MICROSOFT DATA BREACH:
RISK, REGULATION AND MANAGING A CRISIS

The emergency directive (ED) issued on Tuesday 2nd March by the US Cybersecurity and Infrastructure Security Agency (CISA), indicating that Microsoft's Exchange Server application had suffered a significant data breach, serves to highlight the importance of continued and vigilant cyber security systems within businesses.

In tandem with the ED, CISA also issued a twitter alert urging "*ALL organizations across ALL sectors to follow guidance to address the widespread domestic and international exploitation*" of four vulnerabilities in Microsoft's Exchange email application. However, the fix has come too late, as reports have suggested that 30,000 Microsoft Exchange servers have already been compromised, although the precise number is unconfirmed.

The initial cyber-attack is believed to have been carried out by a Chinese State sponsored hacking group called Hafnium who initially exploited a zero-day vulnerability. The attacks included three steps. First, it would gain access to an Exchange Server either with stolen passwords or by using the previously undiscovered vulnerabilities to disguise itself as someone who should have access. Second, it would create what's called a web shell to control the compromised server remotely. Third, it would use that remote access – run from the U.S.-based private servers – to steal data from an organization's network that relied on the Exchange Server software. According to Volexity, a third-party cybersecurity firm that first alerted Microsoft to the hack, breaches began in January with US policy think-tanks being the specific targets for the hackers. The White House has stated that the attack "*could have far-reaching impacts*."

For the US, the Microsoft breach comes on the heels of last year's hacking of a number of federal agencies and corporate systems by Russian hackers, through another third party vendor, SolarWinds. In the SolarWinds attack, hackers planted malicious code in an update of the SolarWinds network management software. Not only was SolarWinds' data breached, but 18,000 of its customers downloaded the code. It has been reported that data from nine US government agencies and approximately 100 companies was compromised during the incident.

SolarWinds demonstrates how quickly a breach of a vendor can spread to its customers, and the Microsoft hack is no exception. In the days leading up to the ED on 2nd March 2021, multiple hackers attempted to infiltrate Microsoft's customers' systems on the back of the original breach. It has been reported that Microsoft Exchange Server users have suffered a third wave of hacking since the 2nd March ED. On 12th March, Microsoft issued a further warning concerning a '*new family of ransomware*', demonstrating that covert groups

FIVE STEPS TO TAKE NOW

1. Security measures must not only be 'adequate' but also checked and verified
2. Ensure vendors and partners maintain high data protection standards
3. Ensure Board and senior management engagement on Cyber risk
4. Conduct employee security awareness training
5. Ensure a robust crisis response plan - and test it

are persistent, particularly where a large global service provider like Microsoft is concerned. Such entities offer a single point of attack. Those groups wading in aren't just from China, but include criminal groups from across the globe.

Some industry experts have suggested that Microsoft applied the patch too late, resulting in the influx of attacks, demonstrating that speed of response is vital if a breach is to be contained. However, what is unusual in this case is how hackers appeared to know about the forthcoming patch and rushed to infiltrate systems before it was released.

Analysts believe as many as 60,000 corporations could be affected with the total number of global Exchange server breaches expected to reach 250,000. Whilst the Microsoft hack is not expected to pose a threat to national security, as with SolarWinds, it does leave organisations vulnerable. The European Banking Authority (EBA) has confirmed that it had been compromised and had taken its email servers offline. Law firms, municipal governments, healthcare providers, and manufacturers have also been affected.

Our summary of the incident is included on the Clifford Chance Regulatory Investigations and Financial Crime Insights page, here:

Microsoft announces widespread hack of Exchange Server software

RISKS FOR BUSINESSES

Regulatory risks

The wide ramifications of the Microsoft data breach proves that cyber security is critical for all businesses.

A cyber crisis is not simply a technical issue, but a significant legal and regulatory incident. The risk of exposure to, and liability for, cyber security failures is at an unprecedented level.

1. Reporting of cyber incidents is increasing significantly and regulators are using new invasive audit and dawn raid powers.
2. Actions have been taken by regulators across the globe, including levying sizeable fines in various European countries under the GDPR (which imposes fines up to 4% of global revenue for serious breaches): including the CNIL in France fining Google €50 million, the AEPD in Spain imposing fines totalling €302,000 on Vodafone España; and the ICO in the UK handing down three Penalty Notices just in October and November 2020, fining British Airways, Marriott International and Ticketmaster £20 million, £18.4 million and £1.25 million respectively for inadequate security measures to protect customers' personal and financial data. US authorities are also increasingly active in this area, with the New York Department of Financial Services filing its first two cybersecurity enforcement actions in recent months and state attorneys general continuing to flex their muscles. The Federal Trade Commission has also stepped up its enforcement efforts, settling a cyber security enforcement action against Zoom just last month.
3. Data related litigation, including class actions, is now a reality.

The risks are more acute than ever, amplified by the Covid-19 outbreak (and related operational pressures, including the fact that many of those who would typically handle an incident may be doing so while remote working).

CLIFFORD CHANCE

Risks of ineffective crisis management

Ineffective crisis management raises the following risks:

1. **Delivering a partial response**: Investigation and containment of an attack by technical forensic specialists is important but only part of effective crisis management. If internal stakeholders and external counsel do not have oversight of this process, the risk is that key legal questions and decisions will not be considered early enough.
2. **Reporting failures**: Under GDPR, firms must notify a potential data breach within 72 hours of becoming aware of it. Delays can lead to enforcement action, resulting in significant fines of up to 4% of annual worldwide turnover. Engagement with financial services regulators, listing authorities and relevant criminal authorities is also critical and can often be overlooked in a crisis. Notifications to multiple authorities are not a tick box exercise – they require strategic consideration and careful choreography. In the US, each of the 50 states has its own notification regime which differs in terms of timing and content. Therefore, close coordination is essential, particularly in view of the fact that authorities share intelligence.
3. **Increased BAU disruption and operational resilience risk**: Cyber breaches may interrupt business services. Failing to resolve an attack quickly will prolong that disruption, bringing with it, customer-facing and operational resilience issues which could subject a business – and its Senior Managers (or equivalent) - to regulatory scrutiny.
4. **Poor or delayed stakeholder engagement**: Internal stakeholders need to have sufficient oversight of the matter so that key decisions can be made. The engagement of Boards must be real and present. Regulators have criticised companies for failing to articulate an appropriate cybercrime risk appetite and for inadequate Board oversight and understanding of incidents. Using case studies can help educate Boards as to the decisions that will need to be taken upon a live incident.
5. **Poor communications strategy**: A cyber crisis can result in significant customer confusion and loss of trust. A sophisticated media strategy is critical and must support the legal response. External counsel can advise on the content of communications in the context of anticipated legal and regulatory risks, as well as how to minimise the risk of internal communications generated during a crisis being disclosed.
6. **Poor customer and employee response**: If a breach is likely to result in a high risk to the rights and freedoms of individuals, or in the US involves sensitive personal identifying information, businesses will likely have to inform those concerned directly and without undue delay. How a business treats its customers and employees during a crisis will inform the risk of enforcement action and the nature of any consequential litigation risk.
7. **Employee risk**: Data or cyber breaches can result from employee misconduct or negligence. If so, it is important to take decisive action. Suspending those who you suspect may be involved is a delicate process and it is important that employment law issues are considered, alongside potential legal remedies such as securing court orders and injunctions to restrain rogue employees (or malicious third parties) from taking further action.

8. **Failure to anticipate and plan for investigations and enforcement**: Multiple authorities may be interested in investigating a cyber incident. How a business mitigates the risk of enforcement action and responds to these investigations while maximizing applicable legal privilege protection will be as important as dealing with the underlying attack.

WHAT GOOD LOOKS LIKE: EFFECTIVE CRISIS MANAGEMENT

If businesses have potentially been affected by the Microsoft data breach, effective crisis management in the early hours will prove crucial in preventing a seemingly minor data breach from rapidly evolving into a full-scale cyber-attack, resulting in significant reputational and financial damage, negative media coverage and diminished customer trust and lengthy investigations.

The Cybersecurity and Infrastructure Security Agency has issued guidance, outlining five steps that enterprises need to take if they have Microsoft Exchange servers.

- Create a forensic image of your system
- Check for indicators of compromise. Microsoft has shared a tool on GitHub to help companies do just that.
- Install the latest patches from Microsoft
- If you can't patch, follow Microsoft's mitigation instructions until you can
- If you discover you've been compromised, implement your incident response plan. CISA has some guidance there, as well.

It is also important to involve external legal counsel as early as possible to ensure that steps taken while in crisis mode do not create additional regulatory or litigation risk. For an incident spanning several countries, the response must take into account the variation in regulators' expectations and be mindful of key differences in legal privilege or professional secrecy protections.

At an early point during a cyber crisis, businesses should reach a view about whether it is necessary or advisable to report the incident to data regulators or other authorities, what to say and when to report. The decision to notify, or to make press releases, about an incident too early or too late, or to say too much or too little, may have long-term consequences.

We understand that deciding whether to report an incident (or not) is an extremely difficult judgment call that must reflect both legal requirements and your strategic priorities. We have advised numerous clients on their reporting obligations to a wide range of third parties.

Our advice on notification reflects a deep understanding of the various, and quite different, regulatory regimes at play. We would balance any recommendation to report in a particular jurisdiction against the risks of that strategy forcing a business to have to report elsewhere.

Expertise and judgement – we will help you to make the right decision

Effective crisis management is preceded by robust cyber response planning and followed by a sound strategy for dealing with the aftermath.

If a large scale breach of customer or employee data across multiple jurisdictions perpetrated by malicious actors occurs, businesses would face the most serious of cyber threats and would require the 24/7 engagement of its internal specialists, external counsel, forensic teams and suppliers. It would further require preparation for the regulatory and litigation risks that may crystallise later.

It is therefore important to:

1. plan for a cyber incident as your ability to manage an incident effectively is only as good as your preparation
2. have a strategy for dealing with regulatory investigations and/or litigation from the outset.

Cyber response planning

Prevention is of course better than cure.

We have worked on some of the world's largest cyber response projects and our work on response planning has stood up to scrutiny, often preventing a cyber incident from escalating into a crisis.

Examples of our work include:

- Reviewing existing cyber and information security plans to make sure they are robust, clear, fit-for- purpose and up-to-date in light of the changing landscape.
- Developing a communications strategy that enables our clients to engage with internal and external stakeholders in a way that reflects the risk of disclosure in any subsequent investigations, enforcement actions and/or litigation.
- Stress testing outsourcing arrangements and third-party supplier relationships to make sure they withstand regulatory scrutiny, particularly around operational resilience.
- Embedding cyber plans throughout our clients' business through training and 'dry run' exercises.

Operational resilience is a particularly hot topic for regulators within the US and across Europe. Businesses are required to demonstrate how they will provide important business services in times of operational disruption. We can help you to manage a cyber crisis, allowing you to focus on business continuity and operational resilience in times of pressure, as well as:

- Providing you with advisory support on regulatory requirements, governance, training, planning and limitation of exposure.
- Assisting with tools and support in relation to self- assessment, including scoping and audit of documentation, potential exposure, contractual implementation and the development of frameworks.
- Providing a playbook of necessary steps, as well as crisis regulatory response including coordination of stakeholders, vendors and communication.
- When dealing with the fallout, guiding you through assessment of the incident, next steps you need to take and the challenges you may face. These may include internal investigations, enforcement actions, injunctive relief, insurance claims and litigation.

Managing the aftermath

Enforcement action can come with significant financial and reputational implications. Throughout a crisis, it is important to anticipate subsequent investigations, enforcement actions and/or litigation.

Investigations

- The risk of investigations being led by multiple authorities would be acute: data protection authorities would look to assess consumer harm and a business's handling of the incident; financial regulators would scrutinise consumer detriment, conduct, systems and controls; criminal authorities may investigate underlying individuals and behaviours; and listing authorities would be concerned about the economic and market impacts.
- We have unrivalled experience of conducting internal investigations on behalf of our clients and responding to external investigations by numerous governmental authorities across different jurisdictions. We have guided numerous clients through all sorts of crises and handled all the pressure points that come with an investigation such as responding to detailed information requests, dawn raids and witness interviews.
- The powers of UK and European data protection regulators are modelled on those of the antitrust authorities. Our deep experience in this area has proved invaluable in understanding how data authorities like the UK's ICO operate. We have extensive experience of dealing with dawn raids, particularly in the context of antitrust investigations (being the most active authorities in this area).

Litigation

- A serious cyber incident may create significant exposure to civil claims, both individual and on a class action basis, supported by litigation funders. Whilst an individual claim for damages may be small, if tens of thousands of customers are affected, such claims can quickly lead to exposures of millions of euros. Litigation can also be used by the subject of a cyber-attack, to place restrictions on the perpetrator of any attack. Where suppliers' failings have contributed to the cyber incident, firms may need to initiate claims to recover a contribution to their losses.
- We can advise on the key areas of litigation risk in core jurisdictions and advise on strategies to be implemented now to help mitigate those risks.

In the event of any follow-on litigation, support is required in all aspects:

- We advise on the potential breadth of claims arising from cyber incidents and have strategies to deal with such claims, including claims for statutory damages under GDPR or relevant US statutes, misuse of private information, and breach of contract.
- We advise on whether clients may be vicariously liable for any loss or damage caused by an employee.
- We have defended multinational companies from class action litigation in multiple jurisdictions.
- We have experience in designing and operating redress and compensation schemes, which can often head off litigation.
- We advise on claims made under cyber insurance policies and can assist in pursuing claims against insurers where disputes may arise.

CLIFFORD
CHANCE

CONTACTS

UK

Samantha Ward
Partner

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

Kate Scott
Partner

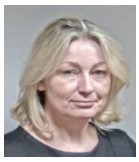
T +44 207006 4442
E kate.scott
@cliffordchance.com

Simon Persoff
Partner

T +44 207006 3060
E Simon.Persoff
@cliffordchance.com

Jonathan Kewley
Partner

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



Cheryl Jones
Senior Associate

T +44 207006 2386
E Cheryl.Jones
@cliffordchance.com

US

Leo Lou
Associate

T +44 207006 1914
E leo.lou
@cliffordchance.com

Daniel Silver
Partner

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

Megan Gordon
Partner

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

Australia

Alex Sisto
Associate

T +1 212 878 4990
E alex.sisto
@cliffordchance.com

Tim Grave
Partner

T +61 2 8922 8028
E tim.grave
@cliffordchance.com

China

Kimi Liu
Counsel

T +86 10 6535 2263
E kimi.liu
@cliffordchance.com

Germany

Dr. Thomas Voland
Partner

T +49 211 4355 5642
E thomas.voland
@cliffordchance.com

Dr. Ines Keitel
Partner

T +49 69 7199 1250
E ines.keitel
@cliffordchance.com

Hong Kong

Ling Ho
Partner

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

Donna Wacker
Partner

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

Italy

Carlo Felice Giampaolino
Partner

T +39 064229 1356
E carlofelice.giampaolino
@cliffordchance.com

Alessandro Sciarra
Senior Associate

T +39 02 8063 4282
E alessandro.sciarra
@cliffordchance.com

Japan

Natsuko Sugihara
Partner

T +81 3 6632 6681
E Natsuko.Sugihara
@cliffordchance.com

Netherlands

Jaap Tempelman
Counsel

T +31 20 711 9192
E jaap.tempelman
@cliffordchance.com

Poland

Marcin Cieminski
Partner

T +48 22429 9515
E marcin.cieminski
@cliffordchance.com

CLIFFORD
CHANCE

Russia

Alexander Anichkin
Partner

T +7 495 258 5089
E alexander.anichkin
@cliffordchance.com

Singapore

Lena Ng
Partner

T +65 6410 2215
E lena.ng
@cliffordchance.com

Kabir Singh
Partner

T +65 6410 2273
E kabir.singh
@cliffordchance.com

Janice Goh
Partner, Cavenagh Law

T +65 6661 2021
E janice.goh
@cliffordchance.com

UAE

Arun Visweswaran
Senior Associate

T +971 4503 2748
E arun.visweswaran
@cliffordchance.com

CLIFFORD
CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ