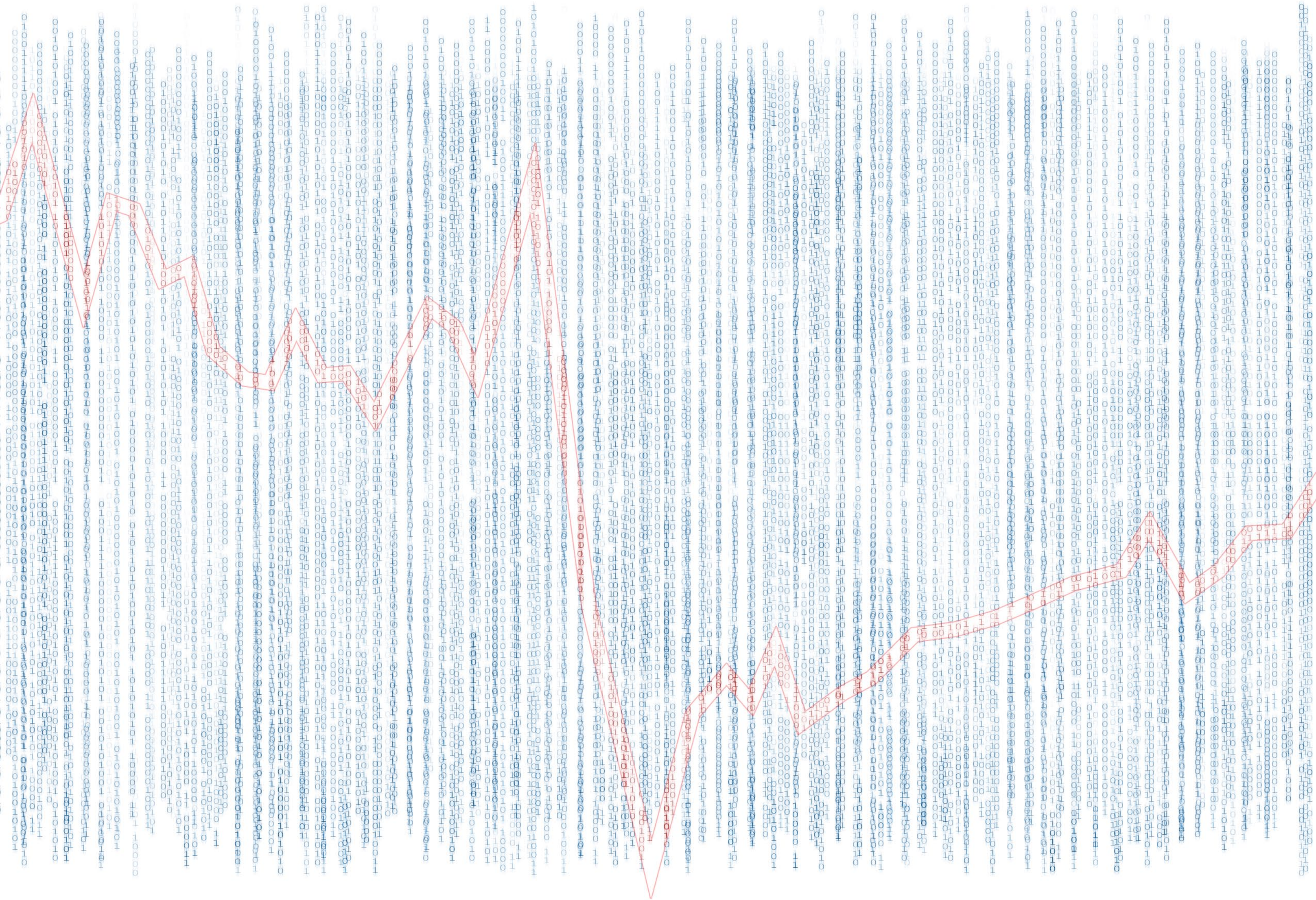
Epic Data Fails: How Companies Can Lose 20% of Their Value in 10 Minutes

A Novaworks white paper about compliance data management and security
September 14, 2015



Novaworks

This white paper examines the security risks that are assumed when a company chooses to outsource the preparation of financial reports for submission to the Securities and Exchange Commission and how a company can mitigate or eliminate those risks. Data security is paramount, and inadvertent data exposure (either due to malicious intent or human error) can cost companies millions of dollars. To eliminate many of the risks that result in data exposure, a company must retain control over its documents and its compliance processes.

Contents

The authors of this white paper have combined over forty years experience with document management and EDGAR.

Scott Theis
President/CEO

David Theis
Vice President, Development

Erin Rybinski
Managing Director

Novaworks, LLC
(585) 424-1700
333 Metro Park, Suite F-500
Rochester, NY 14623

Epic Data Fails

How companies can lose 20% of their value in 10 minutes

One would have to be living in a vacuum to have not read about computer security breaches. On a fairly regular basis, you'll see a news report detailing a hack of a major commercial or government interest. Again and again, the media will cover stories about how personal data was stolen, credit card information was raided, or how a web service was compromised, and how the companies and victims are (or aren't) weathering the storm.

For every story you read, there are more that go unreported. In fact, a recent survey of IT professionals conducted by Lieberman Software Corporation reported that 87% of respondents believed "huge financial hacks" are happening more often than they are reported[1]; 20% of respondents to another survey conducted at the RSA USA 2015 conference reported witnessing the company they worked for hiding or covering up a security breach[2].

While many of these incidents are acts taken up by malicious third parties, there are other data management issues that hit closer to home when it comes to regulatory compliance. Most recently was the early disclosure of earnings information on Twitter's IR web page before the data was actually filed and made available via regular press channels[3]. In another notable case, Google had an 8-K filed and made public prior to complete approval by the company[4].

You would like to feel as though you have control over the information on your computer, particularly when it comes to data as sensitive as your company's financial information. You even want to maintain control over that information throughout its life cycle. Whether you hold that information on a local server, on a cloud computing network, or have third parties managing and formatting it, the big question on everyone's mind is: "Is my data safe?"

It's 10am — Do you know where your data has been?

Let's be honest. Even someone intimately involved with IT and cyber security at your company may not know where your data has been. As the Internet gets larger and encompasses more technologies and devices, so does the network through which your data travels and so do the risks of someone misusing it. While you may think the destination of that e-mail is secure, your data might be passed through portions of the internet (such as a wireless router) that enable third parties to spy on your information.

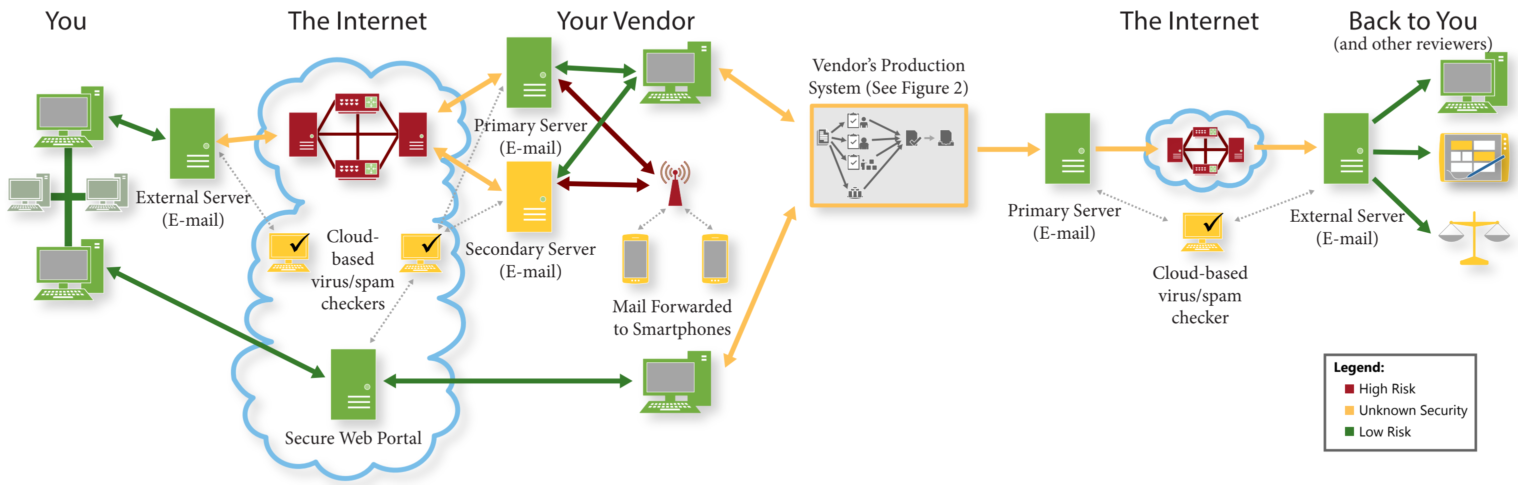


Figure 1. An example of the typical path a document takes when sent to a vendor for EDGAR conversion via e-mail or via web portal upload.

Worse than that, your data may be carried places you never thought of, heard of, or intended.

Perhaps you perform your local work on your secure local area network (LAN). Internally, multiple people at your company collect data, author various parts of your documents, and assemble your company's financial information. At some point, you are ready to send that data to an agent to perform conversion for the eventual filing to the SEC. The transmission to a vendor is likely either via e-mail or perhaps through a secure web portal.

If transmission is via e-mail, you create an e-mail message, attach the file, and press "Send". We like to think that the message is sent directly to the recipient's mailbox. In reality, that is very unlikely. E-mail messages are delivered to a server, and that server decides what to do with the message. The server can send it to another server, deliver it to one of its mailboxes, or copy the message and send the copies to additional servers. A message sent from your computer will typically travel through at least two servers before reaching the inbox of its recipient: your company's outgoing e-mail server (usually a server within your organization or a dedicated/shared third party server) and the recipient's incoming server (which could also be a server within that organization or a shared third party server). The risk of data exposure increases with each server and connection.

If transmission is via a secure web portal, your file can be sent directly and securely to the third party vendor. On the other hand, uploading to a "secure web portal" could be almost as risky as sending that e-mail. Like the e-mail servers, many of these portals will have virus checking, which could use a cloud service or keep backups of your files for unknown lengths of time. The server could be hosted by another party or be a cloud solution. Without your knowledge, your data could be sitting on the Amazon Cloud or Windows Azure platform. The configuration of the web portal could also inadvertently expose your data.

Now that the vendor has your data, let's look a little deeper at the vendor's process (see Figure 2). Once they have your data, it will be placed into the "production stream". Portions may be broken off for work by separate people within the vendor's organization, or your vendor may even outsource your data to additional companies. A perfect example where data is outsourced by a filing agent or financial printer is the creation of the XBRL exhibits for the filing.

The contract staff and subcontracting vendors can be anywhere in the world. Each of their systems is also a potential weak link. The vendor may have a secure portal for their customers, but the steps they take to provide documents to subcontractors might not be as secure. You may not even know if or when your vendor outsources your documents to another party.

At the end of the day, that simple e-mail or upload you thought was going to one recipient could have been forwarded to any number of smartphones, computers or additional parties. Once you click "Send" or

“Upload”, you have no idea where your data is going, who is going to be viewing it, and where in the Internet there are now copies of your data.

File sharing is risky business

Before the Internet, sharing a document usually meant sending it via a courier or the post office. As the Internet became popular, so did sharing files across it. Back when most of us were using dial-up connections, sending files through e-mail or using other methods to send data electronically wasn’t very common because it took a long time and connections were unreliable. High speed Internet changed all of that. Now you can send and receive data in seconds and instantly sync files across multiple computers.

With each method of sharing files, there are considerations. Let’s take a look at the common methods of sharing data and what risks are involved with each.

File Hosting Services

It is easy to share data for filings with services like DropBox, OneDrive, GoogleDocs or any one of hundreds of other services. Having the ability to instantly provide remote workers with up to date data helps to maintain the integrity of that data and makes tracking documents through review cycles much easier. Managers no longer have to make sure one of their team members is working on the most recent version of a document. You might even employ similar file sharing services during the data collection and authoring processes for your financial reports because these services are so convenient and easy to use.

However, they do come with their own inherent risks. Inadvertently overwriting a file is one of them. Unless the service is highly specialized for production work, they usually allow multiple computers to edit the same document. Perhaps you send a document to your vendor, and your vendor turns around and uses a file sharing application to distribute it to their workers. At the last moment, you add a minor change so your vendor quickly puts that file back on the file sharing application. However, one of the workers is doing the lion’s share of the work and still has the document open. He or she completes the work and saves, overwriting the copy with the minor edit. That change is lost and may go unnoticed in review.

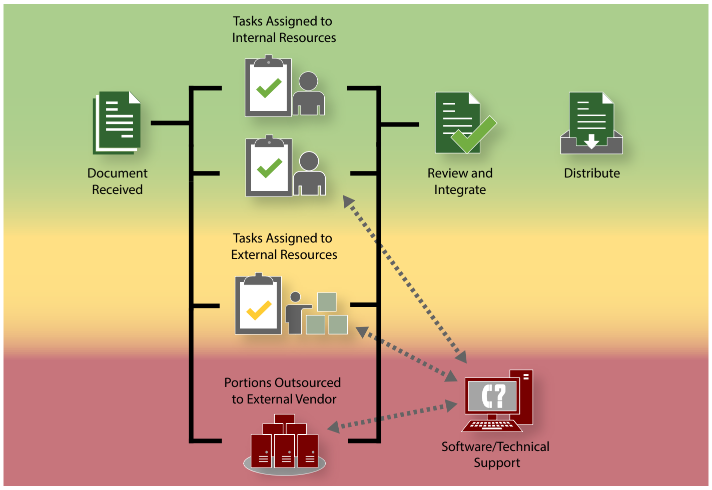

Tasks Assigned to Internal Resources
Document Received
Review and Integrate
Distribute
Tasks Assigned to External Resources
Portions Outsourced to External Vendor
Software/Technical Support

Figure 2. The Vendor Production Stream could utilize unknown entities such as external resources or additional vendors. In addition, documents are often forwarded to software providers in the event of an issue that occurs during any part of the EDGAR preparation process.

While many of these services have published methods of recovering from incidents such as the one described above, the last thing you or your vendor wants to deal with before a deadline is the support desk for a file sharing service.

The convenience of using file sharing services also has led to what many could categorize as an overuse of these services. The ease of placing a document on DropBox for another person to instantly receive it overshadows the risks of using such a service. When you copy a document to a file sharing site, do you ask yourself if you know what sort of security is in place on that remote server? Do you wonder how they handle their back-ups? Do you know how the service provider would handle a security breach: would they report it to their users immediately or, as in the experience of 20% of those respondents at RSA USA, would they attempt to cover it up? Would you know if your data was compromised?

Do you even know where that server to which you just copied your company's earnings release is physically located?

These are difficult questions to ask, possibly because we don't want to think about the answers. Questioning the wisdom of using a file sharing service these days is like questioning the use of smartphones and laptops in the business environment. Both are inherently risky; they place your company's financial data and trade secrets in places out of your immediate control. But, you can take steps internally to make sure your employees have lock codes on their phones and to prevent that one guy from using "12345" for his password. Once you employ a third party service, what controls do you really have?

We'll come back to that later. Let's talk about other places where you may be surprised to find security risks first.

E-mail

Is e-mail secure? That depends on a number of factors and on the answers to a number of questions like: where is your e-mail being served? Where is your recipient's e-mail being served? Is the mail being forwarded to unsecure devices, and where is the forwarded e-mail being stored?

Every time the message is sent – from your computer to a server, from that server to another server, and from that server to the recipient's computer – the transmission can be spied on. Additionally, each server may use a cloud service to check for spam or viruses so your message could be sent to yet another party. Servers may also keep a copy of the message for backup or logging purposes. You are now at the mercy of whoever is running each server, which in some cases may not even be your company or your vendor. To further complicate matters, end recipients may have their e-mail forwarded to a smart phone or multiple computers to allow them to access it remotely. In a matter of minutes your unpublished sensitive financial information could be located on a half dozen or more servers, smartphones, and computers — all of which possess unknown security and integrity.

Then there is auto-complete. This is a neat feature employed and relied upon by most everyone who uses an e-mail client. The auto-complete feature automatically recommends and completes an e-mail address as you enter characters into an address field. We all know how many times a filing goes down to the wire. You're in a hurry so you rely on auto-complete to fill out your address information. You just sent a sensitive document to the wrong party because you didn't notice that auto-complete chose the wrong e-mail address. Many firms disable such features for this very reason.

Software as a Service (SaaS)

SaaS applications are another option that companies use to perform compliance filings. There are tools like GoogleDocs that can be used to author documents, as well as SaaS programs that can prepare EDGAR filings.

SaaS often comes with the illusion of extra security. It's like the old saying: "out of sight, out of mind". The data is on a server out in the cloud, so you don't have to worry about it. Someone supposedly is doing the worrying for you.

SaaS developers earn a living providing these services to businesses, but you can't assume that they have cutting edge security measures in place. When a business hosts data for other businesses, having a reputation for being secure is of the utmost importance, which could mean that they take cyber security seriously. Unfortunately, it could also mean that they might want to keep you in the dark when their security fails.

Another consideration when using any software is how that software will affect your internal security. Software providers strive to make sure their software does not have any exploits that could endanger the computers of their users. In the case of desktop software, you have a certain level of control over what updates you install and when you deploy them, which allows for your internal security team to test for exploits or other problems.

When using SaaS, the software is run or downloaded from a developer's server when you need it. If the server becomes compromised with a virus, that virus can quickly spread to anyone who uses the SaaS application, which makes a SaaS application an enticing target. This is especially true when the SaaS software uses third-party tools like Adobe Flash that are already under the constant scrutiny of hackers.

Additionally, each time you connect to the server, you may be receiving a different version of the software with changes or "hotfixes" implemented silently by a development team, which means that your internal security team has less control over the deployment of the software.

The good news is that there are methods to help you identify risks when using another company's computers or services.

Reducing risk: Service Organization Controls (SOC)

You know about SOC compliance. SOC 1 is concerned with controls in place for financial reporting. SOC 2, on the other hand, might be new to you as it is mainly concerned with technology and cloud computing companies. If you employ a file sharing service or use a SaaS application, then your company has likely demanded to see SOC 2 reports prior to engaging with the vendor. You may or may not have requested SOC 2 compliance from a filing agent or a financial printer, depending on the services they offer.

So you received the report(s) (or you didn't because your vendor doesn't have one), read through what was provided, and someone at your company signed off on engaging with your service organization. But what does that really mean?

When a SOC 2 examination is performed, an auditor is looking for an organization's controls over the Trust Services Principles and Criteria (TSP). The examiner wants to know a) the level of security of the organization's system, b) the availability of the organization's system, c) the processing integrity of the organization's system, d) the level of confidentiality preserved for the information the system processes or maintains for user entities, and e) the level of privacy of personal information that the organization collects, uses, retains, discloses, and disposes of for user entities.

Having that SOC 2 report for a vendor does offer some peace of mind when you are using their services. An independent auditor examined the controls in place, and that report tells you whether anything was lacking. Knowing that your vendor has SOC 2 compliance does mean that you can sleep a little better at night. On the other hand, SOC 2 compliance does not mean that the vendor's software or servers are impervious to a security breach. When something as simple as a stance against hacking can put a target on a company's services[5], you never know when a vendor could come under attack.

The only way to completely eliminate the risk of a malicious user breaching a third party's security measures is to not use a third party service. But is this feasible?

Reducing risk: IT Security Review

Within your organization, you can take steps to make sure if you are sharing files through e-mail and other means that it is reasonably secure. E-mail servers can be configured to only allow secure communications with clients and other servers. This will help prevent e-mails from being read as they are sent from server to server. There are also methods of encrypting the contents of e-mails so only the intended recipient can read the message, regardless of how many other computers receive the data. These security measures must be set up before any messages are sent but it is worth the effort.

Your IT department can also work with your File Hosting Software to verify that it is using secure connections. In fact, your IT department can block the connection if it isn't secure to prevent users from accessing it. IT professionals provide the strongest line of defense against many of the risks of file sharing, but you can only fully control the security of the data while it is in your possession.

Your IT department cannot verify that the recipient of your e-mails isn't forwarding your messages to an unsecure location. Nor can you truly control your document once it is in the hands of another party.

Oops… did I do that?

Using a third party like a filing agent or law firm to create and file your reports can seem like the best answer for EDGAR compliance. If you are confident in the security of your vendor's e-mail servers and the protocols they have in place for file sharing, the experience a filing agent has in preparing documents for EDGAR can be a warm security blanket. They prepare hundreds of filings yearly (or monthly, or even weekly, depending on their size), and they have experience with the SEC and know the stresses of getting the filings submitted at the right time.

Companies try to control and time the flow of information to the public. Not only is timing critical to the performance of the company's stock, control over the flow of information must be performed by law. There is a clear protocol in place for the release of information to the public, but there is also some latitude that allows for companies to ease the blow of bad news or capitalize on the good.

As in comedy, timing is everything. Unfortunately, we're talking about more than just a few laughs.

An inadvertent release of financial data is not only embarrassing; it can be costly to your company, your shareholders, and to your good standing with the SEC. There have been a couple of recent accidents, some quite notable.

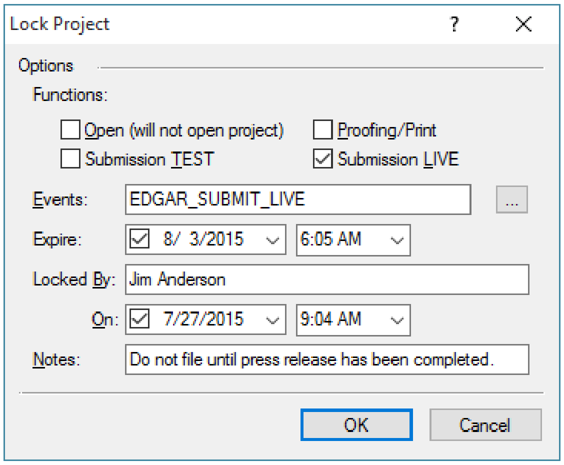
Using a filing agent could seem like the best choice, but it's not the only choice. When you send your data to your agent, do you know what controls they have in place to maintain the integrity of your filing and the timing of your information? What are the filing release protocols internally?

What steps and controls does the vendor have in place? What happens when a worker there makes a mistake and presses "File" before you give your approval?

Is there another way?

Implemented within Novaworks' GoFiler software are controls that allow EDGAR submissions to be locked until certain metrics have been met. These metrics even include time.

For example, the planned earnings press release is 6AM next Tuesday, followed by the release of the 8-K at 6:05AM, and then by an earnings guidance meeting. When the EDGAR project is created within GoFiler, a lock can be established to not allow the submission of the filing to the SEC until after 6:05AM on Tuesday.



Lock Project ? ×

Options

Functions:

□ Open (will not open project) □ Proofing/Print

□ Submission TEST ☑ Submission LIVE

Events: EDGAR_SUBMIT_LIVE ...

Expire: ☑ 8/ 3/2015 6:05 AM

Locked By: Jim Anderson

On: ☑ 7/27/2015 9:04 AM

Notes: Do not file until press release has been completed.

OK Cancel

Figure 3. An example of GoFiler's Lock Project tool, which prevents specified functions from being used until certain metrics are met. Pictured above, a user (Jim Anderson) has locked the EDGAR_SUBMIT_LIVE function, which prevents any user from submitting a Live filing of the project to EDGAR, until a certain time (8/3/2015 at 6:05AM).

This can apply to any form, including effective amendments and other documents that are both market and timing sensitive.

Further, GoFiler has tools to create tasks that control the workflow. Certain tasks can be used to block actions like submission to EDGAR (see Figure 4). Using GoFiler, you can virtually eliminate the "accidental" filing of sensitive information. If you set up GoFiler to interface with your IR website and use it as the portal through which you manage data there, you could also control the timing of that upload.

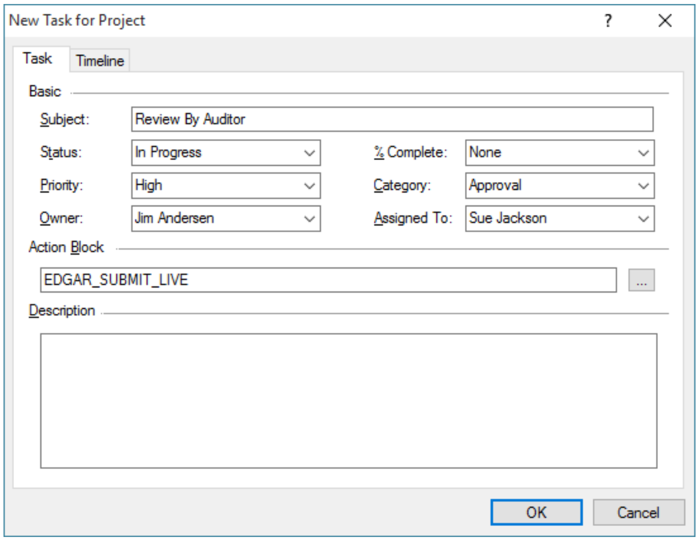
For simple filings such as an 8-K, maybe the question to ask is: why are you not maintaining complete control by editing and filing the document yourself?

Employing the Inside Model

As regulation increases, companies shy farther and farther away from performing their filings in-house. There's a lot at stake, and that idea of having an expert who knows exactly how to deal with EDGAR handle your documents is enticing. In reality, what you are doing is giving up control over your data in order to reduce some filing burden.

This is, in essence, what data security is about: *maintaining control of your data.*

When using a third party provider, you are only in control for as long as the data remains within your company's hands. When using a third party to prepare your financial reports, the protection and security of data must be a top priority, but, in reality, many providers may not have the time, the expertise, or the resources to commit to maintaining a high level of cyber security. As for many of us, pressing "Send" on that e-mail is just something that gets done without putting much thought into the process. Forwarding messages to a smartphone is a matter of convenience, not security.



New Task for Project

Subject: Review By Auditor

Status: In Progress

% Complete: None

Priority: High

Category: Approval

Owner: Jim Andersen

Assigned To: Sue Jackson

Action Block: EDGAR_SUBMIT_LIVE

Figure 4. GoFiler's Task management dialog allows for the creation of tasks to help manage the filing process and a project's workflow. Pictured above, a task has been created to review the project prior to submission. Because this is a critical task that must be performed before the filing is submitted to EDGAR, the Action Block option is being used to prevent the EDGAR_SUBMIT_LIVE function. Until the assignee has completed the task using GoFiler's collaboration tools, the project cannot be submitted by any user, preventing the inadvertent filing of data.

Within your own organization, you know where your data is and who has access to that data. This high level of control that you have over your data throughout its life reduces the risk of unwanted exposure. During the authoring process, there are strict protocols in place to prevent information from being seen by certain parties before other metrics have been met. By placing your data in the hands of another entity, whether that entity is a File Hosting Service, a third party preparer, or a SaaS application, you are giving up that control to varying degrees.

Completing your filings inside your organization minimizes all the risks outlined above. You decide how files are shared within your organization, whether it is via a Local Area Network (LAN), a Virtual Private Network (VPN), or a File Hosting Service. You can limit how your company's employees retrieve e-mail data on smartphones, or deploy company phones that allow remote content wiping and lockouts. You can control which employees can access SaaS applications and set restrictions on what types of data employees can put out on a third party servers. And, you can identify risks involved with File Hosting and SaaS servers.

You control each security decision so you control all of the risks.

If your company could take on the production process for your EDGAR filings, you would eliminate any unknown variable from your compliance workflow. Being able to identify the potential weak links in the document chain would increase your data security significantly. The best method to eliminate many of the risks associated with file sharing and using a third party service is to employ an in-house software solution.

In-house software is installed on a computer within your organization. That computer could be a network location or an employee's machine, but any computer contained on your company's private network enjoys the security measures your network has in place. Software like Novaworks' GoFiler Corporate solution only communicates with outside servers during four processes: the installation/registration process, the uninstall/deregistration process, the update process (to install new versions of the software), and the *Submit to EDGAR* processes. At all other times, the software does not require any communication with outside servers. Further, until you decide to submit your documents to the SEC, your data will always remain protected on your internal network.

Using technical support services from a software vendor is another facet of data management, and you may not be aware that a vendor will send sensitive documents via e-mail to a software support team when one of their workers encounters an issue during the EDGARization process. There are other options for technical support than sending an e-mail, but vendors will often use e-mail because it is easiest and because they are looking for a quick fix for a problem. Once a document is in the hands of the software provider, the technical support representative can perform corrections directly to the file as needed before returning it to the agent.

By employing an inside model, you can also eliminate this hidden risk. For very sensitive documents, the Novaworks technical support team can provide help remotely without the need for you to e-mail any files. Other options for obtaining technical support include using remote services to demonstrate functions, transferring a file directly using a secure protocol, or just the tried and true method of talking you through a problem on a call and working with you until that problem is resolved.

Everyone is concerned about cyber security, but many of us don't realize that there are simple things we can do to prevent security breaches. It's not only about IT professionals and cyber security experts tracking down attackers and preventing data loss. Moving to an inside model to prepare and submit financial reports to the SEC can eliminate a great deal of needless risk, provide maximum control, and keep your data secure. ❖

What You Can Do To Increase Your Data Security

- Talk to your vendors and ask specific questions about your data and the flow of data.
- Ask for SOC 2 reports for any cloud computing, file sharing, or SaaS applications your company uses.
- Work with your IT department to ensure that any File Hosting Software and e-mail servers your company uses block unsecure connections.
- Use internal measures to create and submit critical filings to the SEC. You can perform simple filings (like 8-Ks) that are time-critical without taking on the full burden of preparing all of your EDGAR filings as a means of getting your feet wet and familiarizing yourself and your team with the EDGAR filing process.

About Novaworks

Novaworks is a leading provider of EDGAR conversion and filing software. The company's suite of products includes solutions for a wide range of SEC filers, with each application tailored specifically to provide a wide spectrum of clients with the tools they need. Members of the Novaworks team have been involved with the operational EDGAR System since its implementation in 1993 and were part of the design process, which started in 1984, providing our company and customers with expert experience regarding the workings of the EDGAR System and EDGAR document management. Security and data control have always been an important factor during Novaworks' software development processes and continue to be a driving force for the design choices made during the on-going development of the GoFiler software family.

Endnotes

1. "2015 Professional IT Survey", Lieberman Software Company, May 2015, retrieved from http://www.liebsoft.com/IT-Professional-Survey/.
2. Malik, Javvad, "Ethics, Security and Getting the Job Done", AlienVault, 2015.
3. Simmons, Dan, "How One Tweet Wiped $8bn Off Twitter's Value", BBC.com, 29 April 2015, retrieved from http://www.bbc.com/news/technology-32511932.
4. Ryan, Vincent, "Google's Big 'Oops' Moment", CFO.com, 18 October 2012, retrieved from http://ww2.cfo.com/capital-markets/2012/10/googles-big-oops-moment/.
5. Kain, Eric, "Daybreak Games Hit By Lizard Squad After CEO Threatens Hacker, Surprising Absolutely No One", Forbes.com, 10 July 2015, retrieved from http://www.forbes.com/sites/erikkain/2015/07/10/daybreak-games-hit-by-lizard-squad-after-ceo-threatens-hacker-surprising-absolutely-nobody/.