SNL IR Solutions

IR Website Disclosure:
Data Security Best Practices for IROs in the Digital Age

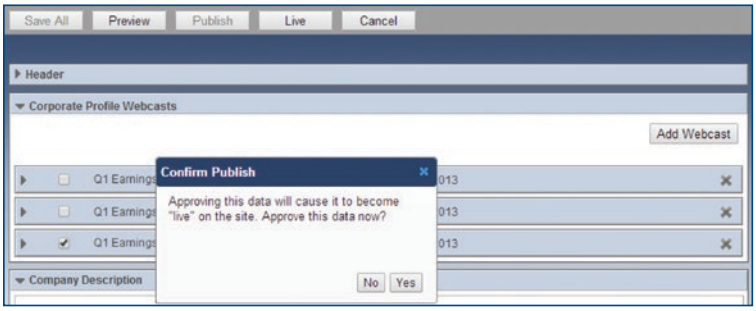
Introduction

In today's Investor Relations environment, stakeholders access new company information primarily through the internet. IR websites, press releases, and document feeds are all sources that analysts and investors rely upon to stay informed. The trend toward instantaneously available information is great for communication, however, it also means that disclosure accidents like premature publications or leaks are all the more visible. That extra visibility has the potential to impact stock price and company reputation within a matter of minutes, presenting a hefty clean up challenge for the IRO.

As technology continues to advance, IR disclosure systems need to keep up with the pace. Problems resulting from sub-par disclosure security have been cropping up in the past few years as documented by The Motley Fool in May, 2011, by CBS News in October, 2012 , and again by MarketWatch in May, 2013 . This guide will explore the IR web content challenges present today, and what kinds of measures to have in place for effective control over content disclosure.

Content Management System

A Content Management System (CMS) is a portal that allows a user to make changes to their website. It's the heart of the site's content, and is thus critical to content security. If the CMS is not secure, it is easy for individuals and programmed web crawlers to find staged information before that information is made public on the site.



A secure CMS should have the following attributes:

Secure Staging Functionality: the CMS should give one the ability to review and approve changes in a password-protected staging environment before those changes are published onto the live website.

Restricted Access: access to the CMS should be restricted to authorized users, ensuring that only users approved by the IRO can make changes and view staged content. A convenient feature that a CMS often provides is the ability to allow different types of access to different users, so that one user can be granted access to publish changes on the site, while another can have access to only review staged updates, not to make updates themselves.

It is important to have a process in place that outlines the proper channels for changing users' access as needs change over time as well.

Secure Document URLs: uploaded documents should be given a URL that is password-protected during staging and thus cannot be viewed by web crawlers or web-savvy individuals until the document is public on the IR site.

Unprotected document URLs were the most probable culprits for several of the earnings leaks that occurred in the past. If a document has a predictable file name in the URL like 2Q_2011.pdf or 3Q_2011.pdf, it is fairly easy to predict the URL for the next document in the series, since it would most likely use a file name like 4Q_2011.pdf. If the new document is uploaded for staging and is not properly protected, anyone could guess the URL and view the document even before it is publicly disclosed.

Predictable URL Format Example:

For utmost security, it's best to have password-protection for all staging URLs, but it's especially important for documents with predictable URLs.

IR Website Support Team

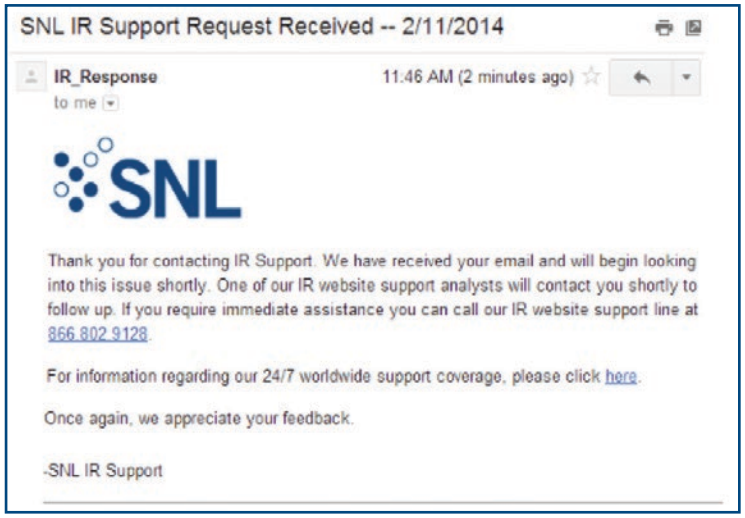
Having a great IR Support team, whether that team is internal or provided through an external vendor, can be a helpful means to manage the IR site. The support team can post new information on the IR site and answer questions on IR site best practices, lessening some of the burden on the IRO, especially during high pressure times like earnings. For those IROs that use an IR team for their site maintenance, the team should have a solid foundation to ensure they have the knowledge and ability to publish content properly.

A great IR Support team should have the following attributes:

IR Industry Knowledge: the team should grasp the significance of the varied IR communications and disclosures that an IRO may want to share on their website, ensuring that embargoed information is kept confidential, and postings are made in a scrupulous and timely manner.

Proactive Culture: the team's culture should place an emphasis on periodically sharing suggestions for website improvements with the IRO, keeping the site looking and functioning at its best.

Organized Task Creation Process: the team should have a solid process in place for following through on requests for updates, ensuring that no request or question goes unattended. This could take a number of forms, including a well-communicated procedure outlining the behind-the-scenes steps for execution, or an automated task creation system that generates a support ticket for each request received.


SNL IR Support Request Received -- 2/11/2014

IR_Response 11:46 AM (2 minutes ago)

to me

SNL

Thank you for contacting IR Support. We have received your email and will begin looking into this issue shortly. One of our IR website support analysts will contact you shortly to follow up. If you require immediate assistance you can call our IR website support line at 866 802 9128.

For information regarding our 24/7 worldwide support coverage, please click here.

Once again, we appreciate your feedback.

-SNL IR Support

Redundancy: the team should be staffed in multiple locations so that if a disaster occurs at the site of one office, critical workflow can seamlessly transition to team members at another location. Documents and procedures outlining how to perform certain updates should always be available across all members of the IR team to facilitate any requisite transitions.

Content Update Procedures

Preparing important IR site updates at the last minute is naturally going to increase the risk of mistakes. Even with the support of a great IR team, effective communication and sufficient preparation are critical to successful content disclosure. Taking the time to set up a few simple processes can go a long way toward ensuring that disclosures are made correctly and on time.

Effective update processes should have the following attributes:

Recurring Event Procedure: a set procedure should be developed in conjunction with the IR team for recurring events like earnings, or conference presentations, so that all parties involved know what to expect and can prepare ahead of time.

Advanced Written Notice: emails requesting an update should be sent with significant advance notice, allowing time to prepare and ask questions for clarity if necessary. Any associated materials should be provided later, after they are finalized, but simply having the description of the requisite changes in advance makes it much easier to prepare for a time-sensitive update. A few hours of notice are good, but a few days are even better!

Finalized Documents: when possible, only the final version of a document should be provided to the IR team or the individual in charge of posting it on the site. This reduces the possibility of confusing similar looking versions of the same document. For situations in which a document has been shared in multiple versions, it is best to explain what has changed in the final version so that before posting, it can be verified as the correct version.

Appropriate Document File Names: documents should be saved with an appropriate file name like ABC_Company_Conference_Presentation.pdf before being emailed to the IR team or uploaded on the IR site. Savvy web crawlers can discern the saved document file name information even after it is uploaded on the website, which could accidentally give away more information than intended, so the name needs to be chosen with care.

Contingency Plan

If faced with the unlikely event of a catastrophe cutting off communication to external vendors, it's a good idea to ensure that any important IR site updates which normally rely on the presence of those vendors could still be made by the IRO or internal IR team. Constructing a contingency plan and performing a stress test to analyze that plan in a mock situation is a great way to review the ability to update basic information on the IR site without the aid of external vendors, in case the need does arise.

These are the key aspects of a good contingency plan:

Understanding of Content Management System: the internal team should receive basic training on the CMS. This umbrella understanding of the portal enables the flexibility to make a variety of website updates.

Prioritization of Updates: the internal team should know which content on the site is most sensitive, like earnings documents and SEC filings, and should work with the content management system host to ensure this content is set up on the back end in a way that allows for easy future updates. This will help prevent situations where the internal IR team might find themselves unable to add information to the site due to a prohibitively complex update process.

Stress Test: the internal team should coordinate a date and time to do a test and take the steps necessary for each high priority update, while any external vendors that normally are involved are on standby. The test should take place without any real time guidance provided by external vendors, so that key process blockages can be identified and fixed.

IR Website Host Security

From a technical standpoint, it's important to consider the increasing sophistication of hackers and the possibility of server failure, and how the IR site is protected against those risks. The website host, whether the hosting is done in-house or through an external vendor, needs to have the following security measures in place:

Capacity, Redundancy, and Up Time Assurance: the host should have multiple servers in multiple geographic locations to protect the stored data in the event of server failure. This will ensure maximum availability of the website under any conditions.

Physical and Environmental Security Measures: the host's data centers should have protections in place to prevent loss of the stored data in an environmental disaster like fire or flood.

Access Controls: hosting facilities, servers, and content should have access limited to authorized personnel. Clear policies for termination of access should also be in place. Web servers should be on isolated subnet with non-routable IP addresses in a clustered HA configuration.

Attack Prevention and Disaster Recovery Plans: the host's systems including servers, workstations, and networking equipment should be subject to regular security updates, backups, and up-to-date monitoring to protect against malicious code, vulnerability, and intrusion. The host should also have a tested Disaster Recovery Plan that provides adequate timelines for bringing back website content in the event of a disaster.

External Auditing: the host should have all of these controls independently examined and certified on an annual basis.

Social Media Management

While SNL's Institutional Investor IR Survey indicates that social media is not currently a critical factor in company analysis on Wall Street, social media can still be a great way for IR departments to reach a broader audience and better connect with analysts and investors. However, it must be done with care and attention. Information shared on these networks is somewhat immortal: users can instantly re-tweet, share, and take screenshots of posts and tweets, keeping that information accessible even if the original tweet or post is deleted. Deleted posts and tweets can often still be found cached in the network's search engine as well. This means that mistaken posts to social networks are difficult and sometimes impossible to rescind. That's where a good social media strategy comes into play. With proper planning, these kinds of mistakes can be avoided.

Multiple Dissemination Channels: social media should be used simultaneously with traditional dissemination outlets like the IR website, SEC Filings, Press Releases, etc. Since social media has such an informal feel, it can be easy to treat posts lightly. However, if a post refers to information released at the same time via an 8-K or Press Release, it gives more weight to the post and heightens the inclination to vet it and plan its timing.

Social Media Process Management: a solid social media strategy should include adequate resources devoted to continued maintenance: who will post content, how frequently, and what kind of content will be posted? Equally important is a plan for monitoring the buzz in the social sphere. Feedback on the company should be reviewed on a regular basis so that the messaging strategy can be adjusted if needed and the company can be in a better position to quickly squelch any rumors that might start circulating.

Limited Networks: an IR social media strategy should include only as many social networks as there are resources available to manage them. It's better to have one or two active and pertinent social networks then several that are irregular and disorganized.

Social Media Use Disclosure: a public announcement about the company's intended use of social media to communicate material information needs to be made to avoid fair disclosure breaches.

Summary

Website security measures need to be up to date in order for sensitive content to be kept protected. This white paper should help guide IROs to ensure that their IR site and content update processes meet the current security best practices. The main points to keep in mind are that with a secure web host and CMS, as well as organized website editing processes, the majority of the preparation is taken care of. Checking to ensure the various points in this guide are in place will make for smooth management of the IR site and will reduce the risk of potentially damaging mistakes or leaks.