



Operated by
Innovative Productivity, Inc.

BUSINESS & TECHNOLOGY

SECTION

Volume 12
Sponsored by McConnell Technology & Training Center

Issue 2
Published by The Clark Group

IN THIS ISSUE

- Bridging the Skills Gap with Emotional Intelligence
- Fluorescent Primers – Faster and More Effective Defect Detection
- Cyber Bullying... A real threat
- Businesses Increasingly Turn to Computer Forensic Techniques



GREG ROWE
Senior Consultant

Bridging the Skills Gap with Emotional Intelligence

Are you ready for the new mix of workforce skills, as dictated by the reshuffling of roles in the global economy? In light of your answer, how hard will it be to train the team members you hire next month? These are pertinent questions that affect how each of us manages our resources and those of our Commonwealth to align individual skills to upcoming market demands. Fortunately, they are also a matter of careful consideration for those who can help guide us past the shifting sands of upcoming educational and training requirements.

Although there's no crystal ball that would cause our workforce challenges to be any less exciting to watch unfold, perhaps it would help to hear from leading thinkers on how to best bridge the skills gap in order to gain a leg-up and a winning approach that'll put you a length ahead in tough competition. This article can help you see around the next bend so as to know what combination of technical and non-technical skills are needed to most effectively navigate the quickly-emerging landscape.

Let's begin with a look at the situation close to home. Dr. Lawrence Holloway, Director of the UK Center for Manufacturing, has studied the skills needed within Kentucky's workforce. As documented by KAM's Pam Mangas Mitchell from Holloway's address at ProsperousKentucky_{SM} 2007, they are:

- Basic Skills, such as math, science, English and literacy;
- Professional skills in engineering, technical and business jobs;
- Interaction skills to promote teamwork; and
- Basic problem-solving skills that allow companies to become innovative.

In other words, preparing for the future is a two-sided equation: shoring-up education in the hard sciences, while also increasing the innovation and collaboration capabilities. Some experts are addressing the latter as indicative of a growing leadership vacuum.

According to a study last year by the ASTD Public Policy Council, 96% of the 100 companies surveyed reported a skills gap in their workforce, looking at current needs and one year out. However, what is interesting is that the three most important missing skills noted were under the headings of managerial/supervisory, communication/interpersonal, and leadership/executive. Related to those skills, 70% of the companies studied said they are experiencing moderate to major leadership shortages. They also expect the gap to get worse.

Is this a reason to fret and bemoan the skills gap? Instead we might look to see how the challenge also provides an opportunity to leap forward and gain an advantage in filling the gap more efficiently than anyone else. Not only is this a local matter, but one of national and global proportions.

Concerning the need for technical skills, given increased international competition from college graduates, our state's educators are working overtime to focus students on the hard sciences. As those of us with young children experience daily, what we learned in high school is now often taught in middle school and below. What is less clear is how we as a society can best address the non-technical skills. Those provide the capabilities that will maintain our lead in communication, innovation, and leadership.

Does this indicate a mandate to further retool schools and revamp higher education? That's an option. However, there are other, more wide-reaching means readily available. One of those is addressed by psychologist and author Daniel Goleman. He has emphasized sharpening our increasingly-important people skills through Emotional Intelligence programs. Emotional Intelligence, or simply EI, includes competencies related to self-awareness, self-discipline, persistence, and empathy. These are at the heart of the non-technical skills called for above. If they are not high on your list of personal strengths, don't worry, there are various avenues for increasing your Emotional Intelligence Quotient (EQ).

Various psychologists and executive coaches are expanding the litany of options for self-assessment and team-assessment instruments in these critical soft skills. They assist in evaluation as well as the tailored improvement programs based on the evaluation. The number and type of assessments used depend on the program outcome desired. One of the most popular appraisals for the general public is described in The Emotional Intelligence Quick Book.

96% of the 100 companies surveyed reported a skills gap in their workforce . . . The three most important missing skills noted were managerial/supervisory, communication/interpersonal, and leadership/executive.

**DR. PAUL GOSSEN**

National Surface Treatment Center

Fluorescent Primers – Faster and More Effective Defect Detection

Three fundamental elements drive the economy: hurry up, it had better be good, and what is it going to cost. Paint and coatings contractors are certainly not immune to the dictates of time, quality and price.

The application of high quality coatings is central to the United States Navy's corrosion control strategy. A defense management report issued in July 2003 by the United States General Accounting Office (GAO) revealed that the prevention and removal of corrosion on shipboard tanks alone costs the U.S. Navy over \$174 million a year and estimated that corrosion-related maintenance accounts for nearly 25 percent of its fleet maintenance budget.

Coating inspections after application of each coat are a key part of the U.S. Navy's quality assurance program. Defect detection in shipboard tanks is traditionally performed visually using a flashlight; however, the human eye cannot detect all coating defects.

Technological advancements in defect detection are assisting the Navy's contractors in the application of quality coatings. To further this initiative, the Navy turned to the National Surface Treatment Center, which is creating an enhanced, standardized inspection technology. This technology is based on using special Optically Active Pigmented (OAP) primers that

emit a fluorescent glow when viewed with special light sources. The left side of photo 1 shows a pit with a holiday illuminated by a standard white flashlight. Even though the primer and topcoat are contrasting colors, the holiday is almost invisible. The right side of photo 1 illustrates the same area illuminated by the special inspection light activating the OAP primer. The holiday glows blue and is easily detected by the human eye.

This technology also helps inspectors see defects in the prime coat before the top coat is applied. Experienced coatings inspectors can find pinholes in the prime coat twice as fast from double the distance with OAP inspection compared to using their white light flashlights. This inspection technology works with wet and cured paint, allowing inspection to be done before the painter dismantles the worksite.

Photo 1

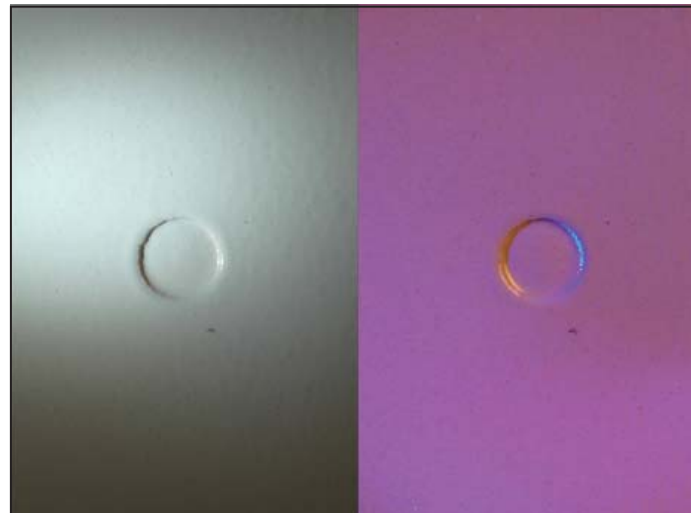
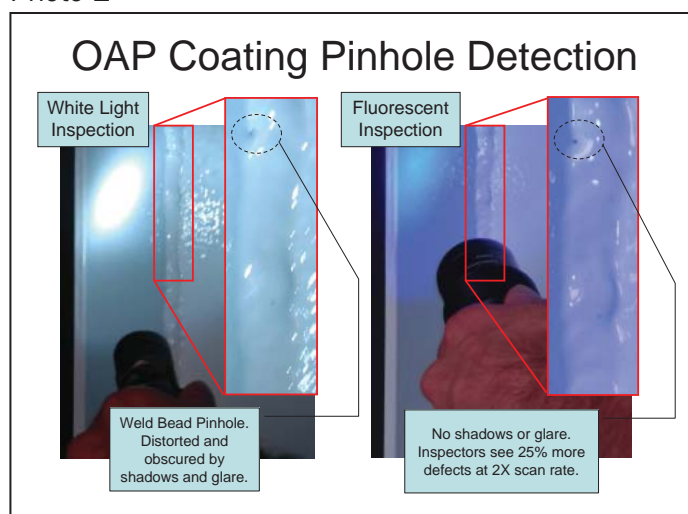


Photo 2



The concept of using fluoresce for defect detection is known to many industries, but in the past, the fluorescent effect was created with ultraviolet (UV) or "black" light. Powerful UV lights used for industrial inspection are bulky, expensive, and the light creates eye and skin exposure concerns for workers.

The National Surface Treatment Center worked with the Navy, its coating suppliers, and leading US manufacturers of LED flashlights to design an inspection system that uses eye-safe visible light to activate the fluorescence in the OAP primer. This eye-safe inspection light can be specified by referencing the new standard ASTM E2501 (www.astm.org). Sure-Fire, a US flashlight manufacturer, engineered the Fluorescinator (p/n U2-BK-PL): a powerful, rugged, handheld LED light that meets this standard but costs less than the replacement bulbs of many high-powered UV lamps. The light is available to the coating industry through Elcometer (sales@elcometerusa.com). US Navy qualified primers with the OAP property are listed on the Navy's Qualified Products List for shipboard tanks (QPL-23236) on www.nstcenter.com.

In summary, OAP primers coupled with the new LED flashlight technology offer the following value-added benefits to paint contractors:

- Reliable detection that offers maximum portability and convenience
- Reduction in inspection time and manpower hours
- Inspection of first application to ensure quality and reduce rework time and costs
- Defect detection in wet or cured coatings
- A cost-effective, high speed, easy-to-use, real-time holiday detection system

Paul Gossen, Ph.D., is Project Manager at the National Surface Treatment Center in Louisville, Kentucky. The NST Center delivers coating technology solutions to government and industry. www.nstcenter.com or (502) 638-4400

**DONNA LAMPE**

Director of Information Technology

Cyber Bullying... A real threat

MTTC was conducting an internet safety seminar at a local high school not too long ago. As we were setting up, I noticed a man talking to one of the presenters, and the presenter was pointing to me. The gentleman approached me asking for a little time at the seminar to show a video. I looked at the DVD and it said Rachael Neblett, Cyber Bullying. Appearing curt I am sure, I merely said that I was not familiar with Rachael Neblett. He replied that Rachel was the Bullitt County student who had been cyber-bullied and consequently, committed suicide. Shocked, I just looked at him and asked, "Was that your daughter?" With tear-filled eyes he said, "That was my baby."

Rachael was 17 years old when she ended her own life. She was receiving threatening messages from someone she did not know on her My Space account. The bully or bullies knew where she was, who she was with, what clothes she wore, what she ate, etc. The police know what computer the message was sent from, but not by whom. The last message she received told her she would be in the morgue before the end of the day.

This article is dedicated to Rachael. If you would like to see a tribute to Rachel, through her father's eyes, visit www.mttc.org.

"Cyberbullying" is when a child, preteen or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, preteen or teen using the Internet, interactive and digital technologies or mobile phones. It has to have a minor on both sides, or at least have been instigated by a minor against another minor. Once adults become involved, it is plain and simple cyber-harassment or cyberstalking. Adult cyber-harassment or cyberstalking is NEVER called cyberbullying.

Here are some tips for parents from www.stopcyberbullying.org.

TALK TO YOUR CHILD

Caution them about responding "in kind." This is not a time for them to lash out or start a cyber war themselves. See if they think they know the identity of the cyberbully or cyberbullies. See if this is related to an offline bullying situation, and deal with that quickly.

IGNORE IT

A one-time, seemingly unthreatening act, like a prank or mild teasing should probably be ignored. (If it's a threat, you must report it.)

RESTRICT THE PEOPLE WHO CAN SEND YOU COMMUNICATIONS

Consider restricting all incoming communications to pre-approved senders, such as those on your child's buddy list. (If the cyberbully is someone on their buddy list, though, this method won't help. In that case the cyberbully will have to be removed from the buddy list and/or blocked.)

RESTRICT OTHERS FROM BEING ABLE TO ADD YOUR CHILD TO THEIR BUDDY LIST

Cyberbullies track when your child is online by using buddy lists, and similar tracking programs. It will let them know when one of their "buddies" is online, when they are inactive and, in some cases, where they are. This feature is usually found in the privacy settings or parental controls of a communications program.

GOOGLE YOUR CHILD

Make sure that the cyberbully isn't posting attacks online. When you get an early warning of a cyberbullying campaign, it is essential that you keep an eye on your child's screen name, nick names, full name, address, telephone and cell numbers and Web sites. You can also set up an "alert" on Google to notify you whenever anything about your child is posted online. To learn more, read "Google Yourself!"

BLOCK THE SENDER

Someone who seems aggressive, or makes you uncomfortable and does not respond to verbal please or formal warnings should be blocked. (Most ISPs and instant messaging programs have a blocking feature.)

"WARN" THE SENDER

If the cyberbully uses another screen name to avoid the block, and manages to get through or around the block or communicates through others, "warn" them, or "notify" the ISP. (This is usually a button on the IM application.) This creates a record of the incident for later review. If the person is warned enough, they can lose their ISP or instant messenger account.

REPORT TO ISP

Most cyberbullying and harassment incidents violate the ISP's terms of service. These are typically called a "TOS violation" ("terms of service" violation) and can have serious consequences for the account holder. Many ISPs will close a cyber bully's account (which will also close their parents' household account in most cases). You should report this to the sender's ISP, not yours.

REPORT TO SCHOOL

Most cases of cyberbullying occur off school grounds and outside of school hours. In the United States, often the school has no legal authority to take action relating to an off-premises and off-hours activity, even if it has an impact on the welfare of their students. The laws are tricky, and vary jurisdiction by jurisdiction. So while you should notify the school (especially if your child suspects who is behind the attacks), the school or school system may not be able to take any disciplinary action.

REPORT TO POLICE

Someone who threatens you physically, who is posting details about your or your child's offline contact information or instigating a cyber bullying by proxy campaign, should be reported to the police. (Although you should err on the side of caution and report anything that worries you.)

TAKE LEGAL ACTION

Many cases of cyber bullying (like the adult cyber-harassment equivalent) are not criminal. They may come close to violating the law, but may not cross the line. Most of the time, the threat of closing their ISP or instant messaging account is enough to make things stop. But sometimes, legal intervention is necessary and may also be the only way you can find out who is behind the attacks.

If you would like more information or perhaps be interested in an internet safety seminar for a group or organization, please contact Donna Lampe at DLampe@mttc.org or (502) 638-4410.



MTTC – providing
innovative technology
enhanced services and
solutions for
National Defense, business,
and workforce customers.

McCONNELL TECHNOLOGY & TRAINING CENTER
Sponsor

THE CLARK GROUP
Publisher

FLORENCE HUFFMAN & BOBBY CLARK
Editors

CAROLYN REED
MTTC Content Editor

(800) 595-4638 • FAX (859) 233-7421
www.mttc.org • www.KyGoldBook.com
mttc@mttc.org • info@theclarkgroupinfo.com

**BILL THOMPSON**

Director of Computer Technology Programs

Businesses Increasingly Turn to Computer Forensic Techniques

Imagine having to terminate a Sales Manager and later you discover that all of his customer account information or proposals cannot be found on his computer or your servers. In another scenario, a female employee files a complaint with your HR department because a male employee was viewing pornographic images on his computer. Finally, imagine entering the cubicle of a poorly performing employee and realize that he is in the process of visiting a gambling web site. How would you respond to these scenarios? In all three of these cases, you are probably going to need more than a simple search of the employees' hard drive files. You will likely need to apply full-fledged computer forensic techniques and gathering of evidence.

Other situations that would probably require application of computer forensic methods include:

- Internal fraud or embezzlement of funds
- Sending of inappropriate e-mail
- Intrusion of network from external source
- Using corporate computer equipment for personal gain
- Leaking of proprietary information
- Encryption/password protection of needed information
- Vandalism due to disgruntled employees or hackers
- Unrecoverable data due to hardware failure
- Accidental data erasure and inadequate data back-up

Most of these cases would require the services of someone appropriately trained in advanced information recovery and data preservation techniques. In situations that will result in criminal court proceedings, such as corporate malfeasance, you are going to need an expert in evidence gathering and documentation. To do less might cause key evidence to be declared inadmissible in court due to "Chain of Custody" protocol requirements. Evidence must be acquired, authenticated, analyzed, documented, and eventually presented in court. Increasingly, investigators must take into account various regulatory requirements such as the Sarbanes-Oxley Act and the Health Insurance Portability and Accountability Act (HIPAA) which affect related issues such as the destruction of electronic records or the preservation employee privacy.

As many companies have discovered, disgruntled or terminated employees can also leave data booby traps that can be tripped when an IT staffer attempts to access employee files. Such data bombs can include the release of viruses, Trojans, worms, etc., in addition to the destruction of information or manufacturing software. Knowing how to discover and mitigate such sabotage is best left in the hands of professional computer forensic investigators who also have the latest software tools for the job. An external resource also eliminates any question of conflict-of-interest motivation and evidence tampering by in-house IT staff.

There are many experts in the field and the number is growing out of necessity. However, many courtsystems and law enforcement agencies have a back-log of cases pending. There are several web sites that can provide a referral should your organization suffer from an incident described above. A good site to begin with is <http://computerforensicsworld.com>.

For additional information on computer forensics, contact Bill Thompson at BThompson@mttc.org or (502) 638-4430.

Emotional Intelligence

CONTINUED FROM / p S1

Along with the half-million people who have taken the self-assessment included in the purchase of Bradberry's book, I had reason to be both encouraged and, quite honestly, not-so-encouraged by the results. The report rates skills in Self-Awareness, Self-Management, Social Awareness, and Relationship Management. It's possible to score high in one and not as high in another. To illustrate, in my case it appeared that I stand high in being socially aware. However, what may be less encouraging is my merely average rating in Self-Management.

Still, that's the whole point. By increasing EQ in identified areas you become a more interactive and innovative team member. And don't worry about being beaten over the head with any bad news. Even though I was somewhat concerned about that, in fact the appraisal's wording hurt less than mamma telling me to hold my tongue if I didn't have anything nice to say. (I love you, Mom).

Similarly, regardless of the assessment you use, the recommendations also tend to be more sophisticated than a slap on the wrist. My Personal Competence Action Plan suggested that during difficult conversations, if I have trouble listening without interrupting, I should take a deep breath and picture the situation as if it were a movie in which I'm a character objectively trying to attain the best results. (Look out Oscars, here I come.)

No offense to any of our dearly loved mothers, but you have to admit that has at least a little more traction than the often-repeated phrase from childhood, "Be nice."

Will this all win me a leading role in today's knowledge economy? Apparently it couldn't hurt, as long as it enables or facilitates the capacity to collaborate better and innovate more. As Bill Gates wrote earlier this year to the Washington Post, "If the United States is to remain a global economic leader, we must foster an environment that enables a new generation to dream up innovations..."

So, will your workforce survive and thrive in the demanding market we face? It certainly can – at least if you embrace the opportunity to take the lead. The most successful endeavors of tomorrow will include teams of technically competent and emotionally intelligent, collaborative workers. By heeding the advice of a host of experts you may determine the future of your company, our state, and, in some ways, even the world.

Yet it all starts here in your own backyard, collectively solving the unique and constantly changing problems we face together. The first step could be as simple as a 10-minute assessment or a badly needed short consultation. Whatever you do, let's all stay connected, committed, and working to the betterment of each of us and us all, being both technically skilled and non-technically attuned.

Contact Greg Rowe at GRowe@mttc.org or (502) 638-4488 for additional information.

Origins of Innovation

In 1995, computer programmer Pierre Omidyar auctioned off a broken laser printer on his Web site for \$14.83 (the buyer was a collector of broken laser printers).

Within two years, Omidyar registered his consulting firm, Echo Bay Technology Group, as eBay.com.

