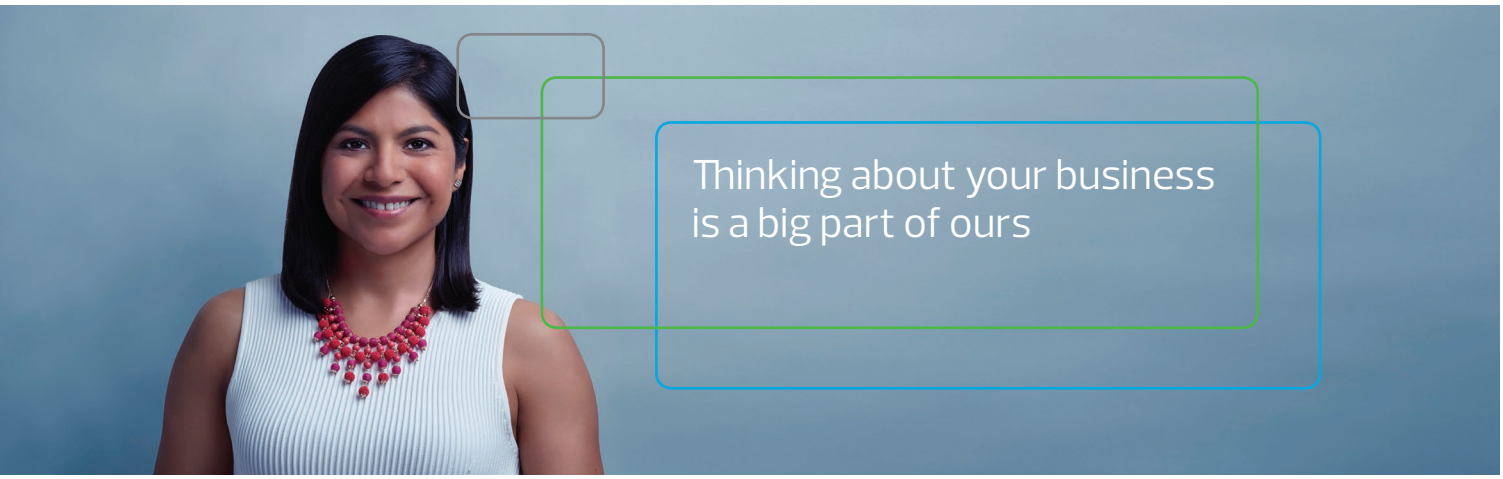


MAINTAINING DATA SECURITY: TIPS FOR FRANCHISORS AND FRANCHISEES

Michael Shatter, Risk Advisory Services

Running a business in the digital age means that, on top of the required operational and customer delivery focuses, there is another layer of complexity in the form of ensuring data security is strong within your business. As online channels provide more opportunities to build customer loyalty and offer increased choice in how customers interact with the business, there are significant benefits to be gained. However, the security risks inherent in an online approach also increase correspondingly.

A business doesn't have to do all, or even most, of its sales and marketing online to be vulnerable to data breaches. Given the high level of connectivity experienced today by just about every conceivable business, it's not an exaggeration to say that every business is a potential target for cyber criminals. Just as businesses needed to focus on disaster recovery and business continuity in the past, today it's just as important to focus on data security and incident response processes in case the business experiences an attack that results in a data breach. To fail to do so is to open the business up to significant risk, much of which could be avoidable with the right cyber security approach in place. For example, most businesses will be subject to the recent Notifiable Data Breach Scheme, where there is a requirement to consider the need to report a breach notification to the Privacy Commissioner.

The potential fallout of a cyber security attack goes beyond simple business disruption, although that's definitely a highly likely aspect of being attacked. If the attack is focused on sabotage, such as a ransomware attack, denial of service attack, or another malicious attack to obtain what is otherwise considered as confidential data, then the business will be impacted and may be unable to operate until the attack is contained and recovered from.

It's important to note that franchisees can be a particularly attractive target for cyber criminals because they represent potential access to a large network of businesses. Depending on the connectivity between a franchised business, a franchise system that provides common tools to each business can be affected by a breach of just one of those businesses. Savvy cyber criminals may be able to use that access to infiltrate the entire franchise network, spreading the attack beyond a single business.

In many cases, cyber criminals target franchised businesses to access both valuable personal identifiable information and financial payment details that these businesses keep on file regarding their customers. Cyber criminals attempt to sell this information for money, so an attack aimed at stealing information is relatively common as you would read in the headlines so often these days. A recent example is the data breach associated with the US hotel chain Marriott.

Cyber attacks in which customer information is compromised can present a significant problem for both franchisors and franchisees because one of the most damaging consequences of such an attack relates to how it affects the brand's reputation and confidence in the brand. This creates an issue for the affected franchisee, the franchisor, and other franchisees in the network who may find that their reputation is similarly affected as collateral damage merely by association.

The responsibility for cyber security in a franchise arrangement likely falls almost equally on the franchisor and the franchisee. Certainly, franchisees should consider it a part of their due diligence to thoroughly investigate, discuss, and agree on how to manage cyber security as part of the franchise agreement. At the same time, franchisors should design their systems and those sold as part of the franchise licensing process to be secure and robust, especially when left in the hands of franchisees who may look at security requirements differently.

This starts at the very beginning of a negotiation. Along with conducting due diligence regarding the franchise's finances and operations, potential franchisees should ask pointed

RSM

questions regarding the security measures and agreements in place to protect the business in case of a breach.

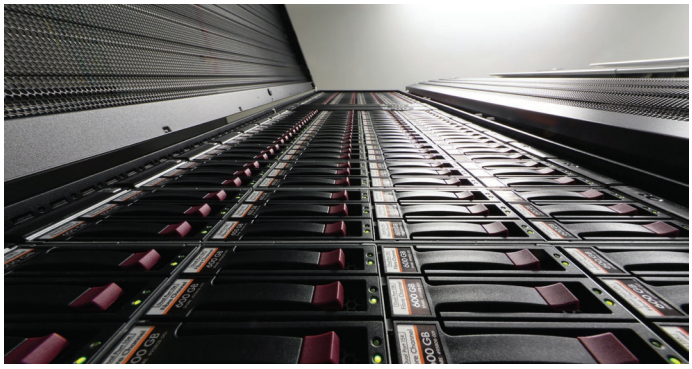
If the franchisee is responsible for setting up their own systems, they need to think carefully about how they'll secure their data and how to maintain a computing environment that they have confidence in to maintain data integrity. This can be a challenge for an entrepreneur whose main interest lies outside the IT environment. Potential franchisees without significant IT and cyber security knowledge and experience should, therefore, seek to partner with an appropriately-qualified advisor or security provider to ensure their systems are set up properly from the start.

It's a good idea for both the franchisee and the franchisor to insist on having a cyber security component in the franchise agreement. This should set out who is responsible for what when it comes to cyber security, along with what recourse either party may have if the other party fails to meet their obligations. For example, if there's an attack on the head office that affects an individual franchisee, would that franchisee be entitled to reimbursement of the resulting costs? Setting these conditions in the original agreement can help avoid issues down the track.

It makes sense for franchisors to insist that franchisees maintain a high level of security. Likewise, franchisees can gain significant peace of mind by knowing that the franchisor is obligated to assist in the case of a security breach. Sitting alongside this is the consideration of cyber insurance. For franchisors, cyber insurance should be a mandatory requirement that franchisees have in place. However, franchisors may be in the best position to work with insurers and help franchisees with the necessary policies.

As a result of the legal responsibilities associated with a data breach, there need to be formal processes in place to deal with a security breach. As part of the Australian government's notifiable data breaches scheme (NDBS), businesses may be required to report data breaches that compromise personal information. Reports may need to be submitted to the Office of the Australian Information Commissioner (OAIC) and to the affected person or people. There are specific processes around this that must be followed; it's in a franchisor's interest to put policies in place for franchisees to follow in case of a breach. This makes it simpler to comply with NDBS requirements and it also helps protect the franchisor's reputation and revenue stream by presenting the business as a capable, security-focused organisation.

Insisting on collaboration with the franchisee also lets franchisors retain an element of control in case of a breach. Since a breach would affect both parties, it's valuable to ensure both are involved in mitigating the fallout. Strong collaboration can help contain the attack, recover quickly, and protect against future attacks. This all needs to be codified within the franchise agreement so there are no questions or confusion if an actual breach occurs. Any such rules or processes around how to respond to a data breach should take into account not just the reputational damage



from the breach itself, but also the reputational effect of how the breach is managed. For example, organisations that sit on news of a breach and don't try to notify their customers are often identified at a later date as not having acted appropriately and in the spirit of the NDBS, which could result in reputational damage that is greater than had the organisation been diligent and transparent about the breach to start with.

Furthermore, with attacks such as ransomware not likely to slow down anytime soon, it's important for franchises to decide on a universal response. For some organisations, the path of least resistance is often to pay the ransom, especially since the amount is usually quite affordable, and regain access to the data. However, there are moves within some governments to make ransomware payments illegal as it is not known where the payments are going and paying a ransomware may be considered a contribution to illegal activities such as terrorist organisations.

During the due diligence process, franchisees should ask questions about what systems are provided, how they're protected, and who is responsible for securing them. This is because there is, of course, a cost to securing systems. This ranges from the cost of anti-virus or anti-malware tools to the cost of ongoing security testing and remediation. It's essential for franchisees to understand these costs upfront, just as they would any other business-related costs.

Given the severe consequences of a major breach, franchisors should consider shouldering a significant proportion of responsibility for helping franchisees set and maintain a strong security posture. If the franchisor isn't responsible for providing any specific systems to the franchisee, it may be worth considering providing training for franchisees who may not be au fait with security.

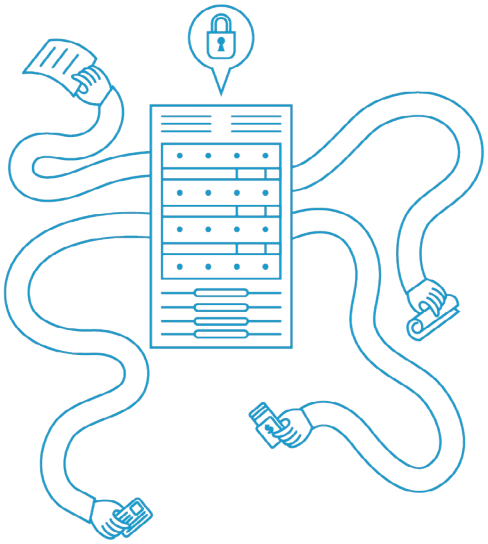
This can help protect the value of the franchise license. There is merit in the logic that if the franchisor is controlling the process, then they can protect the brand, goods and/or services being franchised rather than depending on the individual processes and procedures of franchisees in no coordinated manner.

RSM

Most franchisors provide comprehensive and, often, ongoing training regarding how to run the material aspects of the business. For example, a retail food outlet will provide extensive training on how to prepare the different menu items. However, franchisors rarely provide training in how to maintain the integrity of data in the business systems. This should become a routine part of franchisee on-boarding, and backed up with refresher training conducted at least annually.

Depending on the details of the franchise agreement, it may be desirable for the franchisor to go on-site to provide assistance with establishing systems and secure environments. Doing this from the outset can help build a culture of security within the organisation, which is arguably just as important as having the right technology in place.

Most franchised businesses have physical security measures in place such as locked doors, password-protected cash registers, and staff-only areas. How well these areas remain secure depends, to a large extent, on the security-consciousness of employees. If team members leave doors unlocked, share their passwords with others, and pay no attention to who is actually in the staff-only area, then the business is likely to experience security breaches such as theft. By contrast, if team members take their security responsibilities seriously, then the risk of unauthorised access will diminish accordingly.



The same is true of cyber security. All staff members need to be aware of their responsibilities and the role they can play in keeping the business secure. This includes casual workers as well as full-time or management staff.

Workers aren't the only potential weak link in the cyber security chain. Third-party suppliers can also impact security. Just as there needs to be diligence in regard to the acquisition and transactions associated with franchises, it's recommended that the appropriate diligence is also exercised with how the business contracts with suppliers that are critical to the survival of the franchise. It's important to make sure those agreements reflect requirements for them to provide appropriate level of security to be dependable.

Businesses that take a nonchalant approach to security and privacy will be left behind by those that can demonstrate to a learning customer base that security and confidentiality is a critical piece of doing business on the internet these days. Cyber security is just a part of doing business in today's world; it's no longer a nice-to-have but a must-do for franchises looking to be successful.

For further information, please contact:
Michael Shatter
Partner, Risk Advisory
T 03 9286 8000
E michael.shatter@rsm.com.au