Dr. **Katherine Bean** PhD

July **2014**

Data Security: DUMP – STOP - BAR

A Business White Paper

The threats a business faces every day are growing. It seems now that not a day goes by in which there is not a reported security incident, such as a company losing all of their data to hackers or other Cybercriminals.

The majority of businesses have little or no processes and procedures to help secure the business. It is with this thought in mind, that **Dvana** developed the DUMP – STOP – BAR method to Data Security.

By utilizing the DUMP – STOP – BAR framework, an organization can go from nothing to a fully controlled environment in a matter of weeks.

The DUMP – STOP – BAR approach is to turn data security and, by extension, all business security on its head and approach it from a different perspective. This change of emphasis and approach enables fast growing and progressive businesses to jump ahead of their competition.

Introduction

In general, security and, by extension, data security are primarily concerned with keeping the Cybercriminals out. This is typically accomplished by utilizing:

- Passwords, to secure access and to authenticate users.
- Firewalls, to keep out unwarranted access.
- SSL certificates, to secure communications.

These methods lie at the heart of how most businesses view data security. The problem is that this all works well when everything is working correctly. Unfortunately, when faced by an attack, everything is not working correctly. This is the definition of an attack.

The first question to ask is why somebody might be interested in your data. In recent research, conducted by the Centre for Strategic and International Studies, Cybercrime is estimated at approximately $445 billion per annum, and impacts approximately 350,000 jobs in the EU and US. This is why Cybercrime is now effectively a profession. This would make Cybercrime, if it were a country, the 32nd largest economy in the world, behind the Philippines and ahead of Belgium. This is using the 2013 data from the IMF. This is what your business is fighting.

Most businesses construct their security in a similar way to how a castle is constructed, with a moat around the outside, the keep in the centre, with thick strong walls to keep out the attackers. With data security our model is the same, keep the attackers out with the firewall (moat) and walls (usernames and passwords); allow only trusted people over the drawbridge (usernames and passwords again). Then allow a trusted few into the keep (data access). Unfortunately, in order to operate, we need to allow many users (either services or people) through the firewall, and many people to connect to the data. Which effectively bypasses the defences.

User credentials are the favourite of Cybercriminals, as this will give them trusted access to data and systems. This is why there are so many phishing emails, virus laden emails and the like. I am sure many of these cross your path daily. A data breach in another organization, such as Adobe or eBay, will give up the passwords and usernames that people on your system use. This credentials system is not fit for purpose as it is simple to implement, simple to utilize and simple to subvert. This is what the Cybercriminals are doing on a daily basis, subverting passwords.

Physical access is the easiest to control as, when someone has remote access, they can attempt to access the systems or data from anywhere in the world. This is very difficult to protect against, as the Cybercriminals can be and appear to be from anywhere. This makes blocking them very difficult.

As detailed in the Data Security Levels White Paper, please consider the following four items throughout the rest of this White Paper

1. Transmission method
2. Ease of access
3. Storage type
4. Scope of availability

DUMP

Dump gives a top line thought as to what is needed. In general, dump all the unnecessary items and activities. This can easily be accomplished with a GREAT Endeavour™.

DUMP is an acronym, which stands for:

- **D**elete
- **U**ninstall
- **M**ap activities
- **P**ermanently archive

Delete

Delete all old and superfluous data. This includes the many different copies of folders and files that were generated in the distant past. Typical examples are folders which were created as a backup in case something went wrong with an edit or update. Other examples include, virtual hard disks for servers; old CD ROM disks, which are now never used; copies from software packages that are no longer needed or for which the software is no longer available.

Delete all the data except that which is required for day to day operations. It reduces the possibility of data loss and makes life quicker, easier and more efficient for everything else. Don't forget paper copies.

Uninstall

Uninstall all the software on every machine that is not needed. This includes all the old copies of applications, Java, tools bars, web browsers. Just about everything.

Removing all the old versions and all the items which are not needed for the current employee's work, reduces the risk of a virus infecting an individual computer. It also reduces the need to maintain and update the software, thus saving money and making the organization more efficient.

Map Activities

Find the minimum data set that is needed to perform a task, determine which tasks must be performed by whom. Limit the ability of resources to only the places where the tasks must be performed.

Determine the personnel, the resources and data needed and make those available as applicable. Document everything in detail.

Permanently Archive

First and foremost, it is essential that there is an archive copy of all the data. This archive, our zero copy must be read only. There cannot be any possibility of it being changed or erased. Any data which is not needed for day to day operations is part of the archive or zero copy.

The zero copy must be stored in a physically safe location without access to the outside world, such as in a fire safe in a protective box.

STOP

STOP moves from looking at just the data to a more systems perspective. A GREAT Endeavour™ can be used in this stage to simplify and ensure that nothing is missed.

STOP is an acronym, which stands for:

- **S**ecure
- **T**ransfer
- **O**rganize
- **P**rocesses & Procedures

Secure

Secure access to systems and to data, this means partitioning the data, so that only those who need to access the data are granted that access. The days of wide-ranging data access are past. As fewer people have access to all data, so it becomes more difficult for a cybercriminal to use any particular user' access to compromise your systems. This is especially true for an administrator and the privileged accounts they operate.

To that end, use smart cards or YubiKeys to lock access thus removing the reliance on passwords, they are outdated and prone to compromise and failure.

Transfer

Transfer all business activities to those people who are tasked with performing that activity, take the results from the DUMP stage and apply them. There is no need to make life easier for a manager and give them general access, to "make life easier". Eliminate duplication of activity and simplify how things are done.

Pass control of activities to the appropriate and designated person or people, they are now responsible as well as empowered and authorized. Make sure all media is physically secure.

Organize

Allocate the roles to those who need to perform a particular task. Determine who is responsible and make sure they have the power and authority to complete the task. If they do not have the power or authority, change things so they do. Stick closely to the processes and procedures which are put in place.

Make sure that you solicit feedback on this process and make sure that the process is rigorous. People will want to keep access to data even though it is not their role or job and it violates the security framework.

Processes & Procedures

The processes and procedures the organization currently utilizes will need to be adapted. As things change within departments or groups, then so do the processes and procedures. Make sure they are universally adopted, comprehensive, fit for purpose and are not overly burdensome on those implementing them.

Be proportionate and it will increase productivity.

BAR

With BAR our thinking moves into a more strategic and long term thinking mode. The initial setup for the three different items can easily be done with a GREAT Endeavour™.

BAR is an acronym, which stands for:

- **B**ackup
- **A**ction Book
- **R**ecovery Plan

Backup

Most businesses have a backup of their data, this is to ensure that in the event of a system failure their business can continue. This is a good thing, but it is not enough (or this is insufficient). There must be several different backups and each can be done in a way that makes the most sense, as the intent is to enable business continuity in the event of an attack. The backups must include:

- Onsite and online – protects against user error
- Offsite and online – protects against hardware failure
- Onsite and offline – protects against a system corruption or failure
- Offsite and offline – protects against a local failure

All are vital in their own way. There must be a Permanent Air Gapped Off-site Backup or a PAGO Backup. The backups must be taken frequently and regularly.

Action Book

The Action Book is a predetermined set of actions which are performed in the event of a trigger condition. This means that every data and system related activity needs to have some actions. The Action Book must be used for all actions and not reserved only for emergencies. It forms an extension to the processes and procedures.

The entries in the Action Book must detail who is responsible for triggering the action, how long they have and what happens when they fail to decide (for whatever reason)? The answers to these questions will save vital minutes or hours in the event of a breach. Containing the breach is dependent upon detecting it!

Recovery Plan

If all the steps in the DUMP – STOP – BAR process have been followed, then the Recovery Plan will already be half written. All the important parts will be done, such as who accesses what data and how.

The Recovery Plan is intended to kick in after a serious disaster, this would be something beyond that which the Action Book covers. However, bear in mind that the Action Book is an integral part of the Recovery Plan, as it provides the processes and procedures for all manner of activities.

Summary

As cybercriminals become ever more sophisticated and they employ more and better skilled people to attack your systems, it is inevitable that a data and/or security breach will occur.

It is essential that we change our mind-set from that of the medieval castle, where all intruders must be kept out. This is necessary because, just like the medieval castle, the model is outdated.

In modern business, we need to embrace the idea, unpleasant at it might be, that our systems will be breached.

To work with that inevitable reality, we can put processes, procedures and systems in place ahead of time, to pick up the pieces before there is too much damage and bounce right back. This is what you gain from DUMP – STOP – BAR. It is a security framework, which, while transforming the efficiency of your business, will protect you from the inevitable data breach.

The future is bright, we just need to be prepared!

About Dvana

Dvana is a Management Consultancy, **Boosting Business Productivity** for all our clients.

This is accomplished by deeply understanding the current position of your business and its future direction.

Dvana run Professional Courses aimed at business professionals wanting or needing that extra edge over their competition. The Professional Courses focus on getting results now, whilst building skills for the future.

Talk with **Dvana** today and see how to **Boost Your Businesses Productivity**, become more successful and more profitable.

Contact Information

Web	www.dvana.com	
Phone	(01244) 566 216	UK
	+44 1244 566 216	International
Email	info@dvana.com	

Terms of Use