www.execblueprints.com

books24x7®

ExecBlueprints™

in partnership with Aspatore Books

Action Points

I. What Challenges Are Associated with Using Mobile Devices and Social Media?
Your company's marketing department and employees may love their smartphones and Facebook, but there's no doubt that the communications opportunities they provide can pose new headaches for IT. Specifically: How will employee use be monitored? How will employee-owned devices be integrated? How will company data remain protected?

II. The Bottom Line
Every company needs to independently determine how the use of mobile devices and social media will impact their business. The core question, of course, is whether the benefits (such as the increased ability to find and communicate with customers) will outweigh the attendant risks – both to the company's data as well as online reputation.

III. Must-Have Strategies for Using Social Media Safely and Effectively
While IT will probably not be responsible for generating the content that is posted on social media sites, you should plan to partner with your business and marketing groups to ensure that they have the functionality they need – and that they are focusing on the appropriate channels, updating profiles frequently, and monitoring what is being said.

IV. The Golden Rules for Orienting Users to Security Programs
There really is no 100 percent sure way of keeping data secure if employees are haphazard with the way they handle their mobile devices and social media postings. This is why education about security needs to be a continuous, collaborative, and iterative process involving the use of companywide announcements, trainings, and discussions.

V. Essential Take-Aways
If used prudently, mobile devices can boost productivity across departments but, if they fall into the wrong hands, they can spell disaster. Before deploying such technology, develop a proactive security policy that is endorsed by senior management and user departments, and includes standards, guidelines, and tools that will ensure compliance.

Contents

The IT leaders from Church's Chicken, Aquent, and CareerSpecific.com on:

Security, Mobility, and Social Media: Minimizing Risk in the Era of Sharing

Partha Mukherjee
Chief Information Officer, Church's Chicken

Lawrence J. Bolick
CIO, Aquent

Brian Cain
IT Director, CareerSpecific.com

Like leaders of many organizations, your senior managers are probably now expecting both unfettered use of mobile technologies and social media, and airtight protection of data and devices. And, even though users may share responsibility, the actual puzzle of how to balance accessibility with security ultimately falls to IT. This ExecBlueprint describes how IT leaders can partner with their users to achieve both objectives in an era where consumer use of both technologies continues to expand. First, IT must work with senior management to determine how to best exploit both mobile technologies and social media. Next, IT must establish a security policy that includes standards and limits; for example, not all employee-owned devices can be supported, and not all social media bells and whistles should be utilized. Then, your team needs to inform users of the policy through training, announcements, and discussions. Finally, you need to monitor the policy's effectiveness by tracking not only breaches and employees' social media use, but also areas you cannot control, i.e., what others are saying about your company. ■

About the Authors

Partha Mukherjee

Chief Information Officer, Church’s Chicken

Partha Mukherjee is the chief information officer at Church’s Chicken, a global restaurant chain operating in 22 countries with over $1.2 billion in revenues. He is a technology and business visionary with a proven record of accomplishments in outsourcing, offshoring, and BPO services.

Mr. Mukherjee has a progressive management style and is skillful in managing multi-vendor relationships. As the head of global IT he provides executive leadership, strategic planning, implementation, governance, and support. He has been successful in facilitating the productivity of IT solutions while managing costs and risks.

Finally, his positions in the U.S., U.K., India, and Middle East with service providers and end-user companies have lent him a 360-view of the IT industry.

☛ *Read Partha’s insights on Page 3*

Lawrence J. Bolick

CIO, Aquent

As the chief information officer, Lawrence Bolick is responsible for the creation and deployment of information technology initiatives to meet Aquent’s rapidly growing worldwide needs. He oversees the technical support of the company’s 50-plus offices and develops technology-based business solutions to support the company’s service strategies.

Mr. Bolick has more than 25 years of experience in the information technology and professional services industries. Prior to joining Aquent, he was CIO with Cambridge Technology Partners when the company grew 20-fold into a global systems integrator. He also has held management consulting positions with Big Five and systems integration firms, focusing on the telecommunications and financial services industries. He began his career as a systems engineer at Bell Labs.

☛ *Read Larry’s insights on Page 7*

Brian Cain

IT Director, CareerSpecific.com

Brian Cain has a master’s degree in music composition, but has been working full time in the information technology field for over 10 years. During that time, he has worked for several companies that have ranged in size from start-ups to Fortune 500 companies.

Mr. Cain is well versed in many programming languages and development methodologies. His background in developing Web-based applications has provided him the opportunity to learn about many different facets of IT including database design and maintenance, server administration, router maintenance, DNS configuration, and much more. He has learned over the years the answer is never “No,” but rather, “Anything is possible, but is what you want what you really need?”

☛ *Read Brian’s insights on Page 10*

Partha Mukherjee

Chief Information Officer, Church's Chicken

The Proliferation and Challenges Associated with Mobile Technology

The term, "mobile," today means much more than just phones. Mobile offers several benefits like revenue generation, cost savings, and convenience. Convenience is of key importance, which is why restaurants and QSRs are expecting more and more direct mobile transactions. For example, location-based services and ads are just one service that could be offered up on a smartphone right as a person walks by a restaurant. The iPad and Android will continue to rise in influence, until other device makers catch up. We anticipate that the mobile and social media combination will explode and different industries will adapt according to their business needs and customer requirements.

Prioritizing mobile developments is a challenge, and cross-platform development has not yet been achieved successfully. With greater demand for mobile devices, bandwidth availability may also be a challenge, which the larger telecom companies are already seeking to address. The fourth-generation (4G) technology promises super-fast broadband service that will make wireless video a breeze. However, chip manufacturers, telecom carriers, and device makers need to roll out new security features to help consumers feel secure and comfortable on their mobile devices.

Specific Support for Mobile Devices

While there are countless other devices on the market, there are only four devices that we support currently: Android, iPhone, iPad, and BlackBerry. Most of the usage is for e-mail through our secured network. In the future I am sure that we will have our apps available to customers — a joint strategy that we will plan with our marketing department. We already use the iPads and tablets for our brand standards team that conducts quality surveys in our restaurants. They help us collect information and data accurately and quickly, and have also contributed to a motivated work force as they avoid duplication of work.

It is very important, however, that security be enforced and that users are educated on the consequences. Because we do not want a security breach, we have established policies and technologies. As a matter of policy, we request that our users use their devices in a diligent matter, and report any loss, theft, or any unusual activity on their mobile devices.

We develop most of the applications with close interaction with the user departments that are aware of their features and how they will be used. This iterative and collaborative process throughout the development life cycle helps reduce actual training time.

We do provide training at different levels and in different ways depending on the profile of the users. Users can watch a Webcast or attend face-to-face training sessions; at times we have also adopted the train-the-trainer strategy. Our training materials are available on our intranet, which our users can refer to at any time. We also have a buddy program where the trained staff mentor the new staff for a fixed time and help them come up

Communications surrounding security need to be planned and continuous, and they need to be combined with appropriate training and governance.

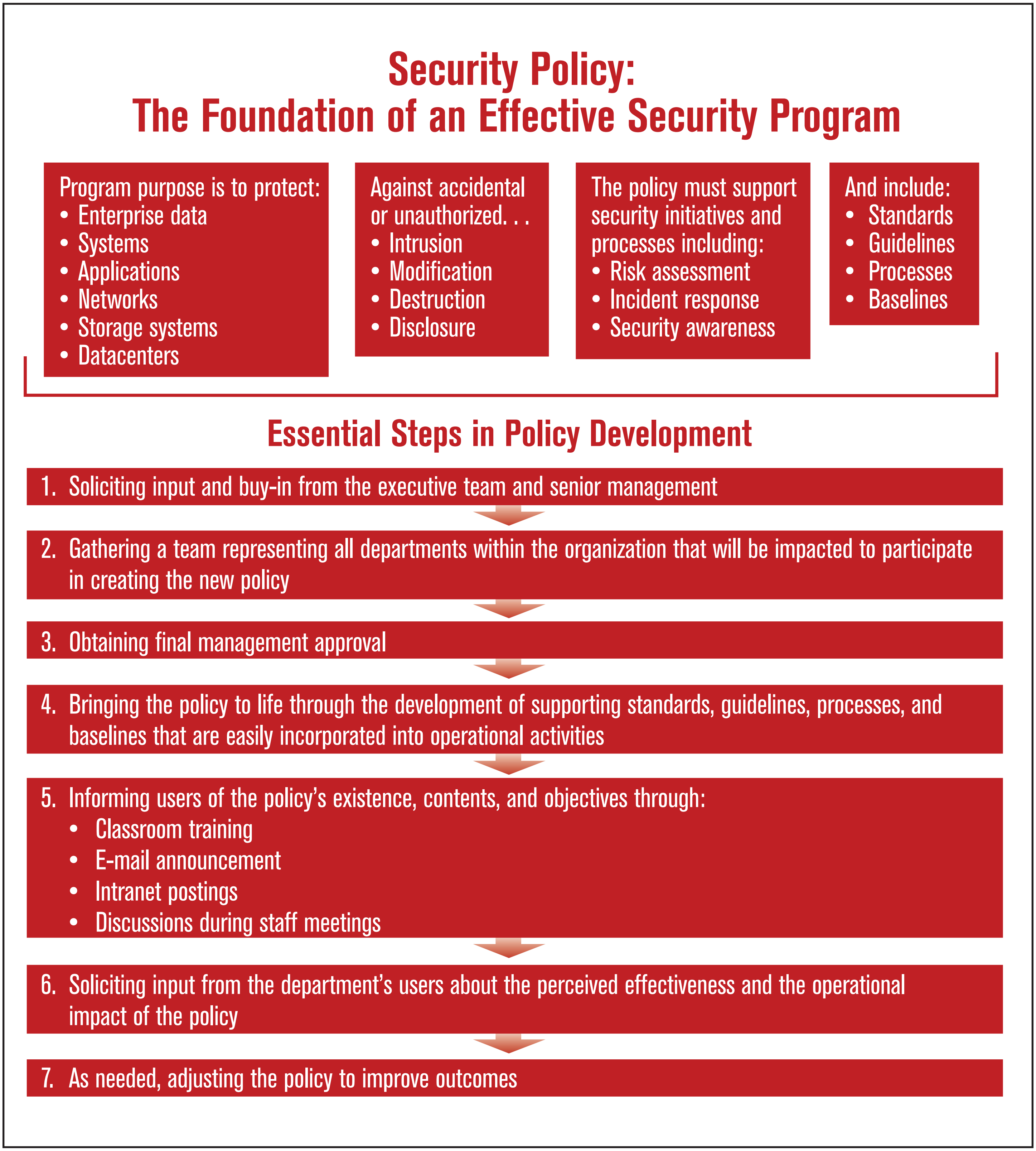
Partha Mukherjee
Chief Information Officer
Church's Chicken

Partha Mukherjee
Chief Information Officer
Church's Chicken

"Today we need to be proactive and not reactive on security strategies."

- *Accomplished in outsourcing, offshoring, and BPO services*
- *Responsible for strategic planning, implementation, governance, and support*
- *Experience includes working with service providers and user companies in the U.S., U.K., India, and the Middle East*

Mr. Mukherjee can be e-mailed at partha.mukherjee@execblueprints.com



Security Policy: The Foundation of an Effective Security Program

Program purpose is to protect:
- Enterprise data
- Systems
- Applications
- Networks
- Storage systems
- Datacenters

Against accidental or unauthorized. . .
- Intrusion
- Modification
- Destruction
- Disclosure

The policy must support security initiatives and processes including:
- Risk assessment
- Incident response
- Security awareness

And include:
- Standards
- Guidelines
- Processes
- Baselines

Essential Steps in Policy Development

1. Soliciting input and buy-in from the executive team and senior management
2. Gathering a team representing all departments within the organization that will be impacted to participate in creating the new policy
3. Obtaining final management approval
4. Bringing the policy to life through the development of supporting standards, guidelines, processes, and baselines that are easily incorporated into operational activities
5. Informing users of the policy's existence, contents, and objectives through:
   - Classroom training
   - E-mail announcement
   - Intranet postings
   - Discussions during staff meetings
6. Soliciting input from the department's users about the perceived effectiveness and the operational impact of the policy
7. As needed, adjusting the policy to improve outcomes

to speed quickly. Training is also mandatory for all the 24x7 help desk staff.

IT Security Challenges

If used well, technology can perform miracles, but if it falls into the wrong hands you can experience a disaster. The truth about security today is that "an ounce of prevention is worth a pound of cure." Organizations are moving away from blindly deploying reactive technologies to deploying preventive processes and technologies or enabling preventive features on their existing technologies.

Security challenges are also becoming more complex, and they range from dealing with the changing IT landscape to properly supporting the rising adoption of social technologies, employee-owned mobile devices, and cloud services. We need to develop governing strategies to support all security endeavors. With so much going on in security today, ethical hacking may soon be offered as a premium service by vendors.

It is important to realize that the only constant is change. As we evolve and utilize more technology, we open ourselves up to more security challenges. Users need to be educated about security policies and also the consequences of being hacked. Communications surrounding security need to be planned and continuous, and they need to be combined with appropriate training and governance.

Implementing and Enforcing Security Policy

Organizations need to have a well-defined security strategy and drive implementation to protect enterprise data, systems, applications, networks, storage systems, and datacenters against accidental or unauthorized intrusion, modification, destruction, or disclosure. We need to be responsible for supporting security initiatives and processes including risk assessment, incident response, and security awareness. The information security team needs to recommend methods of implementing and enforcing security policies; and develop, document, and enforce security standards, processes, and procedures to support the enterprise security policy.

Policies are the foundation of an effective security program. They come before — and are supported by — standards, guidelines, processes, and baselines. Policies must be clearly visible and users must be mindful of their existence when performing their daily tasks. So how do you build and manage a security program composed of effective policies?

The first step in policy development is soliciting input and buy-in from the executive team and senior management. The objectives of the policy should match business operational, compliance, and strategic objectives. Often policies are added to already existing security programs because of a need for regulatory compliance or if additional business requirements are identified.

The next step is to gather a team representing all departments within the organization that will be impacted by the new policy. The team should include anyone who has to ensure compliance as well as anyone who will be significantly impacted by the new policy. Allowing these employees to participate in creating the policy gives them a sense of ownership. When the final policy is released, they will willingly accept and enforce its procedures rather than exhibit the usual resistance that results when employees feel like you're imposing your policy on them.

Once the policy is complete, and final management approval obtained, develop supporting standards, guidelines, processes, and baselines. These policy support documents bring the policy to life in day-to-day activities. Then take the high-level concepts contained in the policy and translate them into tools that ensure employee understanding and compliance.

Anyone impacted by the policy must be made aware of its existence, its contents, and the objectives it's trying to achieve. This is accomplished through awareness training.

Expert Advice

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security requirements designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. The PCI guidelines are a good example of being proactive with security requirements.

We have adopted PCI security policies and have enhanced our security processes to ensure that we offer a secure environment. We have also communicated to our franchisees the need for adopting to PCI standards and enhancing security policies.

Since training must precede the expectation of compliance, you might not be able to wait until your next regularly scheduled awareness activity. Couple the release of the new policy with a multimedia awareness effort, including:

- Classroom training
- E-mail announcement
- Intranet postings
- Discussions during staff meetings

Post-release activities are just as important as those leading to policy implementation. Govern and monitor results to ensure you're meeting the intended objectives. Solicit input from the department's users about the perceived effectiveness and the operational impact of the policy. Using your metrics and user input, make adjustments to the policy or its supporting standards, guidelines, processes, and baselines to improve outcomes.

In summary, effective policy management is critical to a successful security program. Make sure you involve affected groups and individuals in policy development. Translate your policy into tools that are easily assimilated into operational activities. And always accompany policy releases with awareness activities. ■

Lawrence J. Bolick

CIO, Aquent

Policies and Procedures Surrounding Use of Mobile Technologies

Mobile services are an important and growing trend that is permeating all areas of the value chain from marketing and sales (e.g., smartphone advertising) to distribution (e.g., shipping and RFID codes).

For our business, we support a middle ground between the growing number of mobile product choices and the need to have some standardization for support. For example, we support three types of phones (iPhone, BlackBerry, and Windows), and will help employees integrate into our infrastructure for contact sharing, etc., if they select a model that is within those three standards. (A fourth standard, Android, is growing in importance and may displace one of the other three.) If an employee chooses a mobile phone type that is outside of those standards, then we will help to the best of our ability but offer no guarantees.

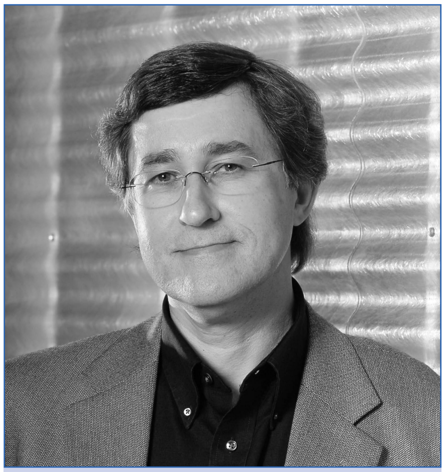
Even though the trend toward consumerization will pose a formidable challenge for IT moving forward, we chose to attempt to leverage this trend. For example, we subsidize the cost of software for phones that we support, and help employees integrate these phones into our network. Employees are, however, responsible for their own training and support. Our help desk will try to assist them with problems but there are no guarantees. The same conditions apply to our Google e-mail system. When we were using Outlook and Entourage, our help desk was heavily involved in e-mail support. Those client-based e-mail applications, in fact, took up the bulk of our support resources. When we moved to Google we took the position that because our employees were using Google at home without assistance, they could, for the most part, do the same with a work account. If they had any questions, they could go to Google Help. We have pretty much adapted now, and our large set of support services for client software has essentially disappeared.

> *There really is no 100 percent sure way of keeping data secure if your employees are haphazard about it.*
>
> Lawrence J. Bolick
> CIO
> Aquent

Protecting Data on Mobile Devices

Data stored on our mobile devices is password protected. Because the Commonwealth of Massachusetts (where we are located) has privacy regulations that stipulate that confidential data stored on mobile devices, such as laptops, must be encrypted, our communications and sensitive data stores are encrypted.

Our updates occur with infrastructure updates. When we moved from our original WiFi system to a later version a couple of years ago, that came with enhanced security. As our infrastructure continues to mature and build out, enhanced security arrives with it. In addition, we remain focused on our process for performing upgrades. Each week, we have a team that meets to discuss current and upcoming initiatives. For example, until recently we had a number of different internal support processes for bringing on new employees — all with their own nuances. When we brought in a more secure system in 2010, we took the opportunity to move each of those processes to that new system. Now we have a single system running these processes.



Lawrence J. Bolick
CIO
Aquent

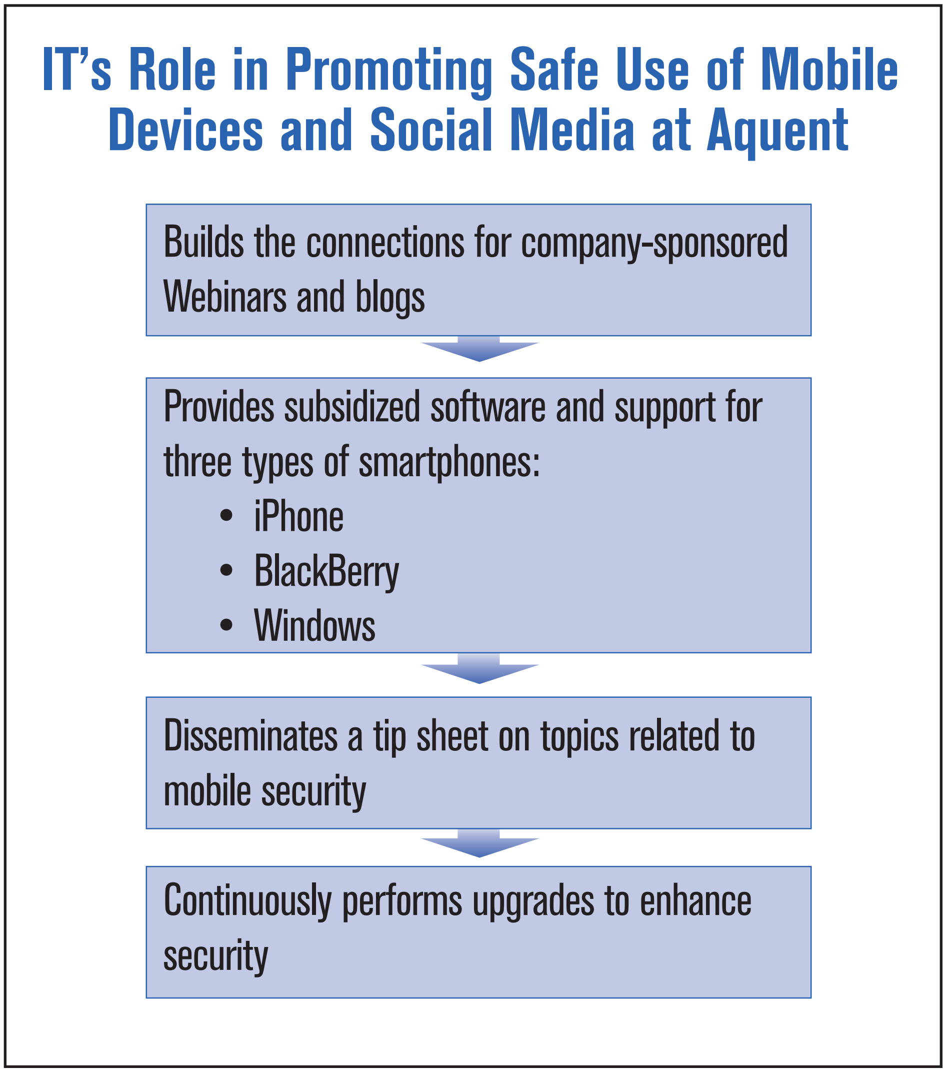
"Social media is really important to us for keeping our talent pool up to date and learning what they are doing or want to be doing."

- *Over 25 years of experience in IT and professional services*
- *Previously CIO, Cambridge Technology Partners*
- *Former chairman, New York City section, Communications Society of the Institute of Electrical and Electronic Engineers*
- *Bachelor's degree, Mathematics, King's College*
- *Master's degree, Applied Mathematics, Virginia Polytechnic Institute and State University*

Mr. Bolick can be e-mailed at lawrence.bolick@execblueprints.com

Top Security Challenges

When working offsite on mobile devices, the process of transporting data safely is one of the top security challenges we face. However, the data is protected because everything we do is encrypted. Another challenge, however, that is just as important is influencing the mindset of the people who are out there using the data. There really is no 100 percent sure way of keeping data secure if your employees are haphazard about it. Our responsibility is to get everyone's mindset focused around the importance of protecting the data that are entrusted to them by encouraging them to pay attention to the right way of doing things. For example, we have a tip sheet on topics related to mobile security. It gives some obvious and not-so-obvious guidance. An "obvious" item might be to not leave a mobile device that you use for work on the dashboard of your car for someone to see and swipe. A less obvious item is to keep visual contact with your laptop when going through airport security because there are scams where someone on the other side of the x-ray machine can walk away with it.



IT's Role in Promoting Safe Use of Mobile Devices and Social Media at Aquent

Builds the connections for company-sponsored Webinars and blogs

Provides subsidized software and support for three types of smartphones:

- iPhone
- BlackBerry
- Windows

Disseminates a tip sheet on topics related to mobile security

Continuously performs upgrades to enhance security

The extent to which using social media can heighten security risks depends on your mindset. While hackers might find out information about you that they shouldn't be getting, you also need to watch what you post, say, on Facebook. Some people go on vacation and place timers on their home lights, but then tell the world on their Facebook page that they are out of town. You will also see things

> *Over the next year, we expect to integrate our core systems more tightly with social media. By their very nature, the information in social media is constantly kept up to date. This offers us an opportunity to refresh the data available to our staff via our core systems more frequently than otherwise would be possible — but only if we take advantage of the integration opportunities that are starting to emerge with social media platforms.*
>
> Lawrence J. Bolick
> CIO
> Aquent

coming out in the business world that don't belong on social media. Consequently, you need to establish policies and procedures around correct use. WikiLeaks is a good example of what can happen — and that information was protected by military and State Department security. Increasingly, systems will be able to cull content from different social media, consolidate the information, and create summaries that previously needed to be provided directly by the individuals themselves.

Present and Planned Use of Social Media

Our business has two important external constituencies: our clients and our talent. The latter group tends to be self-employed individuals who use social media to keep in touch with each other and with the firms with whom they work, including us.

IT performs a lot of the integration with social media mostly through our Web group. That group builds the connections but the actual content is provided by our business and marketing departments. Marketing handles programs like Webinars and blogs. Our individual sales and talent agents also are empowered to create their own social media content, and are guided by policies and procedures from the business. ■

Brian Cain

IT Director, CareerSpecific.com

> *Twitter made a big splash in the social media world, but we found that it was too general for our purposes and did not offer the impact we could get with Facebook and LinkedIn.*
>
> Brian Cain
> IT Director, CareerSpecific.com

Implementing Mobile Technologies

While we do have mobile versions of our Web sites, they are not commonly used owing to the nature of our business, which is to allow employers to post jobs on our Web sites and enable job seekers to apply for those jobs. Currently, mobile devices are useful for browsing, but you would not want to write your résumé on it. For that reason we haven't put a great deal of emphasis on mobile development. While integrating more mobile technology is currently in the research stage, I have no plans to implement it at this time.

Currently I have other projects that are more likely to generate revenue. We would anticipate any type of mobile application as something we would develop and make available free of cost because it is not going to provide any new features that would not already be on the Web site. Consequently, from a monetary perspective, I am focusing on other areas that provide more benefit for the company.

Social Media Sites

On the other hand, social media sites can be quite useful. Our employees focus primarily on Facebook and LinkedIn. Twitter made a big splash in the social media world, but we found that it was too general for our purposes and did not offer the impact we could get with Facebook and LinkedIn. We just started working with LinkedIn, which has been useful in gaining followers and business contacts as well as lead generation. Because we do not currently have an employee who is solely in charge of social media, our profiles do not get updated as often as they should, but they do garner traffic on their own. Presently they are updated approximately once per week.

Being a small company with only four full-time employees, we are experiencing difficulty finding the resources to make a strong presence in the social media world. If that is a company's goal, then they need to dedicate an employee's efforts to this area. Using our company as a theoretical example, our dedicated person would know what is going on within the industry, what companies are being merged, what the media outlets are for that specific industry, and, of course, what is going on within our

Brian Cain
IT Director
CareerSpecific.com

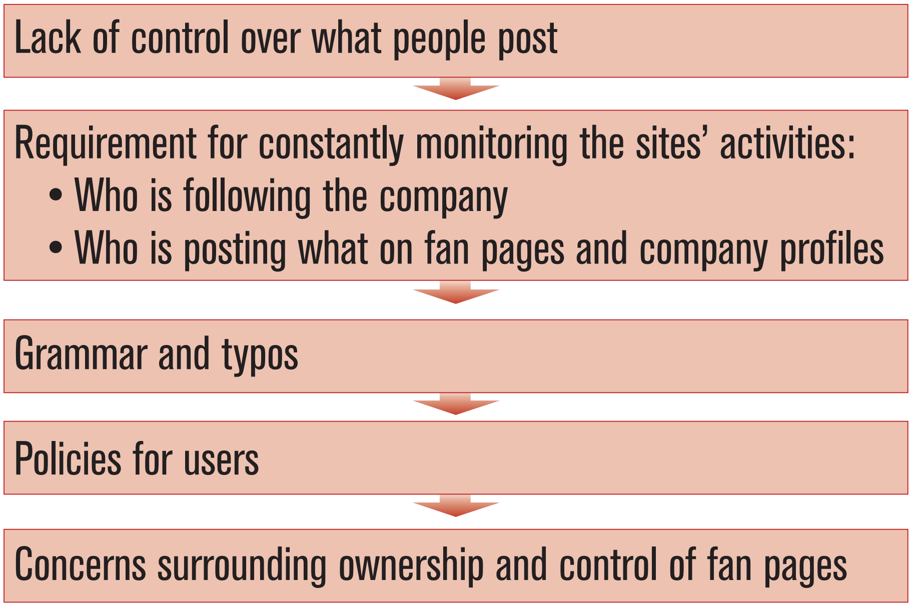
"Each company needs to analyze the usefulness and benefits that they can specifically exploit from mobile platforms."

- *Involved with IT responsibilities at Fortune 500 companies and start-ups since 1999*
- *Well-versed in numerous programming languages and development methodologies*
- *Responsible for server administration and router maintenance*

Mr. Cain can be e-mailed at brian.cain@execblueprints.com

> *In the long term, we are looking at developing some mobile applications for our Web sites so people who have accounts with us can manage their basic information and get alerts while on the go. Right now we rely on e-mail but it would be nice to give them the option of having alerts sent directly to their mobile device.*
>
> Brian Cain
> IT Director, CareerSpecific.com

What Areas Has CareerSpecific.com Needed to Address When Using Social Media?



Lack of control over what people post

Requirement for constantly monitoring the sites' activities:
- Who is following the company
- Who is posting what on fan pages and company profiles

Grammar and typos

Policies for users

Concerns surrounding ownership and control of fan pages

actual sites. The social media person has to do a lot of Internet research and then decide what is important enough to share with end users. He or she would also be responsible for following up on any type of feedback that is posted onto the social media accounts.

Social Media Concerns

We do not have any written social media policies, but all of our full-time employees have LinkedIn accounts, which they continue to update. When they make business connections, they add them to their personal LinkedIn accounts and suggest that others follow our pages. When it comes to LinkedIn our employees are much more active in trying to get the word out about the sites and joining groups that are related to the industries that we serve.

As for Facebook, most of our employees are not regularly active in a professional sense. They use it more for personal reasons; there is no professional link between our employees and their Facebook accounts other than our fan page. If we were a larger corporation we would probably need policies to protect the company, but we currently are not experiencing any problems in this area. If we were to put in policies, I would strongly recommend that anything posted on social network sites should remain personal and not company-related, and be posted on personal time, not company time.

There are also some security concerns regarding social media sites like Facebook and LinkedIn because you do not have control over what people post. This is related to Web reputation and security. You must constantly monitor your sites' activities, including who is following you, and who is posting what on your fan pages or company profiles. You also need to manage the grammar and typos, as well as the policies that you might set for your users. One of the problems with Facebook is that you must have a personal account to set up a fan page, and once you do that your personal account is forever tied to that fan page. If the personal account is being set up by an employee, and then that employee leaves, you may have a security issue. The worst-case scenario is that you could lose control of your page and have to start from scratch. This can happen if the person leaves their position, especially if that is due to a layoff. In such cases you cannot reach that person and you cannot get that page changed. For this reason it is important to have a contingency plan in place. ■

Ideas to Build Upon & Action Points

I. What Challenges Are Associated with Using Mobile Devices and Social Media?

While mobile technologies and social media channels can offer companies numerous benefits including additional opportunities for revenue generation, cost savings, and customer outreach, they can also introduce additional concerns for IT related to increased complexity and security. Specifically, these areas are:

- How can mobile device platforms be effectively and safely integrated into the company's infrastructure?
- How will employee-owned devices be incorporated?
- How will the security of data on mobile devices be ensured?
- How can the use of social media be appropriately supported?
- What policies are necessary to govern employee use of social media?
- How can postings about the company (which the company cannot control) be continuously monitored?
- How will IT acquire the necessary resources to provide all this extra support and monitoring?

II. The Bottom Line

After launching any program or policy regarding the use of mobile devices and social media channels, you should monitor results to ensure you're meeting your (and the company's) intended objectives. Areas of inquiry can include:

- Has the infrastructure experienced any security breaches?
- How well do employees understand security policies and practices?
- What is their degree of compliance?
- How have the new policies and practices affected company operations?
- How has the use of social media such as LinkedIn and Facebook increased or enhanced connections with customers and prospects?
- What impact has the use of mobile platforms had on revenues?

III. Must-Have Strategies for Using Social Media Safely and Effectively

Now that the use of Facebook, LinkedIn, and Twitter has exploded among many U.S. population groups, nearly every company will need to establish some kind of presence to stay current with customers and prospects — as well as the activities of their competitors. Nevertheless, the use of social media channels does require constant oversight: your company needs to not only monitor what its members post, but also what others are saying. Sound practices for interacting in these spaces include:

- Selectively choosing to focus on the social media channels that will best meet your company's objectives
- Establishing policies and procedures about appropriate employee use
- Partnering with the marketing and business departments to ensure they can extract the content they need from social media sites
- If resources allow, designating at least one employee to track industry-related news and trends that will inform the content of your company's postings
- Updating company profiles as often as possible with content that is grammatically correct and typo-free
- Following up on any type of feedback received through social media channels
- Joining LinkedIn groups that are related to the industries your company serves

IV. The Golden Rules for Orienting Users to Security Programs

As technology evolves, companies can be exposed to more security problems, which is why users need to be educated about security policies and the consequences of violating them. Consequently, communication around security needs to be a planned, collaborative, and continuous process with the users and their departments, involving:

- E-mail announcements
- Access to online information
- Tip sheets
- Mentorship activities
- Discussions during staff meetings
- Classroom training

V. Essential Take-Aways

As more industries learn how mobile technology can meet their specific needs, its use will continue to expand — and all companies will need to move away from deploying reactive security procedures toward thinking in terms of developing preventive processes. When using mobile devices, you can avoid a security "disaster" by:

- Limiting the types of devices that can connect to your secured network
- Encrypting all confidential data stored on mobile devices, such as laptops
- Performing timely upgrades of company infrastructure and applications
- Developing a well-defined security policy that includes the following steps:
  - Soliciting input and buy-in from senior management
  - Eliciting the participation of all impacted departments in policy development
  - Translating the policy into tools (e.g., guidelines and processes) that will ensure employee understanding and compliance
  - Providing multi-faceted awareness training about the new policy
  - Monitoring results to ensure that objectives are met
  - Requiring that users report any loss, theft, or unusual activity ■

Ideas to Build Upon & Action Points (continued)

10 Key Questions and Discussion Points

1. To what extent does your company currently depend on mobile technologies? What types of data are currently being generated offsite on mobile devices? Do these types differ by department and product or service line?

2. To what extent does your company (and employees at your company) use social media? What types of messages are generated (e.g., text, graphics, videos, photos)?

3. What standard operating policies and procedures does IT presently follow when deploying mobile technologies? How often are they revised?

4. What hardware and software do you use for your mobile enterprise applications? How do their features match your company's needs? How has the selection of technologies changed in the past three years?

5. Which social media sites do your company's employees currently visit? What role does IT play in setting policy with regard to use of social media on mobile devices? What type of support does IT receive from senior management in other departments on the formulation and enforcement of policy governing social-media access?

6. What are your best practices for protecting all data on your company's mobile devices? How often are updates required?

7. How are company employees trained on the proper use of mobile technology? What is IT's role in training company employees? What is their degree of compliance with regard to company policy surrounding social media access?

8. In the next 12 months, do you plan to introduce new mobile technologies? How will you protect data on these devices?

9. When working offsite on mobile devices, what are the top three security challenges your company faces? How do you presently protect data transmitted over wireless connections? In what ways does use of social media heighten these risks?

10. How is the security and reliability of your mobile technologies benchmarked at your company? Against previous systems and procedures? Against those of comparable companies in your industry?