Explore our library of free on-demand webcasts GET STARTED NOW

Loudoun Website Design - owengotimer.com
We'll design & develop your website to earn new business & keep your customers coming back
owengotimer.com
OPEN

DIGITAL & SOCIAL | DIGITAL MARKETING

No Business is Too Small for These 5 Digital Policies

Kristina Podnar – June 20, 2019

Bob Beauprez once said, "In America, small business is a big deal." Indeed, it is hard to overestimate the role small businesses play in the American economy:

- Businesses with fewer than five employees account for 62% of all businesses in the U.S.
- More than half of all Americans own or work for a small business.
- Small businesses are responsible for two-thirds of all new jobs created each year.

ADVERTISEMENT
Loudoun-Owned Web Design Firm
Owen Gotimer Media
We'll design & develop your website to earn new business & keep your customers coming back
owengotimer.com
OPEN

When you look at the magnitude of their economic impact, it would be easy to assume that small businesses know exactly what they're doing and would be the obvious place to look for advice and best practices.

The truth, however, is that small businesses power the economy *despite* lacking the resources of larger organizations:

- 77% of small businesses rely on the owner's personal savings for their original funding.
- Only 40% of small businesses are profitable.
- The vast majority of businesses that fail, do so because of cash flow problems.
- Employees of small businesses wear many hats, starting at the top. The owners or leaders of small businesses are typically responsible for three or more of the following functions: operations, finance, sales, marketing, HR, customer service, product development, or IT.

When you look at it that way, it's not hard to understand why many small businesses regard digital policies — if they think about them at all — as something they'll get to "some day." But that's very unwise when you consider that few small businesses have the resources to survive the fallout from a crisis involving their online activity.

Owning a small business myself, I understand what it's like to have to make choices about where to spend your resources. I certainly wouldn't give you the same advice I give my global clients. Instead, I've narrowed digital policy development down to five things you absolutely must do to protect your business, your employees, and your customers.

5 digital policy initiatives to start right now

Take privacy seriously.

Know which privacy regulations you're required to meet.

Laws and regulations regarding online privacy vary by country, state, and even industry — as do the penalties, which tend to be significant. Here are just a few examples:

The General Data Privacy Regulation (GDPR)

The GDPR is an EU law that went into effect in May of 2018. It seeks to protect the private data of EU citizens by addressing how companies collect and use data as well as the security of how that data is stored.

What many U.S. companies don't realize is that jurisdiction is determined by the citizenship of the individual, not the physical location of the company. So any American business that collects, processes, or stores data on customers with EU citizenship is obligated to comply with GDPR requirements.

The California Consumer Privacy Act (CCPA)

The California legislature passed the CCPA in June of 2018, shortly after the GDPR went into effect. It's quite similar in its bias toward consumer privacy and its potential impact on businesses. And, as the GDPR extends beyond the EU's boundaries, the CCPA extends beyond California's state lines. So you can't assume you get a free pass just because you're not physically located in California.

However, while there are many similarities between the two laws, there are also a number of technical differences. Resources like this can help you achieve compliance with both laws (if necessary) with a minimum of redundancy.

Brazil General Data Protection Law (LGPD)

The LGPD is Brazil's data protection law, which will go into effect in 2020. The LGPD isn't quite as comprehensive as the GDPR, but it does put similar emphasis on the concept that individuals, not businesses, own their data. It details both compliance requirements as well as penalties for noncompliance.

More companies are passing their own digital privacy laws all the time. In addition, certain industries, like finance and pharmaceuticals, have their own regulatory requirements.

Make a list of action steps

Once you've identified the laws and regulations that apply to you, make a list of all of the requirements. I recommend creating a spreadsheet that documents which laws/regulations apply to you, which countries they apply in, and what you need to do to become compliant.

One tip I like to share with my clients is to prioritize actions that satisfy more than one requirement at a time. (For example, both Russia and China prohibit transferring their citizens' information outside of national borders, so deciding whether and how to establish a local service hub in those countries would take care of two things at once.)

Identify your priorities

If you're starting from scratch, it would be almost impossible to do everything at once. Your best strategy would be to prioritize policy development based on:

- Your level of activity in a particular country, industry, etc.
- The current legal environment surrounding that policy: Is the government aggressively enforcing compliance? Are consumers filing class action lawsuits? In other words, how likely is it that your noncompliance will come to light?
- What are the penalties for noncompliance? If you do get caught, can you withstand the repercussions? Or would you be at risk of going out of business?

Assign responsibility

Once you've prioritized the policies you need to address first, assign responsibility and a deadline by which you'll follow up.

Secure your fort from the barbarians at the door.

Think you're too small to be hacked? Unfortunately, you're wrong: 43% of cyber attacks target small businesses. And it's a bigger deal than you might think:

- 60% of small businesses shut their doors within 6 months of a cyber attack.
- Cyberattacks cost these companies almost $900,000 in damages or theft of IT assets.
- Small businesses lost nearly $1 million due to the disruption of normal operations.

Despite plenty of statistics that prove the barbarians are indeed at the door, barely half of the small businesses dedicate budget resources to risk mitigation. But increasing your security would probably cost less than you think, and it would certainly cost less than a major breach. Here are some effective, relatively low-cost steps you can take right now:

Develop strict policies for internal security.

A whopping 87% of small business have no data security policies for their employees:

RECOMMENDED FOR YOU
Webcast, June 8th: How to Generate Revenue Now
REGISTER NOW

- Many small businesses don't have an employee password policy that addresses things like the characteristics that make a password secure, how often it should be changed, the importance of not writing it down or sharing it with anyone, etc. And, of those that do have a password policy, only 35% strictly enforce it.
- Only 31% install regular software upgrades.
- Only 22% encrypt their databases.

Common practices like bring-your-own-device (BYOD) don't help. And then you have "low-tech" risks, like not restricting physical access to servers that store sensitive information.

This is also an easy and relatively cheap problem to fix. There are plenty of online resources for best-practices regarding employee data security. Find the ones that make the most sense for your company, document them in a digital policy (including the consequences for not following the policy), and implement it. If employees don't take the policy seriously at first, you may have to consistently enforce the consequences until they do.

Outsource the big stuff.

One reason cybercriminals target small businesses is that they know how expensive top IT talent is — and they know that few small businesses can afford it. Fortunately, there are plenty of security-as-a-service firms that can afford top talent, and outsourcing to them is a smart choice for small businesses. Some functions that are smart to outsource include:

- Website hosting
- Payment processing
- Data processing and storage
- Vulnerability testing
- Breach monitoring and mitigation

If you do decide to outsource, your policies should address not only which functions you'll outsource but also how you'll select and vet security providers. Complying with Payment Card Industry Data Security Standards (PCI-DSS), for example, is a must-have. Don't even consider working with a security firm that can't provide proof of compliance. Other things to consider include their policies for making sure employees stay aware of evolving threats as well as familiarity with your IT systems, your market, and your industry (since some industries are more heavily regulated from a security perspective than others). In particular, breach reporting requirements can vary significantly, and you want a partner who knows the requirements for your particular niche.

Your policy should also stipulate that contracts be reviewed periodically based on objective performance metrics. So outsourcing digital security doesn't mean you don't need policies; it just means you need different policies than an organization that handles security in-house.

Protect your intellectual property.

Whether it's an award-winning marketing campaign or the formula for a ground-breaking medical treatment, protect your intellectual property online as diligently as you do your tangible capital investments. Some companies have invested millions in software reporting only to find pirated copies

Get the best of B2C in your inbox:
Subscribe to our newsletter
you@youremail.com
Sign up

ADVERTISEMENT
Loudoun Website Design

investments. Some companies have invested millions in software programs only to find pirated copies being sold overseas. Others have found key sections of coding incorporated into another company's product.

Regardless of the specifics, theft of intellectual property can be quantified in terms of lost sales as well as in the amount of money it takes to rectify the situation. In a global market with a hodge-podge of laws and enforcement efforts, copyright infringement and theft of intellectual property is complex and expensive.

It's much more efficient and cost-effective to protect your intellectual property on the front end before it's been stolen or pirated. Protecting it with a copyright or trademark from the beginning can save you a lot of expense and hassle down the road.

On another note — be just as vigorous when it comes to respecting other organizations' intellectual property. Doing otherwise can get you in serious legal trouble and damage your brand's reputation beyond repair.

The resources below go into detail on some things, even the smallest businesses can do to protect their intellectual property. So decide which of these strategies you're going to employ, formalize them in digital policy, and ensure that all employees follow the policy's requirements.

Start working on accessibility today.

Failing to meet accessibility requirements is perhaps the biggest unknown risk in today's digital landscape.

"Accessibility" refers to whether and how well your site is designed to accommodate users with challenges in sight, hearing, mobility, etc. While most American businesses are familiar with the Americans with Disabilities Act (ADA), many don't realize that courts have ruled that it applies to digital spaces as well as to physical ones. The same is true in many jurisdictions around the world.

In fact, the number of lawsuits filed against businesses whose websites aren't accessible has skyrocketed over the last few years. Not only is defending such a lawsuit expensive, there are other costs as well. About one in five Americans has some type of disability, and they have a combined disposable income of $645 billion per year. Add in their friends and family, and you have another 105 million people who probably won't do business with you any more.

In other words, we're talking about a huge market segment. Do you really want your website to broadcast a "You're not welcome here" message?

Steps toward accessibility

One of the most important things you can do is add an accessibility statement to your website. The point is not to claim accessibility you haven't achieved, but to make a good-faith statement describing your awareness of the problem and your commitment to fixing it.

Aside from adding an accessibility statement, there are a number of steps involved in achieving accessibility compliance. You can start by doing things like:

- Adding captions to videos.
- Adding descriptive alt-tags to images.
- Using the high-contrast text on light backgrounds.
- Providing a number for people to call if they're having problems using your website.

But that's just the low-hanging fruit. You can find additional tips for achieving accessibility in the links below and develop your policies based on what works best for your business.

Keep your digital channels up-to-date.

The internet can change in the blink of an eye. Your customers can abandon one channel for another. Things that were considered trend-worthy one day can be deemed offensive overnight.

And then there are the digital channels themselves. They change Terms of Service in response to new legislation. They change the login and other security protocols in response to a breach.

One of the products or services you use may send out an important patch that winds up at the bottom of everyone's to-do list, representing a much bigger threat than most people realize. The Equifax breach provides a perfect example. They knew about the vulnerability, and they knew a patch was available — they just didn't apply it.

In their defense, however, many organizations have such a myriad of software products that it's almost impossible to keep up. And, in one study, 65% of respondentssaid they had a hard time prioritizing what to patch first. The time required to implement the patches — particularly for a small business whose employees might be somewhat inexperienced — adds to the cost and inconvenience.

The best way to address the issue is through digital policies. A policy that establishes a time table for reviewing channels and establishes triggers for taking action helps keep small problems from accumulating into an insurmountable mess. And, for organizations that do find themselves in such a mess, digital policies help avoid debates over how to fix the problem. When a policy tells employees what to do and the order in which to do it, you reduce the risk of a time-wasting debate and make sure the most important priorities are handled first.

Conclusion

Small businesses have a zillion things to do and limited resources with which to do them. The tips I shared here are only a small subset of the digital policies I work on with my global clients, but they're both the bare minimum and an achievable goal for most small businesses. In other words, almost everybody can afford to do them, and the survival of your business is at serious risk if you don't.

Share Tweet Email

Top Articles



Digital Marketing Tips for 2020

This article was written for Business 2 Community by Kristina Podnar.
Learn more about writing for B2C



Author: Kristina Podnar

Follow @kpodnar

Kristina is a digital policy innovator. For over two decades, she has worked with some of the most high-profile companies in the world and has helped them see policies as opportunities to free the organization from uncertainty, risk, and internal confusion. Kristina has a BA in international studies and an... View full profile ›

More by this author:

- How Should SMBs Approach Data Privacy Laws?
- 2020 Presidential Candidates Get an "F" on Digital Standards
- Is May 25 Doomsday for U.S. Marketers?

Recommended Reports



The Customer Journey: How to Deliver Great Customer-First Experiences



Digital Personalization 101



Project Management Software: 2020 Pricing Guide



The Ultimate Guide to Website Personalization



Modeling ROI for Personalization



The State of Personalization Today

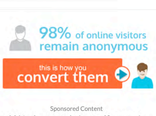
Discuss This Article

Add a Comment

ADVERTISEMENT

Leesburg-Owned Web Design Firm - WordPress Design From $999
How does your small business stand out? A high-quality website is a good place to start. owensgolmer.com/website-design
OPEN

Recommended Content



Sponsored Content
98% of your website traffic remain anonymous



Sponsored Content
The Essential Guide to Content Personalization



Sponsored Content
How to Improve Your Account-Based Marketing

Powered By BrightInfo

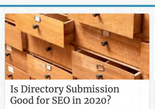
MORE DIGITAL & SOCIAL + VIEW ALL



Digital Marketing Tips for 2020
by Lindsey Flagg - stux / Pixabay We're halfway into the first year of a new decade. Many B2C marketers and business owners have swept their marketing plans under...
3 DAYS AGO



5 Effortless Tips to Create a Hashtag Strategy for Social Media
by Victoria Taylor - Hashtags are a permanent staple for social media users. What originally started as a hash or pound on Twitter on August 23, 2007, by Chris...
2 DAYS AGO



Is Directory Submission Good for SEO in 2020?
by Martin Woods - "Can you still use directory submissions for SEO?" This question crops up repeatedly on forums and it's unsurprising as once upon a time directories were...
2 DAYS AGO



7 Email Marketing Best Practices That Will Increase Your ROI
by Brandon Purdum - As an outreach channel, email marketing offers a great opportunity to connect with your audience, nurture leads and meet prospects at a critical point in...
2 DAYS AGO

BRANDVIEWS ARTICLES + VIEW ALL LEARN MORE