



NEW DIGITAL DAWN: HOW TECHNOLOGY IS CHANGING BUSINESS

BY BARBARA ELMORE

Imagine a globe chock full of mobile devices, where almost everyone is connected to home, or work, or a leisure pursuit, no matter the place or the time of day. Millions of fingers glide silently over small screens. Occasionally, thumbs take over, tapping out a silent message using a language developed only recently.

There's really no need to imagine; that scene appears minute-by-minute in the heart of the developed world and even in not-so-developed countries. Mobile devices wake us up and put us to sleep – and we rely on them for almost everything we do in between. GSMA, a worldwide association of mobile operators, says that almost half of the 7.1 billion people in the world use some kind of mobile device. By the time you read this, devices may outnumber people. That's because some people own as many devices as they have ears or pockets.

That our devices are used in transformational ways by business is not new, either. What is new, and what may continue to astonish us, is the innovative ways people are harnessing mobile devices to suit their needs. Marketing professor Dr. Jeff Tanner puts it this way: "What's more likely to loom on the horizon is not more technology, but the human capital to leverage technology."

Baylor educates many of those leveraging technology. Students from the university's Management Information Systems program have been recruited by business and industry, and also by the government when it needed professionals who could analyze massive data sets. "People who know how to analyze both structured and unstructured data to develop actionable business insight – that's a really hot skill set," says Dr. Tim Kayworth, chair of Information Systems. In fact, he says, the need is great for people who understand the role of information technology and how to apply it creatively to transform business processes and create new ways of connecting with customers. "Melding technical and business skills together is a very good combination," he says.

All universities, including Baylor, need to be thinking even more about business education that turns out people who understand statistics, research and experimental design, Tanner says. "In the last couple of years, 180,000 marketing jobs were created to use Facebook as a marketing channel," he notes. "Those people have got to understand big data and analytics. It's a tremendous opportunity, but it's going to make the quantitative part of business more important."



GETTING VALUE OUT OF BIG DATA

Tanner and others working in the areas of business research and business education provide strong examples of how to leverage technology. He is among those using technology to investigate how customers use technology, and conveying what he learns back to the business. The analysis can eventually transform the ways businesses connect with their customers and vice versa.

Tanner works with a “collaboratory,” a lab that’s part of the Baylor Research and Innovation Collaborative. The collaboratory includes business partners like Teradata Corp., a provider of a data warehouse that makes statistical analysis possible. Other partners include customer behavior expert iSIGN Media Solutions Inc. and Cabela’s, a store that specializes in outdoor gear.

Data analysis can yield what Tanner describes as “actionable research.” This is the kind of investigation that “addresses important academic questions and yields outcomes that companies can convert into revenue streams,” says Tanner. With Cabela’s, Tanner experiments with the integration of web browsing data into existing customer transactions. “This closes the loop from marketing activities to the sale so that you can improve your sales activity.”

New technologies allow merchants to use their own or third-party data to market to customers through different sources: a store catalog, online browsing, call-center marketing or in-store transactions. Cabela’s can also use hunting and fishing license data. An automobile dealer could use data from state license tags. Other businesses might integrate data from sources like the professional network LinkedIn.

In Tanner’s new book titled *Dynamic Customer Strategy: Big Profit from Big Data*, expected this fall, he includes a model that shows the processes of discovery, exploration and operation.

He illustrates the model with research on products that went into a customer’s shopping cart first during Cabela’s Black Friday and Cyber Monday sales. “If items went into the shopping cart first, you had a chance of closing that transaction. We created offers around this product and compared that to standard offers. We were able to increase revenues substantially, but more importantly, we were able to increase margin. So we took the models and we are now back into the discovery phase. This allows companies to get the value out of big data.”

A ‘BRING-YOUR-OWN’ TREND

The number of mobile devices on the market can overwhelm even those whose business is knowing about devices. But allowing individuals to bring their own devices to work is a growing movement that some say can encourage productivity.

Dr. Hope Koch and Lt. Col. Pat Curry, a doctoral student, are studying how the proliferation of devices like iPads and tablets affects business operations. The trend is called IT consumerization or BYOD, an acronym for “bring your own device,” and it started a few years ago with the popularity of iPads and iPhones.

The bring-your-own trend goes against the current of networked offices, where workers have a PC on their desks at work and perhaps another computer at home. The IT department provides the work computers and dictates the software. If someone needs to work after 5, he toils at the computer on his desk.

Now, however, tablets and other mobile devices spring up often at ballgames and in doctors’ offices, affording people the ability to work, play, and run personal errands simultaneously.

GOOD REASONS EXIST FOR THIS LESS-STRUCTURED WORK ENVIRONMENT, SAYS KOCH:

Most employees want to do a good job. Those who have a big workload and use their own devices believe they work faster and better. Recent research released by cloud company Citrix indicates some businesses agree. Eighteen percent of small businesses in the United States, Canada and Australia are achieving productivity gains of more than 30 percent “by adopting mobile workstyles, enabling people to work whenever, wherever and however they choose.”

Mobile devices give workers autonomy. “Having the iPhone lets them move around a bit more and they can do their work when they want to,” Koch notes.

Autonomy influences productivity. Koch uses an example of a pharmaceutical salesperson that might be able to catch a doctor for a beneficial conversation while walking down a corridor. “If the salesperson is dragging a laptop, the odds of him catching the doctor are not so great. An iPad allows you do to that more easily.”

Mobile devices contribute to innovation by encouraging employees to find new ways to do their jobs. Koch notes that a hospital has made standard practice taking pictures of wounds before they are bandaged. This occurred after a nurse used this practice – taking a photo with her cellphone – to avoid having to unwrap a wound so the doctor, who had not seen it, could examine it.

Some businesses can more easily retain their younger workers who are allowed to use their own devices. This is an employee satisfaction benefit because many younger people are happier using their own technology.



Koch and Curry are conducting research with professionals at major companies and have found that an integral part of bringing devices to work is the applications that come with them. That's because BYOD is about more than devices.

"It's more like BYOD + A – it's also about applications that can create issues with the government, for example. Information can't be stored in a place where IT does not know what the vendor is going to do with that information." And if the organization is highly regulated, like healthcare, government or financial services, they have a more authoritarian structure and using outside devices and outside applications is not allowed, Koch says.

But major corporations that only recently forbade personal devices or confiscated those brought to work are encouraging them now. "The challenge for the IT department is managing all of this, and that's what Lt. Col. Curry is studying," Koch says.



ATTACKS COMPLEX, BUT CONSISTENT

Although protecting a business run by mobile devices can be more complex, attacks remain consistent in their content, says Dr. Randal Vaughn, an Internet security veteran who has worked in private business and the military and teaches classes in cyber warfare. "Every now and then you see a new wrinkle – someone comes up with a clever way of attacking."

He believes individual devices require individual responsibility, with each employee acting more carefully when using technology, asking himself whether he really needs another application on his device.

Mobile devices are easier to lose than a desktop computer, and thus can more easily contribute to information "leakage," he notes. For example, an email could contain sensitive information, and the email might be on a phone that someone loses. "People take mobile devices with them all over the place. They are much easier to lose, and data in those devices is more vulnerable." That makes them subject to different attacks than a PC, which is more prone to viruses.

Also, he notes, mobile devices are preloaded with vulnerabilities that may actually be "pulled in" by the manufacturer. "You have to trust your vendors," he cautions.

One of the biggest new criminal attacks that concerns Vaughn is "spear phishing," the name of a scam directed to the "C-level officers" of a company – like the CEO or the COO. In this scheme, attempts to compromise information

arrive in email with a lure to a specific individual. The email tries to get the executive to act without thinking and click on an attachment. The goal usually is to access financials.

Even a small businessperson who is a very good user can be drawn in, Vaughn says. "And then they can install a low-tech infection like software that can read keystrokes." This can capture credentials that are used for a bank account, monitoring when a person begins using his computer and when he connects to his bank. The criminal can add transactions while the bank account's owner is making them.

This kind of crime hits individuals from small business owners to people who manage investment accounts online. "Those types of theft do not get published very much, but it doesn't mean they are not happening."

MORE SOPHISTICATION, NEW POLICIES

Generally, however, newer devices are easy to use, and we have all become a bit more sophisticated. "We have all developed a lot more skill, and we are seeing a little more savvy about what's going on," Vaughn says. "The question is always, 'How do we know we are doing any good?' There is no satisfactory answer, just long-term observation. We see students who have gone out and come back after 20 years, and have made leaps and bounds with the little bit of information we give them."

Securing business information is a matter of education, he says. "You want to motivate your employees to use good hygienic practices with data, like taking care with personally identifiable information." Protecting data and information, protecting customers and safeguarding business assets should be a corporate value, he says. Talking to employees about this is a matter of leadership.

And sometimes, new policies come into being to protect the organization legally. Companies can get in trouble, for example, if they fire an hourly employee who has been working on her own device and claims she is owed for hours of back pay. "Legal and HR departments are on top of these practices and are putting policies in place," Koch says. "Often, non-exempt (hourly) employees cannot use their own devices. Or if an hourly employee does use one and works after hours, he has to get paid for it." This means businesses must develop systems so they will know when their employees are working, even when the work is out of the office.

For businesses that want their employees connected, Vaughn offers basic advice that most parents give their children: Minimize exposure to potential threats. "We keep an eye out for bad people when we're shopping. We look both ways when crossing the street. We don't react quickly – we stop for a second. We don't jump into things."

He mentioned a bumper sticker that urges "Stop. Think. Connect." put out by an organization of the same name (stopthinkconnect.org). "It just says stop and think before you connect. That's good advice."