Need Help Filing Business Tax Returns? Startup-Friendly Accountants Are on Page 16.

January 2017

The Monthly Resource Guide For Startup Businesses

NEW BUSINESS MINNESOTA

Special Report

Protecting Your Business

You've Worked Hard to Launch Your Business. Have You Taken Steps to Armor Up Protect What You've Built? These Experts Offer Their Solutions: **Kenneth Kunkle,** Kunkle Law PLC; **Deb Weingarth and Melissa Young,** ADT Security Systems; and **David Charbonneau,** CMIT Solutions of the Twin Cities SW. Page 4.

Protecting Your Business

***From the Publisher**: Most new businesses take care of the obvious when they launch. They've got a banker, web designer, CPA etc. But they often forget to take steps to protect their business from the unexpected dangers lurking around the corner. Knowledge is the suit of armor that will protect your business.*

To examine this topic for our readers, New Business Minnesota approached this team of experts to write about the latest trends and strategies: ***Kenneth Kunkle,*** *Kunkle Law PLC;* ***Deb Weingarth and Melissa Young, ADT Security Systems; and David Charbonneau, CMIT Solutions of the Twin Cities SW.*** *They will share more information in a free interactive workshop in upcoming months.*

New Business Minnesota will hold its monthly Startup Meetup networking event immediately following the workshop. For more information and to register and RSVP go to: www.newstartupmeetup.com

A Good Security System Should Protect Business, Employees and Customers

Don't Let a False Sense of Security Keep You from an Honest Risk Assessment and Finding Affordable, Effective Solutions.

By Debra ~~Rutlen, Melissa~~ Young and Deb Weingarth
ADT Security Systems

The only thing worse than no security for your business, is having a false sense of security. That false sense will numb you to the real risks you face. It will allow you to justify doing nothing or doing half measures on the cheap.

The end result is that your property and financial records and critical customer and employee information remain exposed to theft. All because business owners think they had the risk covered or dismissed the risk entirely.

Here are some common examples – excuses – we've heard from business owners who don't fully appreciate their security risks:

• **"Hey, I'm on the 6th floor."** They lock their door when then leave each day and think they're secure. What they forget is that there are after-hours cleaning crews as well as appointment-only businesses that are open at all hours, and construction crews and contractors building out space for new tenants or remodeling other parts of the building.

ADT has plenty of videos of thefts by low-paid cleaning crews. Without that video evidence you'd never know who the perpetrators were. They expect suspicious looking thieves, not the normal looking people who clean their office every night.

• **"I have nothing of value a thief would want."** What they forget is thieves don't want to pawn the five-year-old computers. They want the customer information with credit card numbers that are on those computers. They aren't motivated by petty cash in a desk drawer. They want your business check book and company credit card statements.

If you have a copier in the office, they can make a copy of the bank or credit card statement and leave the original behind so you'll never know. Or they may just take the hard drive from your copier (Yes, many copiers store digital copies of everything) and see if they can strike data gold.

Debra Rutlen, Melissa Young and Deb Weingarth, ADT Security Systems Small Business Sales

• **"I don't have to worry. I have insurance."** Many insurance companies require that you have a security system in place. They might not pay a claim if you didn't meet that requirement.

Unfortunately, the real damage is not the lost equipment or cash. The damage comes when you have to notify customers their information had been stolen. Look at the nightmare Target Corp. dealt with. You can bet they would have preferred losing millions in cash to having to tell customers that their credit card data was hacked.

The more protections you put up the better. If something goes wrong, your customers will judge you by the precautions you took to protect them. Negligence is harder to forgive.

• **"We're in a safe area. Nothing has ever happened here before."** Denial never rests. Criminals come from all over the metro and in all shapes and sizes. And – surprise! – they have cars. Finding new territory is not hard. If you don't have a security system, there is little to discourage them from looking around. Most business owners who think the area is safe are going by gut feeling, not police reports or insurance statistics.

• **"The building owner provides security."** You can't outsource your security that way. Your landlord may only be interested in keeping the front door monitored. If you have losses from theft, will the owner pay you? No way. When the only thing between your office and the next is a sheetrock wall, you need to take responsibility for your own security.

Know Your Risk and Manage It

We ask all of our clients to first do their own risk assessment. If you walked into your office or shop after a break in, what's the first thing you would check? What are you most concerned about losing? How would you replace it? How long would it take you to be up and running again? How would this impact your business, employees or customers?

ADT - Continued on Next Page

That assessment will help us put together a plan that fits your needs, starting with perimeter security: alarms, card and door access, controlled access point, intercoms, motion, intrusion and glass detectors, etc.

While the alarm is still important, the newer options involving internet and mobile technology have created a whole new dimension of business security. It now includes monitoring the heat and air conditioning, tracking employee performance and productivity, ensuring employee safety, control of what equipment is on or off, real time notification of who is coming and going, monitoring locked doors and windows and more.

And just about everything mentioned above you can monitor and interact with from you smart phone.

Security systems like we have at ADT are increasingly becoming tools for managing the business. As a new business owner who may be thinking about security issues, keep in mind that eight of 10 small businesses will have security systems of some sort that go beyond mere locks on the door. You're not alone in wanting protection.

Work With Pros

With so many options, it is critical that you work with a professional security company that truly understands burglars, robbers and employees who steal.

Business owners who try and set up a video surveillance system themselves don't know the best place for cameras. They'll buy a package of 12 cameras at a discount store and place them so they all have the same field of view, or capture strong shadows instead of faces.

We know of an owner who had $10,000 in cash stolen. All his DIY security system did was record a great video of a faceless guy walking around robbing him blind. Often times the DIY owner puts the in an obvious place the DVR that stores the security video feed. Smart crooks easily find it and take the DVR along with haul.

For less than $299, he could have deterred the guy from getting in the front window and at the very least, detected when he entered. After that he came to ADT and we designed a new system for him that secured all his points of entry. All three of his shops now have the same system.

Trends and changes

For ADT, the biggest change in the last few years has been our Pulse system, an internet-based overlay of your intrusion system…on steroids. Using a smart phone, tablet or any device with internet access, Pulse can remotely arm and disarm your security system.

Pulse can also remotely control other things, such as turning on the heat or the coffee machine before you get to the office. That means you can also remotely see if the coffee machine was left on – all from your home.

Security used to be something you didn't really interact with much beyond arming and disarming it. Now you can use it every day to check in or perform actions. One ADT client lives in New Orleans and has a store in Eden Prairie. He used to have to fly in and check things out on occasion. Now, with Pulse, the client uses a smart phone to verify the cleanliness of the stock room, who is opening and closing and if the alarm is armed or not.

Conclusion

When you are considering a security system, look at all the risks and select the solutions with the best ROI for you. ADT has been doing this for over 142 years. It's all we do. Look for warrantees and guarantees. Ask about the average number of years customers have been with them. ADT's average is eight years. The industry average is less than three years. That matters.

Find out how many monitoring stations are looking out for your location. More is better. We always have a live ADT person involved in monitoring. Some companies outsource monitoring to another company. Some dealers do the install and aren't involved anymore. Look for a company that will build a relationship with you, check in with you, and most importantly, keep your business secure.

NBM

Call To Action

Set up your free Small Business Security Risk Assessment with one of the members of the dedicated New Business Minnesota ADT Team today! skreyer@adt.com

Debra Rutlen, Melissa Young and Deb Weingarth, ADT Security Systems Small Business Sales, have been handpicked to work exclusively with New Business Minnesota readers. They are from the local ADT office in Shoreview. ADT Small Business Security provides security solutions from alarms, intrusion protection, camera systems and remote systems for small and medium size businesses. Feel free to visit our national website at www.adt.com to learn more about our products and services.

Be Proactive in Protecting Your Computers and Critical Data Files

Beef Up Your Computer Security to Combat Hackers, Viruses, Ransomware, Phishing Scams.

By David Charbonneau
CMIT Solutions of the Twin Cities SW

Much of the news about cybersecurity involve major corporations and government offices – and political parties – being attacked by hackers. The reality is that businesses of all sizes are increasingly targets as well.

Unfortunately, most small business owners don't think they're vulnerable. They think they're too small "Besides," they'll say, "I don't have anything of value to hackers."

You have to recognize what they are really looking for…everything they can get their hands on. They want social security numbers, credit card numbers, birth dates, bank account numbers, transaction information, pet names, medical information and personal information of all kinds.

They can take that information and either use it themselves or sell it online to a worldwide black market. With that information, they can go after your financial resources directly, steal client credit card information you might have on your computer, steal your identity or use your computer as a gateway to any other computer you have access to, such as client's or supplier's.

A business is only as secure as its weakest client, customer or supplier who has any kind of access. Increasingly, businesses are demanding that anyone they are engaged with prove they have proper security measures in place.

Ransomware

A particularly nasty threat is Ransomware, in which a hacker seizes control of your computer and locks you out until you agree to pay a ransom. This has happened to police departments, hospitals, governments and universities, along with countless individuals and businesses.

There is even Ransomware that specifically targets photos on personal computers. What would you pay to get back your family photos?

Typically the Ransomware infects your computer through online transactions, when interacting with an infected site, via email or even plugging an infected flash drive into your computer.

Even on trusted online shopping websites, you can get infected. Someone is selling a really cheap toaster and you bid. You got a great price, along with an extra bonus. You need to be suspicious of all web sites you visit, even the ones you believe are above reproach.

Phishing

People are often the weak point in a security system. A simple email sent to you by "your" bank telling you it's time to change your password. Oh, and there is a handy little link right there to make it oh so easy.

That is the bait. You bite when you click on the link and change your password. It looks just like it came from you bank; if you click on help, it will direct you to your bank's help page.

And now you have given your password to a criminal. And for good measure – "for your own protection" they ask you to verify your account number.

There are a host of other phishing-like scams that trick you into revealing information or allowing viruses into your computer.

Face it. All our computers, smart phones and tablets are under assault and not just at the office. Trouble awaits you at coffee shops or airports when you casually check your email on your smart phone.

What can you do to protect your business?

Firewall

First of all, install a firewall and have it set up properly. When we checked out new clients' firewalls we find that some were not properly set up and some that had never been turned on. You need a firewall that is more robust and sophisticated than the basic one that came with your computer OS. Those aren't good enough for a business.

You need a commercial version that has power, flexibility and regular updates. What is best for you depends on the number of computers you have, the type of network environment, along with the types of applications you use.

Because there are so many variables, it's best to talk to people who live and breathe firewalls so you get the best fit for your situation.

Virus Malware Protection

These applications reside on individual servers and computers and have to properly be installed, enabled and always have the most current virus definitions.

There is always some new virus out there and you have to actively be

 Continued on Next Page

on top of it. We find that it works best when we do it for our clients so it is current and properly done on a schedule. They often get so busy that "little things" like a virus update just doesn't get done.

A lot of these virus and malware attacks are designed to take advantage of weaknesses in the operating system. So it is critical that you keep your OS updated. Microsoft, for example, has security and general updates constantly coming out in reaction to the newest threats. Keep current.

Encryption

If hackers succeed in penetrating your firewall, virus blockers or stealing your laptop at the coffee shop, encryption is the last line of defense. Encrypting all your information with a strong password leaves them with inaccessible files.

You should encrypt your server, email, computers and backups if maximum security is your goal. And change the passwords regularly.

Special Concerns for HIPAA/PCI

Companies involved in health care (HIPAA) or that accept credit card payments (PCI Compliance), face special rules and regulations governing computer security.

For HIPPA, you need to be looking at encryption because handling medical information on patients is a huge liability. A managed IT company like mine has to be HIPAA compliant to work on those systems. Every company interacting with that system has to be HIPPA compliant as well, right on down the chain.

Hospitals, clinics and doctors' offices all have sensitive client information on their computers. If they get hacked, or a laptop is stolen, the privacy of all clients will be compromised. They need to encrypt everything, including email that requires the recipients to have the key.

In addition to privacy violations, hackers can and have shut down hospitals with Ransomware demands, severely limiting their ability to provide proper care to patients.

PCI Compliance is required for anyone working with credit card transactions. To comply, your computer has to pass a security test. And you have to demonstrate that you properly handle all card information by showing policies for handling access, passwords and procedures, etc.

Call To Action

Visit our web site for - CMIT's FREE weekly email covering IT tips for your business or for a free assessment of your network or contact David at (612) 844-1149 or dcharbonneau@cmitsolutions.com

All these regulations have made things much more complex and more difficult to handle so you'll want to work with professionals to manage the process.

It is beyond what most businesses can do for themselves and still have time to run their business. You just can't do both in many cases. Small business owners often think they do it themselves. But then they move from one computer to two, add a server and routers with Wi-Fi, toss in smart phones, tablets and laptops…everything changes.

Managed IT

To stay on top of all things computer and security related, new and small business owners often outsource those responsibilities to Managed IT companies like CMIT Computer Solutions of the Twin Cities SW. We keep an eye on how our clients' systems are functioning, track all software that needs updating or is near the end of its life, and continually monitor the security environment.

Managed IT providers ensure that all your software is up to date. That helps with security issues as well as maintaining software compatibility. There are still businesses out there using Windows XP, which is no longer supported. That means Microsoft is no longer plugging the security leaks that hackers continually discover.

Companies often discover when adding new software that it isn't compatible with older software on their system. Updating can be pretty easy, unless you have delayed so long that you have to buy the newest version. It's time consuming and can be really expensive if a lot of computers are involved.

To avoid that problem, on all new servers we install, we make sure to have space for a mirror system so we can first test new software there before spreading it around the office. Managed IT is meant to be as proactive as possible to control a problem before it get out of hand. That's how we control costs and crises.

Backup and Disaster Recovery (BDR)

When disaster strikes, whether it's a fire, flood or massive system failure, your number one mission is to get back up and running so you can serve your customers.

To do this effectively you really need a disaster recovery plan that spells out a course of action and identifies who is responsible for what tasks. If you have 20 employees, and you die, what happens? Who else has your passwords and contact information? Who calls the IT company? Who alerts suppliers and customers?

Critical to any plan is having current and reliable backups of all your files and you should know where the backups are going. Is it on somebody's desktop on a server in a secure room or in the cloud?

I've have had people proudly tell me they do their own backups, but then are surprised to learn it has been six months since that happened. Some have old tape backups, which no one installs anymore.

Current practices are to back up everything, and then only backup files that have changed. By storing each of your regular backup sessions, you can find the most recent clean version should you get a disabling virus. Just go back to a period before the virus attack and do a clean restore.

It's also critical to test your backups on a regular basis by doing a restore to make sure it is working correctly. If you don't pay attention, you will get surprised.

If you have your backups on the cloud, it could take days or weeks to download everything. If you need it sooner, you need backup solution that gets you back in hours.

A Managed IT company can have that set up properly so when the worst happens, one call can get you on your way to recover.

Conclusion

Protecting your business' computer system requires a lot of technical expertise and knowledge of an ever changing environment. And the more computers you have, the more complex and time consuming it becomes.

Managed IT is the most affordable way to ensure your computers are reliably operating at the highest level and are as secure as possible from all the electronic threats we face each day.

NBM

David Charbonneau is president of CMIT Solutions of the Twin Cities SW, a privately owned company that supports companies and organizations in the Twin Cities to manage their information by applying network expertise to voice, data, video and print solutions and providing proactive support to resolve pending problems before they become complex issues. He can be reached at (612) 844-1149 or

dcharbonneau@cmitsolutions.com

https://www.cmitsolutions.com/cmit-solutions-of-the-twin-cities-sw/

Use Trademark to Protect Your Business, Brand

Trademark Prevents Competitors from Encroaching on the Brand Value You Have Created.

By Kenneth Kunkle
Kunkle Law PLC

With my new clients at Kunkle Law, PLC, I always emphasize how important it is to have the right protections in place to keep their company safe and help it grow. Your trademark is an important part that, and represents all your hard work and investment to get clients and consumers to immediately recognize the quality your brand represents.

Taking full advantage of this requires knowledge and experience in trademark law, so that you can determine what needs to be protected today, what can wait a while, and what isn't worth it.

A trademark is part of the brand that associates goods or services with a particular business. It can include your logo, business name, product name, slogans, and even the look and smell of your products. From a legal perspective, trademarks are a form of consumer protection that reflect a business' goodwill and serve to identify the source of products. When customers and potential customers see your brand, they should think about you and no one else.

The granting of trademark rights is also meant to help you prevent illegal use by other businesses that want to poach your customers and clients by using a short-cut to make themselves seem related to your established and respected brand.

How do I get a trademark?

All you have to do is begin using the "mark" as a way of identifying a specific product or service in a way that consumers will associate that name with your product. This might be right for you if there isn't much competition and you have no plans to expand to other markets. No one else in your local area can use your common law trademark, but someone in a nearby city may also have a right to use it.

However, for most of my clients, the better solution is to register a federal trademark, which has a more in-depth review process and affords you broader protection across state lines. Knowing what kind of protection is right for you takes an experienced lawyer taking the time to work with you in order to get to know you and your business objectives.

What are the benefits of registration?

Registering a trademark with the federal trademark office (and in some cases the state), provides several benefits to trademark owners. These benefits include:

- nationwide notice of the trademark owner's claim and a presumption of valid ownership;
- the right to sue in federal court, with the possibility of collecting additional damages and legal fees from infringers; and
- ability to file registration with U.S. Customs Service to prevent others from importing infringing goods.

A common problem I encounter is business owners who attempt to register trademarks online by themselves. After all, it seems easy and cheap. The problem is that they may be doing more harm than good since there is no assurance that the filing has been done correctly.

For example, I've seen businesses who attempt to register a trademark, only to learn that the mark has been in use by someone else for years.

Others put together applications, and then learn that they have applied for a trademark that isn't eligible for protection yet. While others misidentify or are overly broad (or narrow) in identifying the scope of products or services that their business provides.

While in their minds, they're fully protected; chances are they aren't, but they won't find out until a problem pops-up and by then it may be too late.

If you don't handle trademark registration properly, and defend it, you could lose it entirely.

That's the main reason for working with a lawyer who focuses on trademark law. There are general business attorneys who dabble in trademark law and cheap online services that give you the

Kunkle Law **Continued on Next Page**

impression your trademark is well protected.

However, trademark protection involves more than filling out a form online. Done right, you gain a valuable business asset and also protect yourself from competitors who want to take advantage of what you have created.

Selecting your Mark

When you are deciding on a trademark, I strongly recommend you to choose a name, tag line or logo that has the strongest potential for trademark protection. A strong trademark is distinctive and distinguishes you from your competitors – the more distinctive, the stronger the mark.

For example, if your tag line for a bottled milk product is "good milk," you may not be able to register it because it's too generic. You want something unique. For example, instead of just using the word "chips", Pringles® chose a fanciful name which can be better enforced because it is distinctive.

Trademark Opinions

Many new business owners I meet aren't sure if they need to do anything with their trademark at the early stage of their development, which is a valid question. Money is often tight in the beginning of a new venture, but making the right decisions early is still important.

Consider the case of a new manufacturer that is ready to launch their first product and have invested $20,000 for a product that will carry their logo and tag line. Printing labels, manufacturing and shipping these products without knowing if they can get trademark protection (or at least that they are not infringing on someone else's trademark) places their whole investment at risk if someone shows up claiming their trademark was violated.

Informal Opinions

If there is an urgent need to launch the product, a business can get an informal trademark opinion, which is a quick review of the marketplace to find any obvious problems. For these, I look through existing registrations and investigate other competitors in the space.

These informal opinions can be helpful in assessing whether a mark can be registered or at least how strong the mark is in comparison to others. Unfortunately, an informal trademark opinion isn't as strong as a formal one, and will not necessarily protect you in the event another party claims you have purposefully infringed their trademark. However, it will provide at least a basic review of the most obvious problems.

Formal Opinions

Formal opinions are similar to informal opinions, except that they are typically based on a much larger amount of research into potential conflicting trademarks. The benefit of the formal opinion, besides being much more exhaustive, is that it be used in court to defend against a claim that you intentionally infringed on someone else's trademark.

Business Name

It's a common misconception that registering your business with the Secretary of State is the same as registering a trademark. Your business name on file with the state is just a name and no more. It doesn't become a trademark until you start holding it out to the public. This registration only protects against someone starting a business with the exact same name, not against others selling products or services with that name.

In many cases, the legal name of a business is very different from its products. A good example is the Subway® sandwich franchise, which is owned by a company named Doctor's Associates Inc. The legal name has nothing to do with submarine sandwiches but is named this because one of the founders planned to pay for his medical degree from his restaurant earnings. Understandably, Subway® is now thoroughly trademarked throughout the world.

A good trademark attorney can help navigate through issues like this, by working with you to identify what is and what is not a trademark, and by helping you to prioritize potential trademark issues to determine if the marks are solid, identify what needs to be registered immediately and what can wait.

Enforcement

If you find someone using your trademark and you don't defend it, you could lose it. Once you have trademark rights, you are obligated to enforce them, or risk that the mark will no longer distinguish your business from your competitors. Trademark violations need an immediate response - letting it slide only works against you and is the first step toward your mark becoming generic. Who now remembers the companies that owned the now generic brand names "escalator," "aspirin," and "zipper?"

Domain Names

For most businesses, their website and social media presence are critically important. If you conduct business online, you need to give serious consideration to obtaining a federal trademark registration.

If someone sets up a domain name similar to your trademarks in order to confuse, it can be easier to resolve with a federal registration. When domain names are in dispute, one option is to use the arbitration process called the Uniform Domain Name Dispute Policy (UDRP) to force an infringing party to transfer a URL that infringes your trademark. These are technical hearings so I recommend hiring an attorney for a case like this.

For a small investment, I also recommend the additional protection of getting common variations of your website's URL, including close combinations, common misspellings, and other top-level domains like .net, .biz, .org. and others.

Buying or Selling Your Business

Buying or selling your company are events that should trigger a trademark audit. Consider the repercussions of buying a company and then finding out that the brand is unprotected or may already infringe on another company's trademark. You should identify a list of trademark and copyright assets to maximize the value of your business and ensure that you know what you're buying.

Conclusion

When evaluating, managing or protecting your brands, I strongly recommend working with an attorney who focuses on trademark law so you will have the assurance that the protections you need are in place. Don't wait until it's too late.

NBM

Kenneth Kunkle is the owner of Kunkle Law PLC, a boutique law firm concentrating on trademark, copyright, and entertainment law matters for small to medium sized businesses. He can be reached at (612) 414-3113 or Kenneth@kunklelaw.com www.kunklelaw.com

Call To Action

For more information on trademark, copyright, and entertainment law matters go to www.kunklelaw.com Call today for an initial trademark consultation. *(612) 414-3113.*