CORONAVIRUS: INCREASED THREAT OF CYBER ATTACKS

As Coronavirus forces so many employees to work from home, using a range of different devices, organisations face an increased risk of experiencing a cyber attack.

Key issues

- Communications fraud
- Importance of adapting operational resilience measures in light of coronavirus
- Prevention of phishing, ransomware and other cyber attacks
- Data compromise
- Clifford Chance Cyber Assist

A serious attack could mean significant reputational and financial damage, negative media coverage and diminished customer trust. Cyber attacks can also result in lengthy investigations by numerous authorities which are challenging, expensive, and can require significant management resource.

1. Reporting of cyber incidents is increasing significantly and regulators are using new and invasive audit and dawn raid powers.
2. Actions have been taken by regulators across the globe, including levying sizeable fines.
3. Data-related litigation, including class actions, is now a reality in some jurisdictions.

Where employees are working at home because of coronavirus, exposure to risks of typosquatting and cyber-squatting, phishing attacks or ransomware, amongst others, has increased dramatically, and therefore it is essential to ensure the adoption of measures and processes to prevent these attacks, and to rapidly and effectively respond in the event such an attack occurs.

COMMUNICATIONS FRAUD

In the past few days we have seen an increase in the registration of domain names which are minor variants of genuine domain names used by organisations, as well as registrations of organisation names in new top-level domains for which they do not have a registration.

As an example of these techniques, we find the following:

- misspellings (exampal.com);
- different phrasing (examples.com);
- use of other domain variations (example.net); and
- fake websites, which appear similar to the authentic website in terms of layout, design and content.

Typically, these are set up with mail capability. There may be no website hosted content, or sometimes website content is cloned from a genuine site. This is a strong indicator that someone is attempting fraud – whether targeted on the organisation itself or its clients and customers. Emails sent from this

address may include copied email signatures from people at the organisation which is being targeted.

It is not possible to cover all possible variants of your organisation's name, but we recommend:

- ensuring you have someone inside or outside your organisation monitoring new domain name registrations and taking enforcement measures to prevent further use of fraudulent domain names (various companies provide this service, and there are various tools to do this);
- communicating the risk to staff and having a central contact to whom any attempted frauds are reported;
- ensuring your payments teams are aware of the enhanced risks and alerted to possible fraud attempts;
- if you do not have a trademark registration for your organisation's name, registering it (in at least one jurisdiction in which you operate, ideally via fast track) will facilitate take-down measures; and
- regularly reviewing the adequacy of your domain name portfolio, particularly in light of new top-level domains.

We are also seeing examples of attempted fraud using, e.g., Gmail addresses (made up as, for example, johndoe@gmail.com). These are normally easier to spot, but any communication to employees should mention this.

Finally, there is a long-standing problem with people monitoring trademark registers and contacting owners using invented letterheads with names and logos that look and sound official, in the form of an invoice for registration or renewal fees. This type of activity may also increase in the current environment. As a general recommendation, it is advisable not to pay any "trademark registry" invoice without checking that it is genuine.

IMPORTANCE OF ADAPTING OPERATIONAL RESILIENCE MEASURES IN LIGHT OF CORONAVIRUS

In response to the heightened prevalence of internal and external disruptions suffered by organisations in the market, businesses have implemented increasingly robust measures to ensure that they remain operationally resilient in a disruption event, including a cyber attack.

Given the wide-ranging impact of coronavirus, organisations are now revisiting these measures in order to ensure that they remain fit for purpose. In particular, they have focused on how to offer continuity of business services in circumstances where there is a reduced staff, large-scale home working and a disrupted customer base.

While financial institutions may be subject to specific regulations in this regard, we would expect the following best practice recommendations to apply more broadly with respect to cyber attacks:

1. Key staffing dependencies

Organisations should review their existing cyber attack continuity plans to identify specific individuals or groups of individuals integral to their response in the event of a cyber attack (such as key decision-makers, call centre personnel who would typically be manning an incident response line, or IT

workers who need access to particular equipment). Organisations should consider:

- how these individuals and groups could be affected by coronavirus;
- how they can ensure that key groups such as incident response teams can remain appropriately resourced at all times; and
- whether incident plans should be amended to cater for the increased likelihood of absences, including the identification of suitable deputies for key decision-makers and alternative teams which may be called upon for additional support.

2. Testing

Organisations should test the continuing viability of their cyber incident recovery and resolution plans in circumstances where a significant number of contingency steps, such as managing internal escalations or implementing workarounds, may be impacted by staff working from home.

This should include ensuring that relevant measures can be fully implemented remotely and that relevant employees have the correct infrastructure and access to the correct systems at home to be able to respond properly in the event of a cyber attack.

3. Communication plans

Increasingly, communications, in particular with customers and clients, are held to be as important a metric of the performance of an organisation during a disruption event as the losses suffered by third parties as a result of the organisation's disrupted services.

In the context of a cyber attack, and given the impact of coronavirus, organisations should therefore ensure that their response plans:

- incorporate a comprehensive communications strategy to ensure that relevant parties, including not only customers and clients but also other groups such as regulators, market counterparties and the firm's own staff, are kept properly updated in what may be a rapidly changing environment given the complications raised by coronavirus;
- encompass a wide range of communication channels: for example, telephone channels may become unworkable if key employees fall ill or open-plan communication centres are mandatorily closed, and online channels may be disrupted if third-party service providers are themselves affected by coronavirus; and
- notwithstanding the ongoing disruptions caused by coronavirus, include provisions to actively follow up with customers and clients impacted by the cyber-attack after the disruption has ended to assess whether any harm has been caused, rather than waiting for these groups to raise grievances themselves.

PREVENTION OF PHISHING, RANSOMWARE AND OTHER CYBER ATTACKS

Several measures can be adopted in order to prevent phishing attacks, as well as other kinds of cyber attacks such as CEO fraud, or even ransomware, in this coronavirus home working environment, where cyber criminals can take

advantage of the disruption to usual work and absence of a physical presence in the office.

What follows is a summary of the most relevant of these, explaining their legal effects, both for the employee and for the company:

1. **Reboot your computer daily** and ensure that the operating systems and applications are kept updated.
2. Take care when **downloading attachments** that exhibit any unexpected signs or patterns. It is important to always verify the file extension and not just rely on the associated icon appearing in the email.
3. When accessing **external links from an email**, if they are unfamiliar we advise first looking for information on these using reputable search engines.
4. It is advisable that **information is encrypted**: at the computer system level, at the network level, and in data and communication transmissions. Consequently, pay special attention to the communications you make, establishing secure routes for channels, avoiding the use of public networks and avoiding using personal accounts and devices to access sensitive data. Also establish and continually check the remote connection to networks, avoiding the use of unreliable servers, and using virtual private networks (VPN).
5. Do not directly access any link asking for **personal or bank details**. The most advisable course of action is to gain access from the relevant bank or other service provider's website directly and only provide such information via those portals.
6. Establish **strong passwords** for access to email and other services, and to change them regularly. We recommend implementing two-step verification systems (an additional code to register with or log on to certain services online) that enhance the security of some services involving more sensitive information.
7. **Be suspicious** if the content of messages urges you to take any kind of action as soon as possible, without justifying the need for urgency. Cybercriminals often use a sense of urgency to prevent/deter the user contacting someone who could discover the fraud.
8. Make sure you are **aware of the official channels** your organisation is using to provide information and new developments regarding coronavirus, so that you can be alert to any communications received which are fraudulently claiming to be from your organisation or other entities. Under no circumstances should you download unofficial applications in relation to coronavirus.
9. **If you spot a potential case of phishing** do not reply to the email containing suspicious content, or open any links in it, under any circumstances. Delete it and directly inform your organisation (and the service provider it claims to be from if appropriate).
10. Finally, where a cyber attack has been successful, a fraud has been committed or your organisation's service has been interrupted **establish a clear cyber response strategy adapted to the specific situation**, ensuring it covers both technical and legal responses.

DATA COMPROMISE

The increased threat of cyber attacks goes hand in hand with an increased risk of the compromise of data held by organisations. Data protection and privacy concerns can be raised in many cyber incident scenarios, including where information being sequestered by ransomware or phishing results in inadvertent disclosure of personal information. In the event of a personal data breach, organisations can face stringent notification obligations, often to numerous regulators, and breaches have resulted in regulators worldwide taking action which can involve significant financial penalties. In addition, breaches can result in sizeable damage to reputation and customer trust, and exposure to substantial civil litigation.

Coronavirus , and the wealth of personal data which is being processed as a result of it, bring particular data protection challenges for organisations. We discuss these further in our separate briefing, here: **Coronavirus: The data protection challenges**

CLIFFORD CHANCE CYBER ASSIST

Our ability to respond rapidly to assist you in the event of a cyber attack is facilitated by our **Cyber Assist App** which **enables you to contact us at any time, day or night**.

We can advise you how to access the essentials and communicate when your systems are potentially inaccessible. We can host documents, such as your cyber response plans, on our secure document sites so that you can access critical documents safely and quickly during a crisis, even if your internal infrastructure is affected. We can outline the steps which regulators around the world expect you to take in the vital hours and days which follow and guide you through implementing that process. Our global team of cyber and data specialists is immediately available to you at the push of a button.

For access to our Cyber Assist App, email us at CyberAssist@cliffordchance.com or contact your key Clifford Chance contact.

CONTACTS

Austrialia

Tim Grave
Partner

T +61 (2) 8922 8202
E tim.grave
@cliffordchance.com

Belgium

Pierre-André Dubois
Counsel

T +32 (2) 533 5066
E pierre.dubois.
@cliffordchance.com

China

Ling Ho
Partner

T +852 2826 3479
E ling.ho
@cliffordchance.com

Czech Republic

Michal Jasek
Counsel

T +420 (222) 555229
E michal.jasek
@cliffordchance.com

France

Dessislava Savova
Partner

T +33 1 4405 5483
E dessislava.savova
@cliffordchance.com

Germany

Heiner Hugger
Partner

T +49(69) 7199 1283
E heiner.hugger
@cliffordchance.com

Hong Kong

Donna Wacker
Partner

T +852 2826 3478
E donna.wacker
@cliffordchance.com

Italy

Carlo Felice Giampaolino
Partner

T +39 (06) 4229 1356
E
carlofelice.giampaolino
@cliffordchance.com

Japan

Natsuko Sugihara
Partner

T +81 (3) 6632 6681
E natsuko.sugihara
@cliffordchance.com

CONTACTS

Netherlands

Jaap Tempelman
Counsel

T +31 (20) 7119 3192
E jaap.tempelman
@cliffordchance.com

Poland

Marcin Ciemiński
Partner/Advocate

T +48(22)42995153515
E marcin.Ciemiński
@cliffordchance.com

Romania

Stefan Dinu
Senior Associate

T +40 (21) 6666 139
E stefan.dinu
@cliffordchance.com

Russia

Alexander Anichkin
Partner

T +7 (495) 2585089
E alexander.anichkin
@cliffordchance.com

Singapore

Luke Grubb
Partner

T +65 6506 2780
E luke.grubb
@cliffordchance.com

Lijun Chui
Counsel

T +65 6506 2752
E lijun.chui
@cliffordchance.com

Spain

Carlos Zabala
Counsel

T +34 91 590 7515
E carlos.zabala
@cliffordchance.com

Sonsoles Callejo
Abogado

T +34 91 590 4133
E sonsoles.callejo
@cliffordchance.com

UK

Jonathan Kewley
Partner

T +44 207006 3629
E jonathan.kewley
@cliffordchance.com

CONTACTS

UK

Kate Scott
Partner

T +44 207006 4442
E kate.scott
@cliffordchance.com

Samantha Ward
Partner

T +44 207006 8546
E samantha.ward
@cliffordchance.com

US

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

US

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com