Forbes

Leadership / # Economy

Millennials' Push For Corporate Instant Messaging Could Enhance Cybersecurity

Harry G. Broadman, CONTRIBUTOR

I advise, speak and write on global markets and business strategy. FULL BIO

*Major Data Breach Has Left 15 Million Accounts From This Popular Site Vulnerable (*wk1003mike*)*

Across the U.S. industrial landscape, corporate instant messaging, whether via mobile devices or PCs, is becoming an important supplement to emailing for enterprise-wide communications. In part, because of the expanding roles in corporate hierarchies of Millennials—who, after all, came of age with the advent of instant messaging—and, in part, due to the substantial productivity-enhancing nature of these types of communication protocols, instant messaging systems could, in time, actually rival the use of email for internal corporate communications. They even hold the promise—if structured to incorporate the latest generation of electronic security programs, which are constantly improving—to provide for even more robust protection from the risks of internal intrusions than emailing.

C-Suite executives and Boards of Directors are now ever mindful of cyber-security risks, and are on a tear to get educated on the topic. However, in coming up to speed they should take the time to understand *firsthand* on-going developments in the field and not demure because they have the impression that it is 'all too technical'. It's really not. And, ironically, they will likely come to appreciate that these new means of communicating are actually the mechanisms they should probably employ themselves for the *own* highly sensitive internal deliberations and decision-making to strengthen corporate governance and raise enterprise profitability.

Corporate emailing—of course once a revolutionary means for businesses to distribute electronically rather physically hard-copy memos among their employees—will, for the foreseeable future, likely continue as the mainstay for *internal* communications, and will certainly remain the overwhelmingly dominant form for *external* corporate communications. But the advantages of instant messaging in the internal corporate environment are quickly becoming evident.

Perhaps the most important is the conversation-structuring of thematic-specific exchanges as they occur in real time—a much more natural and efficient way of communicating compared to the *ex post* assembling of buried, disparate threads of emails.

There's also a tendency to compose emails in a formal format—harkening back to the old-style memos—and this almost always places the burden on the reader to decipher what is the real 'ask' by the sender. By design, messaging calls for a shorter composition and thus channels the writer to get right to the point, making it easier for the reader to respond quickly.

It's attributes like these that will help make instant messaging game-changers for enhancing enterprise-wide productivity.

There are significant differences in the fundamental designs of email and instant messaging systems in terms of susceptibility to external intrusions, and they each have their strengths and weaknesses. Both are increasingly incorporating state of the art security protocols, and there is no inherent reason why instant messaging could not bolster firms' resilience to information-related security risks on par with analogous protocols introduced into email systems, and conversely.

But truth be told, in light of the rapid growth of the use of instant messaging in the corporate domain, it's increasingly becoming clear that extra resources are being devoted to strengthening their security. It would not be a surprise as successive generations of instant messaging systems are developed if their security protocols possibly surpass those of emails.

If this were to occur, instant messaging systems may well be able to provide the best of both worlds: increased productivity as well as strong security protections.

Rarely does a day go by when C-Suite executives and Boards of Directors aren't fixated on news of massive cyberattacks and data breaches in some of the country's most stalwart companies. Their biggest concern becomes: "will we be the next target?" That's understandable in light of the responsibilities they hold.

At the same time, they marvel at the startling efficiencies that have arisen in modern intra-corporate communications in the enterprises they oversee, especially because of the growth of instant messaging.

The result is they often have trouble reconciling the two issues.

In part, this stems from the fact that they are not yet fully informed as to the benefits and costs of how these new means of internal business communication actually work. They would do well to focus on several factors to guide their decision-making as to how best evaluate such products.

First, the growing reliance towards enterprise instant messaging is increasingly a direct outgrowth of demands by companies' employees that are market-facing.

Executives in line positions know that their success or failure in closing sales or purchases is driven in part by their ability to obtain information about their customers, suppliers and competitors as quickly as possible. But far more important is for them to have the ready-made capacity to make sure these relevant data are transmitted to their colleagues within their enterprise both quickly and in a format that enables agile internal decision-making. In this context, spending time combining threads of separate emails--often buried--rather than having the data in a ready-to-read systematic conversation structure could well mean the loss of a sale or purchase.

Perhaps even more important is that the shift towards corporate instant messaging reflects the fact that Millennials, the first generation to routinely utilize instant messaging as the primary form of electronic communication, are increasingly filling higher and higher ranks of the workforce.

While Millennials initially embraced messaging as the mode of choice for rapidly sharing information in the social domain, over time they have come to realize it provides a superbly efficient tool for commercial endeavors. Thus, what was once a method to communicate among well-defined networks of *friends*, is quickly becoming the natural mechanism to engender collaboration among like-minded *co-workers* jointly focused on solving a particular business problem or exploiting a new commercial opportunity. Today, instant messaging has become an efficient instrument for corporate team-building in order to explore synergies and test out new ideas to bring to market.

The point is that one way or another as Millennials rise within the corporate ranks, they are going to continue to rely on instant messaging for business communications—not only because it is what they are used to, but also due to the fact that they recognize its inherent efficiency over other communication methods.

C-Suites and Boards would thus do well to embrace this change *proactively* in order to make way for the inevitable. If they do not, they will find themselves in a situation where there are actually *competing* internal communication systems with which to contend. Invariably this will weaken the security of the company's entire internal communications network.

Legitimately, C-Suites and Boards find it hugely challenging to keep pace with the utterly rapid changes underway in the development of internal corporate communications technologies. Their attention often focuses solely on the risks and vulnerabilities they might present.

What almost always gets lost in these discussions, however, are their relative potential benefits. And most importantly, how the various systems can be structured to greatly mitigate exposure to risks while capitalizing on the benefits. This a natural human reaction, but a myopic one. And, it can end up doing more harm than good.

More often than not, this stems from the fact that C-Suites and Boards may not have been sufficiently educated by their in-house cyber security and information technology experts, who, in turn, may find it challenging to differentiate among the plethora of new products coming onto the market, especially instant messaging programs.

Of course, given the volume of such products—which grows larger every year—this is not always an easy task. Still, it must be done. And C-Suites and Boards cannot afford to be shy about asking questions no matter how silly or basic they may appear to these specialists.

In the wake of the recent data breaches that have befallen some of the most well-known U.S. companies, in every instance the affected institutions underwent extensive cyber-security risk assessments to determine if their internal communication systems were safe to use in the future. Sadly, as C-Suites and Boards learned, most did not have secure systems nor reliable crisis management communications tools in place before the attacks occurred.

The cyber environment promises to get only tougher in the months and years to come. Those at the helms of our businesses should seize the moment to get educated now about how to turn the responses to those risks into opportunities for improved business governance and performance.

Harry G. Broadman is CEO of Proa Global Partners LLC; faculty member at Johns Hopkins University; non-executive board director; and speaker. Contact: www.harrygbroadman.com

The link to this column is: http://www.forbes.com/sites/harrybroadman