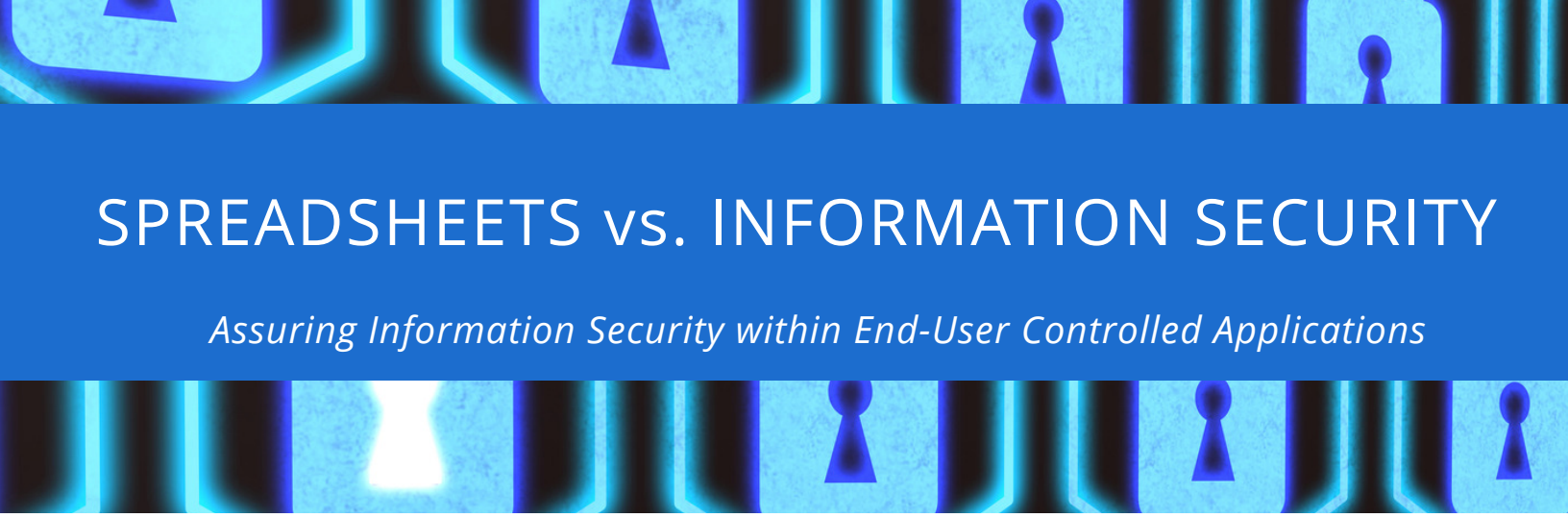
CIMCON Software | Reducing End-User Computing Risk™

# SPREADSHEETS *vs.* INFORMATION SECURITY

*Assuring Information Security within End-User Controlled Applications*

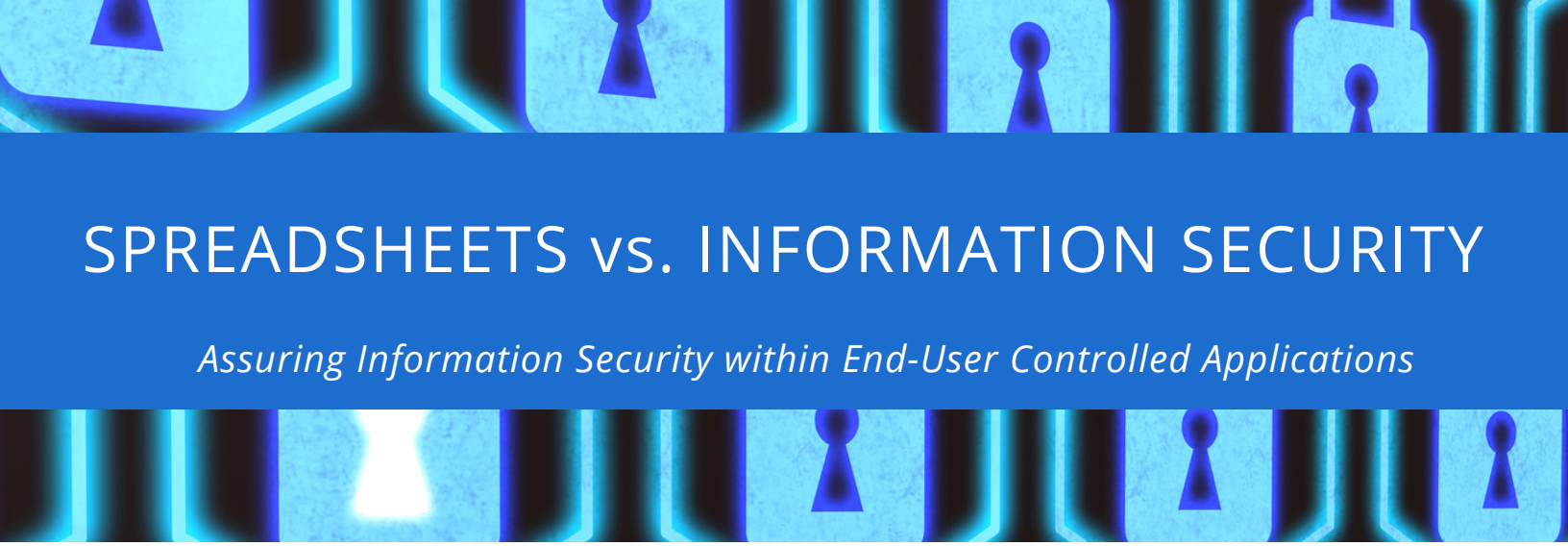
*"IT emphasis has historically been on perimeter defenses such as bigger and better firewalls, antivirus, malware detection technology, and Data Loss Prevention (DLP) tools. However, emphasis on defensive technology alone does not constitute a complete solution."*



# SPREADSHEETS vs. INFORMATION SECURITY

*Assuring Information Security within End-User Controlled Applications*

## Table of Contents



# SPREADSHEETS vs. INFORMATION SECURITY

*Assuring Information Security within End-User Controlled Applications*

## Executive Summary

Hackers, criminals, or even nation states may (and eventually probably will) find a way into your company's networks. In addition, the insider threat, both unintentional and malicious, is omnipresent. Companies that have developed a strong information security/risk management framework are at the best possible advantage to reduce the potential for loss. Including EUCs as part of this enterprise information security architecture is critically important as many of the most significant and damaging data breaches and loss incidents have involved EUCs (especially spreadsheets). Companies need to know which files contain sensitive and business-critical data, where they are located and have an appropriate GRC framework in place. Even though the problem may seem too big to address, companies can protect the information contained within spreadsheets and other EUCs and thus minimize the potential damage to their business.

# Challenges

## *Cyber Risks Have Exploded*

Necessity has made cybersecurity and information security a top concern for both senior management and security professionals alike. Fighting an array of dynamic threats can be challenging. Traditional cyber security tools including firewalls, antivirus, and intrusion detection systems are simply not as effective as they once were because hackers (sometimes state-sponsored) have become more sophisticated and determined in their methods to get around them. Add in the sheer number of devices on which information is shared and stored (desktops, laptops, PDAs, tablets and mobile phones) and the possibilities for attack are seemingly endless.

## *Perimeter Defenses are not Enough*

IT emphasis has historically been on perimeter defenses such as bigger and better firewalls, antivirus, malware detection technology, and Data Loss Prevention (DLP) tools. However, the emphasis on defensive technology cannot provide a complete solution for 3 key reasons:

1. Once defensive systems are bypassed (as they often are) sensitive data is exposed and vulnerable
2. Early detection isn't guaranteed
3. A "wall" doesn't address insider threats – unauthorized access of spreadsheet-based information assets is common

*"IT emphasis has historically been on perimeter defenses such as bigger and better firewalls, antivirus, malware detection technology, and Data Loss Prevention (DLP) tools. However, the emphasis on defensive technology alone does not constitute a complete solution."*

One of the softest targets is end-user controlled (EUC) files that are unstructured and may contain sensitive information such as PII or PHI. Regardless of whether it's in the form of a database or a spreadsheet, such data breaches are extremely costly. New regulations such as the General Data Protection Regulation in Europe amplify those costs. Others like the New York state DFS's regulations on cybersecurity place "SOX-like" personal liability on senior executives. Given the magnitude of the downside, the attack surface for EUCs should be minimized and made an integral part of information security planning.

## *The High Cost of Data Breach*

There is no getting around the huge financial losses associated with data breach. According to Ponemon Institute's 2016 Global Cost of Data Breach study, the average expense of remediating the loss of sensitive corporate or customer information is approximately $4 million and in high profile situations in the tens of millions. A stolen spreadsheet with a list of 10,000 records could cost $1.7 million, with lost health care information costing even more to fix. Add in other related costs such as regulatory fines and damage to reputation and the total financial loss could be much higher.

The majority of these costs are associated with resolving the incident as organizations must pay compliance fines and court fees, invest in forensic and investigation processes, and expend revenue on identity theft prevention services for customers or employees. Additionally, Ponemon's report noted that turnover of consumers directly[1] impacts business costs. From then on out, these organizations must spend more on customer acquisition as the reputational losses associated with a data breach last a long time.

*"A stolen spreadsheet with 10,000 records can cost a company $1.7 million."*

## *Real Life Examples*

There are countless incidents of cyberattacks in the news, many relating to EUCs; however, some of the more recent stories show just how widespread and damaging these incidents can be:

- The 2014 theft of files from Sony by hackers included spreadsheets with sensitive information including salaries of employees and top executives. Not only did the breach have significant legal and financial costs, but the release of this information was also a huge public relations issue and had a material impact on their business. Years after the event, images of these spreadsheets are still on the internet. The company also took a $15 million charge in its Q1, 2015 earnings as a result of this incident. The total direct and consequential damages have been estimated by some industry experts to exceed one hundred million.[1]

- A major data breach occurred at British internet company TalkTalk. In October 2015 it is estimated that attackers accessed over 150,000 individuals' personal information. This resulted in financial losses of £60 million, a loss of 100,000 customers[2] and a regulatory fine of £400,000.

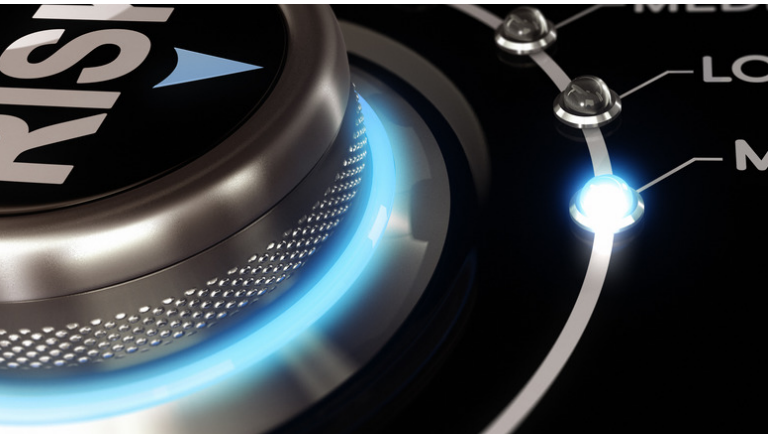
- In July of 2016, it was revealed that hackers accessed spreadsheets maintained by the Democratic National Committee which contained the personal information including names, phone numbers, physical and email addresses, and contribution amounts from thousands of high-profile donors. Again, that information was stored in spreadsheets.[3]

There are many lessons that can be learned from these past breaches but perhaps the most important one is how cost-effective it actually is to proactively mitigate these risks before a breach occurs. As Warren Buffet once said, "an ounce of prevention is worth a pound of cure is understated… and a delayed pound of cure will need a ton of cure".

*"Some of the more costly and widely publicized hacking events have been the loss of sensitive information contained in spreadsheets & other end-user controlled files"*

## *The Pervasiveness of End-User Computing (EUC) Risk*

End-User Computing (EUC) includes many applications and file types (and it has many alternative acronyms including EUCA, EUDA etc.). The defining characteristic is that these files or applications are not controlled by IT and thus don't have many of the protections and controls that exist on enterprise applications. On average, there are 3,000 of these EUC files for every employee. While the scale is vast, the subset of business-critical files is not and thus the issue is totally manageable.



Excel spreadsheets are arguably the most widely used tool for analysis, reporting, and other computational tasks. These models, tools, and spreadsheets often play a critical role in financial reporting processes across all industries. Given their ubiquity, ease of use and flexibility, spreadsheets are also used to list and manipulate sensitive data. These EUCs are highly vulnerable to data loss since they are rarely monitored or controlled. In the parlance of information security professionals, the "attack surface" is huge. End users do not consistently apply best practice password discipline and Active Directory controls have their limitations.

While sensitive information (PII, PHI and perhaps even PCI) can be present in these unstructured EUC files, those files are, by definition, not managed by IT so rarely do they fall under a proactively managed data governance policy. As has been mentioned previously, some of the more costly and widely publicized hacking events have been the loss of sensitive information contained in spreadsheets and other end-user controlled files.

Given their ubiquity and the fact they can contain information that is both proprietary and/or regulated, spreadsheets and other EUCs must be an important consideration when developing a comprehensive information security strategy. Every company is paying attention to cyber and information security but not all are recognizing the related risks inherent in EUCs.

Experts recommend information security policies or standards centered on those end-user controlled assets that are valuable i.e. there is high impact of their loss. Rather than attempting to secure everything, focus on the sensitive assets because it's impossible to cover all of the assets all the time.

In the case of EUCs, the sheer number of files (often tens if not hundreds of millions) precludes encrypting it all. Systematic methods and tools to identify these files and do an automated risk ranking are available. With this quantitative information (which can be augmented with user-supplied qualitative information), the prioritization of which files should have an added layer of protection can begin.

# Soutions

## *Developing a Comprehensive EUC Information Security Strategy*

First and foremost, companies need to accept that their information systems will at some point almost certainly be compromised.[4] With this in mind, it is important to develop a comprehensive information security strategy that can withstand the inevitable breach. EUCs need to be an integral part of that security architecture though all too frequently they are completely ignored because they don't fall directly under IT control.

## *Involve All*

Experts unanimously agree that information security is not just a C-level or an IT responsibility. It must be integrated into the standard three lines of defense in any Enterprise Risk Management (ERM) framework:

1. Front-line employees who must follow a systematic process and apply internal controls to minimize EUC risk that they own.

2. Enterprise compliance and risk functions that provide independent oversight of the risk management activities of the first line of defense.

3. Internal and external auditors (and the compliance team where applicable) who report independently to enterprises' stakeholders on risk management effectiveness.

Everyone must play a role and this usually means changes to how people work. The second line of defense is important in developing policies and procedures; however, it is the line of business employees who carry out the day to day activities and must own the risk.

As time has proven, people are often the weakest link in cyber defense. For example, an employee can click on a phishing email thus facilitating a ransomware attack or can innocently copy sensitive information into a spreadsheet which exacerbates risk. Every week there is a news story of a spreadsheet that was willingly emailed outside of an organization and the employee didn't realize that sensitive data was hidden therein.

## *Foster a Cultural Shift*

A top-down, cross-functional approach is considered best practice to the point it's almost a cliche. Nonetheless developing an "information security awareness culture" is imperative.[5] One should not overlook the more obvious, known vulnerabilities nor the fact that physical facility security is very much linked to cybersecurity. There are many variants to cyber threats and they include physical access to sensitive areas or information.

> *"Security threats can include everything from suspicious emails sent to employees, especially employees in sensitive positions, to a breach in human resources' and financial data management systems, to advanced persistent threats and unauthorized access, to non-public intellectual property and sensitive client data." – "Cybersecurity – addressing rising expectations", Ernst & Young*[3]

## *Perform On-Going Risk Assessments*

Once you have developed your strategy, ongoing risk assessments are necessary to ensure continued awareness and success. These risk assessments should include "the type, sensitivity, and location of their data and systems in order to assess the impact of internal and external threats and vulnerabilities."[6] Wherever possible these assessments should be automated to improve their effectiveness. The strategy should encompass methods for monitoring data being shared outside of a company (e.g. DLP) whether by employees or by third parties.

## *A GRC Framework for EUCs*

Given that EUCs may contain some of your company's most sensitive and/or regulated data, adding EUC controls to a company's Governance, Risk and Compliance (GRC) framework is increasingly warranted. If these controls are already in certain departments for regulatory reasons, they can be extended to other groups and do "double duty" in helping reduce information risk. EUC risk management technology provides the capabilities to identify these operational, information security risks associated with EUCs and ultimately implement controls as necessary.

The benefits of specifically including EUCs within an information security policy include:

- Reduced probability of data loss and the resulting financial and reputational damage
- Ability to detect and reduce the number of EUCs that contain sensitive information
- Having an actionable, quantitative assessment of the departmental or enterprise risk associated with EUCs
- Reduced vulnerability to internal threats, malicious tampering or theft by disgruntled employees

CIMCON Software | Reducing End-User Computing Risk™

**EUC Risk Assessment**

Determine which files need to be protected

**Remediation**

Use EUC scanning technology to find keywords, hidden cells & remove from files

**Controls**

Determine risk exposure by performing automated risk assessments of each EUC

**Automated Monitoring**

Ensure all spreadsheets and high-risk EUCs have automated controls to ensure integrity

**Respond & Recover**

Continually monitor edits to highest risk EUCs, including smart alerts on critical changes

## *EUC Risk Assessment*

It is necessary to quantitatively assess the information risk associated with EUCs so that your organization can define the strategy to mitigate them.

The first step is to determine which files would be most damaging in the event of breach or data loss. Accordingly, it is necessary to identify those files that may contain sensitive data. This detection/ identification can be done in multiple ways; keyword searching, data characteristics, and self-identification. For example, keywords might be text such as 'Password' or 'Account Number'. Characteristics might be patterns that indicate sensitive information such as a credit card (PCI) or social security number.

It is also critically important to understand how EUCs are connected to each other and to enterprise databases. To the extent that an EUC contains sensitive information that mandates further protection, if one understands the data flows they can better assess the true information risk and the steps needed to better protect the information.

Given the magnitude of the EUC landscape in most organizations, the only practical and cost-effective way to comprehensively identify sensitive files, data flows and linkages is to use an automated scanning tool. There are many commercially available EUC discovery tools specifically built to do just this. In addition to automatically scanning your EUC domain, these tools can visually map data flows as well.

## *Remediation*

Once files containing sensitive information have been identified, end users must find the exact location of keywords, hidden cells/sheets and take steps to remove them from the EUC. Most EUC scanning technology includes diagnostic tools that enable this. This diagnostic tool technology can also be used proactively by the line of business, as part of an everyday work practice to periodically check EUCs to ensure that these risks don't enter into the EUC landscape in the first place.

Last but not least, the proper remediation action might just be deletion. If a file/application is inactive and no longer used (which is easily identifiable) then perhaps the easiest remediation step is to simply delete the file. If the file doesn't exist it can't be compromised or stolen.

## *Controls*

EUC files that contain sensitive information (and are approved to contain sensitive information) should have additional security. Modern software tools provide multiple ways to add incremental layers of information security. Using one's home as an analogy, in addition to having a lock on the front door, each bedroom can now have a lock. Automated EUC controls can enhance normal file access permissions so that companies can better protect critical files, have more granular control of file privileges, enforce best practice passwords, and more.

In addition, location-based security can be applied so that if a file is moved from its normal file share location it cannot be used. For example, if an important spreadsheet was stolen or inadvertently sent outside of the company that file cannot be opened. Given that so many data loss incidents involving spreadsheets are inadvertent, and don't involve malicious intent, this safety valve can prevent huge losses.

Another method of EUC control is to protect certain portions of a file so that only authorized users can edit the sections they are approved to edit. Implementing capabilities for the locking of cell ranges, formulas, pivot tables, sheets, and macros at an individual user or group level is smart. This segregation of access can help ensure that inexperienced users do not inadvertently make changes that would compromise data integrity and that malicious attempts (internal or external) to alter a file are blocked.

Last, consider automated workflow capabilities around file change governance so that all edits and modifications must be approved before the file can be used. A key approval criteria should be to scan for sensitive information within the file, especially data tabs that may be hidden to the casual user. During the approval process, only the approver has access to the file so that any sensitive information is not available to other users.

## *Automated Monitoring*

EUC files that have been approved to contain sensitive or confidential information should be systematically monitored 24/7 so that an audit trail of all changes is maintained. One critical dimension of the audit trail is tracking copies of sensitive files. Automated controls can prevent non-approved copies from being used or can be set to track copy behavior so that all files with sensitive information continue to be inventoried and monitored. Anytime sensitive information is entered into a monitored EUC, alerts can be automatically generated.

Another critical audit trail capability is tracking the adding/modifying/removal of file level passwords. If a user attempts to edit a password of a controlled file in a way that it is no longer in compliance with a company's information security policy, that behavior is tracked and email alerts can be sent to the appropriate managers.

Apart from addressing the information security risks specific to EUCs, it is always good practice to monitor business-critical EUCs. These are the EUCs for which an error would cause a significant financial loss and/or have a negative impact on customers and ultimately the company's brand. A software-enabled audit trail of these critical files can also be automatically maintained with no adverse performance impact or burden on the end user.

### *Respond & Recover*

In the aftermath of a successful attack or other data loss event, companies must enter into the disaster recovery phase to ensure business continuity. Endpoint and data back-up is an area of expertise unto itself. However, if that infrastructure is not in place, EUC management technology can assist in disaster recovery. As part of standard monitoring operations, typically the last version of a controlled model/spreadsheet is maintained by the EUC management application. If stolen, or ransomware is present and/or the file is otherwise corrupted, the repository has a "clean" copy of the file that can be immediately put back into use. Having this resiliency in this business-critical subset of your company's vast end-user computing domain is equally important as it is for the IT managed systems.

## Conclusion

Information security that focuses primarily on keeping hackers out is destined to fail because, with the increasing volume and sophistication of attacks, it must be assumed that some will be able to penetrate the many walls. In addition, no matter how big a wall you build, it does nothing to protect you from the information security risks you face as a result of ill intent or accident by those already on the inside. The high cost of data loss suggests that in addition to defensive systems, you also have security systems in place to further protect sensitive data. Given that sensitive data almost always resides within an organization's portfolio of End User Computing (EUC) applications and files, your cyber and information security strategy needs to address that reality. Last, there are software tools available that can help you comprehensively address these risks in a timely and cost-effective way.

For more information, please visit us at cimcon.com.

CIMCON Software | Reducing End-User Computing Risk™

**CIMCON Software, LLC**

Headquarters:
Westford, MA

United Kingdom:
London

## References


1. The Ponemon Institute, LLC, “2016 Cost of Data Breach Study: Global Analysis”, June 2016 [Online]. Available http://www-03.ibm.com/security/data-breach/

2. Silverman, Rachel Emma & Fritz, Ben, “Data breach sets off upheaval at Sony pictures”, December 4, 2014. [Online]. Available: http://www.wsj.com/articles/data-breach-sets- off-upheaval-at-sony-pictures-1417657799

3. www.theguardian.com, February 2, 2016 ; October 5, 2016. [Online].

4. Bissell, Kelly C. & Raduege, Harry Lt. General, USAF (Ret.) Deloitte and Touche LLP, “CFO Insights Cybersecurity: Five Essential truths” 2014. [Online]. Available http:// www2.deloitte.com/content/dam/Deloitte/us/Documents/ finance-transformation/us_cfo cfoi_cybersecurity.pdf

5. Fish, Alan; Kahan, Jaime; Mitti, Ralph; Tsantes, Chip; EY Ernst & Young LLP, “Cybersecurity – addressing rising expectations” October 2015. [Online]. Available “http://www. ey.com/Publication/vwLUAssets/ey-cybersecurity-address- ing-rising-expectations/$FILE/ey-cybersecurity-address- ing-rising-expectations.pdf

6. Maurer, Roy “KPMG: Five Most Common Cybersecurity Mistakes”, May 9, 2015 [Online]. Available http://www. shrm.org/hrdisciplines/safetysecurity/articles/pages/kp- mg-common-cybersecurity-mistakes.aspx