SpectorSoft

Six Obvious Threats to Data Security You Haven't Really Addressed

1.888.598.2788 | www.spectorsoft.com

Six Obvious Threats to Data Security You Haven't Really Addressed

There isn't a day that goes by that the phrases *data breach*, *data theft*, *employee theft*, *insider threat*, *employee fraud,* or *corporate espionage* aren't seen in the news.

There are mediums you allow everyday access to that can be used to raise productivity and meet business objectives, but can just as easily be used to take data out of the business.

In this whitepaper, we'll discuss 3 local and 3 online methods employees have used to steal data, look at what you can do to stop data theft via these mediums and what the reality is when it comes to expectations.

Let's start with one of the most obvious mediums and work through to some of the less obvious.

Removable Storage

USB Devices and (less used these days) writeable CD and DVD drives have long been a common storage and transfer medium.

The Threat

Unauthorized copying of data to these mediums is an easy task – easier in the case of USB drives, but still simple enough in both cases. In July of this year a USB drive (which was within a briefcase) was stolen from the home of an employee of the Oregon Health & Science University that contained over 14,000 records. In this story, the employee wasn't stealing the data, but do note how easy it was for patient information to leave the confines of the employer without their knowledge.

In cases where malicious intent is at play, devices like the one shown in Figure 1 demonstrate how easy it would be, in even the most secure environments, to take data out of the workplace.

Figure 1: An 8GB USB "Watch"

How Do You Lock It Down?

- **Make these devices read-only** – since the issue is theft of data, allowing access to read USB drives and CDs/DVDs may be reasonable. This can be done in Windows via Group Policy. Do keep in mind that both of these mediums can harbor malicious code used to install keyloggers and the like in an effort to gain access to your network.
- **Disable, when appropriate** – if access to these devices is not necessary for a given employee's job, they should be disabled.

The Reality

These are the "lowest hanging fruit" for data leakage – they require the least amount of effort and technical "know-how" to copy data to and should be treated as such. If you are serious about protecting your business, these devices should be the very first to be locked down. If you haven't locked these down already, data is leaving faster than you know.

Printers

There's an old story about a construction company made aware of an employee stealing from the company, so they asked security to check every employee on the way out. Every evening when Joe would walk up to the gate with his wheelbarrow full of his personal tools and lunch box, security would check it and let him pass. Every day this same routine continued… until they realized Joe was stealing wheelbarrows.

Printed documents are the "wheelbarrow" of the modern-day business. Companies spend tens, if not hundreds, of thousands of dollars annually securing data, applications, the network, USB drives, CD burners, and more, only to be brought down by their Achilles heel - the Print command.

The Threat

Printing is a natural part of just about any application, which makes it one of the easiest ways for data to be pulled out of an application. So what's to keep someone from printing copies of customer records? You have the print function disabled in your CRM app, you say? OK, then how about we just copy and paste data into Word or Excel and print from there then?

I sat with a former CTO of one of the largest hospitals in the US and his biggest concern was a single keystroke – Print Screen – when used while in a medical records application. With that one key, data was leaking out of the organization, leaving the hospital outside the well-defined walls of HIPAA compliance.

How Do You Lock It Down?

There are a few things you can do to make printing more secure.

- **Secure Printer Access** – Most every networking platform has the ability to establish security around printing, limiting who can print, times of day, etc.
- **Enable Print Auditing** – Windows supports building an audit log of print jobs so you can have a record that something was printed.
- **Disable the Print Screen Key** – In Windows, it is possible to disable the key with a registry entry.

The Reality

Even when you lock down printers, users with access to sensitive data and a printer can still utilize printers to move data out of the organization. Add to that the fact that you have no way to tell exactly *what* was printed either – only, at best, some record that something was printed from a specific application. There are other ways to use printing that the steps above won't address.

- **Printing to a Home Printer** – someone with a laptop while at work can print to the printer queue on their hard drive tied to their home printer and then allow the documents to print once they connect to their home network.
- **Printing to a PDF** – Also someone with a PDF print driver can print right to a PDF, bypassing printing altogether.
- **Printing Directly** – Most printers also support direct connections over the network, thereby bypassing any security put in place.

Wireless & Bluetooth

Every laptop, netbook and ultrabook today has wireless (as do some new desktops). Nearly all of them have support for Bluetooth as well. These two communications mediums facilitate access to devices and networks, enabling people to get their job done.

The Threat

As long as the employee is connected to the company wireless and company-approved devices, data is safe. Once off the corporate network or connected to an unapproved device via Bluetooth, data can be easily stolen. So a few scenarios exist:

- **Off the Corporate Wireless** – When the employee is at work and subject to IT's filtered and secured environment, it's a lot easier to feel like data can't be stolen. But if employees are allowed to connect to alternate networks (including their home network), they have free reign on where they can go and what they can do.
- **Copying via Bluetooth** – This is one of the most overlooked mediums from a security perspective. An employee can connect their Bluetooth smartphone (complete with local storage) to a laptop, copy data, and delete the Bluetooth connection with no remains that the connection ever existed. Given the maximum range of Bluetooth is 100 meters, it's also conceivable for someone to connect their laptop to, say, a smartphone *outside* the building, copy the data, and delete the connection.

How Do You Lock It Down?

Much like USB and CD-Burners, there are two options:

- **Restrict Changes to the Configuration** – Restricting the ability to add new connections and only allowing access via approved mediums limits the risk of data loss through wireless or Bluetooth. Windows has mechanisms (such as Group Policy settings) to centrally deploy out restrictive settings.
- **Disable, when appropriate** – If Bluetooth isn't needed, it can be disabled. If you're going to disable wireless.

The Reality

The number of companies that have Wireless locked down so that an employee can't connect to their home network is few and far between, leaving wireless as a major gap in security. Bluetooth remains probably the least secured medium, but it does require some know-how to get working.

Webmail

There isn't an email platform or ISP today that doesn't have a web-based email client, so you can't limit your thinking to Gmail and Yahoo. Webmail is a powerful easily accessible sharing medium that allows data to be attached and transmitted quickly.

The Threat

The obvious one is attaching sensitive files to an email. There was a recent story about an employee that attached 8 Excel files to a webmail-based email and sent them to himself and another "freemail" domain account. Just like that, the data was gone.

Another great example of data being shared via webmail is the recent Petraeus scandal, in which General Petraeus used a tactic employed by terrorists to send communications without leaving a trail by placing unsent messages in the Drafts folder and having the intended recipient log into the same webmail account to read the "draft" message and compose a "reply" of their own, also left in the Drafts folder. Now, in the case of General Petraeus, it appears to have been emails of a romantic nature, but you can see the implications if more devious intentions were at heart.

One of the other unmentioned threats is that, while any business that has a firewall or web filter can see that someone went to a webmail domain, many webmail clients use session encryption so you have no idea what was composed, attached or sent out of the business.

How Do You Lock It Down?

This is a tough one. You *can* block every webmail URL you can think of with a web filter, but that's not going to be very effective, as you're going to undoubtedly miss more than a few.

The Reality

Unless you block every ISP in the world, you're not going to be able to block webmail entirely.

Cloud-based File Sharing

With a multitude of web 2.0 tools available, a young workforce that is very web savvy, matched with an IT department that often cannot keep up with the demands of their users, employees are often times turning to solving their own problems by utilizing services they can find on the web for free. Cloud-based file sharing is no exception, with the rapid growth in use of services such as Google Drive, Dropbox, JungleDisk and Box. These services have become a staple in businesses and are leaving gaping holes in your security strategy.

The Threat

A recent news story demonstrates the security risk these services provide:

> The general manager of Zynga's successful online game *Cityville* copied a number of company assets related to the game, along with a backup of his email to a Dropbox account from his company computer, just prior to leaving the company, He then went to work for a competitor *Kixeye.*

Now put your company in the story and any employee with access to customer records, intellectual property, sales data, financials - basically any sensitive company data – and you begin to see the danger.

A recent survey about use of cloud-based services revealed a shocking statistic – according to cloud cost-management services provider *Cloudability* the average number of cloud accounts an employee has is **2.5**. That's 2.5 services your IT department knows nothing about, 2.5 accounts they no control over and 2.5 security holes – *per employee*.

How Do You Lock It Down?

There are two options here. Both of which are somewhat extreme:

- **Block Cloud-based file sharing** – It can be done rather easily, in most cases, by blocking the servers and website. But it seems to be counterintuitive when you consider why an employee chose to use such a service in the first place. The employee obviously wants an easy-to-use solution to copy files to make them available for sharing. So be careful – you may successfully block the more commonly used services (like Google Drive or Dropbox), but miss some of the lesser well-known services that work just as well (such as Minus and SugarSync).
- **Limit use and have IT manage** – some providers such as *Syncplicity* and *Huddle* do have corporate accounts with business-specific features, but the challenge is how does IT keep track of three key aspects to any cloud-based services:
    - **Authorization** – Who should have access?
    - **Authentication** – Are the intended employees the only ones using it?
    - **Usage** –Is it being used for approved purposes only?

The Reality

These are reactive tactics. Much like the TSA requiring passengers at U.S. airports to take off their shoes because of the now infamous "shoe bomber", blocking the file sharing cloud providers only blocks or controls access to the sites you are aware of. If you're serious about blocking Cloud-based file sharing, you need to be serious about just about any site on the web where data can be uploaded and stored.

Social Media

With this one, don't just focus on Twitter and Facebook, but instead think about the many forms of sharing social media takes on with a wide variety of services available to share information with others. Figure 2 shows an example list of providers of a range of services in the social media space.

Figure 2: A sample list of Social Media services

The good news about this list (from a data security standpoint) is that some of these companies are no longer in business. The bad news is that the logos for the now-defunct companies represent many more starting up to take their place.

The Threat

Employees having the ability to store, share and retrieve information without the permission (or knowledge in many cases) increases the risk of data leakage. And don't just think about file sharing as the threat. If an employee can post pictures to a site like Shutterfly, it's entirely possible that they could simply rename a data file to a JPG file and upload it for later retrieval.

On the Facebook/Twitter front, organizations need to be worried about information being inappropriately shared. A tweet of post about a recent development in the company could have adverse implications to the company's reputation, value (if publically traded) or security.

How Do You Lock It Down?

- **Start with Policy** – establish an Internet Acceptable Use Policy that includes a Social Media Policy component to communicate expectations and boundaries to employees.
- **Filter out the major players** – Determine which social media services present the greatest risk and block access to them, as is necessary.

The Reality

This is right there with Webmail – there are too many services out there to block them all and, while necessary, the policy will only do so much to stop someone from doing something inappropriate. In the case where data is intentionally being taken out of the organization, the cold hard truth is blocking a particular set of social media sites will have limited impact.

Coming to Grips with Reality

At no other time in the history of data security has there been so many ways for data to leave an organization. When trying to address these holes in security, you either need to take massively aggressive stances, like basically blocking the entire Internet and not allowing anyone to print anything ever, or you're going to leave yourself exposed.

The reason for needing to take such a radical stance is that you have no *visibility* into how each of these gaps in security is being used (or misused). For example, printing out a report is fine as part of an employee's job, but printing out 50 documents after hours should, at very least, raise some eyebrows.

The problem is that businesses are trying to address these problems by addressing the *mediums*, which isn't the source of the problem. The real source of the problem is the person intending on stealing data – **the employee**. If you're serious about minimizing data leaks in your business, the only logical choice is to monitor employee use of these, and other mediums, to ensure they are properly being used.

Detecting the Threat with User Activity Monitoring

SPECTOR 360 User Activity Monitoring software (UAM) monitors and records every action an employee performs on their work computer – every keystroke, email, IM, web page, application, print job, you name it – complete with screenshots to allow the replaying of activity with Screen Playback. Actions are monitored, discerning the good from the bad, alerting you in real-time to those deemed inappropriate.

With **SPECTOR 360** watching your employee's actions, data leaks that occur across channels where you normally lack visibility (e.g.: encrypted web sessions, printing, and off-network usage) are detectable and are recorded with full detail. All actions are monitored with real-time alerting to ensure you are aware the moment data leaks occur. Actions and data can be reviewed centrally via a dashboard, replaying actions performed before, during and after the activity in question, providing context, evidence and answers.