threat of breach and cybercrime, two areas where email was (and still is) the perfect conduit.

> **An employee's chances of spotting a phishing email are as slim as hitting a specific number on the roulette wheel**
>
> *'Odds of a Bad Bet' report by Wire™*

The digitization of work is beneficial in that it facilitates work and increases productivity, however, the security component cannot be overlooked or underestimated. The new way of working brought about by COVID-19 is not a temporary trend, it was only accelerated, giving rise to what we at Wire™ call "**The Future of Work 2.0**" – that is, the next frontier of remote working.

Work as we knew prior to the pandemic is over and so are our old security standards. Business leaders must consider the long-term communication tools they want to put in place to support their employees' digital communications as well as protecting the organization's digital assets.

Collaboration platforms that are built with a solid security infrastructure from the outset are not only better prepared from the beginning, they are also more capable of evolving and adapting to new security challenges.

MOBILITY OF THE WORKFORCE

Flexible and remote working aren't new concepts, in fact, the number of home-workers increased by 27.7% in last decade - prior to the COVID-19 pandemic (a number now much higher). While this has a net positive impact on employees' work/life balance, it has major repercussions for enterprise security.

The biggest challenge of a mobile workforce is ensuring the integrity of company data outside the four walls of a physical office, its firewalls, and secure internet access. Digital assets are the lifeblood of an organization. Without them, there is no product, no service, no sales. In our recent report, Odds of a Bad Bet, we highlighted the extreme likelihood of businesses suffering from cybersecurity flaws, including the fact that a business is **as likely to avoid a malware attack in a given year as pulling the Ace of Spades from a shuffled deck on one try**.

As companies continue to grapple with keeping high levels of connectivity and productivity, cyberattacks have increased by an estimated 400%. Many of these attacks have been waged within communication tools, revealing underlying security and privacy weaknesses that are not only significant but chronic.

Business leaders must facilitate communication within their large, mobile workforces in a way that protects the company's data, retains its IP, establishes secure connections, and is as usable as the consumer applications that workers are accustomed to using in their personal lives.

74%

of CFOs plan to move at least 5% of their previously on-site workforce to permanent remote positions post-COVID 19.

Gartner Survey, 2020

It will require a paradigm shift in how companies manage the mobility and security of data at scale. Failing to do so will result in a dangerously high level of vulnerability to data breaches, loss of customer trust and significant financial loss something businesses will not be able to afford in the uncertain economic future.

Unfortunately, major security and privacy missteps by popular communication platforms soon revealed that ease of use, compatibility, and efficiency can come at a heavy cybersecurity cost. While these platforms have always carried some cyber risk, the incredibly high numbers of remote workers and the ever rising $6 trillion threat of cybercrime have caused these vulnerabilities to be exploited en masse.

To meet the ever-increasing challenge of remote work and cybercrime, communication platforms will need to be built to a new standard, with infrastructure that prioritizes cybersecurity.

THE VALUE OF DATA

As the modern world has moved away from a manufacturing economy to a knowledge-based economy, our most valuable assets have shifted from physical ones towards intellectual property and data. In fact, recent analysis has found that data has now surpassed oil as the world's most valuable commodity in the global economy.

As with anything valuable, we must carefully consider our actions around protecting it most efficiently. This will increasingly become the case as we move into a new, data-led decade built on rapid technological advancements.

Companies must appreciate the value of their data as an asset, understand the different categories of data that they own, and most importantly, stay abreast of the latest ways for protecting this valuable modern-day asset that is vulnerable to hacking.

Yet with **4 in 10 employees saying that their company CEO under-values cybersecurity**, it's clear that many companies still don't place enough importance on their data to secure it at all costs and hence will remain unprepared for the coming changes this decade.

Collectively, there needs to be a paradigm shift in how organizations can best protect their sensitive data at scale without inhibiting mobility and productivity.

SECURITY AT THE GOVERNMENT LEVEL

Leading with a security-first approach to IT has always been a key consideration in government communications. It's no surprise that dealing with a country's military secrets and government data requires the utmost security considerations given how high the stakes are.

Issues of national and global security are at risk when communications within the government are insecure or vulnerable. So, when deploying messaging and collaboration tools at this level, such high stakes call for the highest of security thresholds.

As governments have added new departments and ministries to deal with the COVID-19 pandemic, this has given rise to additional needs around secure communications. Tools that allow governments to communicate internally with one another simply must take a security-first approach. Factors such as new technology and ease of use may take a back seat when compared with tools that are designed with security front of mind.

Governments also tend to run their communications differently than enterprises. For instance, they don't access the public internet as consumers and enterprises do, but instead use completely sealed internet systems within closed intranet networks. This means a more secure solution is needed to minimise the risk of hacks, with the preferred option being on-premises.

Enterprises can learn a lot from governments' security-led approach to communication tools and their implementation. When governments search for a collaboration tool, it would do well to meet the following criteria:

SECURITY & USABILITY

The most secure option is one with true end-to-end encryption, which is now available without compromising on usability.

PRIVACY

This needs to be up to the highest standard with minimal metadata footprint. In this case, privacy also means security. An on-premise solution is ideal for maintaining privacy within concealed environments.

FEDERATION

Anytime a government deploys a messaging or collaboration platform, this technology must connect with different enclaves. For example, one branch of the government will have its own intranet for communication, but different branches really need to be able to join up and communicate whilst remaining secure. Federation creates a standardized system, which allows different messaging platforms to interact securely.

There has always been a continuous cycle where consumer and enterprise tools impact each other. The pendulum swings, wherein at times government technologies impact consumer applications and vice versa.

Similarly, there's no reason why enterprise and government shouldn't both adhere to high security standards.

CONCLUSION

Notwithstanding recent events, the decade we have entered was always meant to be a pivotal one. With technology enabling borderless communications, businesses were already coping with the need for digital change management to enable new ways of working.

Here we are, at the first half of 2020, building businesses with exciting new technologies and innovations. Yet, there's a lot at stake. Adapting to the changes ahead by fostering the mobile workforce while acting with a high level of responsibility towards security is the future of enterprise communication. Is your organization ready for the future of work?

ABOUT WIRE™

Recognized by IDC, Forrester, and Gartner as one of the most secure collaboration platforms in the market, Wire™ is transforming the way enterprises and governments communicate at the same speed that our founders disrupted telephony with Skype., Our secure solution features messaging, audio, video conferencing, file-sharing, and external collaboration - all protected by the most advanced end-to-end encryption.

If you are searching for the most secure communication solution for your organization, look no further. But don't take our word for it, try it for free today:

TRY WIRE FOR FREE

Or contact us directly for more information.