【新型ウイルス対応】ひと目で分かるリモートワークセキュリティ

PwC 中国日本企業部ニュースレター
2020 年 3 月

概要

新型コロナウイルス感染拡大の最中、自宅などからのリモートワークは従業員の健康と業務運営を管理する最善の方法であるといえます。しかし同時に、実施における情報及びデータのセキュリティは企業及び従業員にとって極めて重要な問題です。リモートワークは利便性をもたらすと同時に、業務システム、重要データ及びオフィスネットワークの運営を非常に複雑にし、情報セキュリティリスクの上昇を伴います。企業は技術フレームワークやデータ管理、従業員の行動等、多面的な観点から、効率性と安全性のバランスをとりながらシステム化を計画・実現することが望ましいでしょう。リモートワーク導入の複雑性による難易度の高さが企業の課題となっていることを受け、PwC 中国は本稿を通じて、**データセキュリティ保護の重点を素早く理解できるよう「ひと目で分かるリモートワークセキュリティ」としてまとめ**、専門家としての見解をご紹介します。

リモートワークの安全性の保証を基本とした上で、企業のデータセキュリティ、特に企業の中核となるビジネスバリューに係る重要データについて、データを取り巻くセキュリティ対策をさらに強化すべきです。ここでは、リモートワークにおけるデータセキュリティの要点をソース管理、アクセス制限、継続的モニタリング、早期遮断といったキーワードでまとめています。

リモートデータ生成及び保存リスク

リスクシーン：リモートワーク環境下においては、企業の重要データの生成と保存はより分散されます。同時にデータへのアクセス経路がより多様化し、業務上の必要性からデータへのアクセス権限をより広範にわたって開放する等の措置が採られ易くなり、結果、データの生成と保存過程における漏洩リスクが非常に高くなります。

対応策の提案：ソース管理、重要性に基づいたデータのグレード別管理、データソースの厳格な管理

リモートワークの運用においては、2 つのデータソースを重点的に管理・統制する必要があります。

1 つ目として、企業のクラウドまたはサーバーでは、データを種類・グレードごとに管理・統制する必要があります。ハイグレードの重要データはリモート・アクセス・アカウントのアクセス権限及びリモート接続方式を厳格に制限しなければなりません。アクセスアカウントについては、リモートワークの実施と同時に合理性と必要性を精査し、不適格または失効したアカウントを適時に削除する必要があります。同時にシステムへのアクセス権限付与の合理性にも注意し、一時的に権限付与が必要なアカウントは厳格な審査・承認プロセスを経るものとし、適時に権限を取り消すことが重要です。リモート接続方式については、VPN 接続方式が推奨されます。VPN 接続ができない条件下では、HTTPS を採用してアクセスチャネルを暗号化し、同時に二段階認証方式を採用してセキュリティを高めることが最善の方法でしょう。こうした設定が難しい企業では、重要データが外部に流出しない方式でデータセキュリティを保障するため、リモートワークに必要な全てのデータはクラウドやサーバーに保存し、リモートワーク用の業務端末等へのデータの移動を禁止することをご提案します。

pwc 普华永道

2 つ目として、業務モバイル端末の使用に厳格な規則を設け、会社で登録管理していない個人用モバイル端末を使用した業務を禁止すべきです。同時に、リモートワーク用の業務端末で生成されるデータは暗号化して保存し、データ伝送時に暗号化データと暗号化パスワードには異なる方式を採用して、別々に伝送することを推奨します。

複雑なネットワーク環境を使用したリモートワークのリスク

リスクシーン:リモートワークは通常のオフィス環境とは異なり、ネットワーク環境がより複雑になります。4G や 5G、家庭用 WiFi、公共 WiFi 等、多様な接続手段が溢れています。接続先のネットワークが必ずしも信頼できるとは限らないため、悪意ある第三者にデータを盗み取られる(フィッシング)可能性は否定できません。また、企業ソフトウェアや個人ソフトウェア、インスタントメッセージツール、ネットワークメールボックス、ネットワークストレージやクラウドストレージ等、私たちは多種多様なアプリケーションプログラムからインターネット接続が可能です。信頼性が不確かなネットワーク環境におけるデータ露出の程度が高まることで、データ漏洩リスクが懸念されます。

対応策の提案:接触制限、業務環境の信頼性保障、ユーザーアクセス制限

データ生成・保存のソース管理に加えて、データの通信と使用をさらに管理・統制する必要があります。クラウド及びモバイル端末、並びにモバイル端末間のデータ交換については、データ通信の全過程・経路において HTTPS 暗号化を施し、データ通信中の漏洩または盗取を防止すべきでしょう。特に注意すべき点として、データ送信に使うメールまたはインスタントメッセージツールはその利用を厳格に制限し、企業のメールボックスや専用通信ツールを使用してデータ通信を行うようにし、無料メールや無料チャットを使用した企業データの取り扱いは厳禁にすべきです。モバイル端末については、接続するホットスポットや WiFi の安全性に注意が必要であり、信頼性が不確かなホットスポットや WiFi への接続は回避すべきです。特にパスワードが不要なネットワークは疑うべきであり、悪意のあるネットワークを利用することによる企業データの窃取の可能性を考え、慎重に行動すべきでしょう。

リモートユーザーのアクセス及び操作リスク

リスクシーン:リモートワークの運用において、ユーザーはシステムにリモートアクセスしてデータ処理やダウンロードなどをする必要があるため、ユーザーID 及びアクセス行為の信頼性確保が課題となります。正当なユーザーになりすました不正アクセスや通常の権限を超えたアクセス、大量のデータダウンロード、センシティブデータの変更・削除を代表とする異常なアクセスや処理等の攻撃により、重要データの大量漏洩または喪失につながる恐れがあります。

対応策の提案:豊富なモニタリング手段の用意、モニタリング頻度の引き上げ

企業はデータライフサイクルの全面的なモニタリングを検討すべきでしょう。クラウドやサーバー上のシステムアクセスといったユーザー行為に注意を払い、ユーザーID とその権限、アクセス時期、アクセス方式、アクセス内容、アクセス頻度、操作内容、データ通信内容等の情報を重点的にモニタリングし、特に短時間内における異なる地域からのログインや多数のユーザーログイン失敗後のログイン成功、ユーザーログイン後の短時間でのシステム上の各種フォルダへの高頻度のアクセス、ユーザーログイン後のデータの大量ダウンロードまたは変更等の行為には注意を払うべきです。また、システムのデータ通信状況(データタイプ、データ通信量、通信頻度等)を重点的にモニタリングする必要があります。リモートワーク用の業務端末においては、ユーザーの重要データに対する処理(データ保存場所、どの通信手段を使用したか、データの USB メモリへのコピー等)を重点的にモニタリングすべきです。さらに、ユーザーのパスワード強度と変更回数のモニタリングも強化し、ユーザーパスワードの暗号化を強化するとともにパスワード変更頻度を高め、パスワード有効期間を短縮する等の措置も効果的でしょう。データライフサイクルにおける重要なシーンのモニタリングを通じて、規定違反行為を適時に発見・是正し、データ保護能力を向上させることが重要です。

データ漏洩に対する緊急対策の管理

リスクシーン：保護の方法にかかわらず、リモートワーク環境下におけるデータの生成・保存・通信・使用はいずれも、通常のオフィス環境と比較してデータ・セキュリティ・リスクが高いです。したがって、企業は転ばぬ先の杖として、体系化された予防法及び緊急対策を事前に検討し、対応不備による損失拡大を回避すべきです。

対応策の提案：早期遮断、セキュリティホールの速やかな修復、バックアッププランの事前準備

潜在的なデータ・セキュリティ・リスクを発見した場合は、適時にそれを遮断して会社の損失を最小限に留めるべきです。具体的な措置として、3 つの分野への重点的な対応が挙げられます。1 つ目はシステムのセキュリティホールの補強及び修復です。リモートワーク環境下では、サーバー・オペレーティング・システム、ミドルウェア、データベース及び関連するオープンソース等のセキュリティホールのスキャン頻度を高め、サーバー及びモバイル端末のセキュリティホールについては適時に修復及び補強をし、ハッカーによるセキュリティの脆弱性を突いたデータの遠隔窃盗を回避する必要があります。2 つ目は異常操作行為の遮断です。上述の異常行為について、発見したリスクを適時に報告し、遮断できる管理・技術体制の構築が重要です。3 つ目はデータ漏洩後の緊急対応です。企業は前もって、リモートワーク環境下におけるデータ漏洩、データ窃取、データ誤操作等のリスクシーンごとに緊急対策プランを策定し、問題に適時に対処すべきです。

データセキュリティ向上のためには、新型コロナウイルス大流行の防止・抑制と同じで、企業と従業員の高い意識と行動が必要です。“ソース管理、アクセス制限、モニタリング強化、早期遮断”を通じて問題を適時に処理し、必要時には外部の専門機関や規制当局の援助を検討すべきでしょう。

このような困難な時期において、PwC 中国のセキュリティチームは企業、政府、ひいては社会全体に対し、新型コロナウイルス大流行下で直面するデータセキュリティ及びサイバーセキュリティ・リスクへの注意を促し、企業の業務再開を支援し、ともにこの難局を乗り越える所存です。

本稿の詳細ならびに PwC 中国のサービスについてのご質問等は、リスク・アシュアランス・サービスサイバーセキュリティ・プライバシー保護サービス部の専門家まで随時お問い合わせください。

ひと目で分かる リモートワークセキュリティ事項

PwCサイバーセキュリティ・プライバシー保護チームからのご提案

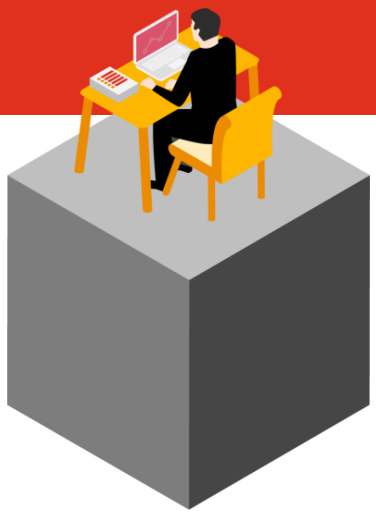
個人へのご提案

- リモートワークにおけるデータセキュリティ環境を確立するとともに、重要文書をそのまま送らない
- ビジネスに関するデータの送信または、共有にはインスタントメッセンジャーを使用しない
- ビジネスに関するデータのコピーまたは共有には、未承認の記憶媒体を使わない
- 安全性の確認できないまたはパスワードが不要のネットワーク環境には安易にアクセスしない
- 疑わしいリンクは安易にアクセスしない。また、疑わしいEメールは安易に開かない
- インターネット上の公共のプラットフォームや第3者にプライバシーに関わる個人情報を安易に公開しない
- モバイルデバイスの保管には最大限の注意を払い、常に安全な環境を確保する
- 正規のウイルス対策ソフトウェアを正しくインストールし適時にウイルスデータベースを更新する
- 信頼できるプラットフォームまたは公式サイトのプログラムを正しくインストールする
- サイバーセキュリティ規制当局に積極的に協力し、サイバーセキュリティ問題を速やかに報告する

法人へのご提案

- 従業員によるリモートアクセスの管理を強化し、適切なIDをもったユーザーのみがアクセスできるようにする。
- 従業員のモバイルネットワーク及びネットワーク使用に関する行動のモニタリングを強化する
- オペレーティングシステムのセキュリティパッチを適時に適用し、不正アクセスや悪意のある攻撃を防止する
- 定期的に重要なデータを別の場所で保管・バックアップし、データ喪失や破損を防止する
- リモートワークセキュリティ緊急対応チームを組織し、適時にサイバーセキュリティインシデントに対処する
- 従業員のサイバーセキュリティ意識を高め、安全な業務環境の構築を率先する

- ✓ リモートワークは便利な反面、セキュリティには注意が必要です。
- ✓ リスクを過小評価せず常に慎重な行動を心がけることが重要です。



お問い合わせ

ご質問等ございましたら、こちらのQRコードをスキャンし、必要事項をご入力ください。
皆様からのお問い合わせをお待ちしております。

pwc 普华永道

お問い合わせ

本稿に関するご質問等は下記担当者までお問い合わせください。

李睿
PwC 中国サイバーセキュリティ・プライバシー保護サービスパートナー
Tel：+86 (10) 6533 2312
Mail：lisa.ra.li@cn.pwc.com

趙元勛
PwC 中国サイバーセキュリティ・プライバシー保護サービスシニアマネージャー
Tel：+86 (10) 6533 5883
Mail：leo.y.zhao@cn.pwc.com

李赫
PwC 中国サイバーセキュリティ・プライバシー保護サービスマネージャー
Tel：+86 (10) 6533 5323
Mail：amber.li@cn.pwc.com

華北

姚皓軒
PwC 中国サイバーセキュリティ・プライバシー保護サービスパートナー
Tel：+86 (10) 6533 7576
Mail：ryan.h.yao@cn.pwc.com

華中

張俊賢
PwC 中国サイバーセキュリティ・プライバシー保護サービスパートナー
Tel：+86 (21) 2323 3927
Mail：chun.yin.cheung@cn.pwc.com

華南

黄景深
PwC 中国サイバーセキュリティ・プライバシー保護サービスパートナー
Tel：+852 2289 2719
Mail：kenneth.ks.wong@hk.pwc.com

翁澤鴻
PwC 中国サイバーセキュリティ・プライバシー保護サービスパートナー
Tel：+86 (20) 3819 2629
Mail：danny.weng@cn.pwc.com

JBD RA チーム

高橋翔太
PwC 中国日本企業部
アソシエイトディレクター
Tel:+86 (21) 2323 3294
Mail: shota.s.takahashi@cn.pwc.com

岡田真実
PwC 中国日本企業部
マネージャー
Tel:+86 (21) 2323 3910
Mail: mami.okada@cn.pwc.com

PwC 中国日本企業部ニュースレター

ご案内の通り、新型コロナウイルスの感染が拡大している状況にあり、且つそれが中国の経済成長や各業界に影響を及ぼすことが想定されている中、PwC 中国日本企業部として一丸となって取り組み、本ニュースレターを作成いたしました。

新型コロナウイルス感染症の影響によって、従来のオフィスワークに加えて、リモートワークが日常的な業務形態として定着しつつあります。一方、リモートワークの普及は利便性のみならずデータ流出のリスクも同時にもたらすことから、今回はリモートワークに関連するデータセキュリティ保護にフォーカスし、課題及び対応策についてご案内いたします。

日々状況が変化しており、今後の中国における事業環境の見通しが立つにはなお時間を要するものと考えますが、本ニュースレターが、中国事業に関わっておられる全ての皆様による現状の把握及び今後の中国及びグローバルの事業展開のご検討にあたって是非お役に立てればと思います。皆様におかれましては、ご健康と安全に最大限のご配慮をいただきたいとともに、現状が速やかに収束するよう心より祈念申し上げます。なお、本ニュースレターに関連してご質問やご相談がございましたら、吉田将文（パートナー）、山崎学（ディレクター）、渕澤高明（アソシエイトディレクター：リスク管理担当）もしくは私までご連絡いただければ幸いです。

PwC 中国 日本企業部統括代表パートナー

高橋 忠利

【連絡先】

高橋 忠利	toshi.t.takahashi@cn.pwc.com	携帯：139-0198-9251
吉田 将文	masafumi.g.yoshida@cn.pwc.com	携帯：150-0027-0756
山崎 学	manabu.m.yamazaki@cn.pwc.com	携帯：137-6187-2783
渕澤 高明	takaaki.ta.fuchizawa@cn.pwc.com	携帯：186-1662-8950

PwC 中国についての詳しい情報は次のウェブサイトをご覧下さい。

ホームページ: http://www.pwccn.com/home/eng/libraryindex.html

本ニュースレター及びウェブサイトに含まれる内容は一般的なものであり、個別案件に関する専門家としての意見を構成するものではありませんのでご注意下さい。

個別案件については、PwC の専門家に相談し、正式な意見を聞いた後で、貴社の対応を決定をされるようにお願い申し上げます。

筆者及び PwC は、上記記事に関して、貴社独自の判断の下行われた行動の結果についての、一切の責任を負いません。

また日本語版は中国語版ないし英語版を基にした翻訳で、翻訳には正確を期しておりますが、中国語版ないし英語版と解釈の相違がある場合は、翻訳の基となっている中国語版ないし英語版に依拠してください。

【防疫应变】
一图看懂
远程办公安全事项

新知
中国专业服务
二零二零年三月

摘要

疫情当前，远程办公成为兼顾员工健康和业务运转的最佳方式。但同时在远程办公过程中的信息和数据安全应引起企业和员工的高度重视。远程办公在开启了方便之门的同时，极大的复杂化了业务系统、重要数据和办公网络的操作场景，进一步扩大了信息安全风险。企业需要从技术架构、数据管理和员工行为等多维度，多领域的系统化统筹，以实现效率与安全的统筹兼顾。面临纷繁复杂的远程办公场景，我们用**一张图读懂远程办公安全要点，一句话理解数据安全保护重点。**

在远程办公操作安全保障的基础上，针对企业的数据安全，尤其是涉及企业核心商业价值的重要数据，还应围绕数据进行进一步的安全防护。在这里我们用一句话总结远程办公中数据安全的保护要点：**控源头、限接触、勤监控、早阻断。**

远程数据产生和存储风险

风险场景：远程办公环境下，企业重要数据的产生和存储更加分散，同时数据的访问和接入途径更加多样，由于办公需要，数据的访问权限需要进步一扩展等，这些均导致数据在生产和存储过程中的泄露风险极大提升。

应对提示：控源头，数据分级管理，严控数据源头。

在远程办公场景下，需重点管控两个数据源头。

一是企业云端或服务器端，需要对数据进行分类分级管控，对于高级别的重要数据，应严格限制远程访问的账户、访问权限及远程接入方式。对于访问账户，建议在进行远程办公同时，整理和排查当前账户的合法性，及时清除非法或失效账户。同时关注系统授权的合理性，对需要临时授权的账户，进行严格的授权审批，并在工作完成后及时收回权限。对于远程接入方式，应采用企业 VPN 接入办公。如不具备 VPN 接入条件，应采用 HTTPS 对访问通道进行加密，同时采用双因素授权的方式进行远程登陆。有条件的企业，我们建议对于重要数据采取数据不离线的工作方式保障数据安全,远程办公所有的操作的数据均在云端和服务端存储，禁止数据传下载至移动办公终端。

二是移动办公终端，应严格限制移动终端的使用，禁止使用未经企业注册或登记的个人移动设备办公。同时，对移动办公终端所产生的数据进行加密存储，并在数据传输时，将加密数据和加密密码采用不同方式分别传输。

pwc 普华永道

远程复杂网络环境风险

风险场景：远程办公不同于集中办公，其所处的网络环境更加复杂，

4G/5G 网络热点、家用 WIFI、公用 WIFI 等，接入网络变得不可信任，可能导致利用钓鱼网路的中间人窃取数据。终端接入种类多样，应用软件的使用更加灵活，企业软件、个人软件、通用即时通信软件、网络邮箱、网盘和云盘等应用程序的使用，使得数据更多的暴露在不可信的环境中，导致数据泄露风险。

应对提示：限接触，保障环境可信，限制用户接触。

在控制数据产生存储源头的基础上，还需要对数据传输和使用进行进一步管控。对于云端和移动终端，以及移动终端之间的数据交互，应对数据通信全链路进行 HTTPS 加密，防止数据在传输中泄露或被窃取。另外需要特别注意的是，对于传输数据的邮件或及时通信工具，需要严格加以限制，应使用企业邮箱和专用通讯工具进行数据传输，禁用公共邮箱和通用及时通信工具传输企业数据。对于移动终端而言，还需要注意接入的网络热点和 WIFI 安全，不要接入未知的网络热点和 WIFI 处理办公数据，尤其是无需密码就可直接登陆的网络，谨防非法网络窃取数据。

远程用户访问和操作风险

风险场景：在远程办公场景下，用户需要远程访问系统并处理或下载数据，用户身份和访问行为都变得更加不可信，假冒合法用户访问，用户越权访问，批量数据下载、高敏感数据的修改和删除等异常访问和操作等攻击行为，可能导致重要数据的大批量泄露或不可用。

应对提示：勤监控，丰富监控手段，提升监控频率。

企业应考虑对数据生命周期进行全面监控。在云端和服务端，重点监控访问系统的用户行为，包括用户身份、授权范围、访问时间、访问方式、访问内容、访问频次、操作行为和数据传输内容等信息，尤其需要关注短时内的异地登陆，多次的用户登陆失败后的登陆成功，用户登陆后短时间的系统各页面间的高频访问，用户登录后的数据批量下载或修改等行为；另外还需重点监控系统接口的数据传输情况，包括数据类型、数据传输量、传输频次等。在移动办公终端，重点监控用户对重要数据的操作行为，包括数据存储位置，通讯工具传输行为，数据 U 盘拷贝等。另外还需提升对用户密码强度和修订次数的监控，建议在远程办公期间，加密用户密码复杂度的要求，同时增加更换密码频率，进一步缩短密码有效期。通过对数据生命周期重点场景的监控，及时发现和纠正违规行为，提升数据保护能力。

数据泄漏的应急管理

风险场景：无论如何防护，远程办公环境下的数据的生产、存储、传输和使用，都会相比于集中式办公环境进一步增大数据安全风险。因此企业需要未雨绸缪，提前考虑体系化的预防和应急管理，避免应对不当导致损失的进一步扩大。

应对提示：早阻断，及时修复漏洞，提前部署预案。

一旦发现可能的数据安全风险问题，需要及时阻断以降低企业损失。具体措施建议重点关注三个领域。一是系统安全漏洞的加固和修复。在远程办公环境下，需要加强对服务器操作系统、中间件、数据库和相关开源组件等安全漏洞的扫描频次，对于服务端和移动终端出现的安全漏洞，需要及时进行修复和加固，避免黑客利用漏洞远程窃取数据；二是异常操作行为的阻断，针对上一小节中的异常行为，从管理和技术层面加强建设，针对发现的风险及时告警和阻断；三是数据泄露后的应急处置，企业需要提前制定应急预案，尤其是远程办公环境下，数据泄露、数据窃取、数据误操作等风险的场景化预案，对问题进行及时响应和处置。

数据安全保护如同疫情防控，需要企业和员工充分重视并积极行动，“控源头、限接触、勤监控、早阻断”发现问题及时处置，必要时寻求第三方专业机构或监管机构的帮助。

在这个特殊的时期，普华永道安全团队希望向我们的合作伙伴乃至社会公众强调疫情下面临的数据安全和网络安全风险，进而更加稳健地恢复工作及生活，携手并进，共渡难关。

如需了解更多关于本专题的详情，请与我们风险及控制服务网络安全与隐私保护服务部的专家联系：

一图看懂
远程办公安全事项

普华永道网络安全与隐私保护团队温馨提示

个人提示

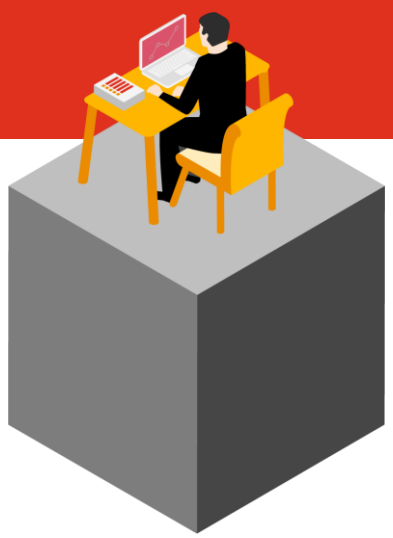
- 不要明文传输重要文件，保障远程办公数据安全
- 不要使用即时通讯工具传输或分享商业数据
- 不要使用非授权存储介质拷贝或分享商业数据
- 不轻易接入未知或无需密码的网络连接环境
- 不轻易点击可疑链接，禁止或谨慎点击可疑电子邮件
- 不轻易向网络公共平台或第三方提供个人敏感信息
- 谨慎保管移动办公设备，时刻确保处于安全环境
- 正确安装正版杀毒软件并及时更新病毒库
- 正确安装来自合法平台或官方网站的应用程序
- 积极配合网络管理部门，发现网络安全问题及时上报

公司提示

- 加强员工远程网络访问控制管理，确保合法身份接入
- 加强针对员工使用移动办公设备及办公网络的行为监控
- 及时推送操作系统安全补丁，防止非法入侵或恶意攻击
- 定期做好重要数据异地备份，防止数据丢失或损坏
- 建立远程办公安全应急小组，及时响应网络安全事件
- 加强员工网络安全意识培养，科学倡导绿色网络办公

远程不停工，安全不轻松 ；

风险无小事，提示记心中 ！



联系我们

如果您有任何其他疑问，欢迎您扫描左侧的二维码填写问卷告诉我们。
我们期待收到您的反馈！

pwc 普华永道

与我们谈谈

如需了解更多本专题的相关详情，请联系：

李睿
普华永道中国网络安全与隐私保护
服务合伙人
电话：+86 (10) 6533 2312
邮箱：lisa.ra.li@cn.pwc.com

赵元勋
普华永道中国网络安全与隐私保护
服务高级经理
电话：+86 (10) 6533 5883
邮箱：leo.y.zhao@cn.pwc.com

李赫
普华永道中国网络安全与隐私保护
服务经理
电话：+86 (10) 6533 5323
邮箱：amber.li@cn.pwc.com

北区

姚皓轩
普华永道中国网络安全与隐私保护
服务合伙人
电话：+86 (10) 6533 7576
邮箱：ryan.h.yao@cn.pwc.com

中区

张俊贤
普华永道中国网络安全与隐私保护
服务合伙人
电话：+86 (21) 2323 3927
邮箱：chun.yin.cheung@cn.pwc.com

南区

黄景深
普华永道中国网络安全和隐私保护
合伙人
电话：+852 2289 2719
邮箱：kenneth.ks.wong@hk.pwc.com

翁泽鸿
普华永道中国网络安全和隐私保护
合伙人
电话：+86 (20) 3819 2629
邮箱：danny.weng@cn.pwc.com

有关普华永道的更多具体信息，请访问我们的主页，

主页链接：http://www.pwccn.com/home/eng/libraryindex.html

我们提请您注意的是，本新闻通讯和网站中包含的内容仅为一般性内容，并不构成针对个别案件的专家意见。

对于个别案件，请您咨询普华永道专家，并征询正式意见后，再决定贵公司的应对措施。

作者和普华永道对您自行决定就上述文章采取措施的结果不承担任何责任。