ONLINE RISK

PERSONAL & BUSINESS BASICS

C.P.R.

ONLINE RISK

Crisis Prevention & Restoration – We are here before the storm - we design and facilitate emergency response plans - to help business restore income streams prior to a crisis; Our job is to focus on business and employee well-being; to prevent a variety of crisis, disasters and emergencies; to prepare & facilitate restoration of business when they are impacted.

Business Well-Being

Our clients are dedicated to changing their communities by taking personal responsibility for disaster recovery; by leading their employees to prepare for the unexpected. They know a few days of no income would equate to a potential close of business and that their employees depend on them to ensure their households run and the community at large holds this same expectation. Imagine what months or years would do to the local economy without businesses looking at the long term impact prior to a crisis; Joplin, MO, Sandy, NJ, All hit by Katrina and Charleston, WV are all examples of areas hit by disasters that required longer than a day or two to recover. Crisis Prevention & Restoration is focusing even broader; we encourage businesses to look at internal crises as well as external; including expected medical leaves and the unanticipated; broken supply chains; building failures and beyond.

ONLINE RISK

The key to continuity, restoration and recovery is to understand the "ripple effect".

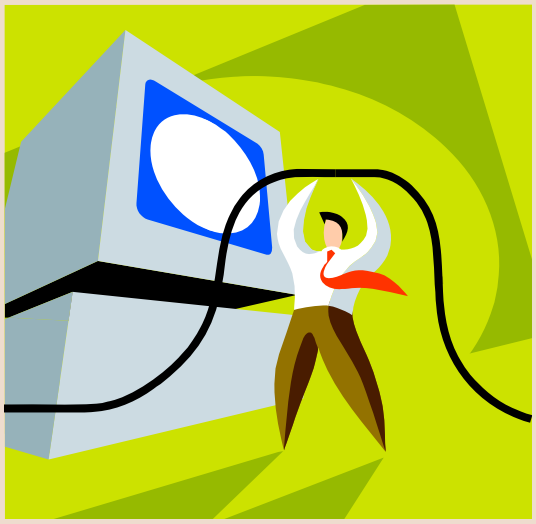
When an emergency, disaster or crisis strikes the ripple effect always happens.

Imagine a pond and your community (personal, business, town or county) as a pebble. A crisis is the catalyst that throws your pebble into the pond. Out flow the ripples to all the community. The ripples happen during good times, during every day times, and during crisis, emergencies and disasters. We effect others and other effect us - our lives, businesses, community, friends and family.

Crisis Prevention & Restoration is a small private start up founded in the North Bay of California. Our partners and consultants have direct real experience with emergencies and the impacts on small business. We span a wide chasm ranging from retails sales, medical office management, medical specialty management, restaurateur, manufacturing, nutraceutical manufacturing and sales, storage, Moms, Dads, Parents and Friends. Our knowledge is just as wide.

WERE YOU A TARGET?

The attack on Target's POS system actually was widespread (not limited to Target). US-CERT is working with Target and other victims to recover from this attack. As in most cyber-attacks the victims aren't a single entity. The Target attack allows us to easily see the victims – Target obviously but also its employees, its vendors, and its shoppers. When a disaster or crisis strikes the ripple effect always happens.



ONLINE RISK

Who is this CERT that's working with Target?

It's Homeland Security and they have two CERT programs.

Community Emergency Response Team is a FEMA Program educates people about disaster preparedness for hazards that may impact their area and trains them in basic disaster response skills, such as fire safety, light search and rescue, team organization, and disaster medical operations.

United States Computer Emergency Readiness Team is a Homeland Security program that strives for a safer stronger internet.

We've relied heavily on information from US-CERT for this article.

ONLINE RISK

Cloudshare Blog

Good News: Vulnerable NTP Servers Closing Down

Published on February 23, 2014 11:00AM by Jérôme Fleury.

"On Monday, February 10th, CloudFlare experienced a large DDoS attack, with nearly 400Gbps of NTP attack traffic hitting our network. We were not the only networks getting hit by massive NTP attacks. Around the same time, OVH reported a similarly sized attack. Since the attack we've heard from a number of other networks that have seen large NTP-based attacks over the last few weeks."

"During the 400Gbps attack we saw 4,259 IPv4 addresses of involved vulnerable servers that were sending attack traffic to our network. These networks were not controlled by the attacker directly but instead were running network time protocol (NTP) servers that responded to commands that would create very large responses, thus acting as a good amplification vector. Specifically, all of these servers were used by attackers to reply large packets in response to the "monlist" command."

Full article - http://blog.cloudflare.com/good-news-vulnerable-ntp-servers-closing-down

ONLINE RISK

DOS ATTACK? DID YOU HELP?

What?

In a denial-of-service (DoS) attack, an attacker attempts to prevent (you) legitimate users from accessing information or services, such as banking, Amazon even Google. *By targeting your computer and its network connection*, or the computers and network of the sites you are trying to use, an attacker is often able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer.

The most common and obvious type of DoS attack is when a network "floods" with information. When you access the URL for a website via your browser, you send a request to that site's computer server to view the page. Servers can only process a certain number of requests at once (much like us – we can only multi task so far), so if an attacker overloads the server with requests, it can't process your request. This is called a "denial of service" because you can't access the site.

ONLINE RISK

DOS ATTACK? I HELPED?

What? I couldn't have helped! I put others at RISK?

An attacker can use spam email messages to launch a similar attack on your email account. If you have an email account supplied by your employer they will take steps to minimize this chance. If you have one available through a free service such as Yahoo or Hotmail, it's your responsibility to minimize this – especially if you download the emails into your computer versus using the online services. We at C.P.R. have minimized these types of risks by switching to Google who has some of the strongest filters and securities in place.

ONLINE RISK

DDOS ATTACK? I WAS USED!?!

In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. **By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a website or send spam to particular email addresses.** The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the denial-of-service attack.

C.P.R.

ONLINE RISK

I WAS VICTIMIZED!

Unfortunately, there are no effective ways to prevent being the victim of a DoS or DDoS attack, but there are steps you can take to reduce the likelihood that an attacker will use your computer to attack other computers.

C.P.R.

ONLINE RISK

I WILL BE PART OF THE SOLUTION!

1. ***Connect to a Secure Network***

   A secure router is one of the best initial lines of defense

2. ***Enable and Configure a Firewall***

   Control the flow of information between your computer and the internet

3. ***Install and Use Antivirus and Antispyware Software***

   Critical step in protecting your computer

4. ***Remove Unnecessary Software***

   The less software you have installed, the fewer avenues for potential attack

5. ***Disable Nonessential Services***

   Such as printer share and file share

6. ***Modify Unnecessary Default Features***

   AutoRun feature in Microsoft Windows systems was a default feature at the time of the Conficker malware and was one of the three ways computers became infected

C.P.R.

ONLINE RISK

I WILL BE PART OF THE SOLUTION!

7. *Operate Under the Principle of Least Privilege*

Consider using a standard or restricted user account for day-to-day activities

8. *Secure Your Web Browser*

Most browsers have security setting under tools or options and all have website where one can learn to set security to a safe level.

9. *Apply Software Updates and Enable Future Automatic Updates*

Updates patch or fix vulnerabilities, flaws, and weaknesses (bugs) in software

10. *Use Good Security Practices*

I. Use caution with email attachments and untrusted links.

II. Use caution when providing sensitive information.

III. Create strong passwords.

C.P.R.

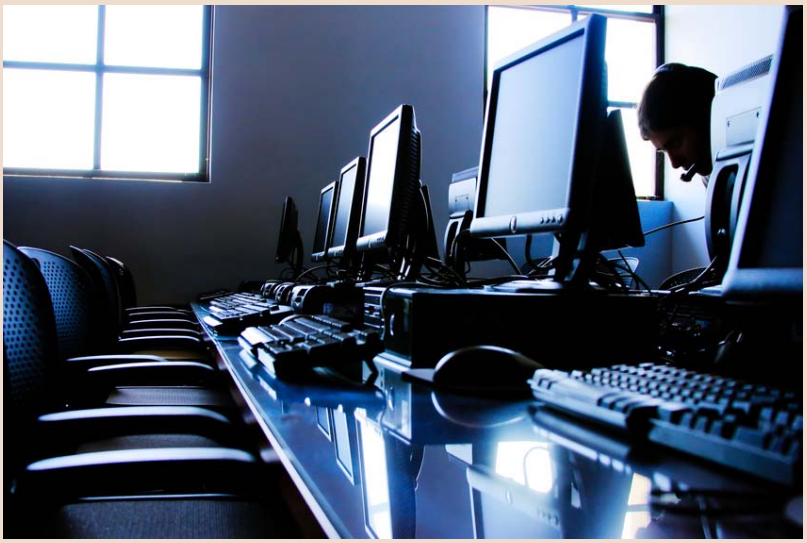
ONLINE RISK

I WILL KNOW THE WARNING SIGNS!

Not all disruptions to service are the result of a denial-of-service attack. There may be technical problems with a particular network, or system administrators may be performing maintenance.

However, the following symptoms *could* indicate a DoS or DDoS attack:

- unusually slow network performance (opening files or accessing websites)
- unavailability of a particular website inability to access any website
- dramatic increase in the amount of spam you receive in your account



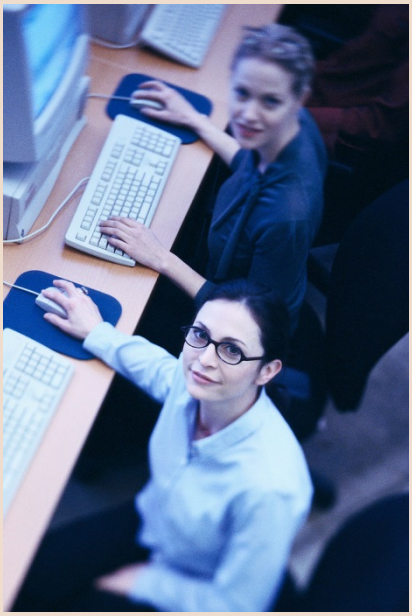
C.P.R.

ONLINE RISK

I WILL TAKE ACTION!

Even if you do correctly identify a DoS or DDoS attack, it is unlikely that you will be able to determine the actual target or source of the attack.

1. Contact the appropriate technical professionals for assistance.
2. If you notice that you cannot access your own files or reach any external websites from your work computer, contact your network administrators. This may indicate that your computer or your organization's network is being attacked.
3. If you are having a similar experience on your home computer, consider contacting your internet service provider (ISP). If there is a problem, the ISP might be able to advise you of an appropriate course of action.



ONLINE RISK

"THEY" HAVE MY INFORMATION!

Lock your computer when you are away from it.

Locking your computer prevents another person from being able to simply sit down at your computer and access all of your information.

Disconnect your computer from the Internet when you aren't using it.

The likelihood that attackers or viruses scanning the network for available computers will target your computer becomes much higher if your computer is always connected.

Evaluate your security settings.

If you hear of something that might affect your settings, reevaluate your settings to make sure they are still appropriate

Sometimes the threats to your information aren't from other people but from natural or technological causes. Although there is no way to control or prevent these problems, you can prepare for them and try to minimize the damage.

Protect your computer against power surges and brief outages.

Back up all of your data.

We happen to like Google for this but we also use Dropbox and Evernote for documents plus additional resources for photos such as the photos on our phones and SmugMug for camera pictures.

ONLINE RISK

I HAVE A VIRUS!! WHAT DO I DO?

1. Call IT support -

If you have an IT support department at your disposal, notify them immediately and follow their instructions.

2. Disconnect your computer from the Internet

Depending on what type of Trojan horse or virus you have, intruders may have access to your personal information and may even be using your computer to attack other computers.

3. Back up your important files

At this point it is a good idea to take the time to back up your files. But realize the malware may attach so be careful with these.

4. Scan your machine

Many antivirus products provide this functionality.

5. Reinstall your operating system

If the previous step failed to clean your computer, the most effective option is to wipe or format the hard drive and reinstall the operating system.

C.P.R.

ONLINE RISK

I HAVE A VIRUS!! WHAT DO I DO?

6. Restore your files

If you made a backup in Step 3, you can now restore your files. Before placing the files back in directories on your computer, you should scan them with your anti-virus software to check them for known viruses.

7. Protect your computer

We've included 12 Actions small business and home users can take to protect their computers. Please, print the handout for easy reference.

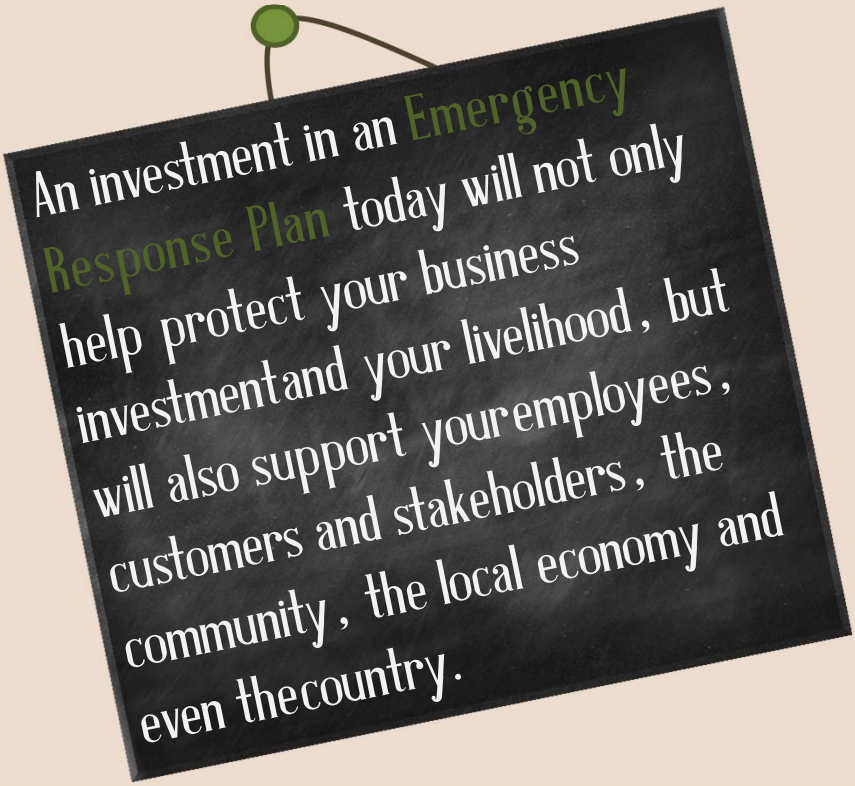
SMALL BUSINESSES & HOME USERS

12 ACTIONS SMALL BUSINESS & HOME USERS CAN TAKE TO PROTECT THEIR COMPUTER SYSTEMS

1. Consult your system support personnel if you work from home
2. Use virus protection software
3. Use a firewall
4. Don't open unknown email attachments
5. Don't run programs of unknown origin
6. Disable hidden filename extensions
7. Keep all applications, in cluding your operating system, patched
8. Turn off your computer or disconnect from the network when not in use
9. Disable Java, JavaScript, and ActiveX if possible
10. Disable scripting features in email programs
11. Make regular backups of critical data
12. Make a boot disk in case your computer is damaged or compromised

C.P.R.
CPR4BIZ@GMAIL.COM
CRISIS PREVENTION & RESTORATION

ONLINE RISK



We would love to work with you. Contact us directly to begin, modify or to take your business emergency preparedness and well being plan to the next level.

If you would like to inquire about Crisis Prevention & Restoration's keynotes, workshops, seminars, coaching sessions or have general questions, please contact us.

You can reach our business manager, at the following email address:
businessmanagr (at) cpr4biz (dot) com
or call 415.891.9107

We look forward to working with you!

Based on FEMA Booklet12pg.pdf

C.P.R.