GRANGEBURN
PROFESSIONAL
SERVICES

White paper

Small Business Security
for
Small Business Owners

GRANGEBURN
PROFESSIONAL
SERVICES

Contents:

1. **OVERVIEW**
2. **COMMON THREATS TO SMALL BUSINESSES**
3. **DATA PRIVACY ISSUES IN SMALL BUSINESS**
4. **RISKS OF TRADITIONAL MANAGED SERVICES PLATFORMS**
5. **CONCLUSION**
6. **ABOUT GRANGEBURN PROFESSIONAL SERVICES**

Overview:

Small businesses are increasingly reliant on technology. While the cost of purchasing and maintaining the infrastructure required to support business technology is decreasing, the potential risks associated with electronic data storage and processing is increasing dramatically. With the rise of “cloud” services, employees utilising their own devices to perform their jobs, and the public’s increasing awareness of data privacy issues, it is becoming a necessity for small businesses to ensure the security and integrity of their data.

Small businesses are also increasingly becoming the target of threats that may have been previously been targeted at only larger organisations. This comes mainly in the form of ransomware, which encrypts entire computers, servers and networked file shares, and attempts to extort payment in exchange for the ability to retrieve this data. Traditional threats, such as destructive viruses and worms, are also still prevalent, and still need to be addressed and protected against in any size business.

This whitepaper intends to point out some of the key areas on which small business owners can focus to increase the security of their data, whilst also keeping in line with the goals of their business and maximising revenue.

Common Threats to Small Businesses

Ransomware

Ransomware is malware that encrypts data, with the aim of extracting payment from the infected user in exchange for decrypting their data.

This malware is delivered in malicious email attachments, via social engineering, and through targeted attacks, as well as an increasing number of additional vectors.

Due to the rapid pace of evolution of this malware, it is very difficult to implement a set-and-forget mitigation for ransomware. The most effective way to mitigate this risk to to ensure timely and valid backups, and monitor network activity for malicious traffic.

Banking Malware

Banking malware is malware that intercepts and/or modifies electronic traffic between the user and the bank. In some cases, this malware hides the true account balance, whilst transferring money to the malware creators.

This malware is delivered in malicious email attachments, from malicious websites, and via social engineering, as well as other attack vectors.

This malware can be mitigated by ensuring any financial transactions are performed in a secure environment only, as well as making sure transactions are checked against bank statements.

Improper or Non-Existant Backup Solutions

Without a proper backup solution, there is no way a business can be certain that they can recover in the event of a failure or security incident. There is also no way that the business can recover any data that they may legally be required to keep.

Improper or non-existent backup solutions usually come from a mis-understanding of the way that backups should work and how they should be performed.

One of the leading recommended backup strategies is the 3-2-1 backup strategy. This is comprised of having 3 complete copies of your data, 2 of which are on different devices or mediums, at least 1 of which is offsite.

Unauthorised Data Storage Locations

Unauthorised data storage locations can be anything from staff USB drives that are removed from the business premises, to cloud services such as Dropbox, OneDrive, personal Google Drive accounts and iCloud. This can lead to loss of important data, either maliciously or inadvertently.

The storage of data in unauthorised locations usually comes about by employees being frustrated by a lack of easy solutions for sharing and manipulating data. They may not realise that they are leaking data from the business when the put a document on Dropbox to finish off at home, or when the grab the USB they have in their bag and copy a clients folder from the server to it for delivery to the client.

Mitigation of this risk can be achieved by giving the employees an easier way to manipulate and share data. This can be done by implementing solutions that allow secure access to data remotely, in a way that can be properly audited and is easy to use. Solutions such as Dropbox for Business, SharePoint and Google Apps for Business are good some of ways that this can be achieved.

Phishing and Email Fraud

Phishing emails are emails that pretend to be from a legitimate source that is asking for information, which then redirects you to a phoney site that requests that information. This information is then stored by the attacker for use with the legitimate site. Common email topics are financial based sites, such as PayPal, large banks and other financial institutions

Email fraud can be general or targeted. A common form of email fraud is an email pretending to be from a CEO or other person with authority to allow financial transactions to third parties. These are usually a request to pay a sum of money to a third party.

Phishing and email fraud come in the form of emails from either a non-legitimate source pretending to be a legitimate source, or, in the case of a more targeted attack, a compromised email account. Attackers who target a company are also likely to register a domain name similar to the target business. As an example, Grangeburn Professional Services' email domain is @grangeburn.com.au, and an attacker may register @grangeburn.net or @grangburn.com.au in order to trick the recipient into trusting the sender. More general phishing attacks are usually part of a campaign by malicious groups to harvest a large number of credentials.

To help prevent employees receiving these emails, a good spam filter is recommended, as well as continuous monitoring and maintenance of this filter.

Data Privacy Issues in Small Business

Do I Need to Care About Personal Information?

Legally, a small business as defined by an annual turnover of less than $3,000,000 in a financial year does not need to comply with the Privacy Act, unless you are classified under one of the exceptions. If you are not sure if you are legally bound to comply with the privacy act, the OAIC website has some guidelines about what sort of business is legally required to comply.

A small business can opt in to the Privacy Act, and in fact the OAIC strongly encourages small businesses to do so, in order to ensure that no personal information is compromised.

Regardless of whether or not you are required to or choose to comply with the Privacy Act, your businesses client data should remain protected at all times. The Privacy Act gives a good framework for this, and poses some interesting challenges for situations that you may not have considered. By building this security of client data into your business practices, you will increase the level of trust that your clients have in your business.

Additionally, attackers are becoming increasingly aware of the value of personal information stored in small business databases. This is exacerbated by the fact that small business security is traditionally less than large corporations due to budget and time constraints.

Consumers are also becoming more sensitive to what personal information is stored and how it is stored. A recent example of a high profile case where personal information was leaked is the theft of personal photos from celebrities Apple iCloud accounts. This was not due to any breach of security, however it is an example of why consumers are aware of the importance of the security of their personal information.

Why is Data Privacy Important?

Government and commercial entities are making big pushes to ensure that personal data is secure and safe from compromise. For example, the *Australian Privacy Principles* (APP) in the *Privacy Act 1988* outline how small businesses must handle, use and manage personal information. The *Privacy Act* is available from the Office of the Australian Information Commissioner (OAIC) website.

In addition to this, your clients will be becoming much more aware of how their data is used, and a lot of clients will be sensitive to the fact that they are entrusting you with their and their clients personal, business and financial data. This can impact the trust that is built between your business and its clients.

What Can Attackers Do With my Business Information?

The most common information that is sought by attackers is financial information that can lead to a direct transfer of money to their own bank accounts. Client credit card information is one of the most common pieces of personal information that can provide a quick turn around to this end. An attacker can choose to use the stolen credit card information to perform fraudulent transactions for their own benefit, or to sell a database of credit card details on the black market.

Other information that attackers look for is anything related to online accounts. This can be in the form of email addresses, account numbers and related passwords for these items. If you are storing your clients passwords, you should make sure that they are stored in a properly encrypted database, as your clients may re-use these passwords on multiple sites. This means that if you store the client email address and password, their account can be very easily compromised in the event that your business is also compromised. This can lead to your clients network or services being compromised. An example of this is the Target breach in America, in which attackers gained access to the contractor that ran the air conditioning system at Target stores. They then used access to the contractor to gain access to the Target internal systems, and from there were able to infect the Point Of Sale terminals at Target stores with malware. This malware was programmed to steal credit cards, and as such, caused a great deal of financial impact to both Target and their contractor, as well as Target’s customers.

What Can I do to Protect Against These Threats?

Proper vetting of any system that is going to contain client information before putting it into production is the best way to protect against data breaches. This can be achieved by thoroughly testing the system prior to a full scale implementation, using dummy data. These tests range from making sure the software will be appropriate for your environment, through capacity planning and to proper security testing.

It is recommended that a small business connects with a trusted partner to perform this vetting, as it is generally beyond the skill set of a single IT worker to perform, and can require more resources than would normally be available in a small business IT department.

Risks of Traditional Managed Services Platforms

Why not Managed Services?

Traditionally, Managed Service Providers (MSPs) have been seen as a wise investment, especially in small businesses. The main reason MSP value propositions are so attractive to owners and managers in small business is the ability for a MSP to provide a fixed price contract, which covers all of the businesses requirements for IT, generally at a price point that can't be achieved by having in-house IT staff. MSPs also sell themselves as having more expertise, and in more areas, than a single IT staff member, as they have access to multiple staff members and vendor expertise in their organisation.

MSPs can also provide a "platform". This usually entails bundling all of their services in to one package, including help desk support, pro-active maintenance of server and network services, remote access clients, anti-virus and backup solutions. As part of this platform and support model, the MSP will usually require that a client has a standardised hardware and software model, in order for the MSP themselves to cut costs for supporting this hardware and software.

While all of the above points are very valid, and can make for a stable, safe and cost effective environment, it can introduce some much more concerning issues down the track.

Business Data Retention and Backups

The most critical part of a business is the businesses data. Without business data, whether that be Customer Relationship Management (CRM) data, accounting data, or Intellectual Property, if this data is lost or compromised, there is a good chance that there will be significant operating and financial impact to the business.

There are also legal requirements with what financial data needs to be kept, and for how long. According to the Australian Tax Office (ATO), your records must explain all transactions, be in writing (electronic or paper), be in English, and be kept for five years, with some information required to be kept longer. Failure to keep this data can lead to penalties to the business.

A good backup solution is a standard service for a MSP, and as such, MSPs will often bundle a backup plan into their service. These backup plans allow the MSP to back up the businesses data locally and offsite, depending on the backup solution provided. This gives the business a good set of data to recover in the event of a catastrophic failure. However, MSP backup solutions often overlook the fact that the business is required to retain these backups for a long period of time.

A good example of data not being retained would be when the business relies on a MSP to provide a cloud backup solution, which backs up data to a private or public cloud service. These services are rebranded by the MSP as their own service, however the hardware and software are actually subscription services provided to the MSP by the upstream provider. This means that the business relies on the MSP to maintain that subscription, and the upstream provider (that the business has no visibility of) to continue to provide this service to the MSP. This also means that the MSP has to continue to do business with the upstream provider and, in the event of a move to a different upstream provider, have a way to move the data to the new provider, in a way that does not affect business data.

Another example would be if the business chooses not to engage the MSP at the end of a contract. In this case, the business would need to make sure that the MSP will be able to provide a copy of the data, in a usable form, to the business. Without the ability to do this, the backups may as well not exist, rendering the backup solution ineffective. To reiterate, it is up to the business, not the MSP, to comply with the legal requirements for data retention and backups. MSPs will have insurance in the event that they are not able to recover data, however this is small consolation if you lose all of your business data. The MSP is also likely to write a clause into the contract stating that they are limited in their liability in the event of catastrophic failures.

MSP Platforms

As stated above, MSPs can provide platforms for the business. This is great for the MSP, as their support staff can easily connect to any client and be sure that they know the systems that they are supporting.

The danger in this is that the client is forced in to using something that isn’t specifically tailored to their environment. This can create frustration for end users, as there is no flexibility for the business to customise this platform to suit their needs. This may not have an immediate, noticeable impact on business performance, however small business needs change rapidly to meet market demand, and as such, small businesses need to be able to alter the way they operate, without having to wait for the end of a contract to re-negotiate the MSP offering to suit them.

Software and Hardware Ownership

MSPs provide what is essentially a subscription to their offering. This means that ownership of this offering is retained by the MSP, not the business that is engaging the MSP. This can create confusion when trying to ascertain what assets are owned and what assets are not, especially if the MSP also provides the hardware as part of their platform.

The business then also relies on the MSP to retain service contracts and hardware support, and to not change vendors and remove support for the products that they are providing.

Conclusion

In this paper, you can see some of the common threats to a small business, the impact of data privacy issues, and the risks associated with engaging a traditional managed service provider.

The common threats are able to be avoided by creating a computing environment that is tailored to your industry, and can provide a specific solution to your individual business needs, whilst maintaining end user experience.

Data privacy is a hot topic at the moment, and there are many legal requirements for your business to keep in mind when it comes to securing your, and your clients', important data. Building an effective and secure environment will help to mitigate these issues.

Engaging a managed service provider has long been seen as a way to cut costs in small business, as well as helping to support users. If your business is considering the services of a managed service provider, it is a good idea to review as much of the managed service providers offering as possible. If the expertise to do this is not available in-house, an external consultant should be sought to review the offering.

All of the above can be addressed by engaging a trusted consultant and IT provider to assess your environment, and build a solution that is tailored to your industry and individual business requirements. Grangeburn Professional Services has built support packages specifically to address these concerns, and have a number of happy clients that utilise our support and maintenance services, as well as as our consulting services, to support, enhance and grow their businesses.

GRANGEBURN
PROFESSIONAL
SERVICES

About Grangeburn Professional Services

Grangeburn Professional Services was born out of a need for something different that the traditional managed service provider offering. We don't rent you a package that is full of things that you may or may not need, and we don't force a "standard platform" on you to make our own lives easier.

We provide leading industry solutions tailored completely to your organisations individual needs, creating an effective and efficient working environment for you and your users.

As part of our services, we allow your business to retain ownership of all software and hardware. We maintain as much or as little of this as you require, and can offer a wide range of support and service packages for your organisation.

Below is a sample of some of the services that we provide to our clients:

- Full support for network, server and end users, including help desk support for day-to-day computing issues
- Break-fix troubleshooting, including hardware, software and network issues
- Warranty and non-warranty services for most major brands including Apple, HP, Acer, Toshiba, and Lenovo
- Strategic planning services for all organisations
- Business process assessment and enhancement
- Consulting services for all computing requirements
- Project planning for business startup and growth

Thank you for taking the time to read this whitepaper, I hope it has helped to address some questions that you have as a small business owner.

Please feel free to contact our office to engage our services, or for more information about our offering. Our details are as listed below:

Office Phone:	03 5571 1114
Address:	82 Brown St, Hamilton, Victoria
Email:	professionalservices@grangeburn.com.au

Author:

Paul Mammone
Grangeburn Professional Services
January, 2017