IT/SECURITY SOLUTION

A critical success factor for IT and security organizations is effective communications, which enable quick decision making and operational efficiency regardless of location or time of day. The mobile channel offers compelling, new communication and operational solutions for IT and security groups. With mobile messaging, you can solve for a variety of IT and security use cases that help ensure business continuity, improve IT and support management, and provide security, authentication and fraud protection.

Business Continuity:

- Automated Incident management
- Network and system outage alerts
- Emergency notifications (One way/Two way)

IT/Support Management:

- Ticket life cycle management; awareness, ownership, updates, conditional escalation, and closure
- Staff appointment reminders, shift and on call change notification, personnel scheduling and shift exchanges
- System health notifications
- IT surveys and feedback

Security, Authentication and Fraud Protection:

- Compliance automation and notification
- Two factor authentication
- Password change reminders and reset
- Fraud alerts

Sample;

Alieu needs to enroll in several benefit programs. From home he accesses the company HR site, and the first task he's prompted to do is create a user account. The account setup page explains that Alieu needs to do three things. First he needs to enter a difficult to guess username and password and his mobile phone number. After Alieu submits his information, his employer sends a PIN to his mobile phone, and he needs to enter the PIN in order to proceed. Alieu also has the option to request a PIN each time he accesses the site, which he does because it gives him added assurance that his personal information is secure.

A poll of Fortune 500 companies reveals at least 1.6 hours per week of IT system downtime. Based on an hourly rate of £56, this equates to a weekly labor loss of £896,000, or £46 million annually.

IT system downtime reflects poorly on overall organization's reputation and negatively affects employee productivity and morale. Yet in today's technology driven world, some downtime is unavoidable.

In today's fast paced business environment, IT organizations need more nimble ways to keep employees informed and computer systems safe. While email is effective much of the time, an incident can take down an organization's email server, leaving management without an efficient and immediate way to communicate with employees. SMS, as the most widely used communications channel around the world, provides IT with an effective and economical way to close that gap.

Alchemy's SMS solutions allows institutions to provide clear, instant details regarding servers and networks. Whether informing employees about a scheduled maintenance procedure or alerting staff to a security breach, your organization can use SMS and IVR to instantly reach employees.

If the problem involves a security breach, you can use mobile messaging to notify employees of the threat, report system status, and instruct them via text to change email or other passwords. Keeping employees informed throughout a server

restoration process eliminates confusion and empowers them with current information and alternate work instructions.

Alchemy's Interactive platform keeps employees informed about server maintenance, security threats or other system outages, enabling institutions to:

- Utilize SMS to minimize missed messages.
- Broadcast a message to all employees or send custom messages to specific groups.
- Bolster employer/employee relationships by providing current information and reducing confusion, concern and frustration.
- Improve productivity and reduce workflow interruptions.
- Increase IT efficiency.

2012 and 2013 were busy years for cybercriminals. Security breaches occurred among numerous high profile organizations, including LinkedIn, eHarmony, Adobe and IEEE, releasing user passwords and other personal information into the hands of hackers with malicious intent. Breaches like these not only compromise the privacy and security of users and corporations, they can seriously damage reputations and brands.

Despite the high profile breaches and the constant threat of cybercrime, the flow of information across the Internet continues to increase. Users embrace their mobile devices for all kinds of transactions and liberally download apps. And at the same time businesses look to BYOD for the productivity benefits it offers.

Whether the data at risk is personal information or corporate IP, cybercriminals will profit from accessing it. Institutions know that their IT organizations and employees must be diligent and systematic about protecting the network infrastructure.

To address the increasing risk, institutions should look at how they authenticate users. Outside the financial industry, most institutions still rely heavily on single factor authentication (such as username/password).

Curiously, one recent study showed that technology companies rank much lower than financial and retail institutions in implementing state of the art security solutions.

Too many companies still rely on usernames and passwords as the only gate to accessing sensitive data or to initiating a secure workflow, such as benefits enrollment, account activations, and payroll management.

Even while users are concerned about data privacy and security, and demand it for their personal information, they still want the convenience of quick and easy access. As the digital age advances, any institution that interacts with its audience (whether employees or customers) must look for ways to conduct those interactions securely.

Verifying user identity is one sure step toward that goal, and two factor authentication is the solution.

What is the "factor" in authentication?

Authenticating identity can utilize three different factors:

- Knowledge; Something known only to the user, such as username and password.
- Possession; Something only the user possesses, such as a physical card, a mobile phone, or a security token.
- Inherence; A characteristic unique to the user, such as a fingerprint or another biometric trail.

Using any two of these factors constitutes two factor authentication. This type of authentication is not a new concept. Many financial institutions already utilize it for a variety of transactions, including account creation and access, bill pay, and funds transfer. And recently, leading global companies like Google, MSN, Dropbox, Yahoo and Evernote have adopted 2FA as their user verification method.

How does Alchemy's 2FA work?

Our 2FA solution leverages the knowledge and possession factors, and provides the latter as a PIN delivered to the user's mobile phone via SMS. With the PIN conveniently in hand, the user can connect to the system or network via a more secure method.

Implementing 2FA is easy and you can deploy it globally. It's popular with end users because it does not require any new or special hardware or software, and also doesn't require the user to divulge biometric information such as a finger print or iris scan.

Two-factor authentication delivers benefits beyond added security. Because you're using a platform that's both scalable and extensible, you can start by implementing 2FA for one business process, and then extend it to integrate with other systems and workflows. Benefits of two-factor authentication:

- Increased security of business critical systems and data.
- Increased ability to comply with regulatory requirements.
- Reduced exposure to fraud claims.
- Improved user loyalty and trust.
- Greater sense of confidence and peace of mind.

- Flexible, scalable, extensible platform.
- Support for multiple use cases such as network/system alerts, reminders, and surveys.
- Configurable settings for PIN creation and management.