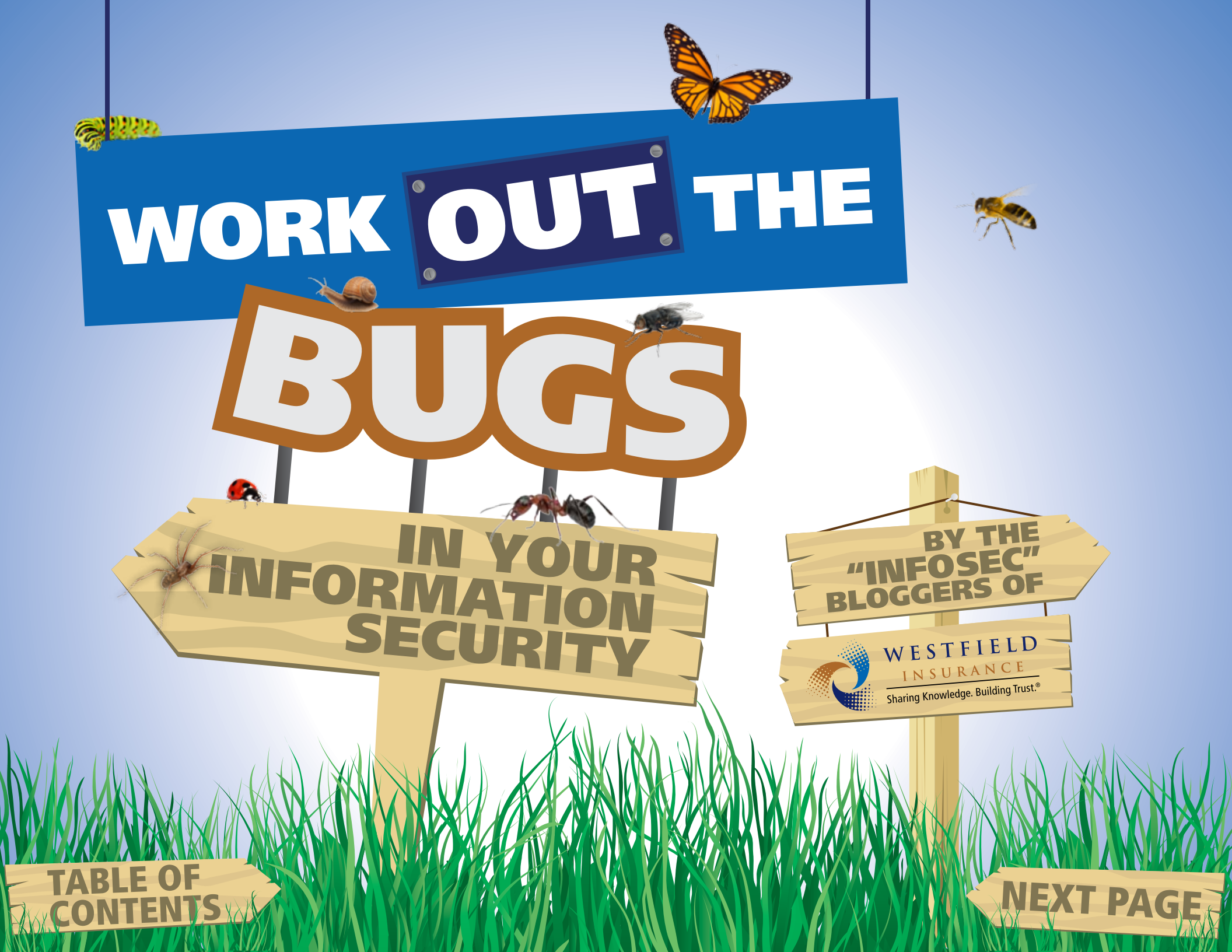

WORK OUT THE
BUGS
IN YOUR INFORMATION SECURITY
BY THE "INFOSEC" BLOGGERS OF
WESTFIELD INSURANCE
Sharing Knowledge. Building Trust.®
TABLE OF CONTENTS
NEXT PAGE

FORWARD

Information is vital in today's economy, and customer expectations about the privacy and security of their confidential information have never been higher. At the same time, hackers and scammers are getting ever more sophisticated at stealing and tricking us out of our private information. Identity theft and other cybercrimes have been the fastest growing criminal categories for several years now. In 2009, cybercrime surpassed the international drug trade in total economic impact.

Good companies invest in technological controls and defenses (firewalls, anti-virus, intrusion detection, etc) and create layers of defenses, similar to the layers of defense in a castle - walls, moat, portcullis, etc. But just like the castle which has a gate in the wall and a bridge over the moat (it has to so people can get in and out to live), the modern technological walls have windows, ports and doors - they have to so you can carry information in and out to get work done.

That means that the most important layer in any company's security is the human firewall - that layer of informed and educated people who can recognize a scam and head off a suspicious call before anyone's information has been compromised. People are the first, the last and sometimes the only line of defense against the hackers and con artists.

In 2004, Westfield started publishing internal tips and reminders about computer and personal security. About half were reminders and announcements of company-specific policies and half were reminders and tips that employees should follow to protect their personal information and home computers. We had terrific success with that approach. People took the tips home to protect themselves and then brought those habits right back to work.

A year later, we opened the distribution list to our independent agents and other friends and family of Westfield. In September 2008, we converted the email distribution list to a blog (http://infosec.westfieldinsurance.com) so our readers could comment and share their own stories and tips. We continue to think that the human firewall is the most important layer in our defenses.

WORK OUT THE BUGS IN YOUR INFORMATION SECURITY

Contents

WESTFIELD INSURANCE
Sharing Knowledge. Building Trust.®

1

MARCHING ORDERS: INFORMATION SECURITY BASICS

WHAT IS INFORMATION SECURITY?

WHAT IS PERSONAL INFORMATION?

WHAT DO SMALL BUSINESSES NEED?

WHAT TO DO WHEN THERE'S A BREACH?

WORK OUT THE BUGS IN YOUR INFORMATION SECURITY

TABLE OF CONTENTS

NEXT PAGE

WHAT IS INFORMATION SECURITY?

Information Security is the responsibility of actively protecting private, personal information and company information systems from unauthorized access. The compromise of such information places customers and companies at risk for identity theft and other significant threats and losses. Access to consumers' private information is a privilege and high-risk responsibility for many small businesses. Because of the increasingly blurry distinction between physical and electronic perimeters, information security is a constantly evolving element of company security.

Businesses worldwide are operating in an increasingly hostile environment. With advances in technology, everyone – businesses and their customers – stand to gain and lose more than ever before. Criminals are getting more creative and more technologically adept every day, requiring companies to keep a vigilant eye on their security practices.

As information becomes easier to access via electronic exchange and the Internet, it is imperative businesses develop a strong understanding and internal policy regarding information security.

Identity theft is the fastest growing type of fraud in the USA, the UK and many other developed countries.

WHAT IS "PERSONAL INFORMATION"?

Personal information includes an individual's name (first name or initial plus last name) in combination with at least one of the following:

- Social security number
- Driver's license number or state identification number
- Account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account

NOTE: In general, if the data elements are encrypted, or otherwise made unreadable, that would not constitute a breach.

"Being wise to your business' need for information security is essential to propelling its success."

- Westfield Employee

WHAT DO SMALL BUSINESSES NEED?

1. **Dedicated security team**: individuals in charge of the coordination and continuous improvement of information security.
   Information security is often thought of as the responsibility of the management and IT teams, but the reality is that information security measures are part of every employee's job requirements.

2. **Password protection**: maintaining complexity standards and safekeeping of passwords from unauthorized access.
   Individuals can gain access to passwords through advanced electronic hacking or from something as simple as a sticky note on someone's desk. Passwords are a key to compromising information security, and businesses need to be aware of employees leaving private information out in the open or available electronically.

3. **Mandatory shredding**: policy stating all office paper must be shredded.
   Even in an electronic age, most identity theft occurs as a result of access to physical copies of the information. All employees should regularly shred printed confidential information.

4. **External defenses**: security systems, surveillance and other physical defenses in place to protect a business and its employees.
   Ensuring the physical protection of employees is inevitably tied to information security. When intruders compromise the external defenses of a business, the personal safety of employees, as well as the security of all vital information, is at risk.

5. **Disaster plan**: preconceived crisis plan to allow for immediate actions when physical or electronic disasters occur.

SECURITY BREACH: WHEN INFORMATION SECURITY FAILS

Laws generally define a "security breach" as the unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information. In most states, laws do not apply to employees or agents using personal information in good faith for a business purpose, as long as the information is not later used for an unlawful purpose or subject to unauthorized disclosure.

WHAT TO DO IF YOUR AGENCY HAS A BREACH

Security breach laws require notification anytime there is reasonable belief that a person's private information is at risk of identity theft or fraud. Most of these laws are very similar to each other, though there are some state-to-state differences. Some states, such as Ohio, require notification no later than 45 days after you discover or find out about a security breach. Some specific exceptions to the 45 day requirement apply, such as a request by law enforcement. You should contact your local legal counsel for specifics.

Businesses can provide notification in writing or by other means as specifically allowed in the law. The notification must include a description of the information which was potentially compromised and an explanation of the consumer's rights. Most states also require you to provide a toll-free contact number for customers to call for more details.

Keep in mind that when your business owns and processes all customer information itself, this law is fairly straightforward. However, if your work requires you to share information with a business partner or vendor, the responsibilities are more complicated. The law requires that the company processing the data notify the company which "owns or licenses" the consumer information and that the "owning" company must notify the consumer.

SECURITY BREACH LAWS

REQUIRE YOU TO NOTIFY PEOPLE IF THERE IS REASONABLE BELIEF THEIR PERSONAL INFORMATION IS AT RISK.

DIFFER FROM STATE-TO-STATE, SO CHECK WITH YOUR LEGAL COUNSEL FOR SPECIFICS.

TYPICALLY REQUIRE NOTIFICATION WITHIN 45 DAYS OF BREACH.

NOTICE MUST DESCRIBE AT-RISK INFORMATION, EXPLAIN CONSUMER RIGHTS, AND PROVIDE A TOLL-FREE NUMBER FOR MORE DETAILS.

2

DON'T RELY ON LUCK: SETTING INFORMATION SECURITY STANDARDS

TABLE OF CONTENTS

NEXT PAGE

THE "I" IN INFORMATION SECURITY

How many people have access to your desk? If you take a moment to consider the traffic around your work area, you may realize that confidential information is actually at a higher risk than you originally thought.

On any given day, your co-workers, customers, maintenance workers and cleaning staff have some degree of access to your work space. Everyone wants to assume these individuals are good people, but even good people can fall prey to temptation.

Information security also extends to the physical perimeters of your facility. Any breach of security could result in additional losses for the business and its customers.

1. Always be aware of the information you leave on and around your desk.

2. Regularly clean off your desk and store confidential information.

3. Shred any documents you no longer need.

4. Protect your access cards and keys.

5. Protect your personal belongings when entering or exiting the building.

Information security is most effective when it is an activity occurring at every level of a business.

Taking actions to protect confidential information in your custody is a daily effort every employee is responsible for. This intensive policy, however, does not require extensive funding. There are many things each employee can do to improve your business' security posture that will only cost your business time and attention.

EASY STEPS FOR EMPLOYEES

You have to assume that people you don't know have access to your space when you're not around. Do what you can to protect your business' and customers' information from falling into unwanted hands. The borders between information security and physical security are increasingly blurry. These days, security is everyone's job.

5 TIPS FOR APPLYING INFORMATION SECURITY AROUND THE OFFICE ON A DAILY BASIS

Make sure that information-sensitive documents, especially anything with an SSN or Drivers License Number on it, are **put away** at the end of each workday.

Lock it away in a secure filing system. Even if the cabinet doesn't lock, it will at least be more obvious when an unauthorized person is snooping through the files.

If you can't lock the papers up, at least put a cover sheet or blank page on the top of the pile to protect the confidential information from casual oversight.

Keep your desk clean of passwords:
If you write down your passwords, do not leave them around your desk for any casual visitor or after-hours maintenance person to see.
If you use the same password for everything, you'll lose them all as soon as any one of those systems gets compromised. So for security purposes, we often create multiple passwords. However, writing passwords down can be just as risky once your sticky-note gets lost or stolen.

3

Collect papers off faxes, copiers and printers as soon as possible:
Don't leave confidential papers exposed to guests and others employees.

4

Turn off your computer at night:
Don't just lock the screen. Your IT team should set up extra protections that will kick in when you shut the computer all the way down.

5

Be aware of your surroundings when entering or exiting the building.
Keep your access card with you at all times and be aware of your surroundings when entering and exiting the building. Challenge unknown people politely, but directly. Don't assume that anyone in the area has a right to be there.

MANAGING MULTIPLE PASSWORDS

MAKE YOUR OWN SYSTEM FOR CREATING SEMI-CUSTOMIZED PASSWORDS THAT WILL BE EASY TO MEMORIZE BUT STILL UNIQUE TO EACH SITE.

MAKE UP YOUR OWN RULES!

PICK A "STATIC" PASSWORD, LIKE "BLUEBIRD" AND MAKE UP A PERSONAL RULE ABOUT THE WEBSITE NAME OR APPLICATION YOU ARE CREATING THE PASSWORD FOR, SUCH AS:

The first digit of the password will always be the second letter of the website's name.
The second digit of the password will always be the number of characters in the website's name.
The third digit will be a dash.

The password at Amazon would be "m6-Bluebird" and at eBay would be "b4-Bluebird". A password in this pattern is reasonably strong because it has all four character classes (uppercase, lowercase, number, punctuation) and doesn't follow the predictable tendency for English speakers to capitalize the first letter and put number(s) at the end.

KEEP IN MIND THAT YOU **MUST**…

Be the only person who knows your exact rules. Do not use the exact rules mentioned here. Make your own choices about which letter, punctuation, etc. Some systems won't allow special characters (like the dash) or may have size limits on the password. Make the best choice you can given the limits of the system and write down only enough to remind yourself what's different (such as "401k - no dash"). If it's an important system (like your online bank), lobby the company to allow stronger passphrases.

Use the information gained from these scans to improve office security and protection.

INFORMATION SECURITY CHECKUPS

Part of managing a small business is to monitor the daily activities to keep operations consistent, effective and safe. You should regularly conduct an internal sweep of your business' office systems and defenses to look out for the simple cracks through which information can become vulnerable.

CHECKUP CHECKLIST

- ☐ See how many people left sensitive documents on their desks. (If you allow the use of thumbdrives in your environment, make sure you watch for them, too. Thumbdrives are high risk devices - very easy to steal.)
- ☐ Prevent tailgating and make sure all visitors are escorted by your employees.
- ☐ Monitor desks for passwords - Walk around your office some night and see how many people keep their passwords on sticky notes right on the computer monitor. Keeping track of passwords is hard. But writing them down and leaving them out for every casual visitor or after-hours maintenance person to see is inexcusable.
- ☐ Make sure everyone authorized to carry an access card keeps it with them at all times.

3

BUZZ OFF!
NO TAILGATING ALLOWED

KNOCK-KNOCK, DANGER'S AT THE DOOR!

TIPS FOR TAILGATING POLICIES

THE GOLDEN RULE(S)

WORK OUT THE BUGS IN YOUR INFORMATION SECURITY

TABLE OF CONTENTS

NEXT PAGE

KNOCK KNOCK: DANGER'S AT THE DOOR!

Most of us usually try to be polite and hold the door for others, especially when the weather is bad. It's hard to fight the urge to be courteous and tell someone "no," forcing them to walk around to the main entrance of the building. Unfortunately, in today's world of identity theft, litigation and physical violence, precautions are necessary to protect the safety and security of our co-workers and customers.

Imagine the risks you expose your business to when you open the door for someone, giving them access to somewhere they don't belong. With unescorted access to your building, an intruder could steal information, compromise systems or worse. If the intruder is a disgruntled claimant, a former employee or a significant other, they could be attempting to get into the building for violent reasons.

WHAT IS TAILGATING?

Tailgating is the art of acting like you belong through the use of social pressure to convince people to provide them with unauthorized access to a building. Tailgaters, or those attempting to gain unauthorized access to your building, represent a real risk for your organization.

Tailgaters approach you from behind, with just the right balance of professionalism and distractedness, and expect you to politely hold the door for them to enter, even though they have no right to be in your building. Good tailgaters come prepared with a plausible excuse why you should "be a nice guy" and break the rules – "It's raining", "My arms are full", "I forgot my key on my desk last night", etc. There is no way to identify a scammer just by looking at him or her.

NO EXCEPTIONS!
Every company needs to have a policy for visitors and must enforce a strict "no tailgating" policy.

Even the smallest of businesses need to establish a policy to protect employees, workers and customers from tailgating. Whatever your entry control procedures are, you should have a strict "no tailgating" policy. Policies should take anyone – and everyone – who accesses the building into consideration.

- Visitors should always be signed in and out of your facility and should always be escorted while in any non-public part of your facility. If a customer or other important visitor comes to the wrong door, politely escort them to your main entrance and get them signed in properly.

- Employees and contractors should be required to show their authentication every time they enter the building. You should not hold the door for anyone you don't know and do not expect someone to hold the door for you – this is an essential part of security discipline.

  If someone does follow you into a non-public part of your building and/or refuses to show their ID badge, immediately go to the nearest phone and call your local security contact. Give them your name, location and a description of the intruder.

Visitor Logs are surprisingly effective at deflecting these criminals to other, easier targets. If you do not already have a Visitor's Log, HERE'S a template you can use.

- Do not let staff hold the door for anyone until you are sure that they are authorized to be in the area. If your building uses security badges and someone tries to follow you through a controlled door, demand to see their badge.

4

E-MAIL
NOT YOUR AVERAGE SNAIL MAIL

DIFFERENCES IN EMAIL SYSTEMS

SECURITY OF HOSTED EMAILS

PERSONAL EMAIL ACCOUNTS

WORK OUT THE BUGS IN YOUR INFORMATION SECURITY

TABLE OF CONTENTS

NEXT PAGE

DIFFERENCES IN EMAIL SYSTEMS

Today, businesses' communication activities occur almost entirely through email. The prevalence of email communication means that large amounts of public and private information is shared on a daily basis among internal and external sources. Subsequently, secure email systems are an increasingly vital necessity for businesses of any size.

THERE ARE TWO DISTINCTIONS BETWEEN EMAIL SYSTEMS:

IN-HOUSE EMAIL

With in-house email, you choose to control your email system through an internal data center and dedicated IT staff. This allows you to monitor your email system security in-house.

HOSTED EMAIL

Many businesses use hosted email either through webmail, like Gmail, Hotmail or Yahoo mail, or an email service, like as XO Communications or AppRiver. Selecting hosted mail means that someone other than your own IT people has a copy of your email on their servers and manages your email for you. If your business uses this type of email, you may need to think about how to keep your emails safe between your computer and the host system.

SECURITY OF HOSTED EMAIL

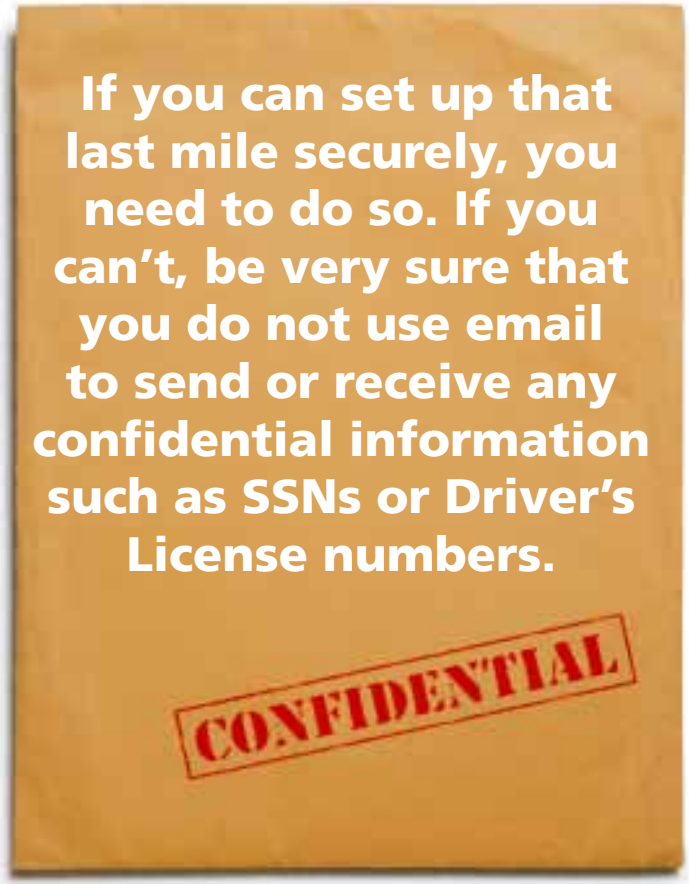
Hosted email adds a layer of complexity to your security arrangements.

Hosted Email: When you use hosted email, the message is leaving your perimeter before it gets back to your co-worker. Since standard email is not encrypted, that message could be intercepted and read by basically anyone during that period while it's outside your perimeter.

The same risks apply when emailing outsiders. More and more companies are implementing secure email in order to protect messages with confidential content. Many of those systems use Transport Layer Security (TLS) which scrambles the message while it's moving from the sender's email system to the recipient's email server but does not protect the message between the recipient's email server and his/her desktop. That leg is a responsibility of the recipient.

While it is dangerous to generalize from just a few examples, all the email services previously mentioned have some way to secure the last mile from their email server to your desktop. XO Communications, for example, has detailed instructions on their webpage explaining the settings and port numbers that you have to set up on each desktop in order to connect to them securely. AppRiver has instructions for how to use the capabilities built into MS Outlook to protect the connection.

Unfortunately, the connection for the users of webmail is harder to make secure. Gmail claims on their website that encryption is available, but a number of requests for help on their discussion groups have gone unanswered. Yahoo has yet to return our request for information.



As with so many aspects of changing technology and communication, the lines between personal and professional life often become blurred. Keeping personal email accounts separate from work email accounts can have some real advantages for your business. However, for an employer, there are legitimate concerns to be had regarding the security of confidential business and customer information. All businesses should clearly define email guidelines and discuss them with all employees.

TYPICAL PERSONAL EMAIL POLICY:

@ Do not permit the use of a personal email account for work related communication. Customers and co-workers expect us to communicate through a consistent channel. In these days of spam and email spoofing, messages from any address other than your regular domain will be met with justifiable suspicion.

@ The employer should retain the right to monitor personal email if they check it on a work computer. Employees have no right to an expectation of privacy in anything they do on a work computer or system.

@ While on a work computer, all the normal rules about professionalism and appropriate use still apply, even when using a "personal" account.

PROS TO PERSONAL EMAIL

HERE ARE SOME OF THE ADVANTAGES TO HAVING SEPARATE EMAIL ACCOUNTS:

It helps to keep business and personal issues separate. Work is completed on the employee's official email account, and they can talk to family and do their internet shopping via the personal account.

It keeps a lot of the spam messages out of your work email box. Spammers can find you in lots of different ways, but some of the most common involve scanning internet chats and shopping sites for email addresses. If you use a work email address and the spammers find you, they can rapidly invade the account - and you can't easily change it because that's where customers expect to find you. In addition, if you use one of the free web-based services like Hotmail or Yahoo and the spam gets too bad, you can always abandon the account and open a new account.

If set up correctly, it's portable. When you're no longer an active employee, you will lose the company-provided email address. A personal address provides continuity during your transition. If you use one of the web-based services, you're not even dependent on your personal internet service provider.

5

PHISHING & SPAMMING
A FLY IN THE OINTMENT

DON'T SWIM WITH THE PHISH

SPAM ANYONE?

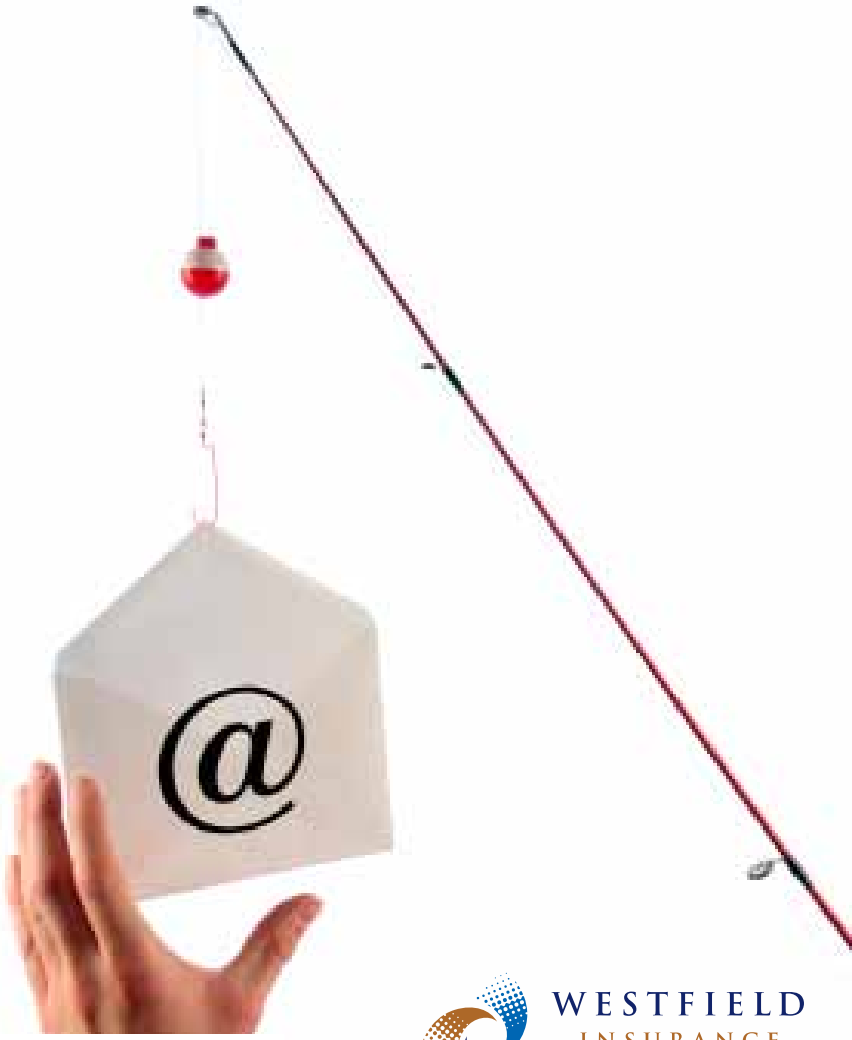
WORK OUT THE BUGS IN YOUR INFORMATION SECURITY

TABLE OF CONTENTS

NEXT PAGE

DON'T SWIM WITH THE PHISH

Phishing is an increasing and serious problem. Luckily, consumers and some tools are getting better at identifying and deleting them. Unfortunately for businesses, many legitimate messages get thrown away because they look too much like phishing messages. TRUSTe and Ernst & Young published a white paper on "How Not to Look Like a Phish".



HERE ARE A FEW THOUGHTS THAT CAN HELP YOU KEEP YOUR MESSAGES FROM LOOKING TOO MUCH LIKE A PHISH:

Don't request personal information from customers via a hyperlink in an email. If you need information, such as an updated address, tell the customer to go to your company's website and log in – not through a provided "convenient" link.

Personalize emails whenever possible. This proves that you know your customer's name. For example, use "Dear John" instead of "Dear Sir".

Don't get your customers in the habit of linking through someone else to get to you. For example, if you are going to provide a link in the email, if should look like www.yourdomain.com, not www.somebodyelse.com?redirect=www.yourdomain.com. Never use the IP address in the link.

Use simple and intuitive domain names and directory paths. The longer the address line, the more likely it is for something to be spoofed and the harder it will be for your customers to recognize the falsification.

Be very cautious about using "click here" links. You may think they read better, but customers should rightly be suspicious of any attempt to obscure the destination of a link. Written-out addresses are better.

Proofread and spell-check all your communications. While more phishers are improving their English, many users still rightly assume that a grammar or spelling mistake is evidence of a possible phish by someone whose native language is not English.

Avoid messages with an urgent, threatening or time-sensitive tone. Don't say anything about passwords and account cancellations.

SPAM ANYONE?

Spam filters are getting better every year to keep up with the ever-increasing flood of spam. But no matter how good the filters get, some spam will always leak through. Consequently, some fraction of good messages will be inappropriately tagged as spam and lost. Your reader may never even know that the message was sent, nor you that the message was rejected.

Rapid changes in spammer tactics makes any list of suggestions obsolete almost immediately. There will never be a definitive list - the anti-spam vendors are justifiably worried about giving the spammers a roadmap showing how to bypass their filters.

GENERAL RULES TO AVOID LOOKING LIKE SPAM

Your subject line is important. A blank subject line (or, worse, a subject line that is ambiguous and generic like "Hi" or "I love you") will almost certainly get your message tagged as spam. A good subject line is also a courtesy to your readers, helping them to more quickly prioritize their inboxes and give your email the attention it deserves.

Mailing to lots of people at once will increase the odds of being tagged as spam. This is a problem for the publishers of legitimate email newsletters with large distribution lists. Use a company-issued email address. Sending from a free email account like yahoo.com or gmail will increase the odds of getting tagged.

Avoid common spam words like "cheap" and the V- word (rhymes with the famous waterfall). That sometimes means completely avoiding certain topics but more often means avoiding flowery, inflammatory or overly-promotional language.

Avoid all caps and multiple exclamation marks.

Avoid images, fancy graphics and html code in your email. Hackers and spammers hide things in those glossy "enhancements". The simpler your message, the more likely it is to get through unmolested.

SPELL-CHECK! Spammers are getting much better at the use of grammatically correct English but bad spelling is still a surprisingly good filter for spam.

If you are sending a newsletter, always include your real contact information and a working set of "unsubscribe" instructions at the bottom of the message. This won't actually help you get past the spam filters – too many spammers just include fraudulent unsubscribe options in their messages – but it is the law.

Try to keep your message under two megabytes including embedded pictures and attachments. This isn't strictly a spam-filtering rule but many mail servers use a 2 meg/ message limit to keep any one message from tying up the lines.

Finally, if you don't get an answer in a reasonable amount of time, follow up on your message. No matter what you do or how good the filters get, some false positives will always exist. The person might be ignoring, you but it's more likely that they never got the message.

6

HACKERS CRAWLING THEIR WAY IN

PROTECTING AGAINST HACKERS

WHO GETS HACKED?

WORK OUT THE BUGS IN YOUR INFORMATION SECURITY

TABLE OF CONTENTS

NEXT PAGE

PROTECTING AGAINST HACKERS

Bill Brenner of CSO Online ran a column about fear and hype by the security vendors, especially around the need to "immediately patch the latest critical vulnerability" in a piece of software. Patches* fix holes in the vendor's software and keep hackers from being able to walk through the back door of your system. Applying patches is important. Security vendors want you to apply the patch immediately in case the hackers are pounding on your door right now. Every minute you wait is a minute of exposure.

But most of us don't apply the patches immediately. It takes your IT shop a few days of testing to make sure the patch won't break something else and to tweak the network so everything runs properly again. The truth is that most responsible IT departments use a layered approach to security. They have tools and policies that will generally keep out the malicious software long enough for IT to complete the tests and apply the patches.

***PATCHES:** bits of code added to your computer to fix a hole. *(Patches can also be used to add a new feature or fix something else in the program but for now we'll stick to security patches.)*

SO WHO GETS HACKED?

According to a Verizon report, nine out of ten data breaches could have been prevented if the company had taken reasonable security measures, most often applying patches that had been available for years. As Brenner points out, why should a hacker bother to write a complicated new virus to exploit the latest hole when you can still make money walking through holes that should have been patched four years ago?

If you have a solid approach to computer security, you can take the time to test the latest patches properly. On the other hand, if you don't have a dedicated IT team, you probably also don't have the staff to conduct the testing so you should set the patches to automatically update themselves.

Of course, if you're not guarding your infrastructure with the basics (strong passwords, current anti-virus and anti-spyware, firewalls, up-to-date on patches even if not up-to-the-minute, etc.), you need to start now.

Hackers hit

HOW PATCHES WORK

In a perfect world, all the code on your computer would do exactly what it's supposed to do and nothing more. In the real world, new code was added on top of existing code to fix a problem or to add some new feature until, over time, the code became too complicated to test for every possible scenario. Hackers found ways to exploit the holes in the code. By sending just the right command in just the right circumstances, they could make the computer do something it shouldn't – like give the hacker permission to install software and take control of the computer.

When such a vulnerability is discovered, the developers who made the software have to figure out how to plug the hole – how to change the code just enough to stop the hacker without shutting down the new feature they added or interfering with some other application. "Patches" are the bits of code to be added to your computer to fix that hole.

7

LAWS
THE "BUTTERFLY EFFECT"

SOCIAL SECURITY NUMBERS:
HOW TO LIMIT YOUR LIABILITY

SHREDDING

WORK OUT THE BUGS IN YOUR INFORMATION SECURITY

TABLE OF CONTENTS

NEXT PAGE

SSN: HOW TO LIMIT YOUR LIABILITY

We all know about the rising threat of identity theft and hear how it can affect a person's life. Along with businesses, legislatures around the country are also under a lot of pressure to do something about identity theft. Here are some tips to help you keep your customers' Social Security Numbers (SSNs) safe. It's not just a good practice - in almost all states, it's the **law.**

GUIDELINES

- If you don't absolutely need the SSN, don't ask for it. Take the field off forms unless it is absolutely necessary.
- If you only need the SSN once, use and destroy. Don't record a copy or make a note "just in case."

IF YOU ***MUST*** ASK FOR THE SOCIAL SECURITY NUMBER, PROTECT IT CAREFULLY WITH THESE TIPS:

Watch records that get posted on a website. Be cautious of spreadsheets with SSNs, which can get found via a search engine. Keep documents with SSNs in secured folders.

For website logins, don't use the SSN unless the website also requires a password or PIN for access.

Several states explicitly ban the selling, renting, trading, etc. of any list containing the consumer's SSN, so don't give out a consumer's SSN to anyone.

Only print or show the last four characters of the SSN.

Unless the message is encrypted, don't request or send SSNs via email.

SSNs may not be printed on any ID card required for the individual to receive products or services. SSNs generally may not be printed on the proof-of-insurance card, including embedding the SSN using a barcode, smart chip or magnetic strip.

TIPS, CONTINUED...

When sending mail, do not print the SSN on anything mailed to the individual unless required by law. Media tend to highlight the technology-based hacks and compromises, but research continues to show that most identity theft is committed based on paper records – the largest single source of stolen SSNs being physical mail theft; second is the trash.

IF YOU DO SEND A DOCUMENT WITH A SSN IN THE MAIL:
Be sure the SSN is not visible through the envelope. Also watch postcards, top-sealed mailers with open sides or envelope window openings.

The "required by law" exception applies primarily to certain HR records like your W-2. There may be a few state laws requiring us to send SSNs by mail either to a state agency or to the individual, but as a general rule, avoid putting any document with the consumer's SSN in the mail unless it is strictly required.

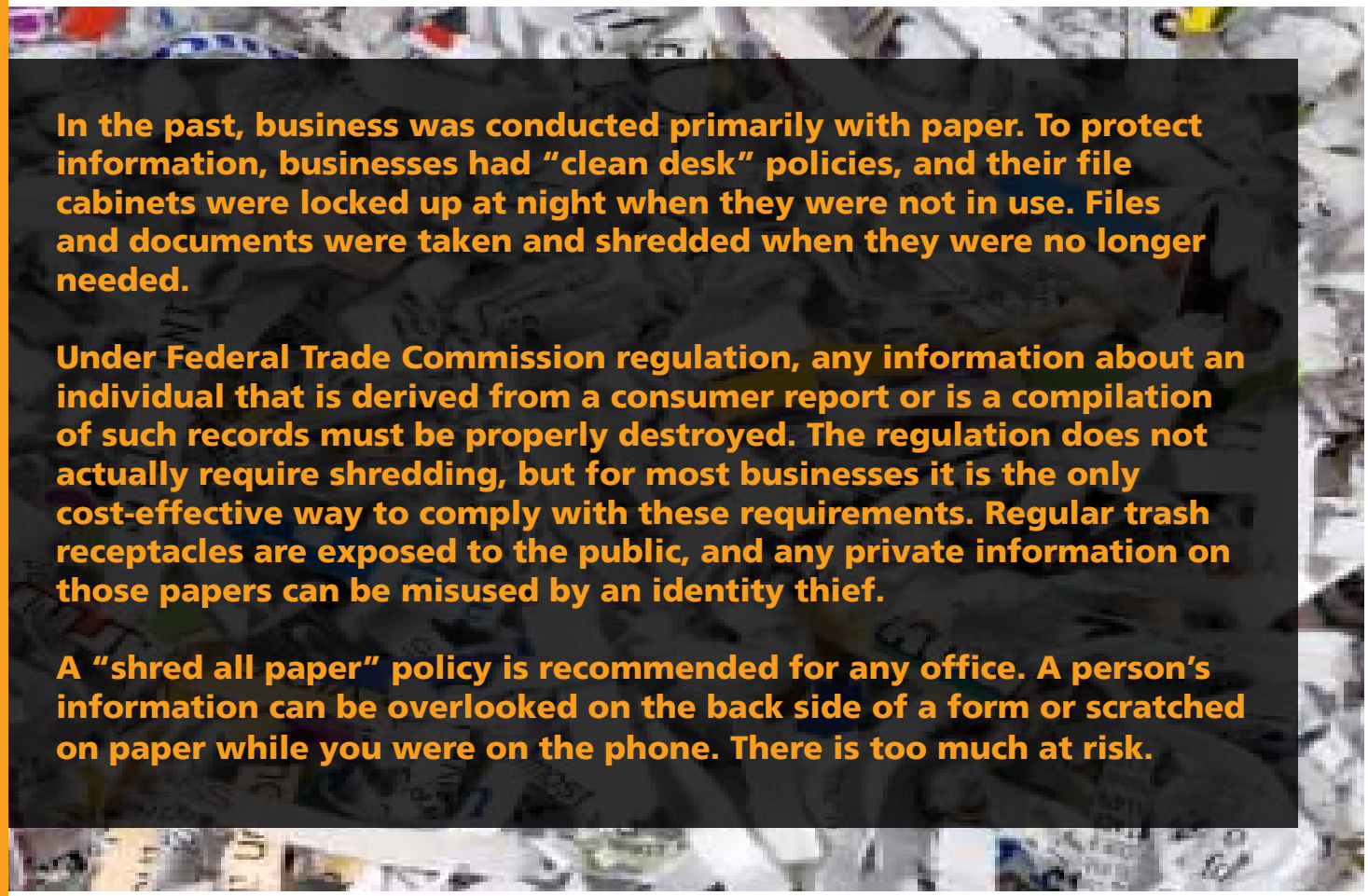
Destroy everything when it is no longer necessary. As soon as that retention period runs out and the record is no longer necessary, make sure that it is properly destroyed.

Paper documents should generally be destroyed by shredding. While the FACTA Disposal regulation allows other means of destroying paper documents, shredding is almost always the most reliable and cost-effective way.

Make sure that all electronic media (hard-drives, floppy-disks, thumb-drives, CD-ROMs) get sent back to your IT department for wipe. Make sure that the data has been irrecoverably destroyed first before donating or throwing away.

SHREDDING

These days, almost all customer information has some connection to a consumer report and is covered under this regulation.



In the past, business was conducted primarily with paper. To protect information, businesses had "clean desk" policies, and their file cabinets were locked up at night when they were not in use. Files and documents were taken and shredded when they were no longer needed.

Under Federal Trade Commission regulation, any information about an individual that is derived from a consumer report or is a compilation of such records must be properly destroyed. The regulation does not actually require shredding, but for most businesses it is the only cost-effective way to comply with these requirements. Regular trash receptacles are exposed to the public, and any private information on those papers can be misused by an identity thief.

A "shred all paper" policy is recommended for any office. A person's information can be overlooked on the back side of a form or scratched on paper while you were on the phone. There is too much at risk.

HOW SHOULD YOU DISPOSE OF OFFICE PAPER?

- Small offices can get away with a personal shredder.
- If your business consists of more than 10 or 15 people in the office, it's probably more cost-effective to contract a reputable shredding vendor who will pick up and properly dispose of your paper. Most shredding vendors will provide locked bins where paper waste can be stored until pickup. Have enough bins to be convenient for your staff.
- New laws are tough – they don't care if information was lost on a disk drive, backup tape or paper report. One thousand records lost on an unencrypted USB drive is just as bad as one thousand records lost through someone "dumpster diving" and finding last month's discarded report.
- Remember to physically protect all reports, printed emails, photocopies of receipts and other paper materials by locking them away securely until they are disposed of. Many companies have worked out recycling arrangements so you can safely dispose of your paper and help the environment at the same time!

Proper protection and disposal of printed information is equally important as the protections we place on information stored on electronic media.

8

SOCIAL MEDIA: GETTING SOCIAL ON THE WEB

WORK OUT THE BUGS IN YOUR INFORMATION SECURITY

TABLE OF CONTENTS

NEXT PAGE

SOCIAL MEDIA

Social media, or Web 2.0, is about sharing timely, dynamic content and interactations with people through social networks. Remember how your parents read the newspaper every evening or watched a newscast on television? The information flow was one way. Websites such as Facebook and Twitter are about sharing information, opinions and experiences in a rapid flow of information.

Businesses and their customers interact with social media every day and probably don't even know it. Whether reading a review on Amazon or watching a video on YouTube, internet users choose to interact with the social web with increasing frequency. Ultimately, this means changes for the way we do business and new and exciting means of communicating with customers, but also greater exposure to risks.

On June 9, 2009 at 10:22am, the 1,000,000th word was adopted into the English language. What was that word? Web 2.0

SHOULD YOU BLOCK SOCIAL WEBSITES?

Whether your business has adopted or is blocking social networks, it is probably time to start considering a company policy.

While the inherent risks and productivity impact of social sites, such as Twitter, Facebook, etc., are a good reason to not allow them in the work environment, you should realize that the use of social media has skyrocketed among businesses and can become an excellent tool for leveraging your brand.

It is difficult to balance a no tolerance policy for social sites while they can also be used as effective marketing and communication tools.

Blocking all non-work essential sites has proven time and time again to reduce employee morale; which in turn has greater impact in reducing productivity.

If you feel your business is behind in addressing this issue, don't feel alone. Many companies are struggling to weigh the risk versus the reward.

SOCIAL MEDIA USAGE:

500 million+
users on Facebook

60 million+
members on LinkedIn

75 million+
users on Twitter

More than 1 billion pieces of content (web links, news stories, blog posts, notes, photos, etc.) are shared each week on Facebook

The fastest growing demographic is those 35 years old and older

THE GOOD

Social networking or social media IS the future of communication. Rather than wait for the newspaper to be delivered, you get news as it happens by the people who are experiencing or involved in the situation. Remember the US Airway's flight that landed in the Hudson River? Well before the media had a chance to deploy reporters to the scene, passengers on the flight were posting pictures and updates through their Twitter account. Companies are using social networks as a tool to market their brand. Have you heard of Blendtec? How about "Will it Blend?" Blendtec CEO, Tom Dickson, became an instant celebrity when he began posting videos of his blender destroying things like iPhones, Guitar Hero guitars, etc. on YouTube. It also helped them sell a lot of blenders. Even Westfield Insurance uses LinkedIn and Facebook to find talent, as well as communicate promotions and events. Blogs such as this one and the Westfield Risk Factors Blog are another way that companies can reach out to current and potential customers. Internally, employees can network between departments, giving them a feeling of being more than just another "employee."

THE BAD

What are some of the drawbacks? First, it is difficult to balance a work culture that embraces social networking while ensuring that it does not impact productivity. It is increasingly more difficult to monitor or limit these activities as social networks extend beyond the desktop and onto cell phones. Additionally, companies may have a difficult time restricting or limiting the content that employees post. A disgruntled employee may post negative information about their employer for all to see. Companies may have human resource policies when it comes to employees posting information about their employer; but how does a company draw a hard line in the sand between moral, religious and political biases and freedom of speech? Social networks are making it difficult for companies to separate an employee's business relationship and their personal lives. On the other hand, employees are learning that inappropriate use of social networking may allow a company to terminate their employment.

THE UGLY

So your company is on the cutting edge of technology and you have an HR policy that addresses social networks; is that enough? Not quite. Aside from the fact viruses, Trojans and other malware have found a new distribution vector, there are many other security concerns. Data Loss Prevention is among the top as employees may maliciously or accidentally distribute sensitive company information.

Depending on the leaked information, your company may be faced with regulatory fines and requirements such as privacy breach. Even if the information isn't overtly sensitive, information may trickle out that may give a hacker or your competitors an inside advantage. Take for example your network administrator who blogs and/or posts questions about Cisco routers and firewalls. A hacker may use that inside knowledge to target the vulnerabilities specific to Cisco products. I am sure there are additional threats that remain to be discovered.

ABOUT THE AUTHORS

Bill Murray, CISSP - Bill currently manages the Risk, Security and Compliance team within Information Technology and is responsible for information security policy creation, awareness training, vulnerability scanning, security event monitoring, incident response, risk assessments, role based access control and disaster recovery planning. Full Bio here.

John Brady - In addition to an MS in Computer Science from Rensselaer Polytechnic Institute, John has extensive experience in several areas of IT ranging from assembler programming to web site content management on cloud-based virtual servers. Full Bio here.

Jake Harris - Vulnerability & Forensics Analyst for the Westfield Insurance. Jake's been with Westfield since 1998, primarily working in the role of Network Administrator, however he's had several opportunities to participate in many of the security focused projects implemented in the past 10 years. Full Bio here.

Jeff Gibson - a Cleveland State University graduate with a Bachelor's degree in Computer Science. He began his IT career in 1990 and not until 1997 did he get interested in the security field. He is currently a Vulnerability Management, Compliance & Forensics Analyst at Westfield. Full Bio here.

Mike Rossander, CISM - Prior to joining Westfield, Mike was a Senior Manager for Ernst & Young's business process consulting practice. Before that, he served for 15 years in the US Army, mostly in the artillery. Mike's undergraduate degree was in physics and education (he was briefly a high school science teacher) and he holds an MBA from Carnegie Mellon University. Keeping with our bug theme, Mike keeps honeybees in his backyard and recently started teaching himself forging (the blacksmithing kind).

COPY EDITING provided by Katie Herbst & Leslie Berzansky, Senior Marketing Specialists for Westfield Insurance and our friends at PR 20/20, an inbound marketing agency and PR firm specializing in content marketing, public relations, social media and search marketing. www.pr2020.com

EBOOK LAYOUT AND DESIGN by Leslie Berzansky, Senior Marketing Specialist and Cody Albert, Designer at Westfield Insurance.

GET UPDATES ON INFORMATION SECURITY TOPICS - **SUBSCRIBE TO WESTFIELD'S INFOSEC BLOG!**