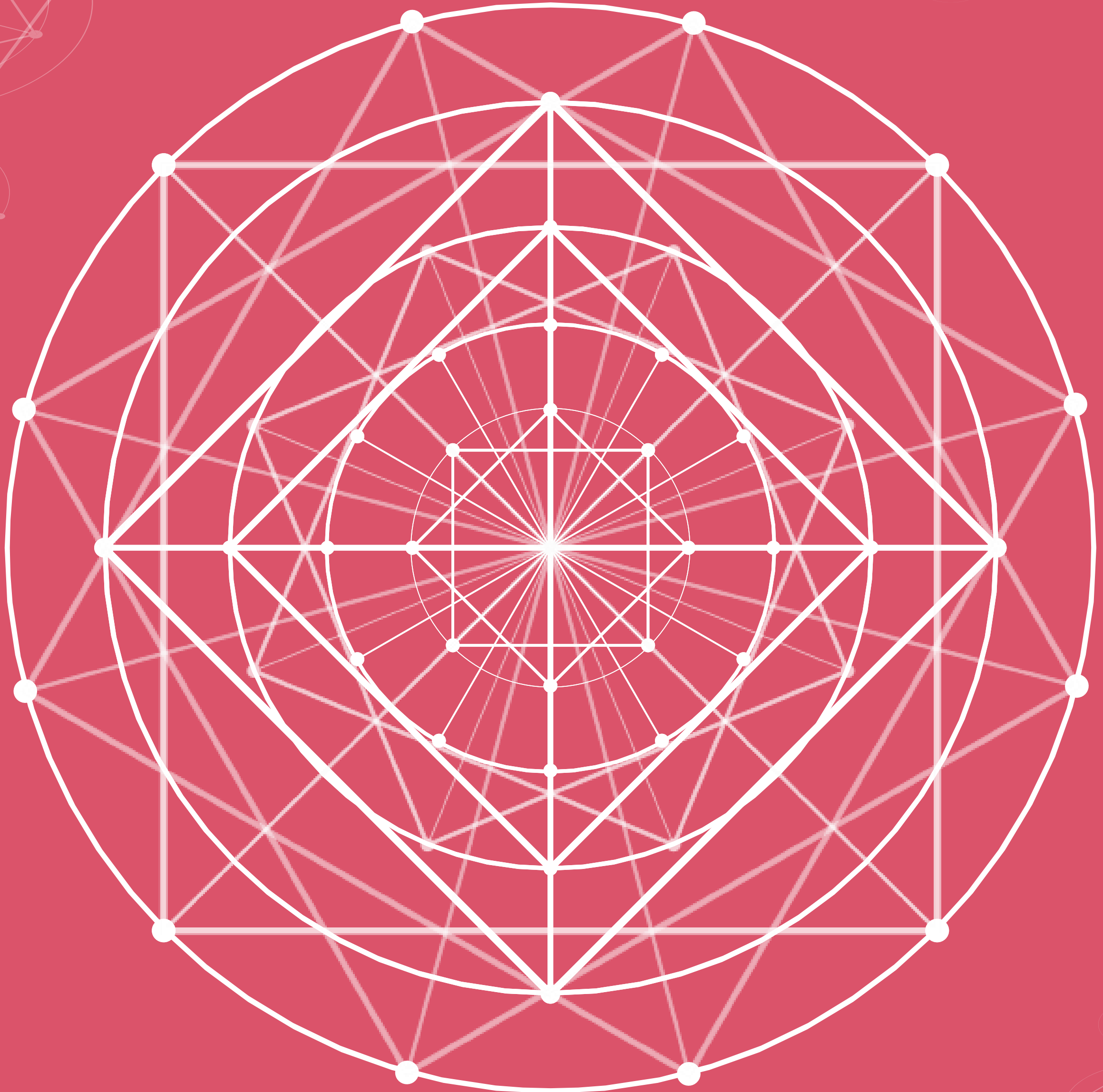


Email Phishing: Culprit behind Ransomware

pwc

Tomorrow's Cyber Security, Today

IRONCAP

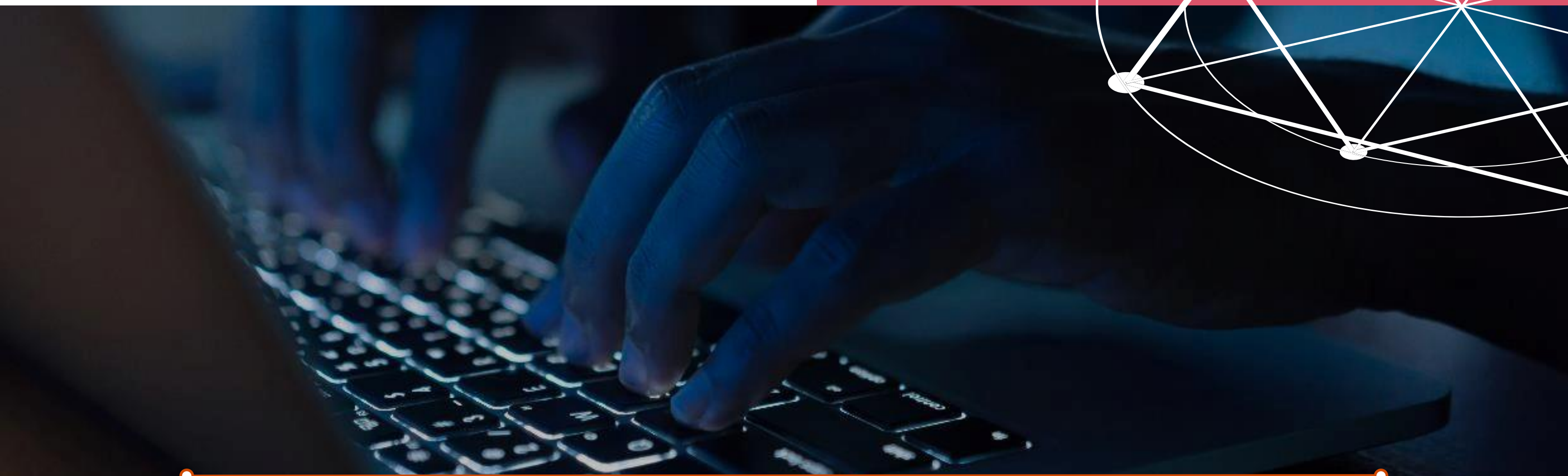
Table of Contents:

1. Ransomware: A pressing danger!

Ransomware has been headline news on a daily basis and is becoming our No. 1 “cyber-enemy”. According to Harvard Business Review[1] in May 2021, ransomware attacks were up 150% over the previous year. The amount paid by victims of these attacks increased more than 300% in 2020. This massive uptrend is further fuelled by accelerated digitalisation creating fertile soil for such attacks. The risk of data exposure will only grow given that remote workers’ personal devices are more vulnerable. According to the Cybercrime Magazine[2], ransomware damage costs are predicted to exceed USD265B annually and attacking a business, consumer or device every 2 seconds by 2031.

Governments and critical infrastructure are not the only targets, ransomware attackers are less concerned about the industry and more focused on scope and scale. They go after large enterprise networks to secure the biggest possible ransom. Therefore, big enterprises e.g., banks, manufacturers and even high-tech companies and cybersecurity providers themselves are popular targets.

The great cloud migration creates further opportunity for attackers blending both email and cloud vectors for financial gain. Emerging incidents such as COVID-19 pandemic expose the cyber weakness of many tertiary fields e.g., healthcare sector which are now overwhelmed with huge influx of new personal data making them juicy targets for attack.



[1] Ransomware Attacks Are Spiking. Is Your Company Prepared? (hbr.org)

[2] Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031 (cybersecurityventures.com)

According to IBM's Cost of Data Breach Report 2021, the average total cost of a ransomware breach is USD4.62M, these costs only include escalation, notification, lost business and response costs, but do not include the cost of the ransom. On ransom amount, Group-IB[4]'s study indicates that the average ransom was around $80,000 in 2019. By 2020, this was nearly doubled to $170,000. This trend is likely to grow exponentially with prediction of the norm shift towards millions soon enough. There is indication that ransomware groups will take on a more drastic approach, in addition to ransomware deployment, data exfiltration and extortion are likely to be the common themes in the future. In addition to the potential operating downtime suffered by these incidents, "kidnapping" of these highly sensitive and confidential data is not only costly, but devastating to a corporation's reputation, credibility and trust, which takes years to rebuild and cost C-Suite members and even the Board avoidable aggravation. Unfortunately, what we see is just the surface covered by the media, in reality the situation is gloomier as victims often settle ransoms unreported, with the ransom payments used to fund future ransom operations by acquiring further human resources, hardware and tools to develop more sophisticated tactics.

Defenders need to understand these techniques to come up with an optimal defence strategy for their corporations. In particular, staying on top of the latest trends and predictions so as to allow sufficient lead time and effort to engineer and implement the right tools for resistance.

[3] Cost of a Data Breach Report 2021 (rackcdn.com)

[4] Annual Ransomware Report by Group-IB 2020/2021 (pathfactory.com)

2. How do they get in?

All ransomware happens with a simple step: To plant a malware into the target systems Without prior knowledge of legitimate access credentials, adversaries can proceed to systematically guessing logon ids and passwords. The drawback to this "brute force" approach is the need to consume significant computer resources and time. More importantly incorrect guesses would inevitably trigger authentication failure and account lockouts, potentially exposing the adversary. Reliance on personally identifiable information (PII) purchased from "dark exchange" is another approach, however the price for PII has drastically increased making it more costly to initiate attacks. It is therefore no surprise to see the growing trend of email phishing given its outstanding success rate. A recent survey[5] of 127 business leaders by Gartner reported that 47% of respondents intend to allow employees to work remotely full-time even if it becomes possible to return to the workplace; 82% intend to permit remote working at least some of the time. Group-IB's study[6] also shows that over a quarter of ransomware was through phishing and in May 2020, the UN[7] reported that the increased cybercrime was caused by a 6X increase in malicious emails.

Unlike other cybercrimes, email phishing makes use of social engineering techniques to prey on human emotions and behaviour: greed, curiosity, fear, and the usual tactic posing as legitimate business or authoritative bodies to pry personal information or login information. Phishers often rely on invoking a sense of alarm or ironically, loss of security! They pretend to be your "bank" or technology service provider with false alert on data breach. You then log in through a fake website to confirm "you are you", thereby stealing login details for the said instances, such as your online banking account or your network access credentials. Some are camouflaged as routine password update or subscription renewal reminders, requesting you to click the link and reveal all your personal information. As you add in your old and new password, the phishers gain access to your "old" i.e., real password and use this to log in and gain your private information. Others simply use phishing links or weaponised file attachments to lure recipients to do that one click!

COVID-19 provides the ideal environment for criminals to lure content with creative stories such as disease tracking, testing, treatment and government stimulus packages to work-from-home employees whose personal devices are relatively weaker in security. Phishing emails using COVID-19-related subject lines or content are the latest method to get the target to click on ransomware links. In 2020, Google reported that they blocked more than 100 million phishing emails every day[8]. This kind of statistics fully reveal the vulnerability of today's email infrastructure and the lack of an effective solution to tackle email phishing. Without an effective defence against phishing, this low cost and effortless tactic will prevail.

[5] Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time

[6] https://www.group-ib.com/resources/threat-research/2021-reports.html

[7] https://apnews.com/article/europe-united-nations-brazil-south-korea-cybercrime-6ba6af57fd96e25334d8a06fcf999e7f

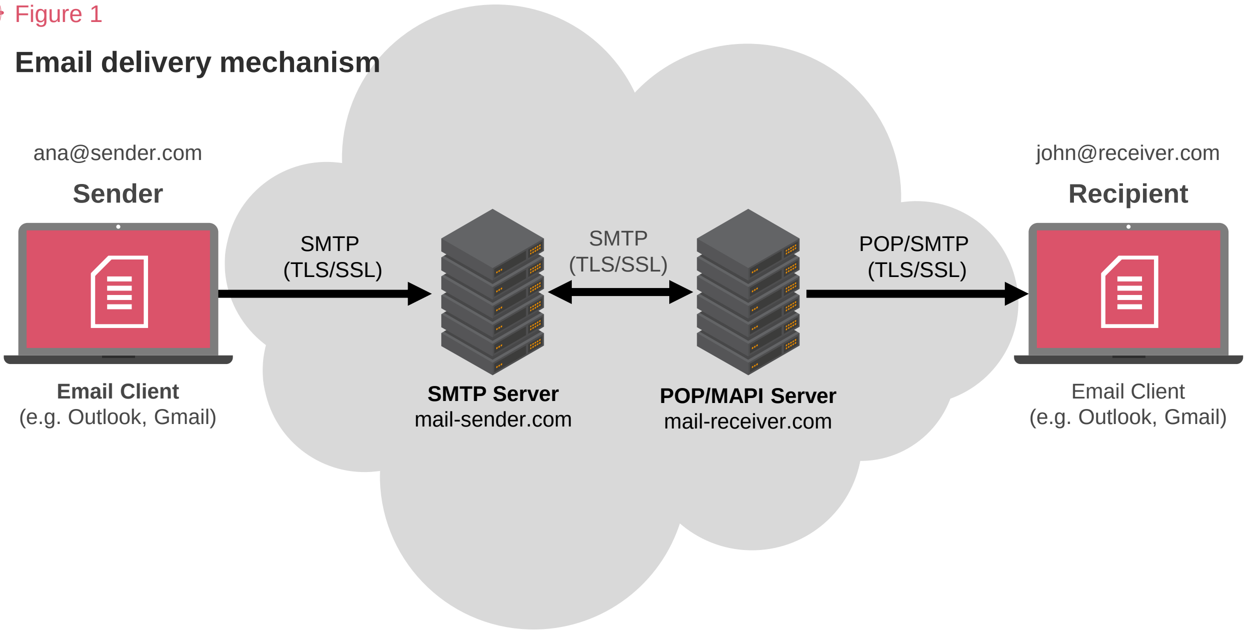
[8] Protecting against cyber threats during COVID-19 and beyond | Google Cloud Blog

3. How vulnerable?

In any email system, such as MS Outlook, Gmail or web-mail, a user needs a software interface called the "Mail Client" to interact with the email server allowing them to compose, send, store, and read messages. These applications adopt a common protocol called Simple Mail Transfer Protocol (SMTP) to transfer email messages from the Mail Clients to and between e-mail servers. Post Office Protocol (POP3) or Internet Message Access Protocol (IMAP4) are e-mail retrieval protocols used to retrieve the e-mail messages from the server to the receiving mail clients as shown in Figure 1 below.

Figure 1

Email delivery mechanism



Since email communication takes place on the internet, email systems often just rely on the existing standard internet security feature: Transport Layer Security (TLS) or Secure Sockets Layer (SSL) that protects the transmission of the content of email messages between senders/receivers and their email servers, but does nothing to protect the security of the message before it is sent or after it arrives at its destination~~s~~.

Authentication to Mail Clients is typically through a username and password, which is vulnerable to attacks as the passwords could be easily hacked[9]. Not to mention that it is NOT mandatory for email systems to adopt TLS or proactively update and validate TLS certificates. Both the sending and receiving email servers also has access to the contents of the message, i.e., open to active man-in-the-middle attacks.

This means cyber-criminals can easily compromise an email account and read any emails or attachments including highly sensitive information and business secrets. The lack of identity authentication further motivates criminals to simply hijack email identity and pretend to be trusted senders to launch phishing attacks.

[9] Enhancement-of-Email-Security-Services.pdf (ijser.org)

4. Today's counteract

Recognising the mounting threat posed by email phishing, official institutions such as the Canadian Centre for Cyber Security issued a number of publications including technical security measures[10], recommendations[11] and guidelines[12]. Similarly, the U.S. Cybersecurity and Infrastructure Security Agency (CISA)[13] issued a stern warning and a recommendation with over 20 steps to strengthen security practices. Likewise, the European Union Agency For Cybersecurity[14] endorsed both preventive measures, technical controls and post event actions e.g., disaster recovery program etc. A statement issued by the G7 recognised that the pandemic has expanded opportunities for ransomware attackers[15] and call upon all countries to effectively implement the Financial Action Task Force (FATF) standards to combat ransomware and to carry out mitigating actions e.g., to employ layered security to prevent, detect, and remediate malicious activity that may be conducted within the network.

Last May, the Hong Kong Monetary Authority issued a circular[16] instructing authorised institutions to critically assess the need for establishing a Secure Tertiary Data Backup to guard against the ever-increasing threat of destructive cyber-attacks. The HKMA also seeks to enhance public awareness on the risk of phishing attacks and provided guidance[17] to the public on the threat and responses. Similarly, the China Banking and Insurance Regulatory Commission publish similar guidance and warnings to the public[18].

Many such guides urge the public to be vigilant and refrain from clicking on any links, whether in email or short messages, that are purportedly sent by their banks. However, the effectiveness of such measures inevitably relies on the public's awareness and can only offer limited protection against phishing attacks.

All-in-all, todays counteract are both responsive and technically costly to implement, not to mention the heavy reliance placed on staff awareness through ongoing training. Some even cause extra stress to employees as shame-and-blame culture often exist in organisations. Before COVID-19 hit, these measures were already challenging even for bigger organisations to fully implement. With the unexpected acceleration of digitalisation since COVID-19, some of them are no longer practicable, for instance, remote working mean that employees' often need to use their own devices communicating through open networks.

[10] Implementation Guidance: Email Domain Protection - Canadian Centre for Cyber Security

[11] Don't Take the Bait: Recognize and Avoid Phishing Attacks (cyber.gc.ca)

[12] Spotting Malicious Email Messages (ITSAP.00.100) - Canadian Centre for Cyber Security

[13] Strengthening Security Configurations to Defend Against Attackers Targeting Cloud Services | CISA

[14] ENISA Threat Landscape 2020 - Insider Threat — ENISA (europa.eu)

[15] G7-Ransomware-Annex-10132020_Final.pdf (treasury.gov)

[16] Hong Kong Monetary Authority circular May 2021

[17] Hong Kong Monetary Authority press release on phishing awareness

[18] 银保监会：关于防范短信钓鱼诈骗的风险提示

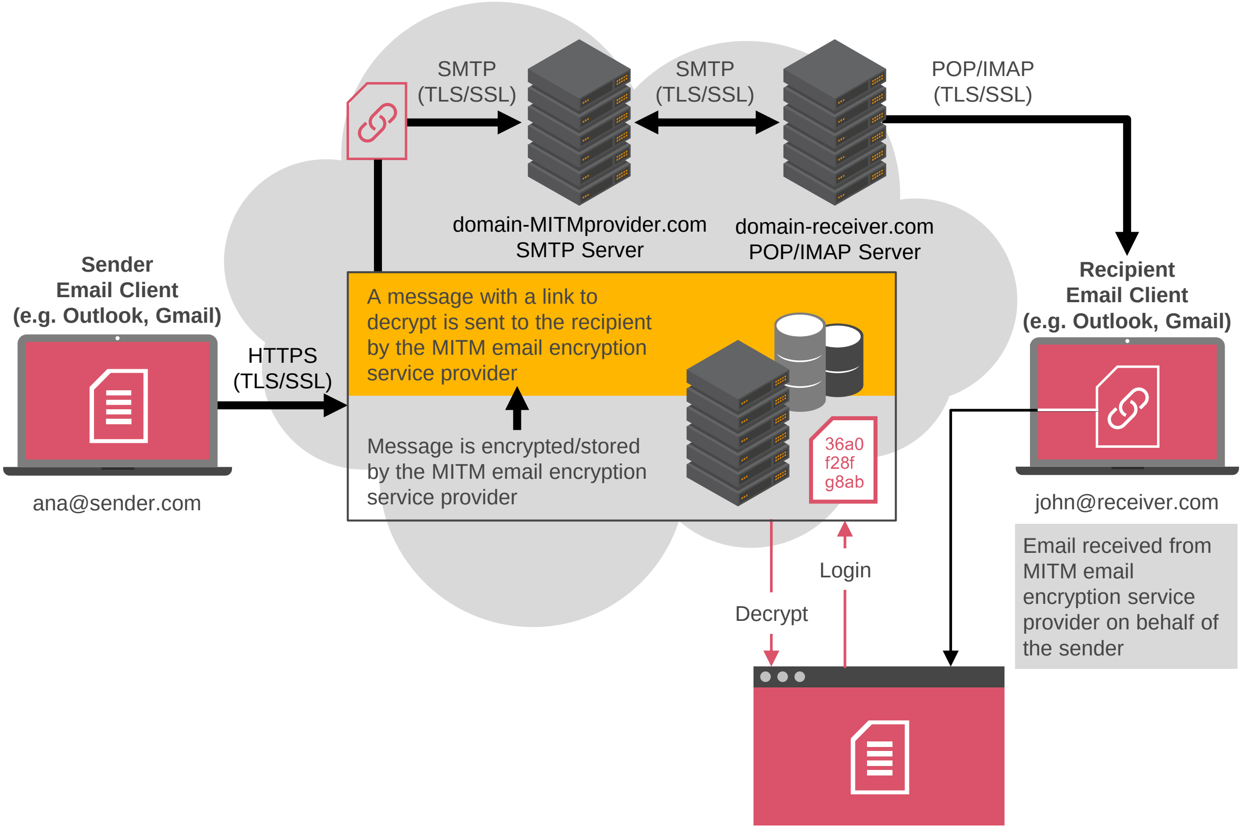
5. The man in the middle

Preventative measures such as awareness, audit email rules with enforceable alerts, restrict email forwarding, etc., offer certain degree of protection. They may create undue burden on email recipients who are, after all, human beings with emotion. These preventive measures are responsive as they require individuals to be on guard with full alert in case email phishing take place at any point in time.

It is therefore not surprising to see other proactive offerings in the market, such as Risk-based Authentication (RBA) and Out of Band Authentication (OOB). The former imposes additional authentication steps according to threat level while the latter offers additional authentication outside of the primary communications channel as shown in figure 2 below.

Figure 2

Man-in-the-middle email security


SMTP (TLS/SSL)
SMTP (TLS/SSL)
POP/IMAP (TLS/SSL)
domain-MITMprovider.com SMTP Server
domain-receiver.com POP/IMAP Server
Sender Email Client (e.g. Outlook, Gmail)
HTTPS (TLS/SSL)
A message with a link to decrypt is sent to the recipient by the MITM email encryption service provider
Message is encrypted/stored by the MITM email encryption service provider
36a0 f28f g8ab
Recipient Email Client (e.g. Outlook, Gmail)
ana@sender.com
john@receiver.com
Email received from MITM email encryption service provider on behalf of the sender
Login
Decrypt

These solutions are popular because the authentication mechanisms are either physical devices e.g., USB token; or visible images e.g., SMS/Biometric that would naturally give a user the feeling that they are protected by this additional layer of defence. However, quite the contrary, it creates a new breed of Man-In-The-Middle (MITM) that stores users’ credentials in centralised servers, making them potential targets for bad actors!

Furthermore, MITM email security solutions are often operated by Email Client providers themselves through which they now possess the capability to decrypt and read all the encrypted emails. In theory, such capability can potentially facilitate commercial initiatives such as data analytics/advertisement; and “back-door” scenario for monitoring needs.

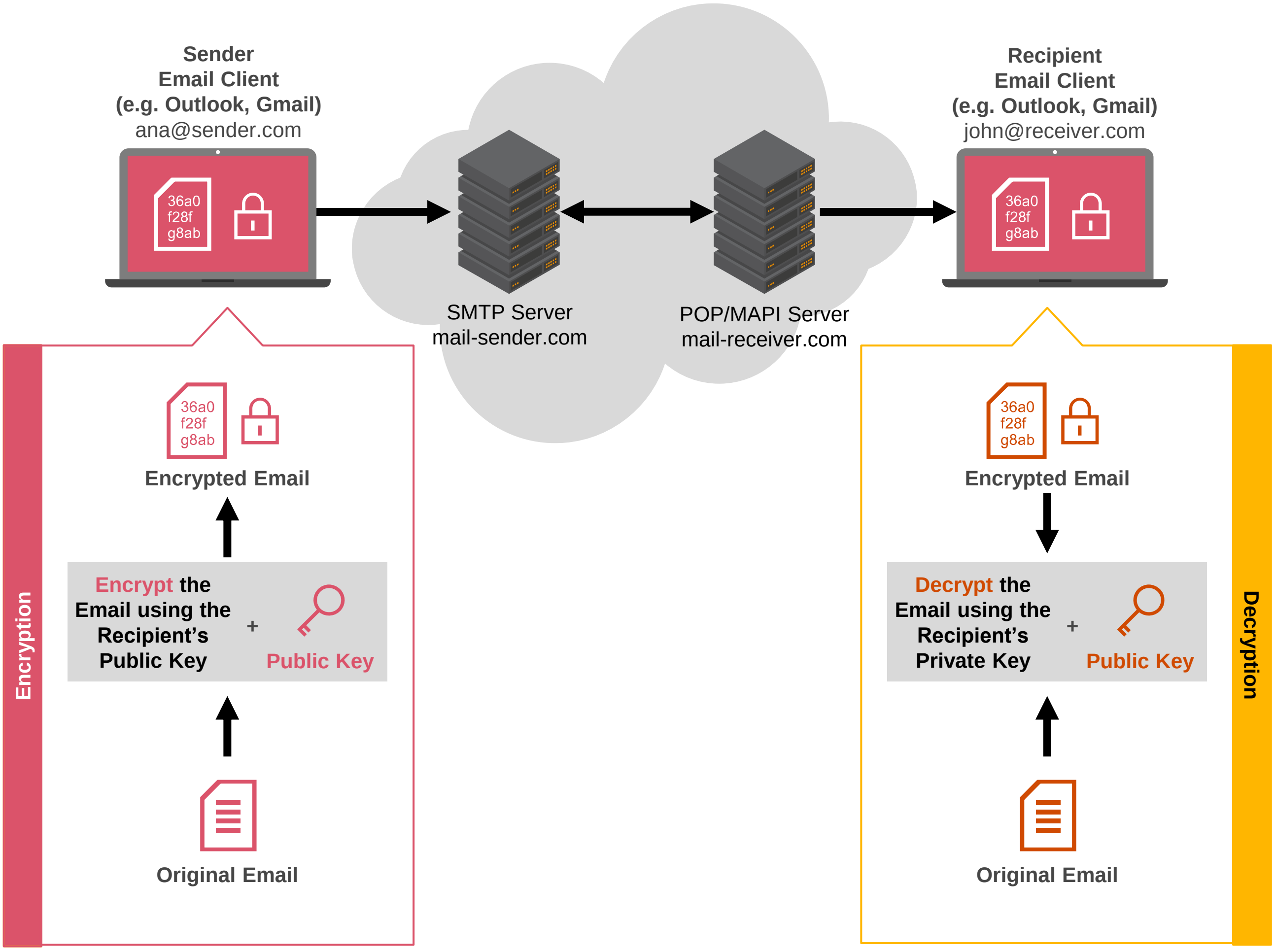
6. Proactive, yet simple

While there is no one single bullet-proof solution, we believe that by keeping things simple (i.e., removing MITM set-up) and proactively tackling the key weaknesses in email communication will provide an effective and economical protection.

Focusing on these two weaknesses: (1) lack of end-to-end protection in the communication flow; and (2) ease of hijacking email identity, it is clear that applying end-to-end email encryption with authentication capability will ensure security at every stage, and protect the messages from being read even by email servers. Senders and receivers are the only parties holding their respective encryption keys for the purpose of message exchange and signature authentication.

Figure 3

End-to-end email encryption



With this design, it is almost impossible for cyber criminals to compromise sensitive information or attachments unless the encryption algorithm itself is cracked.

Today, end-to-end email privacy and authentication solutions are in fact available e.g., Secure/Multipurpose Internet Mail Extension (S/MIME), Pretty Good Privacy[19] (PGP) and GnuPG[20]. However, these standalone solutions may not be seamlessly applied to mainstream Mail Clients (e.g., Outlook, Gmail etc.) thereby significantly reduces their usability. Furthermore, there is also the challenge of initial key exchange between senders and receivers: users need to exchange keys physically via a USB, which may involve hardware token installation. More creativity is therefore needed to simplify this remaining practical issue before wider adoption.

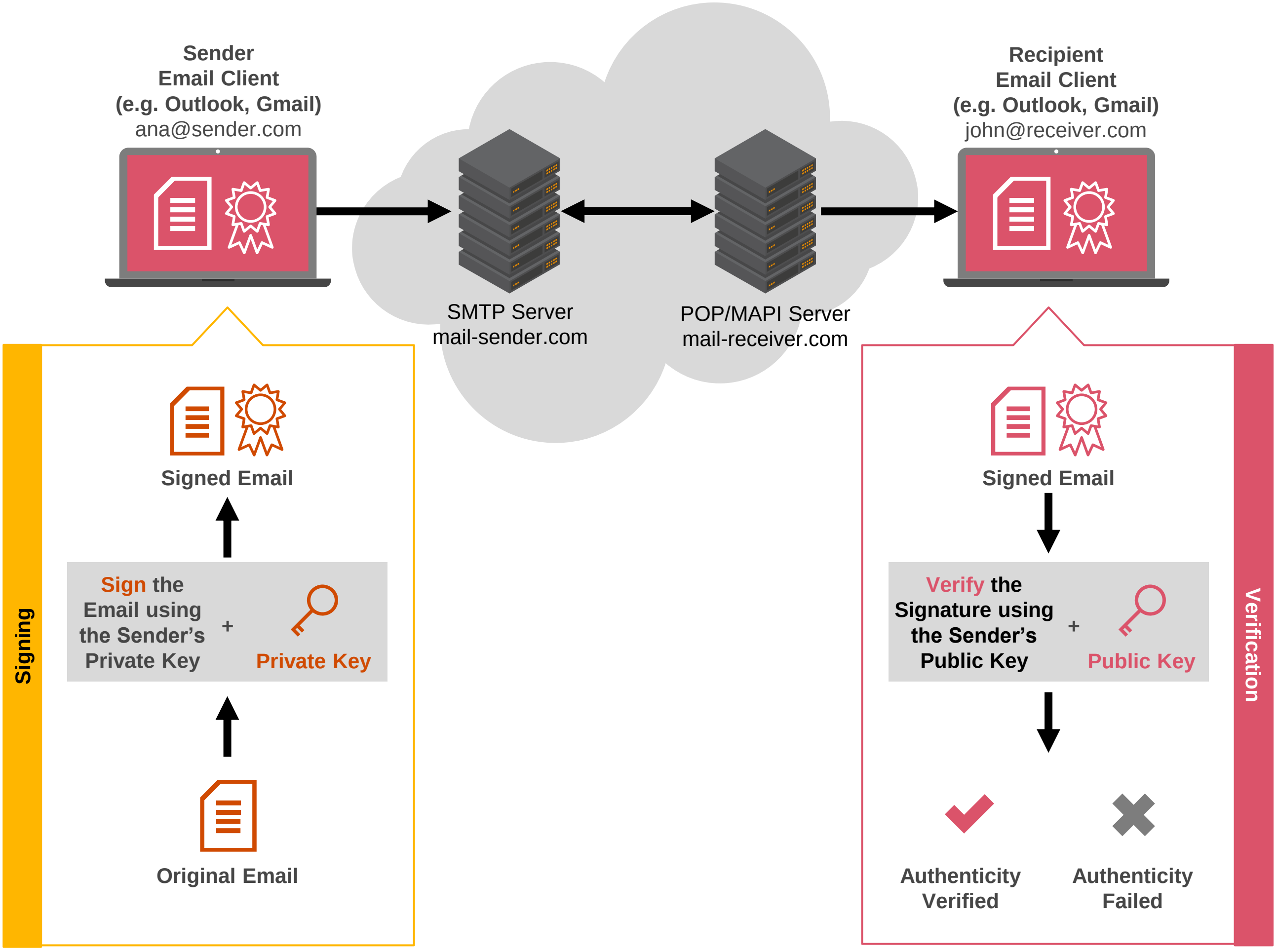
An effective end-to-end solution should work seamlessly with mainstream Mail Clients to improve usability, and be able to overcome the challenge of initial key exchange, such as via a one-off initial random key exchange to secure the first contact between sender and receiver. Further protection should be in place using digital signatures to provide confidence over the authenticity of the sender. This critical step provides recipients with the means to distinguish between legitimate and phishing emails even though they both appear to be coming from the same sender. The figure overleaf illustrates use of digital signature as a means of determining the legitimate sender. Further creativity can be introduced to strengthen identity verification by adopting innovative digital authentication and certification tools.

[19] PGP Tutorial for Beginners to PGP (pitt.edu)

[20] The GNU Privacy Guard (gnupg.org)

Figure 4

Email authenticity using digital signature



7. Best way to resist

While prevention is always better than cure, the nature of phishing is such that there is no one solution that can prevent such attacks entirely on its own. Cohesive effort, leadership and commitment are needed to determine the right strategy and approach.

Like all security measures, we believe enterprises should adopt a holistic approach, addressing the essential aspects including enhancing awareness and governance, while adopting suitable and robust technology solutions that best suit the technical environment that support the entity's business operations. The adoption of true end-to-end encryption would be a key preventative measure, and leveraging the latest verifiable digital credentials would provide the email user the means to verify the purported identity of the party sending the email.

Figure 5

A holistic approach to countering the threat of phishing attacks

1

Awareness of personnel to the risk and nature of phishing attacks remains the first line of defence

Enhance the awareness of personnel in identifying phishing email scams is still critical. Strengthen the ability to identify signs and indicators of attempted phishing would be important to detect and avoid such attacks. Phishing simulation campaigns can also be used to reinforce the knowledge on phishing prevention.

2

Strengthen boundary defence and undertake robust security assessment to prevent and detect attacks

Select and implement appropriate solutions to strengthen perimeter controls, and establish monitoring mechanisms to enable timely detection of threats and attacks. Review technology architecture to reduce potential entry points for attacks, and deploy end-point security measures to provide further safeguards.

3

Focus on resilience beyond the traditional disaster recovery and business continuity model to enable "resilience by design"

Build the ability to protect and sustain core business functions when experiencing a state of disruption to technology, infrastructure, or operational processes supporting mission-critical business services. Prioritise data availability and integrity, during and after a disruptive event, with a focus on maintaining confidentiality.

4

Leverage latest phishing prevention design and digital identity to enable better defence against such attacks

Adopt sound and proven end-to-end email encryption solutions, and supplement it with authentication capability – through the use of verifiable digital identities – to ensure mail content is secured throughout the entire transmission process, and provide an ease easy-to-use mechanism for recipients to verify the sender's identity.

It is however important to recognise that in today’s connected business world, it would not be practical for any enterprise to seek to establish an identity infrastructure that is capable of encompassing all its trading partners. Our knowledge of digital identity infrastructure will be valuable to enterprises that wish to leverage this component in their response to phishing risks. Through understanding the enterprise’s operational footprint and technology infrastructure, we will be able to advise on the design and approach to enhancing the overall security architecture that will better defend against phishing and other cyberattacks.

It is never easy to carry out preventative measures comprehensively and effectively. Taking the right action now will reduce the risks but not totally eliminate them. Being better at cyber defence does not necessarily means more investment; rather it means being smarter and more innovative - choosing the right tools and techniques in tackling the most critical vulnerabilities head-on. In any case, the nature of phishing attacks meant that the response needs to take into account not just technology measures, but also behavioural aspect of individuals who are at the “front line” of the defence against phishing.

Contact us

William Gee

Partner
Innovation and Digitalisation
PwC China
william.gee@hk.pwc.com

Samuel Sinn

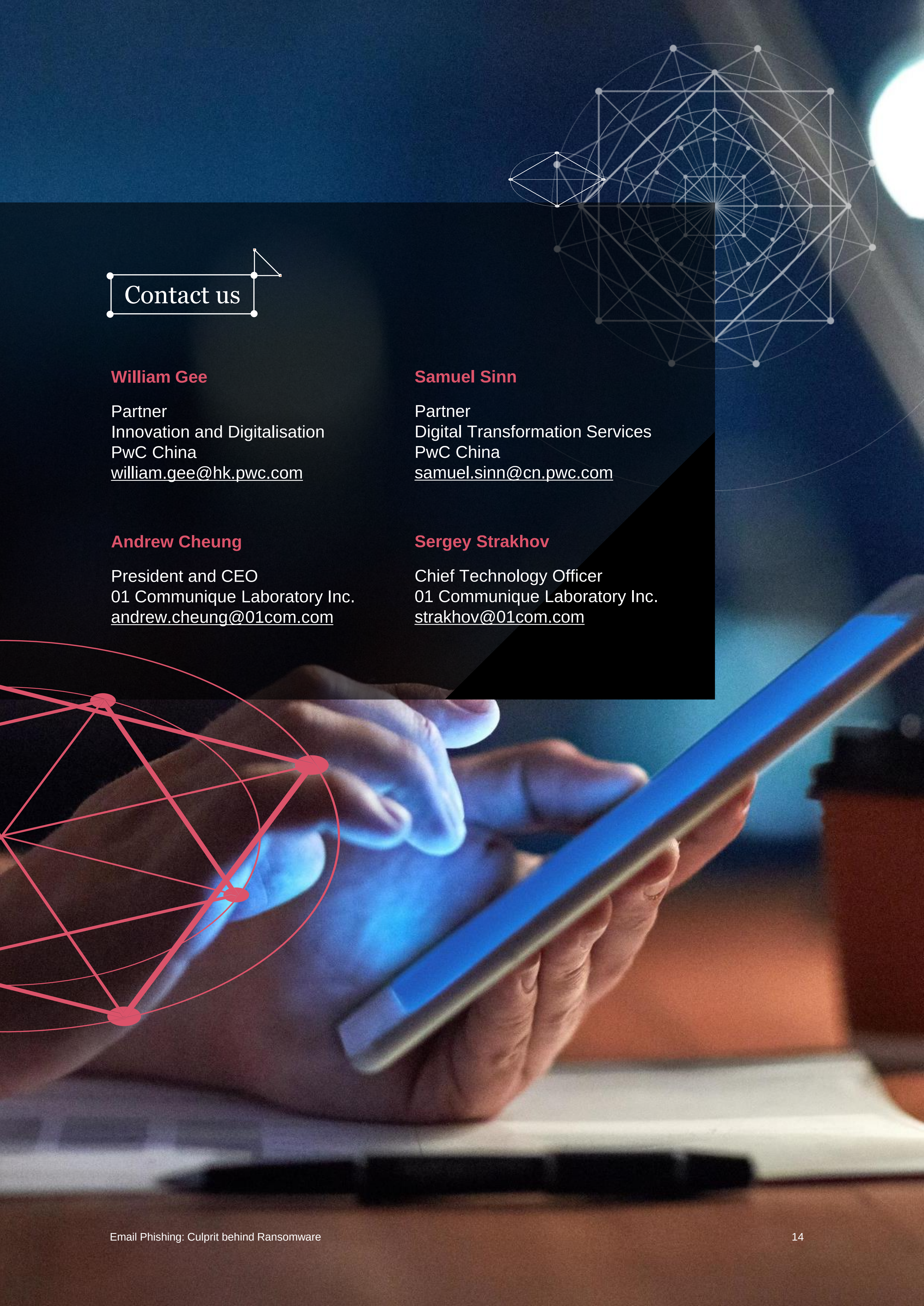
Partner
Digital Transformation Services
PwC China
samuel.sinn@cn.pwc.com

Andrew Cheung

President and CEO
01 Communique Laboratory Inc.
andrew.cheung@01com.com

Sergey Strakhov

Chief Technology Officer
01 Communique Laboratory Inc.
strakhov@01com.com



Additional resources

PwC and IronCAP	Rethinking Cybersecurity in a Quantum World
IronCAP X	IronCAP End-to-end email security
PwC	Digital security in a post-quantum world, time to act now!
IronCAP	Post-Quantum Cybersecurity, The Quanutm Era has begun
IronCAP	Tomorrow's Cyber Security, Today
PwC	Employees and cybersecurity: asset or liability?

Contributors

PwC China

William Gee
Partner, Innovation and Digitalisation
PwC China

Samuel Sinn
Partner, Digital Transformation Services
PwC China

PwC Canada

Asif Qayyum
Managing Director, Digital Security Risk
& Controls, PwC Canada

01 Communique

Andrew Cheung,
Chief Executive Officer,
01 Communique Laboratory Inc.

Sergey Strakhov
Chief Technology Officer
01 Communique Laboratory Inc.

Vicky Chan
Head of Business Development, Asia
01 Communique Laboratory Inc.

www.pwccn.com

The information contained in this publication is of a general nature only. It is not meant to be comprehensive and does not constitute the rendering of legal, tax or other professional advice or service by PricewaterhouseCoopers Limited ("PwC"). PwC has no obligation to update the information as law and practices change. The application and impact of laws can vary widely based on the specific facts involved. Before taking any action, please ensure that you obtain advice specific to your circumstances from your usual PwC client service team or your other advisers.

The materials contained in this publication were assembled on 7 Feb 2022 and were based on the law enforceable and information available at that time.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.