ISG®

Chapter 01

An ISG Report, with Unisys

From Digital Native to **Digital Naiveté**

IN THE SPACE OF A COUPLE OF WEEKS
THE WORLD REDUCED COVID-19 R_0
BUT FORGOT ABOUT THE DIGITAL R_0

The Future is Dead,
Welcome to the New Future

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In early 2020, businesses the world over faced the ultimate dilemma, how to continue doing business or even more importantly, stay in business and operate, all while addressing one of the biggest challenges the human race has faced to date. All this happened while over 50 percent of the global population was locked down at home due to the spread of a biological pathogen, resulting in a low civilian mobility similar to that in the 1950s.

We live on a planet where we are hyper-connected, where privacy and cybersecurity are foremost in our digital minds, but biologically, we still have yet to conquer that same sense of security. And one has dramatic effects on the other. We have become reliant on being digital natives.

Seventy-five percent of all emerging infectious diseases come from wildlife[1]. Never before have so many opportunities existed for pathogens to pass from wild and domestic animals to people, impacting the global economy in ways we have only just come to terms with. Human infectious disease outbreaks are rising, and in recent years, the planet has had to deal with Ebola, H1N1, SARS, West Nile virus and Zika virus all of which crossed from animals to humans. A 2007 study of the 2002-03 SARS outbreak concluded, "the presence of a large reservoir of Sars-CoV-like viruses in horseshoe bats, together with the culture of eating exotic mammals in southern China, is a timebomb[2]." The Zoological Society of London has stated that "the emergence and spread of COVID-19 was not only predictable, it was predicted there would be another viral emergence from wildlife that would be a public health threat[3]."

With the global impact of COVID-19, the commercial world has been forced to assess business models and ways of working just to survive, let alone improve. For years, investment in digital was seen as important, but deemed to be a low risk, especially in the area of normal day-to-day operations. We were digital natives relying on technology to "just do" what we needed it to do but had become digitally naïve to think that it would not have exploitable weaknesses. Specific business cases would easily be deployed for data centers and large infrastructure to ensure that core digital operations would continue; however, locking down all these assets was never truly considered or invested in. Digital investment and security costs appeared prohibitive, and many organizations did not make them a priority.

At the same time, most organizations saw a flexible digital workforce to be of secondary importance with employees needing only to be provided with a mobile phone and a laptop in order to be flexible and have the ability to "work at home." The use of a corporate VPN or other seemingly simple technologies were considered sufficient, although these technologies were vulnerable to those determined enough to breach them.

Corporate hands were rapidly untied as the global crisis unfolded, and business made sure that core operations would continue. In some cases, changes were needed just to ensure that the business survived. Changes that took months to do previously had to be done in days or weeks. Workers were sent home and asked to work on platforms that had never seen the level of traffic. The mantra was, "get my workforce working as quickly as possible, as efficiently as possible." They forgot to add, "as securely as possible." Businesses did their best given the situation they were dealt; however, the true scale of security issues may still not be fully understood. Google has stopped over 240 million spam emails and 18 million phishing attacks globally in one day. The world has changed forever, and given the speed of change, the gates may have been closed after the security horse has bolted.

Looking at the market, while we may have locked down the workforce down to reduce the spread of a biological pathogen (the biological R naught, or contagion level), but inadvertently we may have just increased the digital R naught for many businesses – the scale of which may not be felt for many weeks or months to come. The breaches may have already occurred.

In the modern world, security of data is paramount. GDPR and other security standards are now enforced by law and dictate that this is taken seriously. A breach could lead to fines equal to percentage points of an organization's global revenue – which is significant. In the market, one organization stands alone and has changed the way organizations can move to a flexible working model, safe in the knowledge that they have moved the security dial to make it much harder, if not impossible, for corporate data to be breached over a remote working model.

THE MOVIE ABOUT DIGITAL NAIVETÉ WOULD TELL THE STORY OF INEVITABLE FIREFIGHTING AND PANIC

"It ain't what you don't know that gets you into trouble. It's what you know for sure that just ain't so."

If you've seen the 2015 movie, "The Big Short" – and you should, it's great – you'll know that the movie opens with this Mark Twain quote. It's a perfect quote for the film and an ideal metaphor for what the world has just experienced. For many years, the corporate world has experienced boom and bust cycles in almost every sector from the Great Depression through to the financial crash of 2008. The post-COVID-19 world has exposed massive issues with digital complacency and attitudes toward security, which in the race to address customer demand online, was sometimes overlooked.

Act 1: Accept and prepare for the unthinkable

As Tolstoy said, "The most difficult subjects can be explained to the most slow-witted man if he has not formed any idea of them already; but the simplest thing cannot be made clear to the most intelligent man if he is firmly persuaded that he knows already, without a shadow of a doubt, what is laid before him."

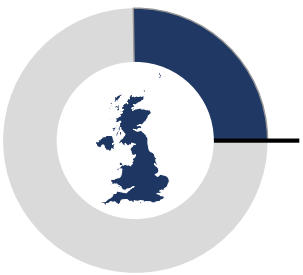
In essence, and why these movie and literary quotes are so apt, is that the pre-COVID-19 corporate horizon was so blinkered, no one could possibly fathom or predict that a zoonotic pathogen – one which crosses from animal to human – might actually do what nature intended it to do, or could they?

Like the script of a movie, cut to Vancouver 2015, the same time as "The Big Short" was playing in movie theaters. A very unassuming looking individual steps up on stage and prepares to give a TED talk. You know the 20- to 30-minute clips we all watch on YouTube? He opened, "If anything kills over 10 million people over the next few decades, it is likely to be a highly infectious virus rather than any war." People watched and respected the presenter, but as with many things, industry took the long game and, through a cost benefit-led approach to risk, adapted slowly, not ever thinking that this was a realistic prediction. That man was Bill Gates and since the outbreak of COVID-19, his TED talk has been watched more than 64 million times with people trying to see if there are any other hidden or missed messages.

Act 2: Adapt or die

Tom Fishburne's famous Marketoonist.com cartoon[i] shows a boardroom full of people proclaiming, "Digital transformation is YEARS away. I don't see our company having to change anytime soon." This is happening while the COVID-19 wrecking ball is swinging toward the boardroom wall, and the cartoon is likely the most used graphic of 2020, if not the next decade. It symbolizes the issues corporations face and the reason for the quotes above.

The inability or refusal to for management and business models to adapt and prepare has led to the biggest market shift since the Great Depression. And now the ability to adapt to new norms and behaviors is a survival-level competency. In the digital age, it is no longer an excuse not to have digital supply chains and an agile operating model which enables an anywhere service. Almost 25 percent[ii] of organizations in the U.K. have had to close or temporarily pause trading with 25 percent[iii] of the remaining organizations seeing enough disruptions to their supply chain that they have had to change suppliers. A fifth overall have had to pay more for the same service.



25%

Organizations in the U.K. **stopped or paused trading**

Source: https://www.ons.gov.uk/

This has caused unsustainable cost pressures on many organizations, resulting in unemployment levels in the U.S. jumping 10 percentage points in a single month[iv] with now almost one in three people unemployed. With 20 percent of the world's population being locked down through government measures[v], it is clear that businesses had to adapt. Granted, certain industries

such as the travel, transportation and hospitality industry have been decimated. The number of airline passengers currently stands at 7 percent of last year's level[vi] with the overall decline for the year predicted to be around 65 percent[vii]. These industries have relied on physical use of a product or service. On the plus side, customer demand has been driven online with increases of between 6 percent for reading materials and 30 percent for food and health products across the retail sector globally.[viii]

Act 3: The impossible made possible – I need my people working right now as efficiently as possible

So how has business been able to undertake a paradigm shift so quickly? In January 2020, we were likely told it would take six to 12 months to roll out a remote working solution or even a hardware refresh – well, thanks to the unthinkable, many organizations did it in less than a week. The ISG Index™, which is recognized as the authoritative source for marketplace intelligence on the global technology and business services industry, identified that of the remaining provider organizations in operation globally, approximately 80 percent of employees were working from home.[ix]

For 70 consecutive quarters, ISG has detailed the latest industry data and trends for financial analysts, enterprise buyers, software and service providers, law firms, universities and the media, and never has seen such a shift. To undertake this mammoth task, employers have had to re-think their entire delivery models, redesign processes, and deploy new technologies, all done at speed.

The end result is that 80 percent of companies monitored for the ISG Index™ report that productivity levels have remained the same or increased[x].

It has taken a global pandemic to show the corporate world that those companies that went digital could survive, and those that had digital agility built in could continue to grow, despite significant challenges.

The fallacy of overly complex, highly managed waterfall-style delivery of projects has been shown to be the wrong model when survival of the company was at stake. Mountains were moved, BUT in doing the unthinkable in unprecedented times, it means that security was perhaps an afterthought. The section title above could have been, "I need my people working right now, as efficiently as possible and as securely as possible."

Does this mean that the story is finished, or will there be a sequel? The world of work will never be the same again, so of course, there will be a sequel, and the story just gets more interesting because doing the unthinkable at speed means things like security will have fallen through the cracks!

CHANGES TO THE WORLD OF WORK – OPENING PANDORA'S BOX

The enormous challenges the world has faced have presented enormous opportunities. Organizations that previously embedded new ways of working into day-to-day operations can plan for both resiliency and competitive advantage while they maintain or improve the customer experience during lockdown.

Through the enablement of technologies to provide remote or at-home working, these organizations have changed the core delivery concepts we have come to know in everything from customer engagement at the contact center to the support of operations and the use of customer data. This offers a glimpse into the new world of work.

- Organizations that have built digital elasticity and resiliency into their operations and that offered a seamless digital channel for customers have survived the crisis much better than those that haven't.
- As new challenges arise, as they undoubtedly will, companies must be ahead of the curve to ensure continuity of core operations and revenue streams.
- Doing this with a workforce that has enjoyed the ability to work at home, have better a work/life balance and feel more in control of their work can only benefit the customer experience and the bottom line.

Rethink your workforce

In the marketplace, ISG is an independent advisor and is therefore able to provide advice on solutions that help clients decide on the best technology solutions and providers position themselves in the marketplace. As part of that, just like with the ISG Index reports, predictions are made which are based upon the best available information and prevailing market winds. In the area of the future of work, it became clear that going forward, we will not all return to an office. Indeed, it is anticipated that the need for office space used as desk space will likely reduce by approximately 40 percent. This will become adaptable collaboration space. The reason for this is that organizations that work with ISG have said their workforce is happier, as productive, and willing and able to work at home much more than the Fridays only typically previously taken.

The new future workforce is a hybrid model

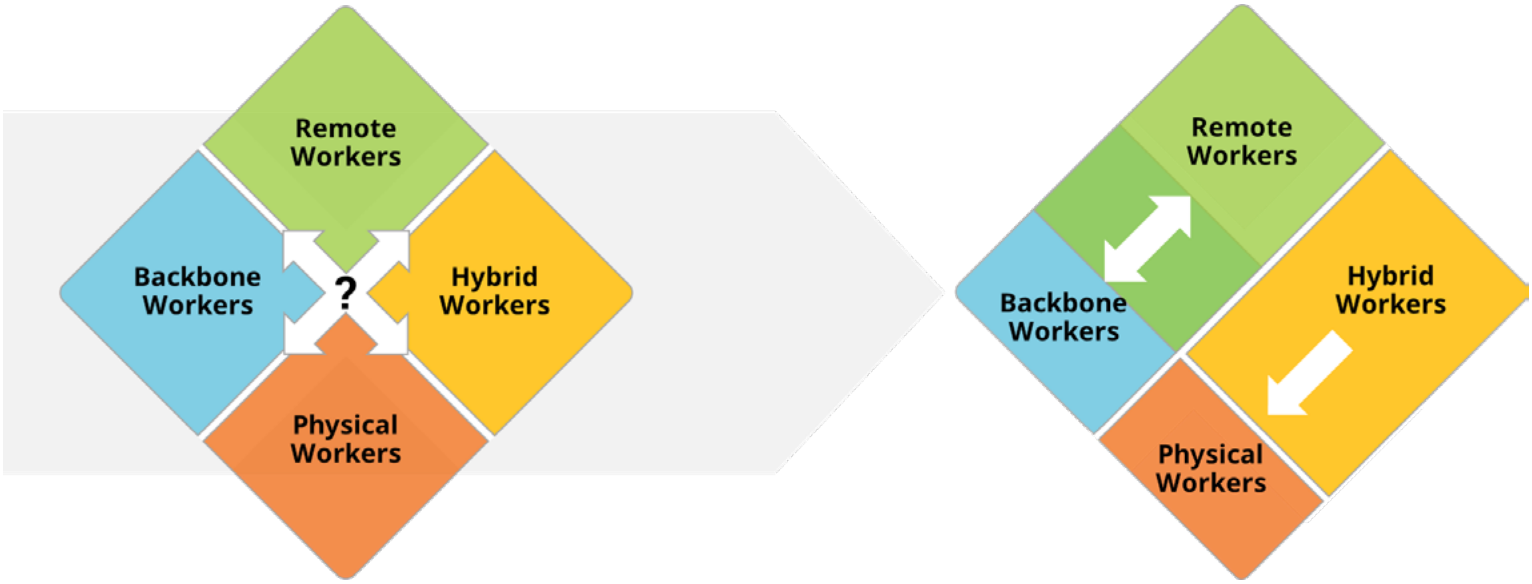
Employees have exercised their judgement and voice in corporate surveys unequivocally stating that they wish to work at home between two and four days a week. This is common from ISG's experience. This means that there will be four types of worker in the future delivery model within organizations.

Physical workers

These workers are people who need to be physically and permanently located in one place. This could be an office, or it could be their home. They will have technology at home that replicates their IT access in the office, but there is little value seen in having this worker travel to a building to sit and work when it is beneficial for them to remain at home. On the flip side, there will still need to be a workforce that does come to corporate offices daily and work. There will be limited change to the employee experience for them.

Remote workers

As the majority of the workforce has indicated that they wish to remain and work at home for a significant proportion of the working week, they will become what will be called, the remote workforce. Using integrated mobile technology, they can work from anywhere without the need for a hard connection to the corporate network. This involves the use of different technologies and processes that will become important later on.



Backbone workers

These individuals are crucial in the smooth operation of a distributed workforce. As we now know, remote workers will no longer "touch base" as often, and the physical worker may well never come into the office. This means that the experience offered by these backbone workers in the technology space will focus on a high level of performance in systems and support to ensure that business as usual in a digital world continues. They will provide support for hybrid assistants aiding the remote workforce, and they will update robotic processes when automation is assisting the remote or physical workforce but will also provide cloud based and mobile digital capabilities. This category includes the back-office functions or human resources, payroll, procurement, finance and IT.

Hybrid workers

The remaining workforce, and likely those that have been part of the 9.3 million furloughed workers in the U.K.[xi] will make up the hybrid workforce. Not all of these furloughed workers will join the hybrid workforce, as some will return to one of the other three types of work, and organizations will need to make decisions about this new way of working. Organizations need to design new business models that can scale as required to meet demand and the wishes of the hybrid worker to work when they want in a new employment model akin to the "uberization of the workforce." Able to work at will, they can meet the demands in industry such as customer facing positions or even in back office in areas such as help desk or in finance or payroll at peak times. This will require an integrated set of technologies that join productivity systems into ERP systems and also integrate time recording systems. Given these requirements, many of these people will need the same technology and backbone support that the remote workforce will need.

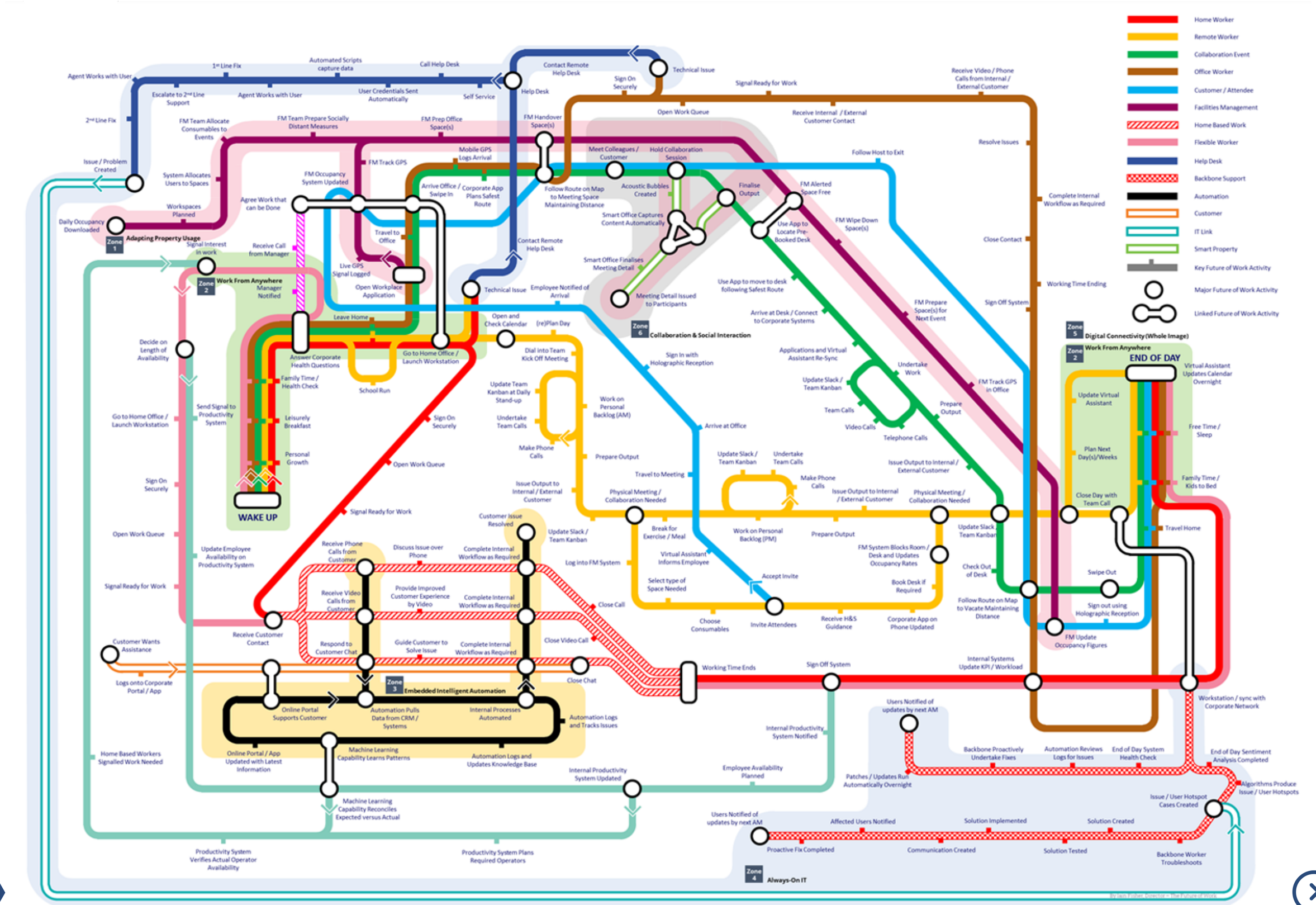
What will it feel like to be an employee in the new future?

In our analysis of what the new future will look like, ISG has identified a number of personas or pathways that each type of worker will experience. Completed in the style of a city transport map, each type of worker has been shown in a typical day – remember, you can be a different type of worker each day. This means you may go from a remote worker to a home worker, a collaboration participant or an event attendee all in the space of a week. This diagram shows all the possible options and the typical activities each type would experience. Behind this is a series of technologies and capabilities that need to be put in place in order for an organization to deliver this successfully. Having started with a people assessment and moving onto the headline strategy for property and technology to deliver core business, organizations can draw a clear pathway to the future world of work.

Connected areas, shown as zones include:

- Adaptable workspace, where facilities will need to accommodate new health and safety measures and monitoring;
- Automation where backbone support has provided the capability for extra value to be provided;
- Collaboration where smart property combined with technology and digital tools provide the opportunity to co-create more rapidly;
- Always-on IT provides assurance that collaboration can happen through cloud-based tools plus silent background capabilities predict and autocorrect issues before they occur.

Around the whole diagram is the key principal of a "secure digital environment," and this means a number of different things to a number of people.


Home Worker
Remote Worker
Collaboration Event
Office Worker
Customer / Attendee
Facilities Management
Home Based Work
Flexible Worker
Help Desk
Backbone Support
Automation
Customer
IT Link
Smart Property
Key Future of Work Activity
Major Future of Work Activity
Linked Future of Work Activity
Agent Works with User
1st Line Fix
Escalate to 2nd Line Support
Agent Works with User
Automated Scripts capture data
User Credentials Sent Automatically
Call Help Desk
Self Service
Contact Remote Help Desk
Help Desk
Technical Issue
Sign On Securely
Signal Ready for Work
Receive Video / Phone Calls from Internal / External Customer
Open Work Queue
Receive Internal / External Customer Contact
2nd Line Fix
FM Team Allocate Consumables to Events
FM Team Prepare Socially Distant Measures
FM Prep Office Space(s)
FM Handover Space(s)
Resolve Issues
Issue / Problem Created
System Allocates Users to Spaces
FM Track GPS
Mobile GPS Logs Arrival
Meet Colleagues / Customer
Hold Collaboration Session
Follow Host to Exit
Workspaces Planned
FM Occupancy System Updated
Arrive Office / Swipe In
Corporate App Plans Safest Route
Follow Route on Map to Meeting Space Maintaining Distance
Acoustic Bubbles Created
Finalise Output
FM Alerted Space Free
Complete Internal Workflow as Required
Daily Occupancy Downloaded
Agree Work that can be Done
Smart Office Captures Content Automatically
Use App to Locate Pre-Booked Desk
FM Wipe Down Space(s)
Zone 1 Adapting Property Usage
Travel to Office
Contact Remote Help Desk
Close Contact
Signal Interest in work
Receive Call from Manager
Live GPS Signal Logged
Smart Office Finalises Meeting Detail
Zone 2 Work From Anywhere
Manager Notified
Open Workplace Application
Technical Issue
Employee Notified of Arrival
Use App to move to desk following Safest Route
Working Time Ending
Meeting Detail Issued to Participants
Zone 6 Collaboration & Social Interaction
Arrive at Desk / Connect to Corporate Systems
FM Prepare Space(s) for Next Event
Sign Off System
Leave Home
Open and Check Calendar
(re)Plan Day
Zone 5 Digital Connectivity (Whole Image)
Decide on Length of Availability
Answer Corporate Health Questions
Go to Home Office / Launch Workstation
Dial into Team Kick Off Meeting
Sign In with Holographic Reception
Applications and Virtual Assistant Re-Sync
Undertake Work
Zone 2 Work From Anywhere
END OF DAY
Virtual Assistant Updates Calendar Overnight
Update Slack / Team Kanban
FM Track GPS in Office
Update Virtual Assistant
Family Time / Health Check
School Run
Update Team Kanban at Daily Stand-up
Work on Personal Backlog (AM)
Team Calls
Prepare Output
Free Time / Sleep
Go to Home Office / Launch Workstation
Send Signal to Productivity System
Leisurely Breakfast
Undertake Team Calls
Arrive at Office
Video Calls
Telephone Calls
Plan Next Day(s)/Weeks
Personal Growth
Sign On Securely
Make Phone Calls
Prepare Output
Update Slack / Team Kanban
Undertake Team Calls
Issue Output to Internal / External Customer
Family Time / Kids to Bed
Open Work Queue
Issue Output to Internal / External Customer
Travel to Meeting
Make Phone Calls
Physical Meeting / Collaboration Needed
Issue Output to Internal / External Customer
Physical Meeting / Collaboration Needed
Close Day with Team Call
Travel Home
WAKE UP
Signal Ready for Work
Customer Issue Resolved
Update Slack / Team Kanban
Break for Exercise / Meal
Work on Personal Backlog (PM)
Prepare Output
Update Slack Team Kanban
Update Employee Availability on Productivity System
Receive Phone Calls from Customer
Discuss Issue over Phone
Complete Internal Workflow as Required
Log into FM System
Virtual Assistant Informs Employee
FM System Blocks Room / Desk and Updates Occupancy Rates
Check Out of Desk
Swipe Out
Signal Ready for Work
Receive Video Calls from Customer
Provide Improved Customer Experience by Video
Complete Internal Workflow as Required
Close Call
Select type of Space Needed
Accept Invite
Book Desk if Required
Follow Route on Map to Vacate Maintaining Distance
Sign out using Holographic Reception
Receive Customer Contact
Respond to Customer Chat
Guide Customer to Solve Issue
Complete Internal Workflow as Required
Close Video Call
Choose Consumables
Invite Attendees
Receive H&S Guidance
Corporate App on Phone Updated
FM Update Occupancy Figures
Customer Wants Assistance
Close Chat
Working Time Ends
Sign Off System
Internal Systems Update KPI / Workload
Logs onto Corporate Portal / App
Zone 3 Embedded Intelligent Automation
Online Portal Supports Customer
Automation Pulls Data from CRM / Systems
Internal Processes Automated
Automation Logs and Tracks Issues
Workstation / sync with Corporate Network
Users Notified of updates by next AM
Internal Productivity System Notified
Backbone Proactively Undertake Fixes
Automation Reviews Logs for Issues
End of Day System Health Check
End of Day Sentiment Analysis Completed
Home Based Workers Signalled Work Needed
Online Portal / App Updated with Latest Information
Machine Learning Capability Learns Patterns
Automation Logs and Updates Knowledge Base
Patches / Updates Run Automatically Overnight
Algorithms Produce Issue / User Hotspots
Internal Productivity System Updated
Employee Availability Planned
Issue / User Hotspot Cases Created
Machine Learning Capability Reconciles Expected versus Actual
Users Notified of updates by next AM
Affected Users Notified
Solution Implemented
Solution Created
Proactive Fix Completed
Communication Created
Solution Tested
Backbone Worker Troubleshoots
Productivity System Verifies Actual Operator Availability
Productivity System Plans Required Operators
Zone 4 Always-On IT
By Ian Fishet Director - The Future of Work

The calm before the storm

It should be noted that in this new world, there's also a win-win for the employee. Overall, they are expected to reduce commute time by over one and a half hours each day based on the average commute.

- This equates to an average of 41 days less time spent commuting and returns back approximately $4,500 per year to the employee.
- In its recent 2020 Global work-from home experience report[xii], Globalworkplaceanalytics.com found that organizations noted a 30 percent productivity increase with an average of five extra hours worked each week by employees.
- Companies can also save on average of $10,000[xiii] per employee by moving to remote working through the reduction of power consumption and paying for space.

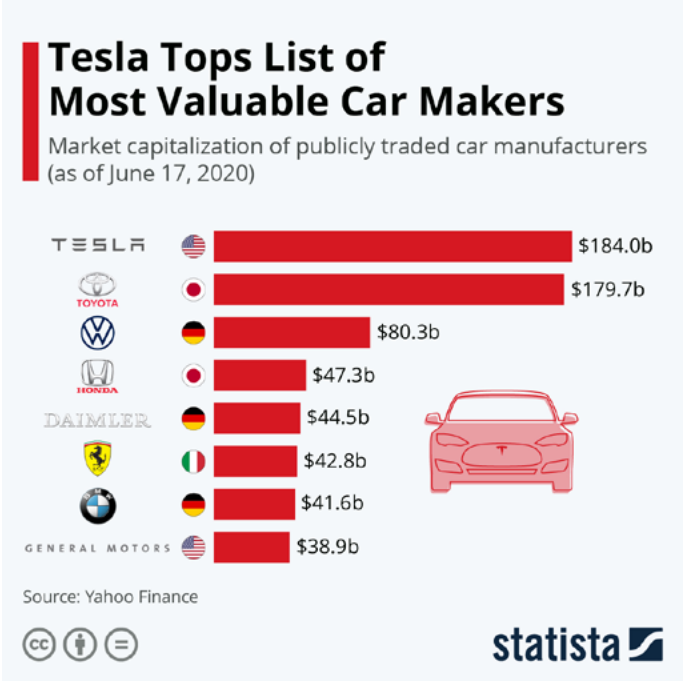
Source:
https://globalworkplaceanalytics.com/whitepapers

By redesigning the business model AND the operating model, there is a positive case for change for both the employee and the bottom line. So that's the end of it, right? Wrong!

Not all digital remote solutions are created equal

As earlier noted, ISG is an independent advisor and is therefore able to provide advice that helps clients decide on the best technology solutions to deploy and helps providers position themselves in the marketplace.

As part of the Future of Work market updates, ISG met with the top providers identified in ISG's Provider Lens™ reports. Having identified the multiple key elements needed to successfully deliver the ideal client solution for the future of work, ISG discussed this with each provider. Through these discussions, a picture of commonalities and unique approaches has become apparent.



Source: Statista

As with many things in life, providers had taken a number of approaches to solve the same type of issues. For example, when you want to buy a vehicle, you only need a chassis, four wheels and seats with a basic level of options to meet your needs, but the likes of BMW, Mercedes and Audi have all taken different approaches, and all are German. The Japanese and U.S. auto manufacturers have taken very different approaches. In this market, one marque, Tesla, has

led the way because it differentiated early and built a future-proofed product that has adapted and is now the global industry leader in clean, non-polluting vehicles.

Finding the "unique" during a mass re-invention of the future of work

Security of the enterprise was one of the key elements of ISG's analysis of the future of work. ISG found a number of solutions to the same problem when speaking with providers, some of which had better features or future proofing than others.

For example, most providers realize that given the global pandemic and the need for workers to get online and work quickly, they were able to offer some form of rapid move to a cloud hosted service, which varied in complexity and security. One offered a bunkered set of hosted applications that were available on any device, but it meant a client could only use them and them alone. In other areas of security, a number of providers thought about the principle of data access and protection of corporate assets. One solution was to provide access through mobile devices using bio recognition as a "key" to the corporate gateway. A possible vulnerability was identified by ISG in the event of the device being accessed when unlocked or stolen. A second option for data protection was the recording of access to the corporate network using the camera on the connected device. This made sense except for the fact that this was a lagging security measure and would only provide investigators or the authorities with evidence of who had taken the data. In the area of security and the access of corporate data, one offering stood out above the rest.

Unisys had identified significant vulnerabilities in the secure access of corporate networks and came to market with a unique offering using software-defined parameters and micro-segmentation, which has inbuilt artificial intelligence and machine learning capabilities to protect corporate networks, while the remaining providers continued to go down the VPN or hardened platform route. This was clearly unique and like Tesla, future proofed as it can be deployed to any device remotely and invisibly to the user. In a world where speed was needed in order for some businesses to survive, there now exists a multitude of security solutions just don't make your final choice until you have read this!

SPEED – BUT AT WHAT COST? AFTER THE CALM CAME THE STORM!

One of the most important areas that cannot be overlooked in the new future is cybersecurity. The World Health Organization has seen a five-fold increase in cyberattacks directed against its employees[xiv] since the outbreak began. According to a recent survey by the World Economic Forum[xv], the economic fallout from COVID-19 dominates companies' risks perceptions. Two-thirds of its survey respondents identified a prolonged global recession as a top concern. Half identified bankruptcies and industry consolidation, with the failure of industries to recover and a disruption of supply chains as crucial worries. This echoes the research undertaken by ISG in its Index™ report. Importantly, the third most worrisome area identified by over 50 percent of survey respondents was an increase in cyberattacks and data fraud.

COVID-19 attack profiles

Unisys identified that there are three big growth spikes that its security experts are seeing after the initial phase of COVID-19.

Phishing

There is a significant growth in phishing against personal and corporate email addresses. This is the fraudulent practice of sending spoof emails purporting to be from reputable companies or your own organization in order to induce individuals to reveal personal or corporate information, such as passwords, credit card numbers or corporate data. Because we are no longer sitting in an office and have blurred the line between corporate and personal by working at home possibly browsing to non-work pages, it is much easier for a hacker to obtain information.

Spear phishing

Corporations are reporting a significant growth in spear phishing against corporate addresses. This is the fraudulent practice of sending emails that look to be from a known or trusted sender in order to induce targeted individuals to reveal confidential corporate information. Experts are seeing a rise due to having staff not in working in offices where they could speak to a colleague or call someone to validate a request. When workers are at home and receive a targeted and time-sensitive request they often do not know what to do and are likely to comply with the emailed request. Training is needed to combat spear phishing.

Vishing

With the rise of data apps that are secure and effectively anonymous, companies are reporting a significant increase in the level of vishing. Vishing is the practice of using voice or data apps combined with a phishing attack. The main reason for the rise during COVID-19 is because many organizations, in the rush to get people working at home to "keep the lights on", had employees using voice calls more frequently, and in an attempt to be helpful and connect people, organizations exposed employee phone numbers.

In some cases, companies are providing recorded messages that tell callers where to reach staff members and even provide the numbers. This is ideal hacking territory. This means that hackers are provided with people's direct numbers to call and in some cases their working patterns also – all of which can be used when direct contact is made.

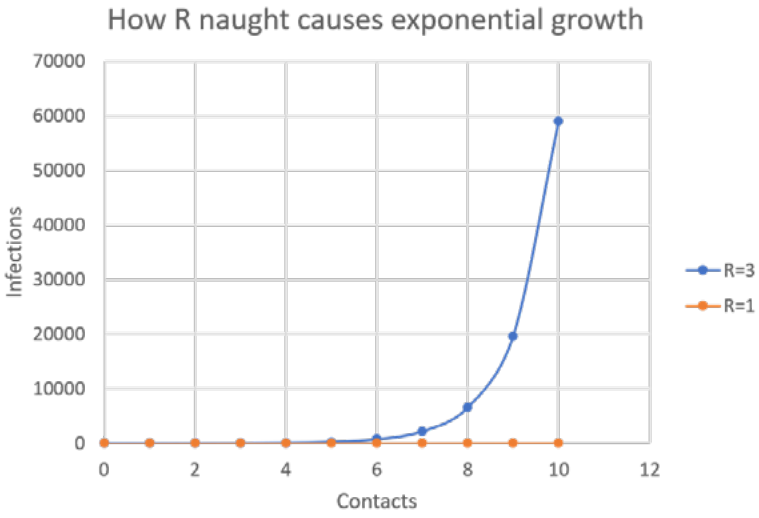
By using apps like WhatsApp, attackers can create fake accounts that look real because the contact data has been provided to them by your company. They then can send you data requests that look very official with little or no way of checking them.

What types of attacks are being seen in the market?

Security experts have seen a greater than 30 percent increase in COVID-19 themed cyberattacks in the last month[xvi].

Google claimed in May 2020 to be blocking over 240 million COVID-19-themed spam messages each day, and 18 million malware and phishing emails[xvii].

This hammers home the point that while work changes had to happen, complacency cannot, or organizations will end up back at the "it'll-never-happen" syndrome we started with.



Source: ISG

The creation of weak points

The requirement to enable people to work at home brought new challenges, as one would expect. Considering that the figure of those who worked at home in the U.K. grew from 4 million in 2019 to over 23.9 million[xviii] due to COVID-19 government-mandated lockdown resulted in the largest mass change to ways of working in history.

Due to the speed of delivery and the ways new work will be undertaken, security aspects were rushed and may lead to breaches that are not yet apparent. We have removed employees and digital operations out of

a highly secure corporate environment that is locked down in security terms, and opened up operations to the masses in a much less secure environment – their homes. We have effectively done the polar opposite of what we are trying to do with coronavirus. Essentially with the virus, we have tried to reduce the R_0 – the contagiousness – and therefore, the spread of the disease. In security terms, business has opened Pandora's box and the digital R_0 for security could skyrocket. By that, we mean the level of vulnerabilities that business has to manage has exponentially grown just like the initial spread of coronavirus went unchecked when R_0 went above a one-to-one spread.

THE CONCEPT OF AN R_0

You may have heard the term R_0, pronounced R naught, the world over during COVID-19 government briefings given in the U.S., U.K. and Europe. R_0 is a term that indicates how contagious an infectious disease is, and it is referred to as the reproduction number. The R_0 of a disease is the average number of people who will contract the disease from one person in the general population who has the disease already. Why is this important?

If a disease has an R_0 of 10, the typically a person who has the disease will infect an average of 10 other people. They each will then go on to infect an average of 10 more people. In this case one person with a disease of R_0 of 10 would infect 10 billion people through 10 contacts. Therefore, the R_0 results in potential exponential growth and replication unless there are protection measures or a vaccine within the community to reduce the overall R_0 number.

What does R_0 actually mean?

Medically, and mathematically only three possibilities exist for the rise or prevention in transmission, which can be described depending on its R_0 value:

- If R_0 is less than 1, each existing infected person transmits the disease on average to less than one new person. In this case, the disease will decline and eventually die out, and the community is eventually free of the disease.
- If R_0 equals 1, each existing infected person transmits the disease on average to one new person. The disease will stay alive and stable, but there won't be an outbreak or an epidemic
- If R_0 is more than 1, each existing infected person transmits the disease on average to more than one new person. The disease will be transmitted between people exponentially, and there will likely be an outbreak or epidemic.

This is important because in a society where the disease has not occurred before, there is no immunity, and the pathogen will be freely transmitted. This is why the R_0 value is so important until a vaccine has been discovered, there have been measures put in place to control the spread of the disease, or the population has been wiped out and no new hosts exist.

According to an article published in BMC Medicine[xix], the R_0 value of the swine flu that killed 50 million people in 1918 was estimated to be between 1.4 and 2.8. When the H1N1 version of the swine flu broke out in China in 2009, its R_0 value was between 1.4 and 1.6. The reason the R_0 reduced was because effective vaccines and antiviral drugs made the 2009 outbreak much less deadly within the affected population.

The R_0 of COVID-19

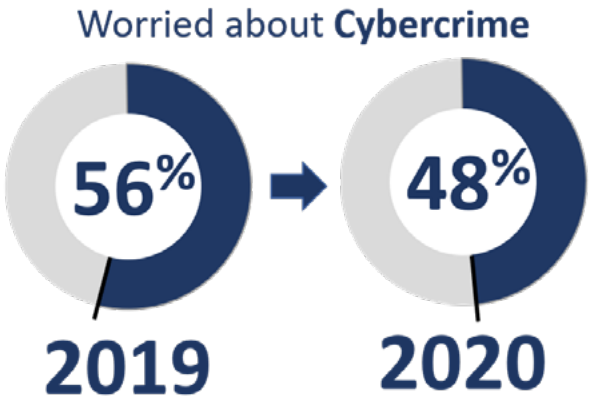
The R_0 for COVID-19 hovers around 5.7, according to a study published online in Emerging Infectious Diseases[xx]. This means that on average, every single infected person that is infected infects 5.7 other people – an exponential increase. Early on, when governments and businesses were assessing impact, the scientific estimate of R_0 was 2.2 to 2.7. This is a huge difference and meant that the way we could address societal issues was only to be achieved through drastic change – resulting in almost half the population of the planet being locked down. The 5.7 number means that one person will have indirectly infected over 6,000 people in through five contacts and 1.1 million people through eight contacts. Business had to adapt in order to have any uninfected people to deliver services and stand a chance of survival.

Digital R_0 – what is it and how to manage it

Now we know what an R_0 is and what that means for exponential growth in a clinical and disease management sense, we need to understand what a digital R_0 means. This is the term we use to describe the likelihood of malicious or harmful activity resulting in a digital security breach of a corporate network.

As you can imagine, in these unprecedented times, businesses had to get employees working immediately and as efficiently as possible – but they forgot to consider employees working as securely as possible. This means that 23 million workers in the U.K. were possibly sent home with ill-prepared or improperly configured devices that may allow a security breach to occur. Should a breach have occurred, the digital R_0 could have been in the hundreds In many cases, the resulting infection or compromise rate would have been several hundred people for the one that was compromised, an exponential spread of an attack.

To be secure, your digital R_0 needs to be as low as possible, and this can only happen by having highly secure systems and devices for workers to use. Just like a pathogen, the digital liability of a hacker's breach of a corporate network results in a high R_0 if security is poor. A low digital R_0 number comes from having state-of-the-art and robust security measures on your network, its access points and the devices that access it.



Source: https://www.unisys.com/unisys-security-index

Having a digital R_0 of zero

Many organizations service both the private and public sectors. Employees who work on sensitive or secret programs, such as government contractors, are typically denied remote access to data due to confidentiality and/or intellectual property concerns. While this is generally a small subset of the overall employee population, these employees become high-value targets if able to access information remotely without the proper security in place. To enable these individuals and the essential organizations they serve to continue to work for remotely, a zero-trust solution that ensures a digital R_0 of zero is the only option.

DIGITAL NATIVES MORPH INTO DIGITAL NAIVETÉ

Two myths need to be busted straight away: firstly, that Millennials and Gen Y individuals know everything about digital, and secondly, that age impedes your ability to understand remote digital usage and that somehow, older people are more vulnerable digitally. Likewise, employees of any age who think they are safe because no one would target them are just as naïve.

Generally, hackers are not targeting you specifically, they are targeting millions of IP addresses, and they have no idea who sits behind the list of millions of IP addresses they are scanning. If the security on the IP address that fails happens to be yours, then you are the weak point. It is for this reason that everybody is vulnerable and all must work and surf in a secure way.

Out of office, out of mind

Meanwhile, according to the Unisys Security 2020 Index results, the perceived risks of shopping online fell drastically to 38 percent in 2020, despite the fact that the COVID-19 pandemic has meant an increased public reliance on online shopping during lockdown. Consumers and corporate employees using work devices surfed and shopped online as physical distancing measures implemented by national governments meant this was the only way to buy some goods. As part of this, people were less careful about the financial data they transmitted online. Cybercrimes relating to identity theft became less of a concern. More than half of respondents (56 percent) were worried about this in 2019, dropping to 48 percent in 2020, suggesting that people are not as focused on cybercrime, despite threats becoming more pervasive. ID or credential theft does not have immediate impact unlike physical theft that happened pre-lockdown, when it was immediately reported. If you have your wallet or purse stolen, the data taken means you lose money, credit cards or a driver's license. Online, the impact can be the same but not visible for some time.

General cybersecurity laisse faire

The 2020 Unisys Security Index identified three main headlines that can explain the apathy over cybersecurity:

1. Britons are more worried about COVID-19's impact on the NHS and the U.K. economy than their own personal health.
2. Concerns about hacking fell drastically compared to 2019 – despite the majority of employees working from home.
3. Natural disasters, including pandemics, jumped from the lowest ranked security concern in 2019 to the highest in 2020.

According to the index, the U.K. was more concerned about COVID-19's impact on the NHS and the economy (61 percent of respondents), than they were about their own personal health (41 percent). Moreover, it was clear that they were less worried about online threats such as viruses and hacking; with levels dropping from 41 percent in 2019, to 31 percent in 2020, probably due to enormity of the COVID-19 pandemic and lockdown.

These changes in attitudes are likely because some people never realize when their details have been hacked and are being used to set up fake IDs, so they don't believe they are being actively targeted or may be victims. The problem with cybersecurity is that ignorance is bliss.

Seniors don't allow complacency to trump convenience

The people over 55 polled in the index are increasingly confident with keeping their devices secure, reporting fraud, and using online banking services – even more so than younger generations. For instance, compared to 45 percent of the older respondents, only a third (34 percent) of those aged 18 to 24 have an anti-virus software installed on their smart phone.

Perception of security

More than three quarters (78 percent) of respondents over 55 claims to be as careful when securing their personal and financial details on their smart phones as they are on other devices. The youngest generation was less wary of mobile threats, with two thirds (65 percent) saying they apply similar precautionary measures to their phone as well as their other personal devices.

Those over 55 are likely to be more cautious about protecting data because they grew up in an era where they had control of personal data. The only publicly available data back then was from phone books or the births, marriages and deaths offices. Today when asked to input date of birth, full name, address, bank details, etc., they are naturally much more cautious and suspicious.

The younger generation, however, has been brought up on digital technology as part of the fabric of their daily lives, without associated awareness and education, and there is an overconfidence in the security ability of devices and software, for example, some believe "Apple can't be hacked." There is also an expectation that the responsibility for security lies with the device manufacturers and software developers.

Naiveté surrounding public Wi-Fi

Free Wi-Fi is a great thing isn't it? Well, many people still just don't seem to realize that when they sit in their favorite coffee shop connected to the free Wi-Fi doing some work, leisurely online shopping or booking a holiday, that all their data, bank cards, personal info, addresses, dates of birth plus whatever data they enter are being transmitted unencrypted, ready for anyone nearby to snoop and steal. If this naiveté teaches us anything it is that we need a wider security refresher for anyone working from home on the issues they can face.

RECOGNIZING VULNERABILITIES

Most people who have home networks don't follow the same guidelines at home that they have to at work. Using home or personal networks and devices such as routers to access and transmit corporate data means that poor security protocols at home can compromise the entire network.

The attack surface has changed

Corporate infrastructure typically is much stronger and withstands attacks. But now attackers only need to go after home networks and their IP space to breach corporate systems or, at the very minimum, breach an unsecured home network and breach a device where they can exfiltrate or mine data from those devices.

This is how the digital R_0 can explode. Employees need to think of their homes as an extension of their offices because the line is now blurred in the new future. This is something that will need to change globally to secure corporate operations. As a quick check, ask yourself:

- Have you changed your default home network password?
- Have you hardened the equipment provided by your telecom provider, according to the manufacturer's specification?
- Do you patch the devices regularly?
- Do you reboot your router every 30 days or so?

If not, then you could easily be putting corporate data at risk. Organizations need to train their employees on how to harden their home networks.

Know the weak points

The IP ranges of home environments for carriers are widely known. If a vulnerability is identified for a home internet router type, attackers can quickly scan the IP addresses at massive volume to see what people they can compromise via various botnets they use to expose your home network. Attacks against improperly configured wireless networks in densely populated areas are also on the rise. The whole population wants widely accessible wireless reception in their home, and it doesn't stop at your property boundary. This means that people can access your network from outside your home if it is compromised.

Convenience can be your downfall

One of the main problems, also one of the most serious, is weak passwords, especially on home networks where it's more convenient to use a simple password for the home Wi-Fi, or even worse, the default password for the router you use. That, way when a new device needs to be connected, you can just shout downstairs, "123456" or "password using @ instead of A." In some cases, an outsider needs only a handful of attempts to gain access.

At the same time around the home, we are all embracing a plethora of IoT devices – thermostats, cameras, refrigerators, TVs, etc. – to make our lives easier and more convenient. What a lot of people don't realize is that many devices store the home network password as plain text on the device itself! All an attacker has to do is find the device (not difficult), hack it to get the password, and they then have access to your entire home network and all the devices on it, including corporate laptops and their connections. This was a glaring vulnerability on some IoT-connected kettles. More recently, a brand of wireless doorbell was found to be leaking Wi-Fi passwords in plain text during the setup process.

IoT creates a very interesting complexity for corporations. On average, each home has at least one automated IoT device from the major suppliers, from smart speakers to door locks and thermostats. Those same devices are also used by corporations to monitor environments in unmanned IoT infrastructures. This means there has been a massive growth in the number of devices to be monitored and managed. The operating systems and the applications of these devices are not like normal servers, laptops and desktops that IT departments are used to dealing with. The coding is not the same, IT teams do not always consider security or monitoring capabilities.

With 5G proliferation growing worldwide, a lot of these devices may not even talk over corporate networks; instead, they could be talking directly to providers, which adds a whole different level of cybersecurity problem management. This need to be addressed now.

Old-fashioned human weaknesses

Over 90 percent of successful attacks are enabled by humans, which means we have a very low awareness and understanding of cyberthreats and risks and how to avoid them. Human curiosity is a killer – take the first worm to hit cyber space 20 years ago – ILOVEYOU – it infected 50 million Windows computers in 10 days because of the irresistible urge to read what people thought was a love letter attachment in the email.

In a highly connected world, where social media enables our desire to peer into celebrities' and other people's lives, we fall prey to these same tactics today with curiosity getting the better of us. It may be, for example, we are informed we've won a prize and we're invited to click a link or open an attachment, even though we know we haven't entered any competitions.

A little while back a news channel ran an exercise at a major London train station where they asked a number of passengers for their passwords to a range of devices including home Wi-Fi, email accounts and phones. In return, the news channel offered them a chocolate bar. The majority of those asked handed over this information in return for the chocolate. There are no words.

Corporate VPN[xxi]

The majority of the IT industry providers still recommend securing access to your network through the use of a virtual private network (VPN). VPNs were designed to protect the network perimeter at a time when that perimeter was still defined and finite. When only a handful of "doors" into a network existed, they could be monitored and maintained.

To better understand how a VPN works, visualize your enterprise's network as a house and a VPN as a door. That door opens for anyone who has a key – or who can force the lock. Obviously, the door is where burglars are going to concentrate their efforts. Practically speaking, it is not that hard to break in. Plus, once they get through the door, there are no further barriers to navigate. They are free to move where they want and steal what they want.

Hackers love VPNs because they are relatively easy to crack. They are doors into your network. Once a VPN is compromised, the attack can propagate laterally and at a great pace from server to server within the data center, with no security controls in place to stop the spread. VPNs therefore represent a single point of security risk for the network and its perimeter.

SECURING REMOTE ACCESS IN THE FUTURE OF WORK

Employees, vendors, partners, customers, and other stakeholders now and in the future will be required to log in from different devices, using different connections, and working from different locations. CISOs, CIOs and CSOs are being asked to secure identities and devices across unknown and untrusted shared common infrastructure. In such a world, the enterprise network has moved from tightly bound to boundless.

How is the network perimeter changing?

IT environments now encompass multiple topologies, including on-premise hardware, private clouds and public clouds. Companies share applications and data with dozens of partners and vendors. Businesses are extending their operational reach and require to provide access to a remote workforce that is itself dynamic and elastic in nature. Consequently, whatever protection VPNs afforded to an enterprise's data and critical assets has been completely destroyed.

Businesses need a new and better way to secure their corporate assets. That can be found in a software-defined perimeter (SDP), which controls access to resources based on user identity, thereby delivering zero-trust security. While the term "software-defined perimeter" has only recently gained prominence in the IT space, ISG has identified one organization that has stood out in the deployment of security capabilities when delivering the future of work.

Unisys has been deploying SDPs since 2006 in the Unisys Stealth® solution. Stealth™ was originally developed to satisfy a U.S. government need to share sensitive and classified information globally at a huge scale across one of the largest and most complex networks in the world. Stealth™ protects data by creating an SDP via identity-based, software-defined, encrypted micro-segmentation.

Eliminating vulnerability

Going back to our analogy of VPN being seen as a house with a door, SDPs, in contrast, can be described as a house with no doors. The exterior is a solid brick wall. With no door, a hacker must destroy part of a brick to remove it. But, because the network is protected by micro-segmentation, the most a hacker can get is one brick and nothing more. Access to the entire house is never possible. Why?

There is no "spoon"

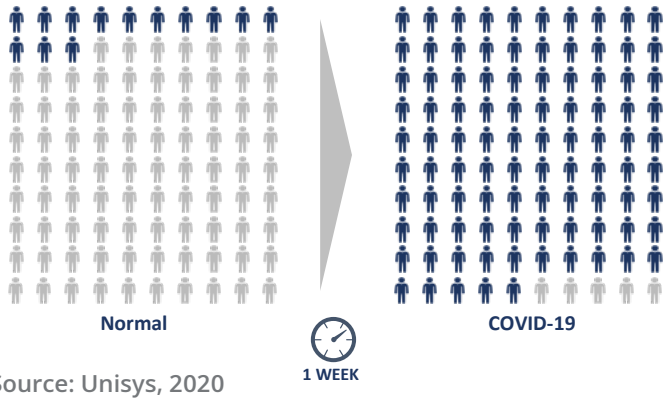
As the famous line from the movie, "The Matrix" goes, "there is no spoon." In this case, there is "no inside." Micro-segmentation has converted an "open floor plan" house into a solid cube of discrete bricks. But there is more to Stealth™ than that. Suppose a hacker succeeds in loosening a brick. Stealth™ has added security features – guard dogs – to watch for exactly that. They instantly surround the hacker, preventing the breach from touching another brick. They also stop the attacker from leaving the premises with the

brick loosened in the attack. This is dynamic isolation. Stealth™ isolates critical data and systems from rogue users to contain an attack in less than 10 seconds, preventing data exfiltration and giving security personnel time to investigate an attack.

Going from 13 percent to 95 percent of employees working from home in a week

Unisys moved almost all its employees to a work-at-home model in less than a week. This would not have been possible using a VPN, which by their nature, are time-intensive to deploy. ISG identified that two key factors stood out with Unisys' Stealth™. Firstly, deployment time is counted in days because a light-weight installation package is pushed onto a user's device, allowing a company to roll out an SDP overnight to thousands of users. Users automatically had a secure connection the next day and nothing else changed because the installation was automatic and transparent providing invisible protection.

Employees Working From Home



Source: Unisys, 2020

Standing out from the crowd – next-generation security

Like Tesla, having a competitive advantage is enough when providing something that others in the market are not. However, ISG sees Unisys excelling in security because of its integration of artificial intelligence and machine learning through the use of device cameras and pattern recognition, adding an extra layer of authentication that secures the corporate network.

The system will, for example, learn to identify you through facial recognition using the device camera. Some critics will suggest that this is not new technology; after all the iPhone has been using microdots since 2017 that are projected to map a user's facial profile, with the face print becoming your passcode. Unisys, however, has also embedded intelligence and pattern recognition, so the system knows that you are usually at your desk between certain hours and the kinds of data you access. It also maps and distinguishes the backgrounds that normally exist where you work. This means that exceptions are easily flagged, which with VPN, would be missed.

A VPN connection can be left open even when you have logged off. This makes penetration of the network much easier and potentially undiscovered for hours until the VPN provider drops the connection. With Stealth, you must be you at the time of access, and a number of factors must add up to prove that fact.

From the market analysis ISG undertook for the future of work core components, Unisys' Stealth™ solution was robust, simple to implement, adaptable, intelligent and provided as close to a digital R_0 as possible on any device.

CONCLUSIONS

As companies continue to assemble solutions to facilitate virtual working, there may be a tendency to embrace speed over security. ISG has seen in the marketplace that providers are providing work-from-home agreements now, which you need to read carefully for security provisions.

This is where a digital security system can be highly beneficial as companies deploy new platforms to support remote workers. A good example is the one provided by Unisys that prevents access to hackers who continually monitor high-value targets for architectural flaws and vulnerabilities.

As with all IT systems, training is vital to ensure all employees understand their roles in securing corporate data and assets when outside the formal office environment.

The nine-point technical security checklist[xxii]

Organizations should put in place the following basic security precautions for all remote workers:

1. Ensure internal and external workers have secure software-defined perimeter (SDP) access and use it for all connections and the validation of users to the corporate network.
2. Require all employees to use endpoint protections (antivirus, personal firewall, etc.). Increase the company's security level to a higher-than-normal setting and turn on logging for employees in geographies with known security issues.
3. Require employees to use company-provided and SDP protected assets whenever possible.
4. For high-risk industries, implement data loss prevention (DLP) solutions for access to a broader-than-normal data range. At a minimum, implement DLP for the most sensitive data if it's not already in place. Use virtual desktops for sensitive applications to prevent the possibility of data exfiltration.
5. Encrypt all sensitive data at rest and in transit. Many companies do the former; few do the latter. An increase in usage of insecure networks by some remote workers significantly increases the theft risk for data in motion.
6. Encrypt emails when possible. Some technologies, such as Microsoft Office 365, have built-in encryption capability. Publish guidelines on the proper configuration and use of these technologies for all employees and partners if not already covered by SDP protection.
7. Avoid public Wi-Fi. The local coffee shop network is at higher risk of being hacked or mimicked. Turn off the "auto-connect" function for all Wi-Fi connections to avoid accidental connection to a rogue hotspot.
8. Educate employees about the importance of being aware of where they are and physically protecting company assets like laptops and hotspots.
9. Instruct employees and provider employees to force the use of screen locks within a shorter-than-normal timeframe and avoid leaving a logged-in device unattended.

Provider work-from-home agreements[xxiii]

Both ISG's and Unisys' view is that solving the immediate security need with your provider in a rational and logical way is more important than making general contractual statements that may trigger enforced waiting periods and potential future litigation. A cool, rational, collaborative approach is essential right now.

The degree to which COVID-19 has impacted the ability of IT and business service providers to work inside their delivery centers has meant that some very real, near-term tactical decisions need to be made for work to continue. And it starts with service providers asking for your approval – in the form of a waiver – to all their employees to work from home, backed up with proper security protocols.

Five steps for providers to work from home

1. Allow a work-from-home waiver

Most service providers with offshore delivery centers have already asked their clients for work-from-home (WFH) waivers. If they have not asked yet, they will be asking soon. Immediately engage your providers if this point has not yet been discussed.

A waiver is a customer's voluntary renunciation of rights in the contract for some period of time. It's the customer's documented willingness to allow the service provider to relax certain specific contractual requirements that might include service level relief, work from home vs. clean room locations, security or privacy relief, scope relief or other specific and clearly articulated relief with reference to specific performance or contractual provisions. A waiver, if acceptable, must carefully define the relevant scope, time and consequences.

We understand granting this is not easy, especially for companies in regulated industries. Handling of sensitive data in "clean rooms" has been a standard for offshore providers for years – and working from home turns the clean room concept on its head. But there are ways to mitigate the risk (see point No. 2 below). It is important to keep in mind that every industry is having to learn how to relax requirements so global commerce can continue.

2. Put a plan into place that addresses data security

Ensure that your provider is thinking about security and bandwidth for their employees now working from home. Ask them if they still use virtual private network (VPN) technology standards and how they intend to monitor activity while employees are connected to and working on your business. If VPN, and not an SDP solution, is the standard, then consider contacting Unisys, which can deploy end point security within hours. Also ask about the training providers are conducting to ensure proper data and device handling, as well as training about safe online behavior to reduce the risk of phishing and social engineering attacks.

3. Do not agree to relax data breach clauses and penalties

ISG is starting to see some examples of providers asking their clients to relax data breach clauses and penalties after granting work-from-home waivers. Do not agree to these. If your provider is asking for this, accelerate point No. 2 above, and engage your internal counsel.

Remember that every contract has a change process, and any change or waiver must be made according to the agreed-upon process on an extremely expedited basis and by mutual agreement. ISG does not recommend using side letters or email to document this change. And, finally, remember that these are not contract amendments; they are temporary measures to provide relief from obligations, not permanent contract changes.

4. Do not think force majeure is required to make these changes

Force majeure is a way for a provider to get contractual relief because of a failure to perform. Making waivers or changes to specific service provisions like work-from-home does not require the invocation of force majeure by your provider. If both parties agree to change conditions, service levels or other aspects of the contract, this can be handled using the process described above.

There are many helpful articles available by legal experts to explain the details of force majeure, but

most experts stress that a contested force majeure event will be litigated and recommend the consumer of services work with its provider to try to solve the problem without resorting to legal action.

Practically speaking, this is no time to initiate a lawsuit to determine if the provider is in default of an agreement to deliver a critical business process for a client. Even if it were, the remedies are mostly irrelevant. Remedies such as termination or step-in rights (which give the client the right to have a third-party step in and take over the work) are simply not appropriate at this time and in this situation.

5. Get your business leaders involved

Right now, you need to maintain a laser focus on working collaboratively with your provider to find solutions for continuity of services, not defaults and terminations. Therefore, we strongly recommend getting your business leadership involved. A key business leader will be more empowered to negotiate and able to make decisions immediately about what scope of work can be changed and how it can be changed.

No service provider wants to fall into breach of its agreements, and it will be ready to work with you to find a solution. If there is friction between your team and theirs, a more senior leader from your side should act as the spokesperson for your enterprise. If there is a problem person on the provider's side, invoke your right to replace that person even if temporarily. If and only if these efforts fail should you consider alternatives like contractual remedies based on legal advice from your counsel. This is a time when advice from a third-party expert can help guide the two sides to a reasonable solution.

Legal protections guidance

In these times of major change, Unisys is seeing nation states becoming increasingly part of the attack surface. The problem has become so big that a lot of cyber insurers have started putting active war riders in their policies to say that if your breach happened due to an act of war, you are not covered. In other words, an attack discovered to be by a nation state is considered an act of war and can nullify coverage.

Most sourcing contracts contain legal protections written to support the risk associated with the use of dedicated equipment in an offshore delivery center. This relates directly to your network and includes robust security monitoring and reporting capabilities to aid in detection of potential data theft. However, recent examples of data theft by partner employees in heavily monitored environments indicate that even the best systems can be circumvented. In fact according to Mathew Newfield, CISO at Unisys, 34 percent of cyberattacks are perpetrated by internal actors. Some of these attacks are malicious in nature while others are completely accidental, such as an employee clicking on a link in a phishing email. This highlights the need to be protected.

As employees work from home in large numbers, the likelihood of an intentional breach increases significantly. In this type of breach, jurisdictional issues may prohibit recovery of damages due to differences in law and ability to prosecute. There is also the very real potential for destruction of evidence and corporate data if an employee's personal networks and devices are used to provide services.

While most workers will play by the rules, the time is now for enterprises to review their sourcing contracts and follow these steps:

1. Pay special attention to location provisions, data confidentiality, limitations of liability and indemnification provisions as they relate to remote workers.
2. Review cyber insurance policies to determine if exclusions exist for remote workers or provider employees who are not using systems that comply with your corporate security policy.
3. Seek out service providers that, like Unisys, provide state-of-the-art scalable security solutions and compare them to your current contractual offering

THINGS YOU CAN DO NOW

If you only do three things after reading this, do the following to ensure you are at the forefront of security and are armed to survive the next challenge.

1. Seek out and identify key market trends in security issues, behaviors and technologies to ensure you are fully protected. Make contact with ISG who can help assess your needs and provide independent market advice to get your organization fighting fit.
2. Join major cyber certification roundtable groups to understand what others are doing. One of the biggest issues CISOs and corporations find is that they only see what they are doing, not how the broader industry is fighting cyberattacks.
3. Seek professional advice on security for your organization and seek out a comprehensive review to implement a zero-trust solution. Arrange a demonstration of Unisys' zero-trust solution.

As Steve Jobs said once, "How does someone know what they want when they've never seen it?" Until you have seen this solution, you won't know the art of the possible.

ABOUT ISG

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 700 clients, including more than 75 of the world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis. Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,300 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data. For more information, visit www.isg-one.com.

ABOUT UNISYS

Unisys is a global information technology company that builds high-performance, security-centric solutions for the most demanding businesses and governments. Unisys offerings include security software and services; digital transformation and workplace services; industry applications and services; and innovative software operating environments for high-intensity enterprise computing. For more information on how Unisys builds better outcomes securely for its clients across the government, financial services and commercial markets, visit www.unisys.com.

Follow Unisys on Twitter and LinkedIn.

For more results and information on the 2020 Unisys Security Index, click here.

AUTHORS

Iain Fisher

Director, ISG

Iain Fisher (@Iain_D_Fisher) is a thought leader in the post COVID-19 future of work area where he leads ISG's European Digital Strategy and Solutions Practice. Responsible for digital agility and the future of work strategies, Fisher works with enterprise organizations and technology providers to champion the change in customer focused delivery of services and solutions in challenging situations. Fisher is also a prominent key note speaker on the subject and prominent blogger on the customer experience.

Kevin Turner

EMEA Digital Workplace Services Strategy Lead, Unisys

Kevin Turner (@kevin_dws) is Unisys' thought leader in the future of work area. Responsible for developing and communicating Unisys future workplace strategy to enterprise clients and market analysts, Turner also works with numerous global clients and partners to deliver successful transformation projects in the U.K. and Europe.

DISCLAIMER

Although the information and data used in this report has been produced and processed from sources believed to be reliable, no warranty expressed or implied is made regarding the completeness, accuracy, adequacy or use of the information. The authors and contributors of the information and data shall have no liability for errors or omissions contained herein or for interpretations thereof. Reference herein to any specific product or vendor by trade name, trademark, or otherwise does not constitute or imply its endorsement, recommendation, or favoring by the authors or contributors and shall not be used for advertising or product endorsement purposes. The opinions expressed herein are subject to change without notice.

ENDNOTES

1 https://www.ncbi.nlm.nih.gov/pubmed/11516376

2 https://cmr.asm.org/content/cmr/20/4/660.full.pdf

3 Prof Andrew Cunningham, The Zoological Society of London

i https://marketoonist.com/2020/04/digital-transformation-2.html

ii COVID-19 data from Office of National Statistics

iii COVID-19 data from Office of National Statistics

iv https://www.theguardian.com/business/2020/may/10/unemployment-due-to-covid-19-is-surely-worth-more-than-a-footnote

v https://www.statista.com/chart/21240/enforced-covid-19-lockdowns-by-people-affected-per-country/

vi https://www.icao.int/sustainability/Documents/COVID-19/ICAO_Coronavirus_Econ_Impact.pdf

vii https://www.icao.int/sustainability/Documents/COVID-19/ICAO_Coronavirus_Econ_Impact.pdf

viii https://www.statista.com/statistics/1107859/shifting-to-online-purchases-because-of-the-covid-19-pandemic-by-category/

ix https://isg-one.com/docs/default-source/default-document-library/1q20-global-isg-index.pdf?sfvrsn=ae0c731_2

x https://isg-one.com/docs/default-source/default-document-library/1q20-global-isg-index.pdf?sfvrsn=ae0c731_2

xi https://www.statista.com/statistics/1116638/uk-number-of-people-on-furlough/

xii https://globalworkplaceanalytics.com/whitepapers

xiii Forbes

xiv https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

xv http://www3.weforum.org/docs/WEF_COVID_19_Risks_Outlook_Special_Edition_Pages.pdf

xvi https://www.infosecurity-magazine.com/news/check-point-detects-30-increase-in/

xvii https://www.infosecurity-magazine.com/news/check-point-detects-30-increase-in/

xviii https://www.businessleader.co.uk/how-many-people-in-the-uk-worked-from-home-prior-to-coronavirus-outbreak/81646/

xix https://bmcmedicine.biomedcentral.com/articles/10.1186/1741-7015-7-30

xx https://wwwnc.cdc.gov/eid/article/26/7/20-0282_article

xxi Four Reasons to kill the VPN: Security, Speed, Simplicity and Savings by Jack Koons, Unisys' Chief Cybersecurity Strategist

xxii https://isg-one.com/articles/a-checklist-to-reduce-security-risk-in-the-sudden-age-of-remote-work

xxiii https://isg-one.com/resource-center/resource-center-articles/how-to-maintain-business-continuity-as-providers-shift-to-a-remote-workforce

An ISG Report, with Unisys

From Digital Native to Digital Naiveté

July 2020

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 700 clients, including more than 75 of the world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis. Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,300 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data. For more information, visit www.isg-one.com.

ISG®

www.isg-one.com