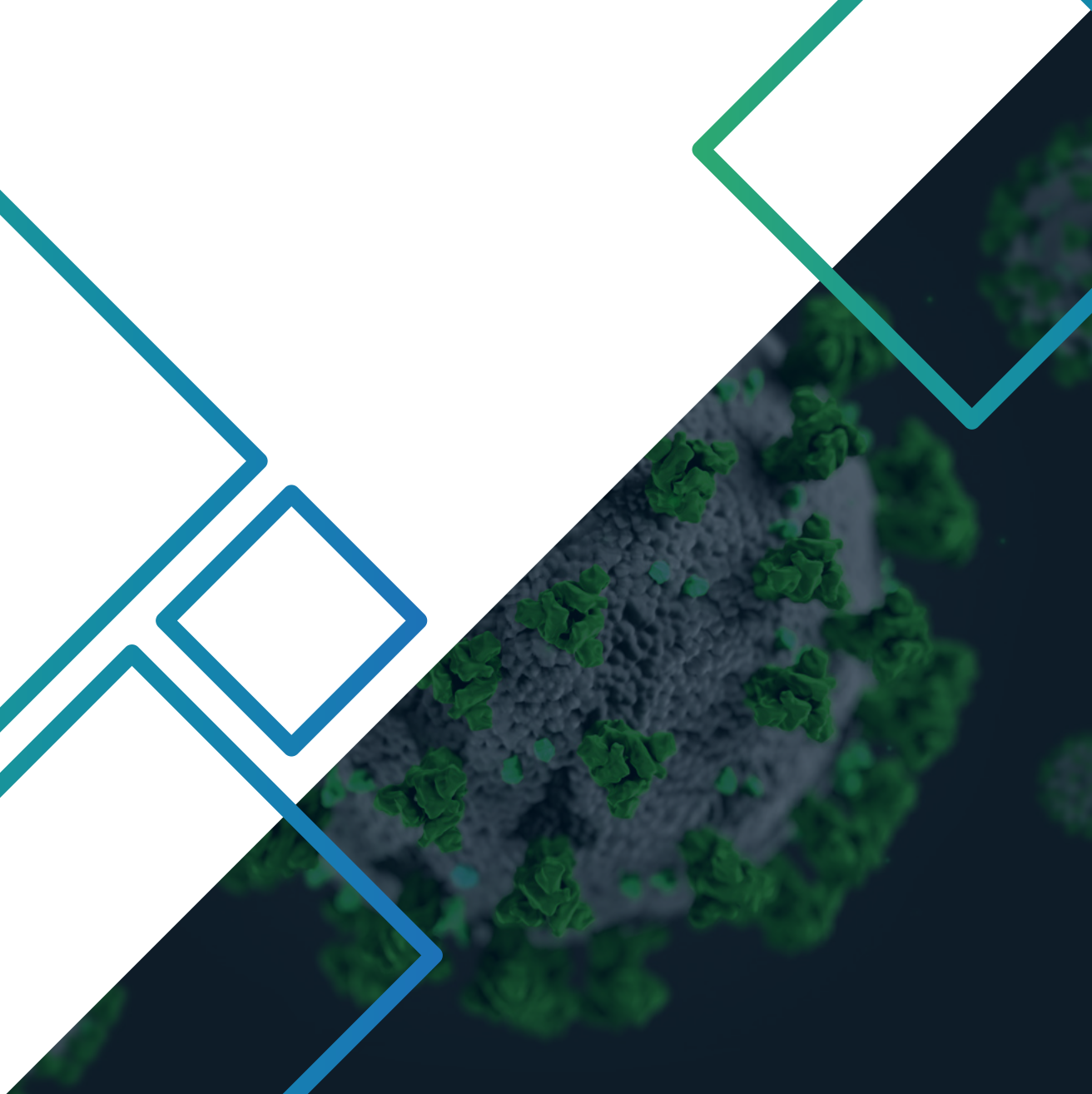
Pandemic Under the Microscope

A Focus on the Cyber Risk Impacts of Working from Home

CyberCube

www.cybcube.com



Society is under attack from multiple invisible threats, some which are biological, and others, digital in nature. The novel coronavirus (COVID-19) is the biological disease, which is spreading rapidly across the globe, fuelled by human movement and social interaction. The pandemic proportions of this virus also allows for exploitation by human actors in the online domain, with no regard to geographical boundaries or physical contact.

In this paper, Aon and CyberCube will explore some of the changes to our digital landscape that have been encouraged by the COVID-19 pandemic and subsequent social distancing measures.

We acknowledge the breadth of possible long-term economic effects of the pandemic, including supply chain reconfigurations, recession-related impacts and government policy adjustments. However, for this research, we will focus mainly on the pronounced shift of the employed to working from home during and post COVID-19.

We will outline some of the security implications of these changes and the new exposures they present to risk managers and the insurance sector.

Finally, we will touch on the work in progress in the cyber risk modeling community to address these "new normal" risk conditions in their analyses.

Looking at data from the period February-June 2020, the pandemic did not present notable new classes of cyber attacks, create major system outages nor data breaches. It did, however, expose new access points for cyber criminals to gain access to systems, exploit distracted individuals and potentially wreak havoc through new critical infrastructures.

But how do you identify, quantify, mitigate or transfer these new risks in a period of such fast-paced change and uncertainty? The insurance markets need to be mindful of these changes and the businesses that they serve must adjust to risk management approaches in-line with the new norms that exist and will continue to evolve for years to come.

What just happened?

The current pandemic has forced many governments to enact various forms of social distancing and self-isolation within their homes. Those who can work from home, are doing so in unprecedented numbers.

These workers are indicating a preference to work from home more in the future. Early signals show that this is supported by employers, who recognize the greater productivity from employees who are working from home, applying flexible hours.

This trend will create new norms that offer opportunities to businesses as well as weaknesses that can be exploited by cyber attackers on a vast scale. Employees will adapt new applications to make working from home more efficient. Many of these will fall outside of normal corporate governance standards and testing and, as a result, they will fall short from a security and risk perspective.

We should expect the sophistication of social engineering lures, attacks on emerging cloud applications and infrastructures, and home networks to increase in-line with new working practices.

In addition, from a business strategy point of view, consumers are not physically visiting stores in such large numbers as previously. Retailers are therefore moving from a physical presence to an increasingly online model.

Feeling vulnerable

Other risk factors associated with the current "lock-down" phenomenon include the general security hygiene and best practice maturity levels that tends to be evident in the home (as opposed to in the office). Of particular significance here are the use of poor passwords on devices including wi-fi routers and the practice of "device-hopping" (where a business user migrates from their corporate device onto a family member's device in order to get their work done – perhaps after a device failure).

There will be increased vulnerability to both opportunistic cyber attacks - such as social engineering that exploits distracted home-workers - and attacks of a systemic nature with concentrated reliance on cloud-based applications and the infrastructures that host them.

In addition, let's not forget that existing cyber risk threats have not disappeared during the pandemic. Ransomware has been the biggest emerging trend in recent months. Aon notes that insurers are still grappling with the rapid rise in ransomware claims over the last 18 months and that working from home may exacerbate this response, by delaying the timeliness of incident response, especially in the wake of a ransomware infection.

As mentioned above, an accelerated shift to online retail has various implications for cyber risk. Well-established cyber criminal behaviour such as form-jacking (the scraping of credit card information from web-forms), spoofing (taking consumers to a malicious site that looks identical to the retailer) and phishing for financial credentials should be expected to grow both in severity, frequency and complexity as we move through and out of the Coronavirus pandemic.

Social engineering

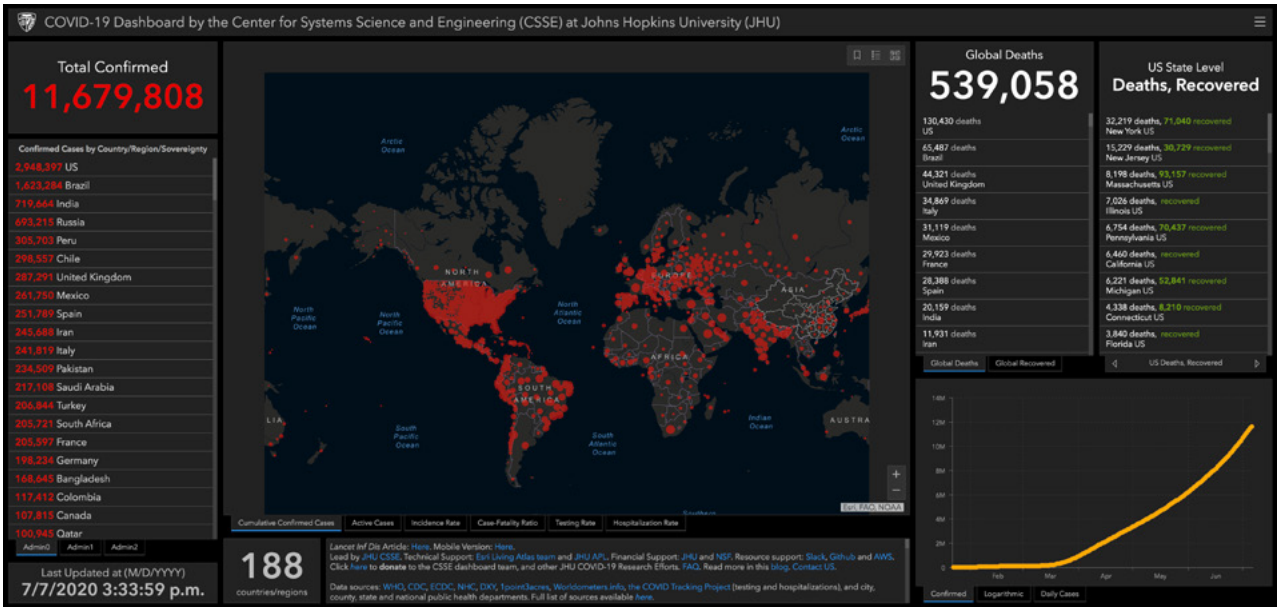
COVID-19 has been used as a social engineering "lure" since the outbreak started and has been inadvertently aided by tools developed to help map the pandemic's spread across the globe.

The **COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE)** at Johns Hopkins University (JHU) is one of the interactive maps being used by criminals to track where COVID-19 has had a significant impact. At the time when this report was published, the US, Brazil, India and Russia had been among the countries with the highest confirmed cases. There are clear correlations between cyber attack volume and this data.

In a work-from-home environment, social engineering attacks exploit the decreased differentiation between "work" and "play" for workers, which can lead to lower levels of attention given to keeping systems and data secure.

Furthermore, too many hours worked with too few breaks will lead to fatigue which, in turn, can result in mistakes being made. Hackers have been known to attack at times where targets are at their most vulnerable and this expertise is likely to be applied in innovative ways when attacking a remote workforce.

Maliciously-crafted documents, activated by clicking on email attachments, or even hacks into email accounts themselves, are relatively easy to perpetrate. For example, an employee complained to her payroll department that her banking information had been changed. Payroll investigated and found an email record from the employee requesting the change. Upon further investigation, the company discovered unauthorized logins to the employee's Office 365 account from an external IP address. A malicious actor had likely obtained her Office 365 credentials and was able to use her email account to request a change in banking information.



Cloud computing

As individuals have moved to work from home, they are increasing their usage of cloud resources and exploring the possibilities that cloud computing brings.

For example, Microsoft says that it has seen a 775% rise in Microsoft Teams usage since the COVID-19 pandemic became prominent in February, 2020[1].

For more detail on how the cloud is defined and how vulnerabilities might occur, see box-out Focus on the cloud.

Many users of cloud technology have been restricted by their employers in the applications and platforms they can access. Outside of the confines of corporate governance, the (cloud) world is their oyster. CyberCube has already noted that remote workers have been making use of a broader range of cloud applications since the pandemic began.

> **hastily deployed and misconfigured virtual networking tools pose the greatest threat to firms**
>
> **Aon**

Importantly, they have been doing this largely without oversight or governance from their employers. In many cases, the new applications will not meet an employer's security or reliability benchmarks. Aon's view is that hastily deployed and misconfigured virtual networking tools pose the greatest threat to firms in the COVID-19 work-from-home era.

A recent example is the "Zoom" meeting tool, which had to work quickly to patch vulnerabilities in its platform.

CyberCube has noted that popular cloud applications have been stress-tested through the COVID-19 lock-down. This will probably be beneficial in the longer-term and result in more robust applications. In the short-term, however, users of applications that have not had time to mature will be targeted.

[1] *www.azure.microsoft.com/en-us/blog/update-2-on-microsoft-cloud-services-continuity/*

Focus on the cloud

Underlying all of this cloud usage is "the cloud" itself. Of course, there is no "cloud" as such but, rather, an intricate and complex set of infrastructure and software assets that make up a cloud ecosystem. There is still study and modeling required to be done, to fully understand the workings, dependencies and potential points of failure that are now an inherent part of the cloud ecosystem that we are all becoming more reliant on.

Modeling disruption to "Infrastructure as a Service" (IaaS) is not enough - we have to consider the comprehensive cloud ecosystem when attempting to evaluate cloud risk and plan our usage of cloud assets in a business content. According to a 2020 Flexera study[2], virtually all (93%) of enterprises already use at least one cloud service.

As we model potential cloud outages in order to better understand the potential impacts of increased remote working, it is vital that we assess the dependencies that exist across IaaS, Platform as a Service (PaaS) and Software as a Service (SaaS) cloud elements in order that we fully understand what cascading effects could exist to create risk accumulations.

Definitions

Infrastructure as a Service (IaaS) is the practice of delivering a full compute stack — including servers, storage, networking and operating software — as an abstract, virtualized construct.

Source: www.techopedia.com/definition/141/infrastructure-as-a-service-iaas

Platform as a service (PaaS) is a category of cloud computing services that provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an application.

Source: www.en.wikipedia.org/wiki/Platform_as_a_service

Software as a service (SaaS) is a model for the distribution of software where customers access software over the Internet. In SaaS, a service provider hosts the application at its data center and a customer accesses it via a standard web browser.

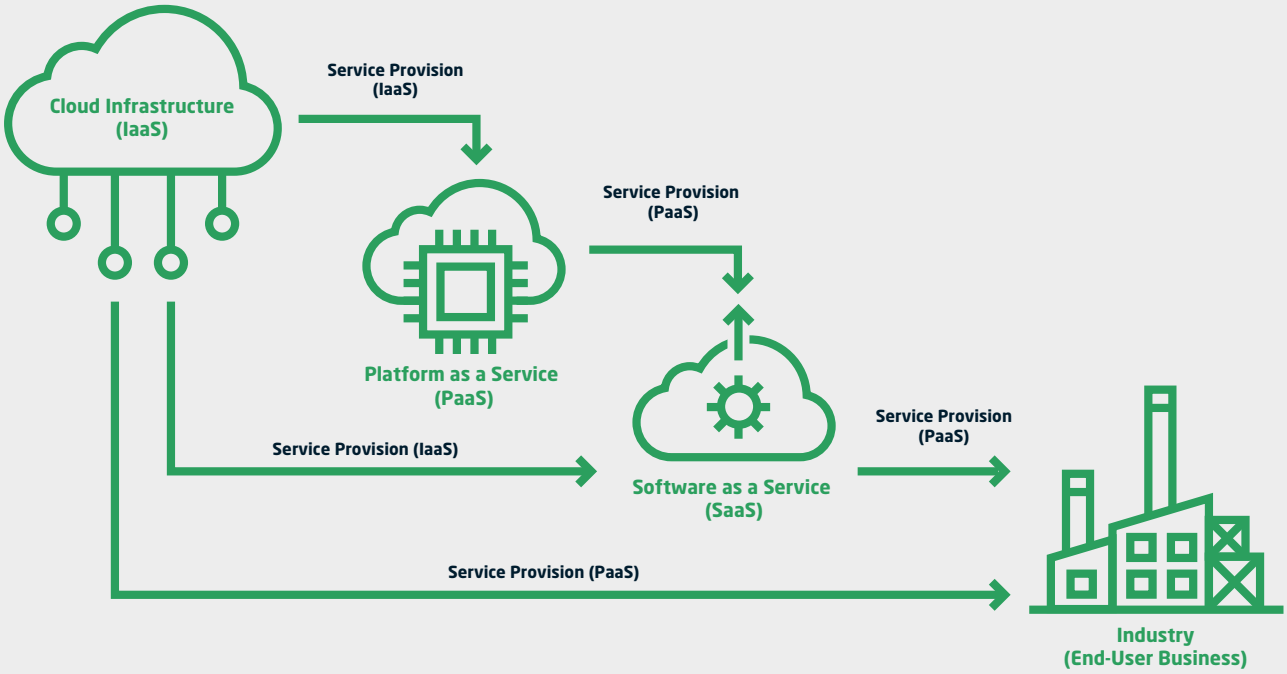
Source: www.techopedia.com/definition/155/software-as-a-service-saas

[2] *www.flexera.com/blog/industry-trends/trend-of-cloud-computing-2020/*

The failure, for example, of a major IaaS provider such as Google or Amazon would not only affect the end-user businesses that host their own application on that provider's infrastructure but, in addition, any cloud platforms and applications that the IaaS provider supports. Many of the cloud platforms and applications that support important business functions such as Human Resources, Customer Relationship Management and Finance have now become an important part of business operations for many companies

The loss of one or several of these cloud services could prove to be disastrous to a business should a prolonged outage be experienced.

Cascading Cloud Failure



The Google infrastructure failure in July, 2019 is a quintessential example of a cascading cloud failure in the wild. A combination of human-error and software failure led to the loss and poor performance across multiple US regions for a period of up to 4 hours and 25 minutes.

This infrastructure failure, in turn, had a cascading effect on end-user business and other cloud services (including some of Google's such as its "G Suite" services and Google Cloud Storage instances). Importantly, this failure was not caused by a malicious attacker of any kind. In our view, the deliberate attempt to bring a major cloud provider to its knees could result in much longer downtime and, in turn, larger impacts.

Security response

As it seems that home working is here to stay and likely to grow, companies will have to face new security and risk challenges and develop a new way of thinking in terms of keeping these users and their data secure.

> **In short, "cyber security at home" cannot be handled the same way as "cyber security at the office".**

Aon cyber security risk experts suggest that organizations will need to refocus cybersecurity controls to be more user-centric, with a focus on new remote access vectors, endpoints (e.g. laptops, bring-your-own devices), and any remote applications or cloud-technology platforms that users are now utilizing on a day-to-day basis. This will require a shift from some of the traditional architectures and approaches to control, to a model where users are permitted to operate in a decentralized and remote fashion, while still applying reasonable security controls where possible.

For organizations that have had to implement and enable large remote workforces, they must navigate the change management issues that are introduced from a cybersecurity and risk standpoint. For example, many employees and staff may find themselves working remotely for the first time in their careers. Many will face a lot of fear, uncertainty, and doubt regarding how they can continue to function remotely, while still meeting the security requirements and expectations of their employers. Organizations should invest in training and communicating with users regarding the revised requirements, policies, and expectations that the organization has in place in the new remote environment.

Any organization that rapidly deployed new technology, applications, services, or systems at the onset of the pandemic should now be focused on taking a look back and ensuring that they have implemented best practices in security configuration and architecture. Many organizations are discovering that their rapid deployments, while necessary, may have introduced undesirable security vulnerabilities in the environment, which should be remediated before they are exploited by malicious actors, or which may permit unintentional information sharing or leakage by users.

> **rapid deployments, while necessary, may have introduced undesirable security vulnerabilities**

Here are a few practical starting points:

- Businesses need to mandate and support strong passwords on home routers and end points
- Wherever possible, multi-factor authentication (MFA) solutions should be mandated and enforced
- Device operating systems will need to be carefully monitored and controlled from the standpoint of both patch management, vulnerability assessment, network configuration (open port hygiene) and threat detection/mitigation
- Thought should also go into how post-breach analysis, incident response and digital forensics will be carried out when staff are remote from IT support and security teams
- Staff security training will need to be adjusted and expanded to consider topics such as extended cloud application usage, Virtual-Private Network (VPN) technology, the dangers inherent within Internet of Things (IoT) devices as well as some of the topics mentioned earlier, which includes "device hopping".

Businesses that are too small to support these teams should think seriously about selecting partners to take on these responsibilities. Again, adoption of these best practices should not be seen as a one-time investment but, rather, part of a continuous improvement security programme that constantly measures risk and reacts to improve risk posture.

However, according to a recent survey by the Cyber Readiness Institute[3], 40% of small businesses in the US feel that post-pandemic economic uncertainty will prevent them from making necessary cyber security investments.

Finally, some more fundamental shifts in corporate cyber security might include the wider adoption of zero-trust security models (essentially, a system of denying all access to networked resources until users have proven their credentials). CyberCube has spoken about this method in more detail in a blog by Emmaunuel Thioux in April 2020[4].

[3] *www.helpnetsecurity.com/2020/04/13/small-businesses-remote-working/*

[4] *www.insights.cybcube.com/technology-series-zero-trust-defined-in-a-few-words*

Insurance market dynamics: Aon

The uncertainty presented by the COVID-19 pandemic, and the potential for increased cyber claims because of vulnerabilities introduced by a rapid pivot to a fully-remote workforce, has propelled insurers to take stock of capacity deployment, attachment point and rates.

However, Aon notes this was only accretive to the market changes already being experienced through Q1 2020, given Errors and Omissions (E&O) losses and the increased frequency and severity of ransomware attacks. Aon continues to see the cyber insurance market transition to "hard market" conditions, with premium increases becoming the norm, noting that the pandemic has accelerated this transition.

Insurers are still grappling with the rapid rise in ransomware claims over the last 18 months. Aon believes that ransomware proliferation will continue to drive cyber claims trends for the foreseeable future.

Risk modeling response

As the pandemic situation continues to play-out over the coming months, it is imperative that cyber risk analysts and catastrophe modelers are acutely tuned into the changing threat landscape to model and analyze the risks of yesterday, today and tomorrow.

Aon notes, however, that cyber models must strike a balance between stability and responsiveness of results, and generally will not "see trends coming" without looking at leading indicators. In this situation, it's important to look carefully at current threat intelligence, combined with the expert judgment that actuaries and catastrophe modelers can provide, to adapt existing model results appropriately.

CyberCube is dedicated to creating financial models to quantify cyber risk. For cyber insurance accumulation modeling, model stability is critical. While cyber risk is dynamic in nature, catastrophe and accumulation modeling for insurance, by contrast, tends to be more static.

Therefore, we are actively monitoring leading signal and benchmarking data during the pandemic that can later be used to quantify exposures for a given company or subset of companies (microsegments) and learning how these various micro segments are performing in this new environment.

CyberCube's Portfolio Manager catastrophe model has a number of existing scenarios in our 29 scenario classes, that reflect the types of accumulation risk that the pandemic is intensifying such as a major cloud outage, or the failure of a major Internet Service Provider.

As we are contemplating future model versions, we may calibrate the model to reflect the new environment; increased reliance on cloud technology, less secure at-home networks and infrastructure, and increased exposure to malware and phishing, for example.

Conclusion

The global COVID-19 pandemic of 2020 created new tactical opportunities for cyber criminals. They took advantage of a need for information from the most vulnerable in our society in order to stage socially-engineered attacks, steal digital credentials and profit financially.

Looking at data from the period February-June 2020, the pandemic did not present notable new classes of cyber attacks, create major system outages nor data breaches. It did, however, expose new access points for cyber criminals to gain access to systems, exploit distracted individuals and potentially wreak havoc through new critical infrastructures.

But how do you identify, quantify, mitigate or transfer these new risks in a period of such fast-paced change and uncertainty? The insurance markets need to be mindful of these changes and the businesses that they serve must adjust to risk management approaches in-line with the new norms that exist and will continue to evolve for years to come.

Maybe, however, what is of greater significance are the lasting changes to the way in which people are likely to live subsequent to the pandemic. The changing dynamics that now exist in the areas of home-working, online retail and use of cloud computing (to name just three) have changed for the longer term in our view and this, in turn is creating a new landscape of cyber risk.

The insurance markets need to be mindful of these changes and the businesses and individuals that they serve must adjust to risk management approaches in-line with the new norms that exist and will continue to evolve for years to come.

Darren Thomson has been following the pandemic's cyber effects in a series of blogs in the past few months

These are:

- Coronavirus & IT Risk - Is the Pandemic Creating New IT Norms?
- Coronavirus & IT risk - Is the Pandemic Creating New IT Norms? (Part 2 – Business Change)
- The Coronavirus & IT Risk - Our Reliance on the Cloud
- What Do Pandemics Do to IT Risk - Impacts of Home Working
- Coronavirus Highlights the Need to Stand up to Social Engineering in Cyber Attacks

They can be found on cybcube.com

Authors

Darren Thomson, Head of Cyber Security Strategy, CyberCube

Jon Laux, Head of Cyber Analytics, Reinsurance Solutions, Aon

Rebecca Bole, Head of Industry Engagement, CyberCube

Editorial Management

Yvette Essen, Head of Content and Communications, CyberCube

United States

CyberCube Analytics
58 Maiden Lane
3rd Floor
San Francisco CA94108
Email: info@cybcube.com

United Kingdom

CyberCube Analytics
51 Eastcheap
1st floor
London EC3M 1JP

Estonia

CyberCube Analytics
Metro Plaza
Viru Väljak 2
3rd floor
10111 Tallinn

www.cybcube.com