October, 2014

eFileCabinet®

Protect your Livelihood

with a Business Continuity Plan

Can your business survive a disaster?

How prepared is your business in the case of an unanticipated disruption to 'business as usual?' If there were a fire, flood, or a security breach, how long would it take you to get back to work? And how many days can you afford to be shut down, without possibly shutting down permanently?

Click here to take our free online risk assessment to see how prepared your business is to survive in case of business disruption.

Your growth and profitability can be instantly sabotaged if you neglect some basic principles. Proper document management is an integral part of your business continuity plan.

In February of 2006, Fosselman & Associates of Anchorage, Alaska, suffered a total building loss due to fire. Mere weeks away from tax deadlines, the building was completely destroyed. Because they had already made the choice to be a paperless office, all essential business files had been backed up, stored, and protected off-site. They were able to open the following day by noon in a rented building with ten years of tax returns and critical documents intact and on hand. Because they were prepared before this disaster struck, they actually ***gained clients*** through a situation that could have potentially shut them down forever.

Topics

- Surviving Disaster
- Security Risks and Potential Vulnerabilities
- Risk Mitigation Strategies
- The Importance of Document Management

Today, companies face an unprecedented number of potential calamities. The frequency and severity of natural disasters seem to be on the rise. In 2012, nine of the top 10 most expensive natural disasters happened in the U.S. In fact, 2012 was the third costliest year for insured losses on record.

Security risks to information from both outside and inside sources are a constant threat. It is estimated that employees are responsible for most data breaches. 58% of cyber security incidents are caused by employees, with 34% of those incidents caused by employee accidents in handling data, and approximately 24% by unapproved or malicious data use (www.verizonenterprise.com/DBIR/2014/).

While it is difficult to calculate the cost of these data breaches, Forrester Research estimates that the average security breach costs a company between $90-$305 per lost record, and that does not include costs associated with losses of customer confidence and company image.

> "If you think compliance is expensive, try noncompliance."
>
> *– General Paul McNulty, Former Deputy US Attorney*

In addition to natural disasters and security breaches, malicious or accidental threats to your livelihood can include power outages and system failures. Whatever the disaster, the statistics are frightening: 25% of businesses do not reopen following a major event (Insurance Institute of Business & Home Safety www.disastersafety.org). It is difficult to survive such a disaster without a plan in place, yet 48% of small businesses are operating without any type of business continuity plan, even though 95% of those businesses indicated they felt they were prepared (Why your company needs a business continuity plan, www.travelers.com/prepare-prevent/protect-your-business/business-continuity/why-you-need-a-plan.aspx).

Know where potential vulnerabilities lie. Having a strategy in place before an event happens will help maximize the chance your business can recover. Planning for a catastrophic event—or a disruption of any sort—should happen well before disaster strikes. A business continuity plan is one of the very best investments your company can make. Plan to minimize disruption, because when business is interrupted, ***it costs money.***

There is excellent information available about mitigating risk in case of emergency for your business. FEMA and www.ready.gov have business continuity steps outlined:

1. *Conduct a business impact analysis to identify threats or risks**
2. *Identify, document, and implement methods to recover critical business functions and process*
3. *Organize a business continuity team and compile a plan in case of business disruption*
4. *Conduct training for your team and routinely improve your plan*

* Multiple fillable worksheets to help determine business impact are available at www.ready.gov/business/implementation/continuity

A master copy of the plan should be maintained with multiple copies stored so that team members can quickly review roles, responsibilities, tasks, and reference information (www.fema.gov/media-library/assets/documents/89510).

DOCUMENT MANAGEMENT IS INTEGRAL TO BUSINESS CONTINUITY

Security of your business data is more important today than it has ever been. If your environment is like many organizations, document management and file retention are where a great deal of potential vulnerabilities exist. Whether on-premise or in the cloud, there are certain security features your DMS should provide:

Role-based Security: Role-based security features can determine what kind of access or capability is granted to different users based on their role in the company.

Audit Controls: Sophisticated audit controls help determine activity patterns. Every click should be logged as part of an audit trail.

Automatic Logoff Settings: Allows you to set defaults for how long a session in your DMS can be idle before it is terminated.

Data Encryption: Data should be encrypted while at rest and in transit. Although some banks still use 128 bit encryption, look for a DMS that uses 256 bit SSL/TLS encryption technology.

Web Portal: Information can be securely sent to clients and portals through a secure web portal which requires login access. This eliminates the need for emailing attachments, faxing, courier, or costly UPS/FEDEX mailing.

Compliance: DMS standards should be fully compliant with all FINRA, HIPAA, SEC, and NASD regulations.

Physical Security: Data should be backed up in 2–3 different locations in highly secure facilities. All sites that store data should have sophisticated climate and temperature control and fully redundant electrical power systems.

As doing business becomes more mobile, security becomes even more critical. Potential threats that interrupt business are a rapidly growing concern for nearly all businesses. Protect your business by carefully analyzing your organization's risk profile, establishing a business continuity plan, and utilizing the right document management system. General Paul McNulty, Former Deputy US Attorney, said, "If you think compliance is expensive, try noncompliance."

Invest the time and effort required to formulate a plan, and invest in a secure DMS. Doing so will minimize your overall security risk while maximizing your return on the investment. It might just be the best investment you ever make.

For additional information about document compliance, download our white paper: *Document Retention Basics: Best Practices for Accounting Professionals*

Legal Disclaimer

All information provided on this document, website, links, downloads are in good faith and for general information purposes only. We do not make any warranties about the completeness, reliability and accuracy of this information. Any action you take upon the information on the documents, websites, links, downloads and any recommendations is strictly at your own risk. No claims, promises or guarantees about the information provided are made. We are not liable for any losses and damages in connection with the use of any or all of the information and tools provided..

As doing business becomes more mobile, security becomes even more critical.

Contact Us:
877-574-5505
www.efilecabinet.com

2989 W. Maple Loop Drive
Suite 300
Lehi, UT 84043