The abrupt shift to remote working has amplified cyber security problems

For most companies, traditional solutions won't work when people who need access to data are working from home, write Thomas Koehler, Paolo Cervini and Jonas Vetter

The COVID pandemic has forced most companies into distributed and virtual settings. Companies had to swiftly adapt their organisations to social distancing and elevated economic uncertainty. This adaption manifested itself in the form of fast deployment of digital tools to allow for remote collaboration and distributed work, and more agile and self-managed work processes.

Video conferencing tools, like Zoom, Skype, and WebEx, as well as collaboration tools like Confluence, Slack and GitHub have largely replaced physical meetings and work – at least for now. In addition, decentralisation led – in general – to higher acceptance of cloud solutions as well as distributed storage and computing of documents. On top of changing internal organisation and processes, companies are increasingly exploring how to move parts of their business online and rely less on brick-and-mortar outlets, leading to a massive increase of digital information exchange.

Many tech-savvy and agile companies were able to make the switch in almost no time. Other traditional incumbents are taking more time to establish work capabilities for their workforce. Yet, regardless of transition speed, digital natives as well as low-tech incumbents are in the process of making a massive leap into the digital age. This high speed of the transition, however, is amplifying a dilemma companies were struggling with for decades: The lack of information security.

Cyber security – a known problem

Cyber security, i.e., the protection of digitally stored IP, trade secrets and customer data, had been a weak spot for many companies. Consider the demise of Canadian Nortel Networks caused by cyber-attacks with the goal of trade secret theft. At Nortel Networks, several passwords of senior executives were stolen and used for an extended period of time to obtain access to trade secrets.

While the causes of this theft remained obscure, there are common attack techniques that tend to work time and time again. Victims are commonly tricked into typing in their credentials into a forged website. Oftentimes, this is triggered through an email that links the user to the site. Another way victims are regularly lifted off their passwords is if they use them with different services with one of them getting

hacked. Institutions like the "Hasso Plattner Institute" offer services to check whether credentials have been leaked in recent breaches.

A third common way to get hold of other people's passwords is to simply try them out. This tactic proves effective especially with unlimited-trial portals. A so-called "brute force attack" will uncover most access codes typically within hours, unless additional security measures such as "two factor authentication", "captchas" or extended retry intervals have been implemented.

While most of the exact chains of events of successful hacks are almost impossible to reconstruct, the subsequent rise of Asian competitors in the sectors once dominated by Nortel and other Western companies, like Ericsson and Nokia (formerly NokiaSiemensNetworks), was widely attributed to a large numbers of similar attacks. Many of these have also targeted US-based companies like CISCO Systems.

Nowadays more than ever, corporate espionage and hacking and stealing of IP has become a business discipline – with the threat not only coming from Asia. Desperation of many businesses due to dire economic outlooks, isolationism of nations and the new security gaps have amplified the willingness to obtain competitor information.

Take car manufacturers. These companies typically go through great lengths to get hold of their competitors' newly released models to test and often dismantle them to get more information on the parts used and build process. This is mostly seen as legal. Daimler, for example, used a cover entity to rent and test Deutsche Post DHL's own electric van Streetscooter. Deutsch Post discovered what Daimler was doing through the van's location data as it had made numerous laps around Daimler's test track. The company later accused Daimler of industrial espionage. Daimler argued, however, that it was just "Mystery shopping".

The impact of the pandemic

The sudden shift to remote work has massively amplified the problem of protecting proprietary information. As companies had to implement remote access technologies fast (or upgrade existing infrastructures) to ensure business continuity, they often fell back on improvisation. This led to the frequent neglect of even the most basic security and compliance protocols.

The teenage daughter of a CEO (…) used her father's corporate laptop to surf the web. There, she stumbled over an advertisement for a free IQ test…

For instance, many companies with a lack of company laptops practiced "bring your own device" to keep up and/or used remote access software to telecontrol equipment left at the office. Other R&D-heavy companies with hardware products allowed engineers and researchers to move their entire workstations home as well as the components they needed for testing.

We see that regardless of the need for physical on-site presence or storage and regardless of the level of sophistication of a company's adoption of digital tools, in the age of inter-connectedness it is much easier to gain unwarranted access to trade secrets of competitors. At the same time, the attackers have upped their game. Just recently, US law enforcement discovered a sophisticated attack by a notorious Russian hacker group with state ties, targeting employees working from home of dozens of Fortune 500 companies. Malware was deployed on common websites. The actual attack, however, occurred only when PCs seemed to be part of major corporate or government networks, leaving only privately used PCs unscathed.

We identified three main reasons.

Distributed creation and storage of information is a door half open

Hastily implemented remote access solutions pose a great risk. Faulty configurations are highly likely when rolling out remote infrastructure under time pressure. Infringements and attacks are foreseen to rise significantly. It is usually only a question of *when* these infrastructures get attacked.

Most employees are not accustomed to working from home and are overwhelmed by distractions, forgetting to secure devices against unauthorised use.

An unsecured new device typically gets attacked within minutes. Large scale undirected automatic attacks target every PC, laptop or phone that is not secured and thoroughly patched.

But even if software and equipment are state of the art, there are risks that come with the need to speed up the rollout. Hastily installed systems tend to be prone to configuration errors. This can be considered the technical equivalent of securing the main entrance but leaving the cellar door open. One has always to remember that while the defender must get everything right, an attacker must find just one security hole to have success with his/her endeavour.

Our always-interconnected world is a low risk environment for gaining information about competitors' plans. We have seen reputable western companies crossing the line, outrightly spying on competitors, especially in economically challenging times. While in the past trade secrets of other companies were difficult or dangerous to obtain – it is now almost as easy as sneaking through a half-closed door.

Remote employees are easy targets

Besides technical breaches, major risk lies within human nature itself. Most employees are not accustomed to working from home and are overwhelmed by distractions, forgetting to secure devices against unauthorised use. Further, they simply do not know whom to contact if something unusual happens. In consequence, they are at a higher risk of becoming victims of cyber-attacks, whether it is a typical malicious email that comes with a malware load or a simple data loss by family members using the equipment just for a quick lookup on the internet.

While there are no detailed studies available on how large the problem really is, anecdotal evidence gained when speaking with CIOs of companies that make heavy use of remote work speak volumes. A recent example from Munich, Germany depicts the potential risks: The teenage daughter of a CEO of a leading real estate firm used her father's corporate laptop to surf the web. There, she stumbled over an advertisement for a free IQ test. Curious, she downloaded the software and tested herself. The software, however, had a secret payload. It brought in a hidden program, a trojan horse, that drained the PC of work-related documents and tried to use the remote connection to the corporate network to infect other PCs in it. Fortunately, the damage could be discovered and limited to the single laptop (which needed a replacement) as the CEO had a direct line to the forensics team.

But it is not only family members who fall victim to these attacks. Most of the time it is the employee who is overwhelmed and confused when confronted with an unexpected situation – e.g. when an email with an ominous attachment shows up in the mailbox.

Distributed setups complicate security breach discovery and counterattacks

The remote setup makes the discovery of cyber-attacks significantly more difficult. Before the crisis, security was mostly perimeter-based with firewalls separating the outside from the inside to keep bad actors. In the age of cloud services, remote work and collaboration, there is no single line of defence, since there no longer is a common understanding "what is inside and outside".

From a security management view, the whole infrastructure gets extremely complicated. Simple negligence or a single misconfigured device can be sufficient for an attacker to breach a system and often subsequently large parts of the corporate infrastructure. Consider, for example, the devastating cyber-attack that stopped operations of container shipping company Maersk for several days in 2017 and led to damages of more than US$ 200 million. The attack had originated from a subsidiary of the

company in the Ukraine, where an update of a locally used accounting software contained a malware component. Within a matter of minutes, the global network of Maersk had been brought down, rendering several thousand servers as well as PCS useless.

How can you protect yourself?

When confronted with rising complexity, a secure distributed company requires the rigid application and implementation of a few simple rules. Researching the cases of security and compliance breaches and working with our clients we identified three stages for creating a secure system for trade secrets and IP while converging into a digital organisation:

1. Investigate and document the "real secrets" and focus on protecting this information

Over recent years, we experienced the demise of the perimeter-oriented security model in which sensitive information was physically shielded off. With the ongoing trend to cloud services, inter-company-collaboration and now remote working, this traditional understanding of security is no longer practicable.

… physically storing (essential information) in ('air-gapped systems') without a network connection. All other information can be secured with (…) anti-virus applications…

To account for these shifts, we propose to set the focus on identifying and protecting only what is *essential* for your competitive positioning, separate it from the other information flows in your organisation and protect it by every possible means.

The nature of this type of information is different for every business. It may be source code for the newest product, but also simple trade secrets like calculation schemes or customer records. The question to ask is whether it would cause harm when received by competitors.

In our experience and research, we found that typically only 3-5% of corporate data is actually *essential*. For this limited amount of information, every security measure possible and reasonable should be taken. This can go as far as physically storing them on systems without any network connection ("air gapped systems"). All other information can be secured with industry standard measures, e.g. anti-virus applications, under the premises of enabling efficient work. In any case, managers should familiarise themselves with the notion that information *will* be hacked, stolen, and copied someday and put in place contingency plans.

2. Give access to information on a "need-to-know" basis

Once information has been categorised as "real secrets", it is time to ensure its absolute integrity. While all other information should be treated as common goods within the corporation (given that no compliance needs, such as GDPR requirements, stand against it) limited-access information should only be given out if verifiably required. The public sector and the military work that way already, and present a blueprint for what needs to be established in the corporate world.

As this approach stands opposed to the idea of openness in the corporate world, its implementation is a daunting task. It may at first be unpopular and put off. We therefore recommend implementing a software solution that automatically tracks all file access within the organisation for a period of at least one month to get an understanding of what is really going on within the organisation and contrast the results with what was identified as essential information. Based on the results, strict access rules should be defined and implement.

Of course, these changes need to be communicated, especially in organisations starting from a background of openness. Make sure to communicate the reason for these measures.

3. Establish state-of-the-art models to track information usage and actively deny suspicious access

While separating highly valuable information seems complicated at first, there is no way to avoid implementing solutions that do just that.

For most companies, “air gapping”, as the simplest and most secure solution, won’t work, especially if people who need data access are working from home. We therefore recommend implementing strict access rights and track every access while archiving any state of the system.

While more practicable than air gapping, these systems typically create a lot of work to establish access allowances and maintain those rights. Several software solution providers are working on concepts that automate these processes, sometimes incorporating AI and machine learning. Software like Varonis, SolarWinds ARM, NetWrix, STEALTHbits, LepideAuditor, and ADAudit Plus can analyse how users work with data. They can determine the role of the user, and fix permissions in a way that is helpful to keep corporate trade secrets and IP where they belong. Solutions like these could be – if implemented right – the missing link for building the bridge between high security and high availability.

In sum, the abrupt shift to remote work has not created the issue of a lack of cyber security but has significantly amplified it. Yet, as with digitalisation in general, the acute need should be used to make a leap to protect businesses in the information age. The way that CEOs and CIOs act now will determine if the current crisis will lead to a drainage of IP and thus a massive loss in competitiveness, or instead to the creation of strong and resilient knowledge organisations.

Notes:

- *This blog post expresses the views of its author(s), not the position of LSE Business Review or the London School of Economics.*
- *Featured image by Philipp Katzenberger on Unsplash*
- *When you leave a comment, you’re agreeing to our Comment Policy*

Thomas Koehler is CEO of CE21, a technology and cybersecurity consulting company located in Munich and Cologne. He is the author of a dozen books about cyber security, and a research professor at the Centre of International Innovation, Hankou University, China.

Paolo Cervini is associate partner at ECSI Consulting and based in Milan.

Jonas Vetter is manager at ECSI Consulting and based in Milan.

August 12th, 2020 | Information & Technology | 0 Comments