



## Five Tips that Can Protect Your Company from an Embarrassing Leak of Confidential Information

Uzi Yair, CEO GTB Technologies

*A recent Forrester survey of 305 security and email professionals revealed some scary but realistic statistics:*

- 1 in 3 companies investigated a breach of confidential data last year.
- 1 in 4 companies experienced an “embarrassing” leak of confidential information.
- 1 in 5 emails contains a legal, financial or regulatory risk.

*If you are like most corporations, you are finding yourself in the midst of an information explosion. Sensitive data is no longer controlled under lock and key in datacenters or file cabinets. Sensitive data is everywhere. This article discusses five helpful tips that will change the way you think about your company’s competitive advantage and help you prevent the next data leak that could put your company out of business.*

### **1. Recognize that Your Most Valuable Assets Aren’t Locked in a Safe.**

Whether you are in the banking or transportation industry, your corporation is fueled by the sensitive data. The Brookings Institute estimates that 80% of a company’s intellectual property is no longer represented as tangible consumer products, but as intangible, digital assets like:

- Research and development data (source code, drug formulas, and engineering diagrams).
- Customer private data (credit card numbers, social security numbers, and bank account data)
- Marketing strategies
- Sales forecasting data
- Client lists
- Merger and acquisition plans
- Research and analyst reports
- Spreadsheets and tables that calculate valuable business data

In today’s global economy, this data is transferred across the enterprise, between departments, partners, contractors and overseas outsourcers. That means your sensitive data – worth hundreds of millions of dollars – is everywhere. This valuable data is no longer controlled under lock and key in a datacenter or in file cabinets. This data is stored on laptops, file servers, databases, workstations and USB drives. This information explosion is changing the way corporations must now view and protect their assets and instead of investing in old network security technologies like firewalls, companies are investing in Data Loss Prevention (DLP) technologies that will keep “tabs” on where sensitive data is going, who is using it, where it is being saved and whether or not it is being protected or used appropriately.



## **2. Realize Laptops Are Valuable Safes with the Easiest Locks to Crack.**

Most of us think of our laptop as a productivity tool. They offer convenience and accessibility allowing us to get our job done from anywhere with the ability to communicate with anyone. But thieves see this productivity tool as a treasure trove of coveted information. If you live in an urban area you know – thieves go to great lengths to break into cars and homes to steal computers granting them access to the valuable information stored there.

Why should enterprises care? Because chances are, the majority of your competitive advantage has been created, copied or stored on your employees' laptops. Do you know what sensitive information has been stored on individual's laptops? Of the employees who had their laptops stolen today, would you know if they had sensitive information like client lists or customer private data stored on their laptop?

More frequently than ever, laptops are being targeted by crooks looking to make their next quick buck. The assets stored are a treasure trove of identity information, customer bank account information, client lists and confidential data that may never be recovered. Know what files contain sensitive data – particularly your customers' private data – and know if they are stored or copied to laptops. Once they are on the laptop, expect this information to turn up missing. Look for DLP vendors who are capable of taking an inventory of the data stored on laptops, monitor what data is being copied from the laptop to storage devices like memory sticks and be able to protect valuable information stored there.

## **3. Beware of the Spreadsheet.**

When valuable assets are stored on laptops and work stations, it is likely they take the form of a spreadsheet. Spreadsheets have become the ad hoc business tool of choice for a variety of mission-critical activities from crunching your company's financials to storing customer lists. When we see spreadsheets sent outside of the protective walls of a corporation, we often see credit card and social security data. Often, we do not see just one or two accounts; we see thousands (sometimes tens of thousands) of names and numbers. If these spreadsheets have not been properly protected, tracked or monitored it is conceivable to lose as many as 50,000 customer names, credit card numbers, bank account data and social security numbers, unknowingly in one file. Wouldn't you like to know what is in the spreadsheets your employees are sharing with third-party processors, contractors, vendors and overseas partners, and if they are in compliance with data protection regulations?

Because over 159,550,898 records have been stolen to date, the data privacy rules are quite clear. Any information leaving the company with two forms of personally identifiable information (PII) must be encrypted. While it is important to protect all PII, we usually see mass abuses contained in spreadsheets and particularly by good employees who were sending these spreadsheets through their Hotmail or Yahoo personal accounts to crunch data from home after dinner. DLP technology can be programmed to look for confidential data or sensitive PII and take action to protect your enterprise by blocking, quarantining, redacting, or encrypting the data, ensuring compliance with data protection standards.

## **4. Bear in Mind Rules Were Made to Be Broken.**

1 in 5 emails contain a legal, financial or compliance concern. When it comes to employees and protecting your sensitive data, think of this as an example of the Pareto principle -aka "the 80/20 rule" - at work. It is estimated that 80% of security breaches come from 20% of your employees who:



1. Are knowingly breaking compliance rules to get their job done, close an important deal or meet a critical deadline
2. Are unaware they were breaking a compliance rule
3. Don't care about compliance rules

Remember the old adage, "Rules are made to be broken?" Employees are going to break a rule now and then. Expect your data protection and compliance rules to be broken. In addition, while employees should be forgiven for trying to do their jobs, close deals and meet deadlines, it is entirely unacceptable to leave the business exposed to the damage caused when compliance rules are ignored. Luckily, this is one area where DLP technology can help tremendously. Whether or not your employees are going to do the "right thing" or completely disregard your compliance rules, DLP technology working behind the scenes can now spot sensitive data as it is about to be compromised or leaked and enforce data protection standards. This means you can avoid ruffling employees' feathers and still protect the business.

#### **5. Remember, Everyone Makes Mistakes... Really Bad, Embarrassing Mistakes.**

Ever fat-fingered an email and hit send to the wrong recipient? Ever hit the send button on an email and wish you hadn't? Ever email the wrong attachment? Or worse, send confidential information about your customer to their competitor? Unfortunately, this happens all the time and often it costs your company a client, a new customer or worse creates legal nightmares and brand damage.

When employees unintentionally break data protection compliance rules to get their job done, the reality is, they are like the rest of us who, on occasion, make mistakes – really bad, embarrassing mistakes. With new DLP technology it is possible to save the business from these types of blunders. It is possible to set policies that block messages from ever going to competitor or quarantine emails that could be questionable and ask the sender if they really meant to send it.

#### **Data Loss Prevention Is Right around the Corner.**

Protecting sensitive data is not a "nice to have" feature – it is a critical need. While new data protection strategies are necessary, they must go hand-in-hand with the right technology. Companies are now protecting data by identifying what is sensitive and building enforcement policies with DLP products capable of controlling where data should and shouldn't go as well as how it should travel – should it be allowed to travel through Yahoo!, MSN or copied to a CD? If so, encrypt sensitive private data within the document to be in accordance with data protection regulations. With DLP technology, companies have many options to protect data on the move. The new approach to achieving balance is through a combination of DLP technology, the new data protection enforcement policies, and with continued employee awareness and training.

New data protection strategies are necessary and 100% accurate protection from data leakage is the goal. Companies turning to DLP products to protect their sensitive data should look for the following features:

- Real-time performance
- Virtually zero false-positive rates
- Policy enforcement actions with the ability to encrypt, redact, block, and quarantine sensitive data and ultimately protect your business.

In this day and age, it is impossible to expect your employees to be fully cognizant and ready to comply with all data protection compliance rules. Look for a DLP technology that can



protect sensitive data without slowing down your business or frustrating employees trying to do their job. With the right solution, you can meet data protection compliance guidelines by encrypting, redacting, blocking, or quarantining sensitive data before it damages your business. An added bonus for your investment - the technology is often cheaper than employees' training!

