Small business digital policy guide

be safe online

AVG

Socialize

Most employees will have their organization's best interests at heart but in an era when everything is mobile, the boundaries between private and work life are blurring, making it difficult for even well-intentioned workers to steer clear of tech trouble. What does that mean in reputational, legal and financial terms for your business?

As mobile technology, social media and the associated issues surrounding them restructure conventional business practices, will you be ready to meet the new challenges?

Introduction

With the rapid changes in hardware, how we make connections, how we access content and how we interact with technology, there's never been a more exciting time for business.

Judy Bitterli is a Senior Vice President at AVG. She blogs about online experiences at http://blogs.avg.com

The advent of social media, mobile devices and the accompanying tools are benefitting us in ways unimaginable a decade ago. As smartphones and tablets have integrated fully into our home and business lives, the pace, scope and capacity of work has increased - but so has the potential for problems.

Social media, too, has changed the landscape, largely for the better, but there are important issues to consider as we become ever more accessible and interconnected.

It may feel as if you need to expand or incorporate an IT team, even if until recently your company has been managing the transition to digital with little or no internal support. But considering the average cybercrime incident cost $8.9 million in 2012 – according to the Ponemon Institute Cost of Cyber Crime report - and experts say attacks, particularly using viruses, worms and malware, are increasing, it's integral to a healthy business to have the understanding, policies and infrastructure in place to meet these threats.

But with some essential safety advice and tips for managing things such as social presence, your business can make the most of emerging technologies.

Social recruiting

You've probably heard about the recent college graduate who was headhunted over social media, with her personalized job offer posted on Instagram and Facebook.

It was a coup for Detroit-based ePrize, a national digital marketing agency, which drummed up industry kudos and media attention for its creative use of social networks.

Crucially, ePrize chose Samantha Banky in part because she was an early and avid adopter of social media. She, like the brightest and best job candidates, embraced it as a platform to launch her professional career.

More importantly, ePrize recognized the potential for social media as a recruiting tool, promoting its presence on various channels not only to clients but to valuable job candidates.

By harnessing social media's capacity for recruiting and vetting candidates, organizations are gaining exposure to the kind of people they want to attract, taking some of the work out of managing postings and applications, and displaying the character of the workplace.

Social followers are likely to share any job vacancies you post, letting your connections do the legwork for you. Plus, with individuals following your social presence, you may even turn the head of an exceptional candidate who didn't think they were in the market for a career shift.

The ease with which social media provides insight into a prospective employee is one of its best features, though be wary of the legal perils: read on for expert advice on how to stay above board. But bearing in mind how quick and simple it is to get started - and how effective an estimated 90% of employers find it - what are you waiting for?

The ease with which social media provides insight into a prospective employee is one of its best features

Social branding

Is your business on board with social media? If it isn't, you can bet your competitors are - and they're loving it. Whether you are using social for recruiting, brand awareness or building customer loyalty, it's a winning scenario.

Social sites and industry-specific networks are providing cost-neutral ways to attract and retain both employees and business. See the following page for more information about smaller or newer players in the social stakes.

Moreover, social channels provide opportunities for marketing, promotional, brand awareness and customer or client loyalty efforts. Businesses can build links with potential employees or clients by demonstrating a flavor of what life is like in your workplace and giving them the chance to see how they might fit in with the ethos and atmosphere.

There are also examples of best practice and things to avoid when using social media in any business-related capacity, including:

- Resisting the temptation to make your organization's social presence too salesy, publicity driven or all about recruiting. Offer followers something of genuine value, such as industry news, successful campaigns or even just something funny
- Keep posts brief but not boring and certainly not offensive or risque.

Resist the temptation to make your organization's social presence too salesy, publicity driven or all about recruiting.

Neither should content be aggressive, condescending or unpleasant towards a rival. Interact with followers, which builds trust and increases the likelihood of retaining and capturing new followers who will share your content. Responding to posts and questions puts a human face on a business - plus it's just polite

- Be careful who the business entrusts with its social profiles. An intern or someone inexperienced with technology or the business's objectives, or someone with an axe to grind, could embroil the business in a damaging controversy with just a few keystrokes.

Social climbers

Apart from the obvious channels - LinkedIn, Twitter and Facebook - other social sites and industry-specific networks can be good places to invest in, both in terms of recruiting and for building brand awareness and loyalty.

Google+

With around 360 million active users, Google Plus boasts perks, such as a group video service. More crucially, actively engaged Google Plus users can get a boost in search rankings - what better way to promote your business?

Instagram

A specialized app for capturing and enhancing pictures of your business's atmosphere, without the need for a photography degree.

Dribbble

One of the up-and-coming social sites that are industry-specific. Dribbble gives designers and creatives a place to showcase their work.

Pinterest

Visually display your organization's unique aspects, such as an appealing work space or a company night out, while luring followers. In turn, users can keep tabs on what potential employees are up to and establish whether they might be a good fit for your company.

YouTube

Promote your organization's values and benefits through peppy presentations that demonstrate your strengths. Just keep it genuine, interesting and, most of all, short.

Tumblr

A social media blog site where employers can get valuable insight into a job candidate's ability, initiative and commitment.

Policy minded

Social media has helped the hiring process in many ways, but if you don't know how to use it correctly you could be setting yourself up for a costly lesson.

A robust policy should outline the stance on social media or mobile device usage during and outside work time

The occasional personal Facebook updates aren't always bad for business: if a reporter, for instance, tells their followers over Twitter or Facebook about an exclusive hitting the pages or the screens later in the day, it could create a buzz around the company's site.

But plenty of scenarios can spell trouble if there is no clear social media policy for employers to turn to when things go awry. A robust policy should outline the stance on social media or mobile device usage during and outside work time, and the consequences of violating it.

Though the courts are still catching up to the evolving social sphere, legal experts say a company's safest position is to have a comprehensive framework for averting and dealing with problems.

Case in point: what rights do individuals have to LinkedIn accounts that were created or expanded in a work setting? If someone sets up a business in competition with their former employer, could their LinkedIn account be considered proprietary information?

On a related note, how should a business respond to false or negative statements from competitors, former employees or failed job candidates? What about an employee whose private social media activity reflects poorly on your business, or reveals information that could be advantageous to competitors?

Even if social media isn't directly incorporated into your business, it's an issue that can't be ignored.

Left to their...

Bring Your Own Device, more commonly known as BYOD: it's an acronym that holds both promise and fear for business owners of all sizes and industries.

With smartphones becoming the go-to gadget, and tablets and laptops rounding out the mobile device trio, it's becoming ever less likely that your employees will arrive at work without at least one internet-enabled device. So how can businesses both protect themselves and make the most of BYOD?

On the plus side, the BYOD trend can improve employee productivity and accountability, whether or not it's company issued or a personal device approved to be used for work.

But there are both practical issues and the potential for security problems as employees may be taking sensitive data with them wherever they go - home, out socially or in other non-secure settings.

For a start, who covers the service plan and other charges for things such as security software, cloud storage, data downloads and apps? If an employee is expected to use their personal device for work, who is responsible for things such as repairs or upgrades? What if the individual is travelling abroad

for work and using a business-issued device to make calls home to their loved ones? What if their device is lost, stolen or otherwise compromised?

Another practical consideration is the pressure put on company WiFi or networks when many personal devices can access them, even just to update mobile software or apps.

Do your employees understand basic safety procedures for mobile devices, such as using security software, password protection, encrypting sensitive data, only allowing legitimate downloads, taking care on unsecured websites and when using public WiFi networks and disabling Bluetooth when not needed?

...Own devices

It can be a logistical nightmare for IT departments to coordinate different devices operating on different platforms, all with separate service plans and capabilities.

But in the BYOD world businesses must put a premium on ensuring data only leaves the office a secure manner. In this regard, it can be easier if not more cost-effective to distribute devices that employees can expect to use for some personal matters.

Either way, do you know where your company info is going? Smartphones show the user's location whenever the device is on them, and can build a profile of travel habits and activities. Is there a concern that where your employees can be found, so can sensitive company data?

Is there a concern that where your employees can be found, so can sensitive company data?

Furthermore, data is collected through apps and other mobile device functions and can be shared with third parties without the user's knowledge. Could this mean things such as contact information for customers, clients, patients or others is inadvertently going to third parties, such as analytics companies and advertisers? Apart from concerns about hackers, lost hardware or other data-breach possibilities, there are questions around how employees may use company data stored on their devices, especially if they no longer work for you. For instance, what happens to contact details for your customers or clients? If they're calling an ex-employee, do you stand to lose business?

Employees also may store or backup data on cloud computing services, such as Google Drive, Dropbox and Apple iCloud, which can be accessed on mobile devices. These services can provide flexible working solutions, but they pose potential problems. Experts say even encrypted data can be accessed, particularly if the terms of service state that the cloud provider can disclose account information to law enforcement or third-party sources.

Data breach

Cybercrime and problems associated with employees using their personal devices at work, known as BYOD, are putting strains on SMBs. Experts say, however, there are ways to reduce these threats, starting with appropriate policies.

External attacks are responsible for **92%** of data breaches, with **1%** traceable to business partners, according to Verizon's 2013 Data Breach Investigations Report

Nearly **60%** of full-time employees participate in BYOD, but only **20%** have signed a BYOD policy, says Verizon's 2013 Data Breach Investigations Report

76% of network intrusions resulted from weak or stolen credentials; **40%** from malware; **35%** from physical attacks, such as ATM skimming; **29%** from leveraged social tactics, including phishing, according to Verizon's 2013 Data Breach Investigations Report

Most breaches would be easily prevented, with **78%** of techniques reviewed to be in the low or very low category of sophistcation, says Verizon's 2013 Data Breach Investigations Report

According to the Ponemon Institute's 2012 Cost of Cyber Crime report, the average cybercrime incident cost **$8.9 million.**

78% of firms whose employees BYOD have no policy. Of those bringing their own devices to work, **17.7%** say their employer's IT department doesn't know, and a further **28.4%** say their IT departments ignore BYOD. Statistics are from a report conducted on behalf of Logicalis, an international IT solutions and managed service provider

Keeping safe

When it comes to security, experts say the focus should be on the data, not the device. Two elements are imperative in order for businesses to be in the safest possible position.

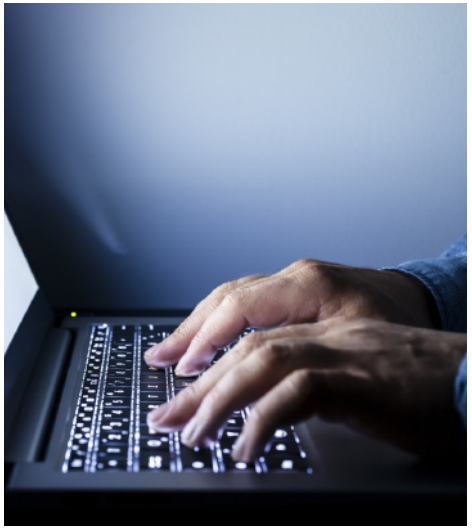
In other words, putting stringent controls on what devices employees can bring into the workplace is a losing battle, and resources are better spent on managing how those devices are used. This doesn't have to be an onerous task, and can be achieved by applying a number of checks.

Firstly, organizations should regularly audit what mobile infrastructure, devices and apps are in place in order to create a strategy that identifies weaknesses and offers solutions. Verizon recommends an audit should:

- Determine if unnecessary data is kept on devices, clearing what's not needed and monitoring what remains
- Collect, share and analyze tactical threat intelligence and incident data for the purposes of detection and defence.

According to the FBI, organizations are increasingly being targeted for data that could prove valuable in the wrong hands, such as employees' private details or confidential client information. If you assume general or professional liability insurance policies will provide adequate protection in such scenarios, you could be making a costly mistake.

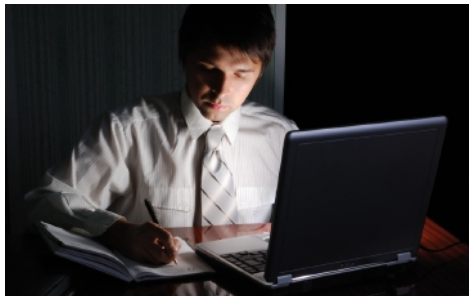
A necessary safeguard could be cybersecurity or liability insurance, which the U.S. Department of Homeland Security states is "designed to mitigate losses from a variety of cyber incidents, including data breaches, network damage and cyber extortion." More information is available from the U.S. Department of Homeland Security at http://www.dhs.gov/publication/cybersecurity-insurance



Best policy

Just as experts advise businesses to create a social media policy, every SMB should have a solid, comprehensive BYOD policy that every employee understands and adheres to.

Businesses worry more about the security implications of BYOD than the effect on employee productivity. That was the verdict of 1,650 information security professionals who were surveyed on Holger Schulze's Information Security Community LinkedIn group. While 70 per cent said they were worried about loss of data or malware infecting their network, only 54 per cent said BYOD posed concerns about how hard staff would work. Crucially, only 6 per cent said they were ready to embrace BYOD across their business.



Expert advice is available and BYOD policies should be tailor-fit for individual businesses.

But certain policy elements will be universal, including:

- Required security software must be used and kept current, the original operated system will be left in place and the user will not 'jail break' the device
- Employer and employee will agree to whether the device can be shared and with whom, how, for what purposes and to what extent (if any)
- Access to certain websites and personal use that could be deemed illegal, threatening or offensive (such as cyberbullying campaigns targeting coworkers) will be prohibited
- Certain business data, such as confidential client information, will not be downloaded to, stored on or transferred by personal devices
- Any sensitive data downloaded or stored on the device (such as in e-mail) will be securely deleted
- The employer has the right to remotely delete data if a device is compromised.

Go Ahead

Coping with the fast-paced changes in technology can feel like a full-time job in itself. And while the genie is out of the bottle - there's no going back to the days when people weren't intrinsically connected - there are plenty of opportunities for businesses to grasp the power of the new social environment.

Learn more about internet security at www.avg.com
Join us on Facebook www.facebook.com/AVGFree