

"Insider Tips from Connectability to Make Your Business Run Faster,
Easier And More Profitably"

IT Insight

Issue 12: September, 2015



Inside This Issue...

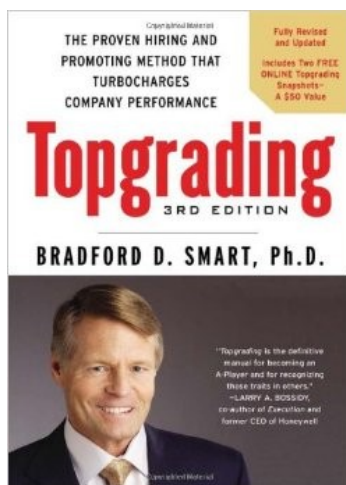
**1 TopGrading:
Acquiring and
Retaining Talent**

**2 Welcome to the
DARK Web**

**3 7 Deadly I.T. Sins:
Un-Encrypted
Files**

4 Backup Audit

**5 Connectability
Disaster
Recovery**



TopGrading: How To Acquire and Retain Top Talent

As business owners we all understand the importance of hiring and retaining top talent. Talent is what drives our companies and gives us a competitive edge in the marketplace. Even if your company has an amazing culture, it doesn't mean anything unless the right people are working in the right positions.

So as business owners how do we make sure an applicant is suitable for a particular position? Well, one method is called Topgrading. Topgrading is a technique for interviewing new prospective employees to gather a clear picture of their personality and their previous work history, but be aware, Topgrading is a more time consuming process than the average interview cycle.

Generally companies use behavioural interviews, but these interviews only delve into a small number of previous work challenges, not the entire picture of an applicant's personality, strengths and weaknesses.

The Topgrading process begins with a detailed job description that accurately outlines the skills, experience and personal qualities necessary to be successful in the job. Each candidate is then tasked with completing a comprehensive career history form that outlines their professional journey from high school to the present.

Next, a two-person team trained in Topgrading techniques conducts follow-up interviews, which last between two and three hours, and explores the applicant's education, work experience, and career goals. The top candidate must then arrange phone calls between the hiring company and bosses from all their previous positions over the last decade.

The interview questions should draw information about past personal and professional experiences to help the interviewer understand the candidates thought process, values, and methods of interaction. Examples include: "Describe the most influential experiences that shaped your values and personality." Or "What were your targets in your last job and how well did you perform in relation to these goals?".

Topgrading requires considerably more preparation than traditional interviews, both from the perspective of the interviewee and the interviewer. The interviewee should prepare by spending time thinking of real-life examples that demonstrate key interpersonal skills and personality traits. The interviewer must prepare by selecting 15 to 20 criteria on which to compare and score candidates, and must review the career history form and resume of each candidate to formulate interview questions.

Each candidate must now be given a separate score from each interviewer based on the list of competencies required for the position. A list of strengths and weaknesses is then created and candidates are separated into one of three categories: A, B and C. A represents the top 10 percent of candidates, and under the Topgrading system only these applicants are eligible for hire.

This is just a very basic overview of Topgrading. If you feel these techniques and strategies would be useful for your business you can read the full book "Topgrading: The Proven Hiring and Promoting Method That Turbocharges Company Performance" by Bradford Smart.



The 7 Deadly I.T. Sins

Un-Encrypted Files

Welcome To The Dark Web

Almost everyone has heard of the Black Market, but what about the Dark Web? The Dark Web is a place where you can access web content that exists on a “**darknet**”, a network that hides inside the public Internet and requires specific software, configurations or authorization to access.

The content on the Dark Web isn’t indexed, so finding it’s impossible unless you know exactly what to look for. The easiest way to connect is through an anonymity network called **Tor**. Tor can be used to search the “Surface Web” anonymously, but it’s mainly used on the Dark Web. Tor bounces searches through volunteer computers called “**nodes**”, making it difficult to track the origin of a search.

A large portion of this “dark market” is dedicated to **illegal activities**. It’s estimated that of the hidden services on the dark web, 15 percent relate to drugs, 9 to fraud, 4 to hacking, and 3 to porn. If you want to “buy” a virus to infect someone’s computers, the dark web is the place to go!

The dark web is a marketplace for illegal activities, but it’s also used daily for a **wide variety of purposes** by normal people, journalists, the military, law enforcement, and activists. In fact, the routing protocol that powers Tor was developed by the U.S. Department of Defense to protect government communications.

From these beginnings, the dark web has evolved into something dangerous and seedy. For example, the founder of the dark website “Silk Road” – an eBay for illegal substances – was recently sentenced to life in prison! Unless you’re a hacker, willing to immerse yourself in this unsafe world of anonymity, we recommend **avoiding the dark web**. Remember, even though you cannot see it doesn’t mean it’s not there.

If you’ve been watching the news it’s likely you’ve seen stories about data breaches at major retailers like Target, The Home Depot, JPMorgan Chase, and Sony.

Unfortunately these are simply the most well-known and recognizable data breaches. Small data breaches happen **every day**. And here’s something that makes it easier for the hackers: **NO FILE ENCRYPTION**.

Without file encryption your private data could easily end up in the wrong hands, not only putting yourself at risk, but potentially also putting your customers’ data at risk. Even if your business escapes the threat unscathed, your customers could very well decide to leave you because they can **no longer trust you** to protect their confidential information.

One of the most important steps to encrypting your files is using an **ENTERPRISE GRADE** cloud solution.

Although DropBox may do what you need it to, it was primarily designed as a consumer grade technology with protection for consumer grade information. So it won’t stop a determined hacker. In fact, DropBox has **already been breached**, so it’s clear they aren’t as focused on security as many of the business specific platforms out there.

There are several alternatives to DropBox that offer higher levels of encryption (the same protection the military uses), as well as additional features like file locking, and infinite revision tracking.

One highly effective options is provided by **AnchorWorks** a division of **eFolder**. eFolder is a large US based firm with data centres in both the US and Canada. One of their numerous cloud products is called **Synched Tool** which works as a document sharing platform for internal use and a backup application for external needs.

By using a cloud application with state-of-the-art security and a broad range of features you can protect your business in the event of a computer failure or a security breach, while at the same time seeing **cost reductions** and increased mobile functionality.

If you want to make sure all your data is backed up and protected from data breaches, or find yourself a highly rated business cloud provider, call us at 416-966-3306 and we’ll be happy to help.





Gadget of the Month: BitDefender Box

In one of our earlier newsletters we talked about the Internet of Things (IoT) and how new devices are being released every day to **leverage the internet** and make our lives easier. For example a laundry machine that can be turned on from a smartphone, or a thermostat that can be adjusted from your phone or laptop.



With the IoT comes an increased need for **home security**. If you can control your garage, locks, lights and cameras through WiFi then they're all hackable.

The **BitDefender Box**, one of the first products designed to ward off home hackers, essentially acts as a very strong antivirus and antimalware program that filters your results before it ever reaches your devices.

The accompanying app also allows you to install updates, identify vulnerabilities, and make performance improvements remotely. Using the app you no longer need to install updates and make changes on each and every device, you can just do it **all from the same place**.

It even allows you to turn on something called Private Line that protects your devices even when you're connected to another Wi-Fi network.

The BitDefender is easy to install and costs only **\$200**, a very reasonable price to pay to protect your home, especially if you have many internet connected devices.

A Cautionary Tale:

A couple of weeks ago I was chatting with a colleague and swapping "war stories." Here's one he told me, about his experience doing some work for a local Toronto business. It's a perfect example of learning a hard lesson about the importance of adequate backup.

A couple of months ago, the client had phased out its last Windows 2003 server in anticipation of Microsoft discontinuing support. But that left them with only **one** Active Directory server on their network. Unfortunately, **that** server failed one fateful weekend.

They weren't totally unprepared: they had secure cloud backups for their critical data. And they had **planned** to install a backup Directory server; but they just hadn't gotten around to it. And without a backup of Active Directory it required a **complete** rebuild of their directory, from the ground up. That meant reinstalling software and re-creating users, mailboxes, profiles, etc. It took **many** hours of work before they were fully up and running.

Frankly, they were lucky: they had data backups, and they were on a Managed Services contract so their only additional cost was the replacement of the disk drive that failed. But *what about the indirect cost?* Having no functional network or email for days on end wound up costing them **thousands** in lost productivity.

The irony is that it would have taken just a couple of hours to completely avoid this issue, if they had taken the proper steps a few weeks ago. Because every hard lesson should also be a **teachable moment**, we want to share 2 important lessons with you:

1. Make absolutely sure that you have either a **backup Active Directory server**, or, **at least**, a current backup of your Active Directory data.
2. Test your backups **regularly** to make 100% certain that you can recover your data if you actually need it!

Please check the back page for an offer that will help you sleep peacefully, knowing that your IT environment is *really* disaster-proof.

Connectability's Referral Program Help us help you!

As many of you know, we get most of our customers through referrals and we're always looking for ways to grow our business.

To entice you to spread the word to friends, family, and business contacts we'd like to offer **\$100** for making an introduction with a bona fide business prospect. If they sign up you'll get **\$1,000** as a thank-you for putting us in touch! Simply by helping us you can reduce your IT costs!



Joke of the Month:

Bill and the Computer Scale

While Bill waited at the airport to board his plane, he noticed a computer scale that would give your weight and a fortune.

He dropped a quarter in the slot, and the computer screen displayed:

“You weigh 195 pounds, you are married, and you’re on your way to San Diego.” Bill stood there dumbfounded.

Another man put in a quarter and the computer read: “You weigh 184 pounds, you’re divorced, and you’re on your way to Chicago.”

Bill said to the man, “Are you divorced and on your way to Chicago?” “Yes.” Replied the man.

Bill was amazed. Then he rushed to the men’s room, changed his clothes, and put on dark glasses.

He went to the machine again. The computer read: “You still weigh 195 pounds, you’re still married, and you just missed your plane to San Diego.”



Protect Your Data: Backup Audit

Backups are critical and everyone knows it. Unfortunately, when most people think of backup they only think about backing up the files they use on a **daily basis**. But what about things like the Windows Active Directory or your archived email data?

Lots of companies have backups, but are they the **RIGHT** backups? Is all of your critical data being backed up, or are you missing something that could cost you time and money if you experienced a failure? Are your backups safe and offsite? Is your backup data actually usable? Can you share your backed up data with others in your company?

These are the questions that need to be answered to ensure your business is properly backed up and secure in the event of a disaster.

That’s why, **until September 30**, we’re offering a **FREE**, 2-hour backup audit to the first 10 businesses who sign up. We’ll make sure that you really are “disaster-proof”. We’ll come to your office and sit down with you to discuss the way you share and use files, evaluate the current network and backup infrastructure, and identify areas for improvement. Finally, we’ll present our recommended backup strategy and implementation plan.

Time permitting, we can also scan your network with our automated tools to identify other issues like lack of antivirus software, low disc space, improperly configured firewall, and malware intrusions.

Our cautionary tale this month demonstrates exactly why you need to be sure your backups are in place for **EVERY** essential piece of data in your company. A small lapse could leave you with significant downtime in the event of a disaster.

We work with many of the top backup providers on the market, so we will only recommend the solution we feel offers you the best combination of features, value, and security and not the one that offers us the biggest bottom line.

This backup audit comes with no cost and no obligation. We will not employ high pressure sales tactics because frankly we don’t enjoy being “sold” any more than you do. We will simply evaluate, research and recommend a solution we feel will offer you the necessary functionality, while meeting your organizations budgets.

So don’t wait! To sign up **NOW** for your free backup audit call us at: 416-966-3306, or email info@connectability.com and put “Backup Audit” in the subject line.

Connectability To The Rescue

No one can predict when an IT failure will happen. That’s why prompt response is a key element of professional-grade IT support.

A couple of weeks ago we were on a sales call. On our way out the door, the client mentioned their Internet was down and they were waiting for Bell to arrive to repair it. “Well,” we asked, “why don’t we have a quick look?”

As it turns out, the problem had nothing to do with Bell and had the client waited, they would have been no closer to a solution. Fortunately, we were able to diagnose and resolve the problem, and within 30 minutes they were back up and running.