INFORMATION RESOURCES MANAGEMENT COLLEGE

Fall 2005
Volume 10, No. 4

# Info Tech Talk

A Journal on Enabling Information Technologies by the IRMC Organizational Transformation & Technology Dept.

## *Humor in the eClassroom*

**By Lt Col Chuck Stribula, USAF, PMP**

Inside this issue:



***…the potential for significant gains is there, if humor is integrated into the curriculum intentionally (versus added as an afterthought).***

### Overview

After two years of teaching here at the IRM College, I've found my natural tendency towards humor is gradually finding a home. Recognizing that for various reasons, some are reluctant to employ humor in their teaching arsenal, I resolved to write this article not so much as an expert, but rather a seasoned practitioner of humor in a variety of settings. And while much of this article applies to any classroom environment, I'll be sure to address several issues particular to those relating to technology.


I'll start by operationally defining just what I mean by "humor"; this may not be as obvious as you think! I'll then address some specific techniques, as well as payoffs and risks, highlight several places in the classroom where humor may help, and discuss some considerations to keep in mind when using props. Interspersed throughout, I'll include lots of examples of what's worked for me (and what hasn't). I'll wrap up with a few resources, for those who want to pursue this topic further.

As to research on this subject, I found evidence on both sides (no effect vs. significant positive effects). Interestingly, I didn't find much mention of negative effects (aside from some risky topics, which I'll discuss later on). My own experience has been that the potential for significant gains is there if humor is integrated into the curriculum intentionally (vs. added as an afterthought).

### What is Humor?

So, why did the computer cross the road? Groan. Well, as they say about beauty, humor is in the eye of the beholder; it's very subjective. Between generational, regional, international, political and cultural differences in perspectives and background, there are more than enough sources of potential disagreement as to exactly what "funny" is. While this makes use of humor challenging, we should not discount it as a powerful tool just because of the difficulties associated with its use.

For the purpose of this article, I'm defining "humor" to include both explicitly humorous material (e.g., jokes, comics and props) as well as what I call "psuedo-humor; light material that illustrates a teaching point in a creative way (e.g., analogies, metaphors and anecdotes). I believe this definition will focus us more on results ("better learning", if you will), rather than efforts ("I used a great Dilbert, yet no one laughed"). An example of this is a handout I distribute in my lessons on risk management and decision making. It contains several relevant quotes, ranging from witty ("The prospect of hanging focuses the mind wonderfully" - Ben Franklin) to thought-provoking ("If you choose not to decide, you still have made a choice" - Neil Peart, Drummer for "Rush").

Another example of "pseudo-humor" is personal anecdotes that have analogies woven into them; they often lead to those

*(Continued on page 2)*

# Humor in the eClassroom (cont.)

*(Continued from page 1)*

"aha" moments when every student suddenly "gets it." My favorite one concerns requirements analysis. I start by displaying a chart that contains a table with missions/tasks across the top and systems down the side. I highlight the gaps and overlaps it can reveal in a mission area, and introduce the idea of an appropriate level of redundancy. I then explain how I used to take the top of the line Swiss Army knife backpacking with my Boy Scouts, until I realized it did all of its many jobs poorly, including several I didn't need. Then I whip out the new multi-tool I use, highlight its advantages, and conclude with "*How much redundancy is in your IT backpack?*" Works like a charm!

**Tips and Techniques**

Good applications of humor in the classroom should be simple, easy to remember, relevant, personal, and real. Projecting a Dilbert at the start of a lesson is good, but how does it enhance the leaning environment? A few simple concepts here will have a great effect on our students learning.

Start by letting your students know that humor is welcome in your classroom. Incorporate something funny up front; ideally before you formally begin your first lesson. Before any of my students arrive, I sneak a ceramic jar labeled "Ashes of Problem Students" onto the podium. And yes, it has real ashes in it (from my fireplace). I've actually caught some students peaking in! The danger here is you have to be prepared for your students to rise to the occasion. One group recently taped a piece of paper over "Students" that said "Instructors"; I knew right away they were going to be a lot of fun (I was right). Another thing I do is put a relevant Dilbert on the cover of my student's binders; it helps create a positive, yet slightly irreverent, atmosphere, which I can then build on verbally. Using an audio clip to "announce" your arrival (e.g., "Elvis has entered the building") is another idea to consider, assuming you have a remote control that works from outside the room.

Keep it simple! Lengthy jokes, with elaborate set-ups, run the risk of not only ruined punch-lines, but also confused (or hostile) students. One example of this for me was the "Action Item" comic (downloadable at http://www.fatalexception.org/action_item.html). Projected on a screen it's an eye-chart (albeit a hysterical one, IMHO). To make up for that, I display it before students arrive in the morning, or early in their lunch break, so they'll have time to enjoy it at their leisure. I also save it to their classroom sharespace on the U drive, so they can share it with coworkers, etc. In fact, any humorous artifact that generates a noticeable positive response from your students is fodder for their sharespace. You may even find (as I have) that they start saving their own "gems" there, which you can glean from!

By keeping humor simple, your students may remember the associated learning better. We tend to remember significant events better (e.g., where were you when you heard about 9/11?). Humor, used appropriately, can make a teaching point more significant. An example of this is the "Mystics Pearls for PMs" I've borrowed from Prof. Mike Mears, one of my instructors while a student in DSMC's Advanced Program Management Course at Fort Belvoir. Each one was a short sound-bite (e.g., "Never pass up an opportunity to keep your mouth shut"), with a few amplifying/clarifying bullets that conveyed some real-world wisdom from the SOHK (School of Hard Knocks -- thanks, Gill).

Humorous material can relate to the instructional material in a number of ways. It can be quite explicit or, it might merely introduce a topic, as with a quote from Mark Twain I use to introduce the concept of experiential learning ("A man who holds a cat by its tail learns something he can learn in no other way."). I then display the "Tabby Tote", which I'll spare you, in case you love cats! If you're like me, however, do an Internet search for "Tabby Tote." Yikes!

And remember to relax. It's one thing to stretch a little in this area; it's another thing to force yourself into uncomfortable uncharted territory. Walk before you run! Being yourself is much more likely to make it real with your students. I once tried a few classroom techniques Stan Boddie uses with exceptional success only to find myself realizing I'm not Stan Boddie. I've got to be me! Give your humor a personal touch will also make it real (duh); why use someone else's anecdote if you've got one you've experienced first hand? Even if it's not as close a fit in terms of relevance, you'll naturally convey more energy if it really happened to you. And make sure you're comfortable with the classroom technology. That'll not only help you to be more relaxed, it'll also help your technology-dependent humor flow more smoothly.

**Payoffs and Risks**

While the use of humor with students can enhance their experience in several ways, there are also some minefields to navigate. And those mines can negate some or even all of the benefits. Don't be afraid, though; just be aware!

Again, the research here is not as clear as I'd prefer, but my own anecdotal evidence is strong (at least it's strong in my

*(Continued on page 3)*

*(Continued from page 2)*

own mind!). Benefits can include increased comprehension/ retention of material, faster understanding of specific learning points, better student participation (both quantity and quality), and increased bonding of students (as long as they're not bonding to mutiny against you). You may or may not actually perceive these benefits, but I'm convinced they exist, based on my own experiences and the degree to which they resonate with my logic.

So, what can go wrong? To start with, the technology may let you down. Projectors may not project, speakers may not speak, remote controls may not control, and videos may not "vid?" Well, you get the idea. As I mentioned earlier, be familiar with the classroom setup in advance, especially at TDY locations new to you. Call in advance to discuss what's available with your local contact and show up extra early the first day (or even the day before, if practical). If there are relevant backups you can bring (e.g., portable remote control, hardcopy handouts, files on a flash drive, etc.), then by all means, bring them. Finally, be sure to have a backup plan. As the Boy Scout motto says, "Be Prepared!"

The humorous material itself can also disappoint. For starters, there are three risky subjects I need to address; politics, religion and sex. I'm not saying to avoid these altogether; just tread carefully -- they're minefields! It's one thing for a student to introduce these subjects; it's another for you to set an example. I once had a student respond to my self-depreciating comment about my family's lack of computer literacy by saying "so, you're basically saying you're of Amish descent?" The class (and faculty) loved it, although I've avoided using it since then, as I may discover the hard way that I have students of actual Amish descent in my class! Another example of a dodged bullet was a lesson Matt Newman and Stan Boddie developed, in which they compare enterprise architecture to a human skeleton. They enhanced this by playing the "Dry Bones" song ("The head bone's connected to the neck bone."), combined with a funny video clip of a dancing skeleton puppet. It was a perfect analogy, and they preserved its effectiveness partially by chopping the audio file just before the words "now hear the word of the Lord" played. Cultural sensitivities are another thing to consider; some hand gestures, for example, are humorous in our culture, yet meaningless (or even offensive) in others. My best advice is to be careful while also being ready to apologize as needed. There's also the risk the joke may bomb; your students just might not "get it." This can lead to confusion ("what did he/she say?") or lost time with explanations, which can also disrupt the lesson flow. Finally, there's the issue of negative student feedback. While I don't believe we should act out of fear, we should give some thought to how our students might react to a given use of humor.

**Uses in the Classroom**

So where can I insert humor in my classroom? I'm glad you asked. In addition to the pre-class opportunities I gave examples of earlier, there are several places within the learning environment that lend themselves to humor, such as ice-breakers, introductions, breaks, and the academic content itself, handouts. I'll discuss some considerations of props in my next section.

One good way to get your students "creative juices" flowing is with an ice-breaker" exercise. While this drill isn't inherently humorous, it is a good place to start, with a scenario that's a little irreverent, yet relevant to the lesson. One way I do this is to throw out a key term, such as "transformation," and task my students, in small groups, to define it. I further limit them to plain English, with no buzz-words, while showing a Dilbert with the characters playing "buzzword bingo." A shorter example I've used is to put a chart on the screen with two shiny dimes and ask "what is this?" with the hint that it's what we're seeking. Then I reveal text that says "New Paradigms" -- get it? New Pair of Dimes? It's a groaner, but it works.

Another place is during introductions. I have each student give their name, office, job title and one non-work interesting fact about themselves. While some of the "interesting" facts are humorous in their own right, I'll also include some self-depreciating comment about myself. Not only does this get a few laughs, it also helps depict me a more human, and thus more approachable by my students. I've also worked humor in when introducing small-group exercises. I build up my student's anticipation by telling them I'll use a "highly scientific process" to determine who briefs and in what order. After they're all ready to brief, I open my browser to an online source of random number sequences (www.random.org). Since the website really is based on hard science, I get some laughs by contrasting their white paper on atmospheric noise with the t-shirts and mousepads they sell online.

As I mentioned before, breaks are useful for displaying more lengthy comics. Another example I use is an automated slideshow I let run over lunch with several charts that parody the inspirational posters we sometimes see in office hallways and cubicle areas (e.g., "Not All Pain Is Gain"). Breaks are also a chance to follow-up on student's humorous inputs, whether to encourage helpful examples or rein in those you consider inappropriate. And they're good for attending to uncooperative technologies.

*(Continued on page 11)*

# *What's New with Enterprise Architecture*

**By Carolyn Strano**

As business environments and the infrastructure supporting them continue to increase in complexity, the value of using enterprise architecture (EA) as a mechanism to better understand the interrelationships that are critical to the success of the enterprise is becoming increasingly important. The overall theme of two recent conferences emphasized using enterprise architecture to help shape and mold the strategic direction of the enterprise and enable better performance through increased effectiveness and efficiencies.

The Gartner Group EA Summit, which was held in Gaylord, Texas, on September 13th and 14th, provided several sessions that shared best practices in applying enterprise architecture to help transform the enterprise and provide greater flexibility and agility to be responsive to its stakeholders. Carolyn Strano, an IRM College professor, moderated a panel on a federated approach to enterprise architecture, which was well attended and shares best practices of the panel members as well as addressed challenges and issues. Ms. Strano was also a member of the Program Advisory Committee for the conference. John Sullivan, the enterprise architect for the Environmental Protection Agency (EPA), explained how EPA is using EA to guide business transformation, solve interoperability challenges with all levels of government, and leverage the Federal EA to collaborate lines of business with other government agencies. He discussed the importance of training and education so that everyone in the enterprise understands how EA is used to influence decision making from a holistic perspective. Mr. Sullivan is an alumnus of the IRM College at the National Defense University and he spoke highly of the value that this educational experience provided. John Sheridan, the Assistant Secretary of Information Architecture and Management for the Australian Department of Defense (ADoD), described how the ADoD evolved from thinking of EA as a theoretical concept to now using the U.S. DoD Architecture Framework (DODAF) in a practical manner to guide improvements in business processes and their supporting systems, enabling better defense for Australian citizens.

**"EA is a means toward rapid transformation of DoD business processes and systems to better serve the troops who are defending the nation. "**

The annual e-Government EA conference was held in Washington, D.C. on September 19 through 21. The entire conference theme focused on using EA for value, alignment and results. The three tutorials and three track sessions were focused on best practices and sharing lessons learned to build and manage EA programs and use them effectively to provide value to the enterprise. Keynote speaker, Greggory R. Garrett, President, Volkswagen of America and gedas USA, noted that EA adds rigor to a firm's value creation process and that architects have to tools to assist with change. In another keynote address, Dick Burk, the chief architect for the U.S. Federal Government, stressed that EA for results in the federal government is nothing less than the transformation of government. Paul Brinkley, Special Assistant to the under Secretary of Defense (Acquisition Technology & Logistics) for Business Transformation, Department of Defense, stressed that EA is a means toward rapid transforma-

*(Continued on page 12)*

# The Coming Age of Useful Robots

*By Paul Flanagan, John Feeney & Nathan Cormier*

The early part of the 21st century may be the "Golden Age" for robots. The present is the time when robots will begin to earn the labels of being useful, effective, and cost beneficial. Robots will begin to interact with humans on human terms and in places made for and used by humans.

Until recently only industrial robots had reached the stage of development where they could be called useful. In highly constrained environments factory robots can weld, paint, and assemble with extreme precision. In this role they can outperform human beings. As a result manufacturing is faster and the resulting products are cheaper and better. Clearly these types of robots are useful.

In this century robots will move from the confined factory floor to the home, the workplace or wherever humans go. In these environments the robot will have to adapt, as the world and its inhabitants will be unable and unwilling to adapt to them. Robots will move into the human world for two simple reasons: (1) they can, that is; they will have the technical prowess to adapt to the human's world and (2) humans will need and want them.

There are three technological advancements that are combining to allow robots to enter the human world. They are: (1) sensors; (2) navigational software; and (3) processing power (Frauenheim, 2004). These three advancements coupled with advancements in low cost manufacturing result in the perception that robots can be cost efficient.

Perception is a difficult entity to manage in robotics as virtually everyone knows what a robot is. Or at least they think they do. But the average person's image of a robot is formed from movies and television shows. These fictional robots are nimble of mind and body whereas their real world counterparts are far less adroit. As an example, in the IRM College's Critical Information Systems Technologies course we demonstrate the iRobot Roomba vacuum cleaner. It vacuums the classroom floor at the push of two buttons using a factory set "random walk" method (Garfinkel 2002). The Roomba picks up dirt and small bits of paper. It gently bumps into objects and scurries along walls. It refuses to fall off the instructor's raised platform. It costs about $250. In most more of our student's opinions it is worth the cost. Our $10,000 research robot running undergraduate student produced C++ code, and includes an impressive set of sonar, infrared and physical sensors, but moves too slowly and performs too limited a set of functions to impress the same set of students. Students will observe the research robot's actions, and proceed to ask, "But can it make me coffee?" Although both robots perform what they do well, the cost and perceived value are different.

As robots grow in technical prowess, the need for this technology is very much evident in healthcare and military applications. Healthcare has been described as being in the midst of a growing crisis. The growth of two key groups has contributed significantly to this. The first is the aging of the United States population. For persons aged 65 and older the population is expected to grow from 35 million people or 12.4% of the population in the year 2000 to 71.5 million people or 19.6% by the year 2030 (U.S. Census Bureau, 2004). For persons aged 85 and older the growth is even greater, from 4.2 million people (1.5% of the population) in 2000 to 9.6 million people (2.6% of the population) in 2030 (U.S. Census Bureau, 2004). The second key group is nursing professionals. Current projections show a 20 percent shortfall of registered nurses needed by 2010 (DHHS Division of Nursing, 2001).

One solution to the shortage is to import nurses from less developed countries, however a nursing shortage is expected to grow in those countries (Angle and Gruber, 2002). Health care robots are a viable alternative to importing nurses. With improved robotic technologies (hardware, software, sensors, etc.) the role of robots in health care is poised to make an impact on the situation. It should be noted that other countries such as Korea, Japan and Australia are facing similar demographic situations and are working to develop health care robots.

There is already limited use of robots in health care. Some research projects such as Pearl, a nurse-assisting robot, are showing promise. While there are technical issues with Pearl (battery life, navigation issues) researchers are pleased with 'her' progress thus far (Jejeh, 2004). While Pearl is a research platform, there are robots being deployed as well. For example, there is Mr. Rounder a robot that makes hospital rounds for a surgeon at the Hackensack University Medical Center, allowing him to see more patients (Weintraub, 2005).

Military applications are another area where the use of robots is increasing. Unmanned Aerial Vehicles (UAVs) are one notable example where technology can determine tactics. Once these

*(Continued on page 10)*

# The Identity Theft Nightmare

*by James Kasprzak*

**The Emergence of "Identity Theft"**

Identity theft has become a greatly feared, highly publicized crime in the United States. If you believe the journalists and the security industry, it is one of the fastest-growing and most costly category of criminal activity. The Federal Trade Commission estimated in 2003 that ID theft had affected 10 million Americans over the course of the year 2002 and had cost $53 billion ("Financial Institutions," 2003). A different source, the Better Business Bureau, estimated that 9.3 million Americans were victims of identity theft in 2004 (Singletary, 2005).

The most extreme cases of identity theft are startling enough to be featured in Sunday newspaper supplements. These horror stories describe individuals whose lives were terribly disrupted when they became victims of extended financial frauds. One study examined the most serious cases (only 178 people) in very great detail. The victims in these cases individuals suffered multiple, continued attacks on their credit, legal standing and personal reputations. They were plagued by debt collection agencies and refused credit for mortgages and loans. About 19% had home mortgages taken out in their names; 73% had new credit accounts opened without their authorization, and 65% owed money on unauthorized personal loans. Victims reported that their identities had been used to obtain drivers licenses, write bad checks, and obtain cell phone accounts and other services. In the worst cases, the marriages and personal relationships of victims were disrupted, they were denied financial entitlements, and they had mail, phone or utility services interrupted. An astonishing 29% actually were arrested for crimes committed by an identity thief ("Identity Theft: The Aftermath," 2003). Public concern over identity theft has become so widespread that the FBI now considers it one of the top computer crimes (Davis, 2004). The Federal Trade Commission has had identity theft as its number one complaint from the public for the past five years. Of the total number of 635,000 complaints the FTC received in 2004, 39% were identity theft, almost double the percentage of the runner-up – Internet auctions (Krim, 2005).

**The Changing Nature of "Identity Theft"**

Up until relatively recently, a victim of identity theft was far more likely to be suffering at the hands of a purse snatcher, a greedy relative or a light-fingered credit card thief. But there have been some significant changes in the nature and intensity of these threats which require new ways of doing business, and new forms of protection.

The methods by which criminals have stolen the majority of personal data and passwords have been generally low tech, personal and limited in scope. For example, a few years ago, consumers were warned against "shoulder surfing" -- criminals looking over the shoulder of a person at an ATM or a PC, in order to obtain information or passwords ("Ontario Provincial Police," 2004). Such techniques are relatively risky for the thief, slow, and obtain relatively small rewards.

As Internet commerce has attracted wealth into cyberspace, it has also attracted the kinds of predators who filch merchandise, forge checks and practice other frauds in malls and retail stores. Up to very recently, most cyber thefts were targeted at individuals, just as muggers steal one wallet at a time. Within the last three years, however, there have been many attempts to steal thousands or millions of data records at a time for quick resale to criminal gangs. Large personnel and financial databases have drawn the attention of such predators. Willie "The Actor" Sutton said that he robbed banks because "That's where the money is." Similarly, sophisticated cybercriminals are drawn to collections of personal data, because these masses of information represent more potential for profit than trying to steal one credit card number at a time. One stolen credit card number is only worth about $10.00 in the underground market, so it only makes criminal sense to steal credit card information in wholesale lots (O'Brian, 2004).

There are many employees who are poorly paid, or perceive

*(Continued on page 7)*

*(Continued from page 6)*

themselves so, and are willing to copy a credit card number for ten or twenty dollars. This person may be a clerk, a mail-room employee, even a Post Office worker. A waiter in a restaurant may run a credit card through a machine called a "skimmer" before processing it through the credit card company. The thief then sells the information to a group which uses the credit card number to buy products or encode it onto phony credit cards ("Ontario Provincial Police," 2004).

Overwhelmingly the greatest means of information theft is through internal sources and misuse of otherwise authorized data collections (Radin, 2005). The first large scale identity theft occurred in 1996 when a home improvement company in Houston stole personal data from customers and sold it for $250,000. More recent thefts of personal data include a clerk at the New York State Insurance Fund who took data on customers out of office files and bought goods and services using their accounts, and a medical worker who opened up credit accounts using the names and financial information of patients (Davis, 2004). Such thefts are increasing in number and in dollar amounts. In January, 2005, a Long Island help desk worker was convicted of stealing the identities of thousands of victims and selling these to specialized criminals who bilked victims for more than $100 million in losses (Krim & O'Harrow, 2005). By copying credit reports from banks he obtained information which victimized more than 30,000 people. The information was passed on to more than 20 people who used it for fraudulent transactions ("Help Desk Worker," 2005). Identity thefts are increasingly originating with employees who have access to information and use their positions to steal personal data ("Stop Thief," 2003).

One interesting trend in personal data theft is the fact that small as well as large databases have been targeted – anyplace that valuable information is collected and stored. The authors were surprised to find cases in which collections of credit card numbers and customer data had been stolen from retailers, a pet health store, and even a blood bank ("Stolen Laptop Contains Information on Blood Donors," 2004).

The more spectacular thefts, of course, are done where especially large quantities of files are kept. Thousands of credit card numbers were stolen from BJ's Wholesale, Inc., H&R Block, Inc., and database keeper Axium, Inc. ("Stolen Computers," 2005). A shoe store chain lost the data of over 100,000 customers through an Internet hack in 2005. A database containing customer information for 103 stores in its chain was stolen. The data included personal information as well as credit card numbers. The company first learned about the theft after a credit card company alerted it to a suspicious pattern of activity in the accounts of its customers ("Stolen Data," 2005).

The risk also goes up with especially sensitive (and therefore especially valuable) data, such as medical, financial and even educational information:

-- In 2003, about 7,000 patients in the Indiana University School of Medicine had their personal information and social security numbers stolen. A computer on the university network was breached by hackers, and while confidential medical files were not accessed, more than enough material was taken to allow the hackers to sell the data for criminal purposes (Horne, 2003).

-- At the University of Texas at Austin, students ran multiple attacks upon a database of current and former students and employees resulting in one of the largest thefts of personal data in an academic database. Over 55,000 individuals had social security numbers, addresses, and work information accessed. The culprits attacked through the Internet, and managed to download about 50,000 names in the database. The information was recovered before the culprits had a chance to misuse it (Read, 2005).

-- In 2004, LexisNexis had profiles of 32,000 U.S. citizens, including basic personal information, stolen online. The material was accessed using a stolen identity and passwords. The LexisNexis subsidiary that was attacked was Seisint, Inc., which sells data to businesses, law enforcement, and private investigators. It claims to have more than 20 billion records on U.S. citizens (Goldfarb, 2005).

-- ChoicePoint, one of the largest and most advanced collectors of consumer data, notified the public that hackers had entered their systems and stolen credit card information. At least half a dozen citizens in Los Angeles had their identities stolen. At first it was thought that only citizens of Californians were affected. Later, legislators from other states discovered that their citizens had also been targeted. ChoicePoint, based in Georgia, collects billions of items of data on American consumers, everything from credit cards, retail purchases, vehicle registrations, and identifying personal history information (Bogen, 2005).

**Protecting Databases**

In our review of recent developments in personal data theft, we have seen several trends emerging.

- There are more professional criminals involved, including organized gangs.
- They are increasingly targeting files, databases and other collections of data on individuals, in addition to thefts of single transactions or sets of data.
- Data is now targeted everywhere it is kept, on or off computers, on storage media and on backup files. Laptops are favorite targets.
- No files are too large or too small to be stolen. Individual retailers, small government offices, medical clinics and pet stores have all found their business records stolen or abused.
- The thieves are often current or past "insiders" who know

*(Continued on page 8)*

# Identity Theft Nightmare (Cont.)

*(Continued from page 7)*

where data is kept and how to access it. The term "insiders" includes present and former employees, vendors, employees of corporations performing outsourced services and business partners.

Trent Henry, an analyst with the Burton Group, says that corporations will increasingly look to apply digital rights management, encrypting business data to limit how information moves throughout the company's system. Even if a hacker gains access to strongly encrypted data, he cannot use it without very considerable expense and effort -- if at all. Certainly the average sneak thief can't access such files ("Stop Thief!" 2003).

Encryption is becoming an increasingly affordable and practical means of protecting stored business files. Speedy encryption requires computer power, something which is continually getting cheaper. Large databases are always performance sensitive, and the amount of time required to encrypt and decrypt information has been unacceptable until relatively recently. New computer chips developed since 2001, with multi-gigahertz clock speeds, are capable of doing online encryption with acceptable loss of performance. Data in some active databases often cannot be encrypted because operations can be adversely affected. Data "at rest", however, should be highly protected. This includes backup tapes and other media, data storage devices being transported, and archived records. The FBI and MI5 (the intelligence service of the UK) have both had laptops with security information stolen, but both had their files protected with strong encryption programs. While both organizations were concerned with their respective losses, the chance that the data would actually be decrypted and misused is much smaller because of their precautions (Gold, 2000). News reports of other thefts, including some in Japan and Europe, show that it is an increasingly popular business practice to encrypt important business data wherever it may be, and to password protect systems, individual machines and even important specific files ("Client Data Stolen," 2004). The Bank of America could stand to learn this practice. In 2005, it lost an unencrypted backup tape containing the personal information of 1.5 million federal employees. Unfortunately for Bank of America, the tape included data on ranking senators who announced hearings on the protection of personal data (Hendricks, 2005).

Another method of protection is to provide an audit trail for all accesses to internal databases. The Internal Revenue Service is one organization that restricts access to its very sensitive files. There are a great many people who would love to see the income tax records of other individuals: business competitors, parties to lawsuits, partisan politicians, even neighbors and family members. Beyond this, there is normal human curiosity: how much money did Marilyn Monroe make? IRS policy is to record all accessions of the income tax files of prominent figures. In fact, IRS employees may not access their own files, the files of friends and relatives, or that of their co-workers. A computer records all such accessions and reports them to an investigating authority. In some organizations, employees may be fired for unauthorized searching of files. One FBI employee was fired and arrested for "surfing" the FBI database for interesting cases (Dizard, 2004).

Yet another approach to protecting these databases would be to require banks, credit corporations, and information brokers of all sorts to protect their databases by simply enforcing normal computer standards. For example, Congress has passed several acts to increase the penalties for those stealing identity information, and increased security requirements for financial institutions. Banks and other entities have thus far resisted all such efforts because of the costs that might be involved. The temper of the time, however, has been changing. It was a small enough matter when individuals were mugged one at a time for their ID data. It is an entirely different matter for hundreds of thousands or millions of individuals to have their data stolen in gigantic thefts ("Lawmakers Call," 2005).

Security personnel, legislators and businessmen have become acutely aware of the vulnerability of the personal data of Americans. The scope and intensity of the frauds known as "identity theft" endanger some basic business processes in our society, whether or not they are online. For example, some experts are cautioning consumers that some necessary kinds of legitimate information transactions may expose them to unacceptable risk. Among these are loan forms, contest forms, job applications, resumes, and college and scholarship paperwork (Radin, 2005) (Davis, 2004). We will need new laws, new regulations, and new technologies to face the unexpected dangers of the Information Age.

**References**

Bogen, M. (2005, March 4). Identities stolen from agency. *The South Florida Sun-Sentinel*. Retrieved March 15, 2005, from http://www.sun-sentinel.com/business/custom/consumer

Client data stolen from home builder. (2004, June 23) *The Japan Times*. Retrieved March 15, 2005, from http://202.221.217.59/print/news/nn06-2004/nn20040623a8.htm

*(Continued on page 9)*

*(Continued from page 8)*

Davis, S. Identity theft and your online job search. (2004, December 10) Retrieved March 14, 2005, from http://developers.evrsoft.com/article/internt-marketing/online-business2/ identity-theft-and-your-online-job-search.html

Dizard, W. FBI analyst faces trial for surfing law enforcement systems. (2004, March 17). *Government Computer News*. Retrieved March 22, 2004, from http://www.gcn.com/vol1_no1/daily-updates/25279-1.html

Financial institutions make it easier to report identity theft. (2003, October 29). Associated Press.

Gold, S. (2000, April 19). FBI laptop stolen. Krim, *Newsbytes*. Retrieved March 15, 2005, from http://www.secretcomputer.com/data-security-news/FBI-stolen-laptop-2.html

Goldfarb, J. and Sullivan A. LexisNexis says 32,000 profiles stolen. (2005, March 9). *Reuters*. Retrieved March 15, 2005, from http://story.news.yahoo.com

Help desk worker admits role in large id theft. (2004 September 14). *USA Today*. Retrieved March 18, 2005, from http://www.usatoday.com/tech/news/computersecurity/infotheft/2004-09-14-id-theft_x.htm

Hendricks, E. (2005, March 6). When your identity is their commodity. *The Washington Post,* B1, B5.

Horne, T. (2003, February 28). IU center's computers breached by hacker. *Indianapolis Star*. Retrieved February 5, 2005, from http://www.indystar.com/print/articles/3/025875-2223-P.html

Identity theft: the aftermath 2003. (2003, September 23). *Identity Theft Resource Center*. Retrieved September 27, 2004, from http://www.idtheftcenter.org

Krim, J. (2005, March 23). Banking rules address theft of customers' private data. *Washington Post*, E1, E7.

Krim, J, and O'Harrow, Jr., R. (2005, March 10). ID thieves breach LexisNexis, obtain information on 32,000. *Washington Post,* E1, E4.

Lawmakers call for investigation into securing information databases. *Atlanta Journal Constitution.* Retrieved March 7, 2005, from Homeland Security Monitor. http://www.homelandsecuritymonitor.com/Docs/HSM092004.htm

O'Brien, T. (2004, October 25). Identity theft is epidemic. *New York Times.* Retrieved from http://www.nytimes.com/

Ontario provincial police: protecting yourself from identity theft" (2004, August 12). *Mondaq Business Briefing*. Retrieved September 27, 2004, from http://www.mondaq.com

Radin, D. Connected: online may be safest place for your data. (2005, March 10). Retrieved March 15, 2005, from http://www.post-gazette.com/pg/05069/468809.stm

Read, B. Hackers seize more than 50,000 social security numbers from U of Texas database. (2003,March 7). *Chronicle of Higher Education*, Retrieved January 5, 2005, from http://chronicle.com/free/2003/03/2003030701t.htm

Stolen laptop contains information on blood donors. (2004, June 16). *SANS Newsbytes*. retrieved March 15, 2005, from http://www.sans.org/newsletters/newsbites/newsbites.php?vol=6&issue=24

Singletary, M. (2005, February 13). When id theft starts at home. *Washington Post,* F1, F5.

Stolen computers have Wells Fargo customer data. (2004, November 2). Retrieved March 15, 2005, from http://siliconvalley.com/mld/siliconvalley/news/editorial/10079221.htm

Stop thief. (2003, December 19). *Red Herring*. Retrieved September 27, 2004, from http://www.redherring.com/PrintArticle.aspx?a=8123&sector=Capital

## Identify theft:
## *We will need new laws, new regulations, and new technologies to face the unexpected dangers of the Information Age.*

*This article is abstracted from "Data Protection and Identity Theft" by James Kasprzak and Mary Anne Nixon, published in the Journal of Information Assurance and Systems Protection (April, 2004). Full text provided on request.*

# Robots (Cont.)

*(Continued from page 5)*

types of vehicles were used merely for reconnaissance. Their use has expanded to include "strike, force protection and signal collection" (U.S. Department of Defense 2005). UAVs can be as light as one pound or as large as 40,000 pounds. And they are changing the way the Department of Defense meets its mission. Robots help the other branches of the military also. The Army uses small unmanned ground vehicles (SUGVs). SUGVs, will detect the presence of chemical and biological weapons, identify targets for artillery and infantrymen, and ferret out snipers hiding inside urban buildings (Baard 2004). Eventually robots may take an active role in the actual fighting. Often the military develops the most sophisticated technologies and these work their way into the civilian sectors. This is likely in the area of robots with first-responders, police, and firefighters using robots in ways similar to the military.

Micro-UAV

In summary, robots are becoming more adept. Their improving technical prowess and decreasing costs bodes well for the coming of truly useful robots. Whether these machines sweep the floor, aid in providing health care to seniors, or help the troops defend freedom, they are fulfilling important needs. It is this confluence of needs and capability that is ushering in the on-coming age of useful robots.

**References**

Angle, C. and Gruber, A. (2002). Carebots: The Future of Home Healthcare. MIT Alumni Association. Retrieved on 19 September 2005 at http://alum.mit.edu/ne/whatmatters/200207/index.html

Baard, M., (2004) Robots may fight for the Army, Wired News, Retrieved on 26 September at http://www.wired.com/news/technology/0,1282,63036,00.html?tw=wn_story_related

DHHS Division of Nursing. (2001). 2000 National Sample Survey of Registered Nurses Preliminary Findings. Rockville, MD: U S Department of Health and Human Services, Health Resources and Services Administration, Bureau of Health Professions, Rockville, MD.

Frauenheim, E., (2004) Robo-servants set to sweep into homes, CNET News.com: Retrieved on 3 October 2005 at http://news.zdnet.com/2100-1040_22-5419675.html?tag=nl

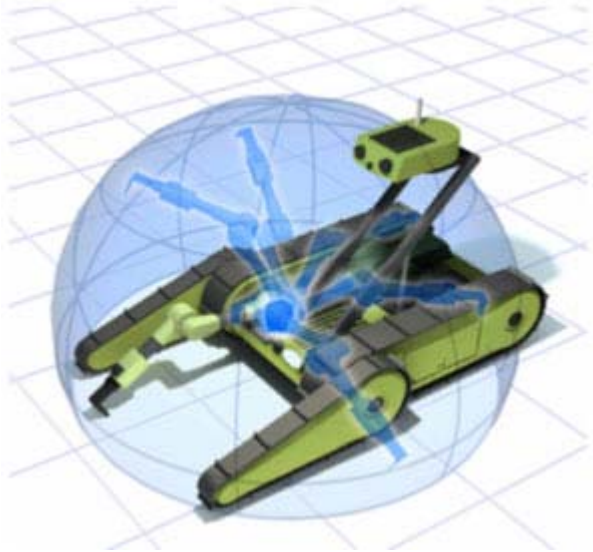
Garfinkel, S., (2002) iRobot Roomba, Technology Review.com Retrieved on 26 September at http://cache.technologyreview.com/articles/02/10/wo_garfinkel100902.asp?p=1

Jajeh, D. P., 2004. Robot nurse escorts and schmoozes the elderly. Retrieved on 18 September 2005 at http://www.intel.com/employee/retiree/circuit/robot.htm

Weintraub, A. 2005. Meet Mr. Rounder. Business Week Online. Retrieve on 24 September 2005 at http://www.businessweek.com/magazine/content/05_13/b3926011_mz001.htm

U.S. Census Bureau. 2004. Table 2a. Projected Population of the United States by Age and Sex. From U.S. Interim Projections by Age, Sex, Race, and Hispanic Retrieved on 24 September 2005 at http://www.census.gov/ipc/www/usinterimproj/

U.S. Department of Defense. (2005) Unmanned Aerial Systems Roadmap 2005-2030. Retrieved on 26 September at http://www.acq.osd.mil/usd/Roadmap%20Final2.pdf



Small Unmanned Ground Vehicle (SUGV)

# Humor in the eClassroom (cont.)

*(Continued from page 3)*

The actual lesson material can sometimes be framed in a humorous light, although unless we're explicitly teaching humor, that's going to be rare. One example of that is some role-playing I facilitate with my students after discussing structured decision making ("Analysis of Alternatives"). I tell my class we're going to pick a college and divide them into three sections; high-school students, their parents, and a financially independent group of rising graduate students. We brainstorm factors and options with some hilarious results (e.g., "party school" vs. financial aid vs. job placement rates). After helping them acknowledge how complicated this is when done manually, I get them refocused by demonstrating an example of an automated tool that can simplify the mechanics of the decision making process.

**Props**

Sometimes the written or spoken word isn't enough to convey the full humor of a given application. In those situations, we resort to…calling Mom and Dad for help? No! We use props! While they have some practical considerations, they can, if chosen wisely, maximize the benefits to our student's learning.

Naturally the prop has to be relevant; it should illuminate the subject, not obscure it. Props should also satisfy a few logistical considerations, such as ease of use, reliability, portability (such as for TDY offerings), and availability (can't use it if you can't find a place that sells it).

I'll start with an example that didn't work out. I once found a light-up "Applause" sign in a mail-order catalogue. For only $25, I got the sign and a remote control, with an applause sound effect! While it seemed quite relevant to conclude student presentations with it, I stopped using it based on some issues I hadn't considered. I found that students were already clapping after each presentation, before I could get the sign going. I also was disappointed with the range of the remote control; it was just shy of the distance to the back of my classrooms. And while I could compensate for that by sitting closer to the podium, I decided it just wasn't worth the effort.

A more successful use of props (in addition to my jar of ashes) would be pipe cleaners. Huh? Yes, you read correctly; pipe cleaners! Cliff Poole used to hand them out before his classes to give students a discrete way of staying engaged in some of the more tedious lessons. He also found they were a way of sending subtle feedback to the instructors (e.g., a noose hanging from a student's laptop means it's time to move on).

**Resources**

So, where do I get good material, you may ask? Good question! While I've already discussed use of your own experiences, there is help out there. Employ your students! By creating an environment that says "humor is welcome here", you may be pleasantly surprised at how your students respond. Encourage them to role-play; it's really a great way to leverage humor. It also helps them get into the scenarios of case-studies more deeply than they otherwise would. One exercise I use tasks my students to design a new sport-utility vehicle. I encourage role-playing, telling them to have fun and think boldly. It's a rare offering where I don't have at least one group of students include a funny picture or video in their presentation (e.g., one of Suburban Auto Group's series of "Trunk Monkey" TV ads). I've noticed the substantial content of those groups is usually richer as well.

There are also lots of online resources available. In addition to Internet searches for sound effects and other audio/video clips, there are archives of the various comic strips out there. And while there's often a fee to subscribe, you can then use keyword searches to home in on exactly the right material for your subject matter. Internet searches are also useful for deeper research in this area; I received thousands of hits in reply to "humor in the classroom" in preparing this article.

**Conclusion**

We've taken a look a range of issues here, from techniques and suitability, to resources you can tap into. I hope you've found this article helpful, whether you're a seasoned pro or a newcomer to the use of humor in the world of academia. Oh, by the way; the computer crossed the road because (drum roll, please), it was programmed by a chicken!

# *What's New with Enterprise Architecture* (Cont'd)

*(Continued from page 4)*

tion of DoD business processes and systems to better serve the troops who are defending the nation.

Several sessions in both conferences discussed the importance of service oriented architectures and data architectures in providing the information needed for effective and efficient business processes that enables capabilities to improve service to customers or in the case of the federal government citizens. The Association of EA Organizations, held a session at the e-Gov EA conference to introduce some of the existing organizations that are promoting the maturity of the EA discipline. Carolyn Strano represented the National Defense University's Information Resources Management College at this event in which she briefly introduced the IRM College's EA Certificate Program, the EA content on the NDU Knowledge Net and the EA community of practice, a web based site that enables information exchanges for those practicing and studying the EA discipline. The new peer reviewed Journal of Enterprise Architecture which published its first issue in August 2005 also debuted at the e-Government EA conference. Information on the IRMC EA Certificate program may be accessed at http://www.ndu.edu/irmc/programs/ea.html, the NDU Knowledge Net at http://knet.ndu.edu/, the NDU/IRMC community of practice at http://community.ndu.edu/CommunityBrowser.aspx, the Association of Enterprise Architecture Organizations, and the Journal of Enterprise Architecture at www.aeajournal.org.

---

"The views expressed in this publication are those of the authors and do not reflect the official policy or position of the National Defense University, the Department of Defense or the U.S. Government."

**Here's Our Web Address!!!**

http://www.ndu.edu/irmc/elearning/infotech.html

***CHECK OUT OUR PREVIOUS ISSUES!***

**INFORMATION RESOURCES MANAGEMENT COLLEGE**

**The World Leader in Information Resources Management Education**

300 5th Avenue Marshall Hall (Building 62)
Fort Lesley J. McNair, DC 20319
(202) 685-2096
http://www.ndu.edu/irmc/

**Director: Dr. Robert Childs**

**Dean of Faculty & Academic Programs: Dr. Elizabeth McDaniel**

**Chair, Organizational Transformation & Technology Department : Dr. Judith Carr**

**Newsletter Editor: Dr. Les Pang**