MI Insurance Brokers Limited

CHUBB®

網絡保險 保障企業數據更容易
Cyber Insurance made simple

Text: Tiffany Lung

要防範網路罪犯接觸你的資金和資料數據，聽起來似非常複雜，但其實只要實行幾個簡單的措施，便可有助保障你的業務。

許多董事或行政人員錯誤認為公司規模太小、無足輕重，因此不值得花費資源來防範網絡罪行。在毫無防禦措施下，不法分子可以利用精密的軟件在網絡裏尋找企業作攻擊目標，然後破壞其生產力及商譽，甚至使之虧損。

數據顯示受到網絡攻擊的中小企受害者當中，高達 93% 表示業務遭受嚴重負面影響。而最令人憂慮的是，超過 30% 受害者的商譽長遠受損。以近日所發生之資料外泄事件為例，受影響的企業不單商譽受損、業務受阻，更要面對六位數字的勒索金額、有可能被政府罰款及受影響客戶興起的訴訟。

那麼，甚麼是常見的網路犯罪模式？以及有甚麼最佳及最具成本效益的防範措施呢？

攻擊實體電腦系統

一般企業對個人電子設備（如筆記型電腦、USB 記憶棒等）沒有作出周全保護，因此當授權者使用這些設備連接到僱主的電腦網絡後，就會危害企業內部的伺服器及/ 或硬件。

定期舉辦網絡安全實踐工作坊是行之有效的方法，鼓勵員工採取防禦措施，令不法者無法入侵其筆記型電腦、USB 記憶棒和其他個人設備。另外，設定限制部份員工存取敏感資料，亦是個萬全之策。

身份驗證及權限攻擊

存取儲存的資料數據時，授權者重覆使用保安程度低的密碼（例如「123456」或直截使用「password」），不法者就容易入侵和破壞企業的系統了。此外，心懷怨憤的員工也可能蓄意破壞程式、甚或與未獲授權的同事共用敏感的資料數據，造成所謂「偷擁權限」。

最快捷簡單解決上述問題的方法之一，就是規定員工需使用及定期更換結合英文字母、數字及符號的密碼。而每次員工離開公司以後，密碼會自動更換，帳戶亦會被設定為停用。

惡意網絡內容攻擊（勒索軟件）

網絡罪犯利用惡意軟件，例如：「蠕蟲」或「木馬程式」，從外面把企業的資料庫加密或封鎖，再「兜售」非常昂貴的解密鑰匙。「網路釣魚」亦是另一種常見的網絡攻擊程式，員工只要打開看似毫無詭詐的電郵連結，惡意軟件就會自動下載到電腦內。

要排除潛在問題發生，最好定期更新系統，並且要密切監察系統和使用者。另外，企業亦可從可靠的來源下載較先進的保安系統，加強保護電腦系統。

阻斷服務（DOS）攻擊

分散式 DOS 攻擊是人為攻擊，利用龐大網上流量癱瘓企業網站，使之無法正常運作。非蓄意的 DOS 攻擊則可源於單一服務點的技術故障，原因是過度依賴沒有做好多重保護措施的系統或服務供應商。

要應付此類事件，只要設立網路事故應急計劃，便可縮短應變時間，甚至解決潛在問題。

購買網絡保險

企業要更周全地保護資訊科技資產，最後一個步驟就是購買網絡保險。網絡保險不但能夠將業務中斷、資料損失及重置、調查、危機溝通、違反私穩條款、罰款及其他法律程序處理而引致的財務損失轉嫁至保險公司，也讓企業在發生上述事故時得到保險公司及其合作夥伴提供的解決方案，令業務儘快回到正軌。購買網絡保險不單令您安心，所需要的成本肯定遠比受到網絡攻擊後停業所花的費用為低。

公司簡介

MI 保險顧問有限公司 (MI Insurance Brokers Ltd) 歷史悠久，致力為客戶及企業提供一站式專業保險中介服務，擅於安排特別的保險產品，包括馬匹、高端醫療保險、私人收藏品、遊艇、電腦網絡、綁架勒索保險、董事和行政人員責任保險等。MI 保險顧問團隊會以其豐富經驗和專業知識，協助客戶挑選最實惠和最合適的保險方案。若想獲取更多資訊或對保險有疑問，請遊覽網站 www.mibins.com 或電郵 enquiries@mibins.com 或致電 2511 2775。

免責聲明

Although stopping cyber criminals from accessing your funds and data may seem dauntingly complex, there are several simple and affordable ways your business can help protect itself…

Unbelievably, many businesses wrongly believe they're too small and globally insignificant to justify the cost of protecting themselves against cyber criminals. With no defences to stop them, the crooks use sophisticated software to scan the web for companies whose productivity, profitability and reputation they then destroy.

Alarmingly, 93% of SME victims of such attacks report suffering severe negative consequences for their businesses. Perhaps most worrying of all, over 30% of victims apparently experience lasting damage to their reputation. Take the recent data leakage incidents. Besides losing credibility and sales due to service disruptions, affected businesses face the threat of six-figure ransom demands as well as possible government fines and lawsuits from disgruntled customers.

So what are the most common forms of cybercrime and, more importantly, what are your company's best and most cost-effective safeguards against them?

Attacks on Physical Systems

Enterprises' internal servers and/or hardware are compromised by poorly protected personal electronic devices (e.g. laptops, USB memory sticks, etc) authorised users' connect to their employers' computer networks.

Regularly arranging safe practice workshops is a proven way of encouraging staff to prevent crooks from corrupting their laptops, USB memory sticks and other personal devices. Restricting access to sensitive information to senior-level staff is another sound policy.

Authentication and Privilege Attacks

Authorised users' repeated use of weak/easily hacked passwords (e.g. '123456' or unbelievably 'password' itself) when accessing stored data mean it's absurdly easy for crooks to cripple companies' systems. Resentful staff may also deliberately sabotage programs or share sensitive data with unauthorised colleagues via a practice known as 'privilege creeping'.

One of the quickest and easiest ways to avoid the above problems is to insist staff use and regularly change strong passwords combining letters, numbers, and symbols. Passwords should also be changed automatically and accounts rendered inactive each time an employee leaves the company.

Malicious Internet Content ('Ransomware') Attacks

Cyber criminals use malicious malware/software such as worms and Trojans to externally encrypt and lock an enterprise's database before 'selling' them a costly decryption key. 'Phishing' is another common web application attack via which employees are emailed innocent-looking links that automatically download malicious software onto their computers when opened.

Regularly updating older systems, that are especially vulnerable to increasingly sophisticated hacking techniques, and closely monitoring both systems and users are excellent ways of eliminating potential problems. Enterprises can also download the latest security software from trusted sources as a safeguard to their systems.

Denial of Service (DOS) Attacks

Distributed DOS attacks are human-initiated and disable enterprises' sites by flooding them with so much online traffic they stop functioning. Non-deliberate DOS attacks result from single point-of-service technological failures caused by over-dependence on systems/service providers with insufficient redundancy protection.

Implementing a Cyber Incident Response Plan and forming an emergency team made up of internal staff and outside service providers will accelerate your company's ability to respond to and resolve such problems.

Purchase Cyber Insurance

The final step for enterprises wishing to more fully protect their IT assets is to purchase cyber insurance. Often pre-packaged with several of the solutions outlined above, cyber insurance provides protection that will quickly get your business back on track. Available cover includes reimbursement for expenses resulting from business disruption, data loss and restoration, investigations, crisis communications, breaches of data privacy, fines/penalties and other legal proceedings. Ultimately, the cost of such peace of mind will always be far less than the expense involved in shutting down a business in the wake of cyberattack.