Internal Network Crisis Communication

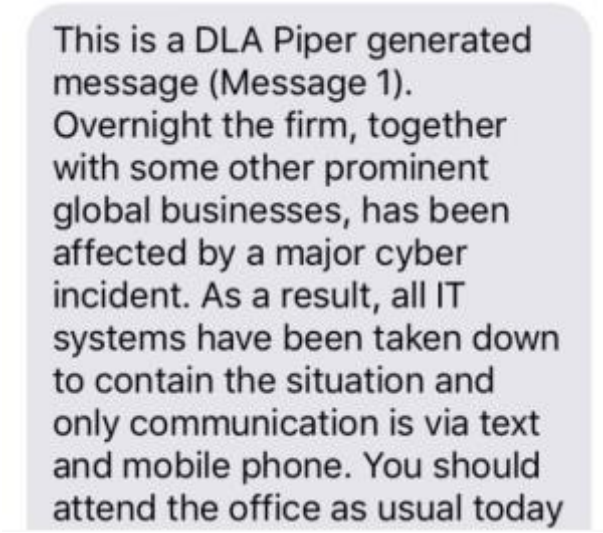
August 2017

It happened in the middle of the night..

“Global law firm DLA Piper has told Australian staff it has been the victim of a "major cyber incident" overnight.”

As mentioned in a series of news stories that introduced the world to the Petya Ransomware cyber-attack. Similar in nature to the “WannaCry” virus that infected hundreds of thousands of computers in May – it basically shut down the computer. In the case of Petya, a screen with a demand for US$300 worth of bitcoin to restore access was all that was visible and accessible.

DLA Piper had to move fast. A message was sent via SMS which stated:



They had to ensure their staff all over the world did not turn on their computer. If they did, the virus instantly took hold. Malware of this nature is exploiting deficiencies in cyber security in networked systems everywhere. It means that IT Managers need to have a communication plan that can be implemented the instant its required.

More from the source:

“AP Moller-Maersk, a Denmark-based oil and shipping company confirmed they were also hit in the so-called Petya attack which had affected "multiple sites and select business units".

"The WannaCry incident of a month or so ago was a wake-up call for us on how this can start impacting across networks," the special adviser to the Prime Minister on cyber security, Alastair MacGibbon, said.

"We've always known this could happen. From a government point of view, our Computer Emergency Response Team will be reaching out to industry to make sure we're giving the right message."

After the WannaCry attack, organisations were advised to review and harden their IT security systems. We cannot know if the Petya attack was limited as a result. Over 80 companies reported they were victims of the attack. Ukraine and Russia seemed to be worst affected, and the theory was the Ukraine govt was the actual target. Four arrests have made so far.

This all highlights the need to have a comprehensive communication plan with employees and especially for global multi nationals.

Ransomware attacks are increasing

According to a recent report there were 638 million ransomware attacks in 2016. This it says is 167 times the attacks that occurred in 2015. The prediction is that this will grow in 2017. The sobering fact is – ransomware is big business for cyber criminals. About $209 million in ransom payments were made in the first quarter of 2016.

Once a computer is infected, companies are paying to get the files decrypted. It goes against all advice, but what do you do? Usually the files are not recoverable without a decryption service of some kind.

Its obvious prevention is cheaper than the cure, however in the case of Petya and many others, the ransomware is exploiting security vulnerabilities in their operating system. Microsoft issued warnings to install a security patch in the months after WannaCry, and the theory is those who did were protected.

Another concern is ransomware is not confined to your PC. Increasingly, reports have confirmed, Android devices can also be affected. To protect yourself and your company, ensure your staff are only downloading and using verified apps.

In the case of DLA Piper it was all but too late however the speed they could send a message to staff might, have prevented even more pain. For staff, the most effective method of receiving a message is on their smart phone. Most are never far from their phone and its often the first thing people check when waking up. Your smart phone is also probably the best security token in two factor authentication requirements. Banks especially are asking you to confirm a text message pin when accessing secure areas.

Send a message that everyone gets…no matter what!

A proper communication plan must check a few boxes:

1. It needs to send a message to all staff no matter where they are
2. The message needs to be Omni channel – email, SMS and push notifications at least
3. The Admin should be able to tell if the email has been opened, SMS delivered and the push has been opened. If a user swipes the push you can tell its opened.
4. The message should go out simultaneously and from one unified dashboard

This could be further enhanced by posting to the company website, or social media channels – if the message is not sensitive. However, it is not enough or smart to rely on social media to get a crisis message to everyone.

Companies are increasingly turning to dedicated smart phones apps to manage crisis and network communication. UgoRound offers companies both crisis and Omni communication and employee tracking options.

You can track and trace an employee during set or specific work hours or you can send a message through the app which will be received wherever they are in the world.

This is all done by a secure invitation and join process for staff members. This means a verified and trusted member is joining the group and they can input credentials that further identify them to the Admin.

A crisis communication strategy should include a geo aware communication platform. Trusted administrators should know where their employees are and if they are in danger or can be re-deployed based on their proximity. This could save lives in the case of a crisis or incident or save millions in costs associated with time sensitive information.

Location based messaging is a proven and effective method for internal and networked company communications. Be it a multi-national or if you have employees in the field, when a message needs disseminating you can do so from your UgoRound central command with confidence.

Everyone gets the message with UgoRound.

Contact Us for you company crisis communication plan.

References:

http://www.abc.net.au/news/2017-06-28/ransomware-virus-hits-computer-servers-across-the-globe/8657626

https://fightransomware.com/news/ransomware-roundup-2016-saw-gigantic-increase-ransomware-attacks/

http://www.androidauthority.com/ransomware-attacks-android-increased-751266/

UgoRound will connect you to your City

Wait…seriously?