Website Security: Protecting the Face of Your Business Online

Your website is the face of your business online and it needs to be protected. It is extremely important to ensure that your website and its supporting information assets are inventoried and essential steps are taken to secure the website. Key items that are part of a "Website Security Checklist" include:

- Safeguards in place to protect intellectual property such as logos, video, and other printed and electronic material through copyright, and registered trademarks;
- Webhosting and site maintenance contracts are current and reflect business needs;
- Domain name is protected from hijack and renewal schedule is followed.
- Disaster recovery procedures in place to ensure site is operable in the event hosting company suffers an outage.
- Have a system of intrusion detection in place that is layered and includes a firewall, antivirus, and periodic website anti-phishing audits.
- Keep software, applications, and patches up to date.
- Have a cyber-security insurance policy in place.

Email Security: Every business should train employees not to open unknown attachments and should have an email security application in place that blocks messages with known viral delivery extensions including .vbs, .bat, and .exe.

Monthly Musings:

Every Business Needs a Risk Management Plan

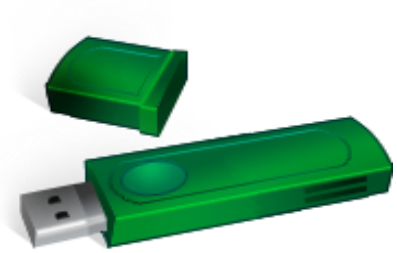
Businesses face many risks on a day to day basis and any number of these risks can have dire consequences if adequate plans are not made to manage and mitigate them. The creation of a risk management plan is a critical component to the business planning process and without sufficient forethought given to business risks all other aspects of a business plan can be rendered moot as it is difficult if not impossible to continue to execute any plan should the business succumb to any number of business risk,

One key element that is often overlooked in the business planning process is adequate funding for risk management. Without setting aside dedicated funds to manage and mitigate risks, the business leaves itself exposed and vulnerable and often has gaps in its internal controls, financial management and accounting, and information security. It is the unfortunate consequence of underfunding risk management that losses suffered by a business that had not adequately planned for and mitigated a risk tend to be higher, more severe, and business interruption is often prolonged impacting the financial viability of the business going forward.

The greatest risks that a business can avoid are the ones that can be accounted for, managed, and mitigated through a well-funded and comprehensive risk management plan. Failure to incorporate risk management into the business planning process leaves your business, employees, and customers exposed. You put a lot of effort and energy into building your business and you should take all the necessary precautions to ensure that it will continue to thrive even in the face a significant business risk event. So take the time to protect your business and consult with a Risk Management as a Service (RMaaS) provider today.

Wrally Dutkiewicz, MBA CFE
Owner/Principal Consultant
FastPepper Solutions

Delete



box or enter quote or tagline he

Securing USB Drives

USB drives pose a significant information security threat to a business. If it is absolutely necessary that data be portable and stored on a USB drive the following security measures should be put in place:

- Have a written policy that specifically indicates what information is allowed to be stored on a USB drive and train employees on the policy.
- Ensure that the USB drive is encrypted with all the following measures:
    - The USB drive encryption uses a “lock and key” protocol that only allows the USB to be used on an approved device.
    - The drive itself is encrypted with a high-level onboard security application;
    - Documents saved on the USB drive are password protected.