**CIS 5600: Information Security Management**

Lab 2: Security Cyber Awareness, Cryptography, and Risk Management

Bernice Templeman

**Document:**

Part 1:

* Install GPG4Win, review the documentation, examples, and perhaps check out some YouTube videos that describe how to use GPG4Win.
* Create a public key and send to me (class instructor) via email at least 3 days before the submission is due. Once I have your public key, I will email your team my public key and an encrypted message that you must decrypt using GPG4Win and public keys.
* Copy and paste my unencrypted message into your lab submission.
* Write a 1-2 page (single-spaced) summary describing your lessons learned about cryptography and use of the GPG4Win tool.

**<Unencrypted message goes here…>**

**<1-2 paged summary goes here…>**

**The lessons I learned about cryptography and the use of the GPG4Win tool include that**

***cryptography is part of Cybersecurity and*** is important to us because *with the growing volume and sophistication of cyber attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security. .[1]*

*In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important homeland security mission.* [2]

*Cybercrime will cost the global economy $445 billion in 2016 — more than the market cap of ExxonMobil ($360 billion), Facebook ($368 billion) and Amazon ($397 billion), according to an estimate from the World Economic Forum's 2016 Global Risks Report.*

*The best way to fight this cyberwar is to get back to basics, like knowing how many computers a company has and gaining control over them in seconds.*[3]

One of the basic methods is Cryptography. Cryptography has been around since the ancient Greeks and Romans sent secret messages. [8] Julius Caesar used the “Caesar’s cipher” encryption technique. The Germans used the Enigma machine in World War II. Today, there are many encryption algorithms.

Cryptography is a science that applies complex mathematics and logic to design strong encryption methods. Achieving strong encryption, the hiding of data’s meaning, also requires intuitive leaps that allow creative application of known or new methods. So cryptography is also an art. [4]

*“Encryption is the most effective way to achieve data security. To read an encrypted file, ypu must have access to a secret key or passwors that enables you to decrypt it. Unencrypted data is called plain text.encrypted data is referred to as cipher text*.” www.webopedia.com/term/e/encryption

*Open standards are made available to the general public.They are developed and approved and maintained by a collaborative and consensus driven process. Thet facilitate interoperability and data exchangeamong different products or services and are intended for widespread adoption. www.itu.int/en/ITU-T/ipr/...*

Open standards help ensure **cryptography** is secure. Symmetric encryption is a method of encryption involving the same key for both encryption and decryption. Public key encryption, which is not symmetric, is an encryption method that is widely used because of the enhanced security associated with its use. [5]

Gpg4win (GNU Privacy Guard for Windows) is encryption software for files and emails.

Gpg4win enables users to securely transport emails and files with the help of encryption and digital signatures. Encryption protects the contents against an unwanted party reading it. Digital signatures make sure that it was not modified and comes from a specific sender.

Gpg4win supports both relevant cryptography standards, **OpenPGP** and **S/MIME (X.509)**, and is the official GnuPG distribution for Windows. It is maintained by the developers of GnuPG. Gpg4win and the software included with Gpg4win are [Free Software](http://fsfe.org/about/basics/freesoftware.en.html) (Open Source; among other things free of charge for all commercial and non-commercial purposes). [6]

This short study was put together parallel to the product "Gpg4win"[1](https://www.gpg4win.org/ShortStudy-Sustainable-FS-example-Gpg4win.html" \l "sdfootnote1sym).

Gpg4win is an installation package for Microsoft Windows which contains numerous help programs and extensive German documentation besides the actual encryption application "GnuPG". The objective of this project is to improve the usability of the encryption software GnuPG and to therefore facilitate the use and operation of cryptography for laymen computer users. For this purpose, in addition to the simple installation of the software, the integration of the command line tool GnuPG into graphics user interfaces such as "Outlook 2003" and "Sylpheed Claws" is also promoted.

In this way Gpg4win intends to replace the outdated GnuPP[2](https://www.gpg4win.org/ShortStudy-Sustainable-FS-example-Gpg4win.html" \l "sdfootnote2sym), which has not been updated for a while. It is hoped that such a standstill situation can be avoided for Gpg4win. The objective of this short study is to discuss the corresponding measures.

Version 1.0 of Gpg4win has updated the software. This short study suggests a strategy of how a self-sustaining project can develop. The goal is to facilitate a more sustained further development of Gpg4win.

Starting point for the short study are the general success factors for Free Software projects, as well as the problems regarding an sustainable further development of GnuPP, Windows Privacy Tools [3](https://www.gpg4win.org/ShortStudy-Sustainable-FS-example-Gpg4win.html" \l "sdfootnote3sym) and comparable approaches.

While this study is concerned with Gpg4win, more general conclusions may also be drawn, especially for products which are the result of a bigger project and are targeted towards Microsoft Windows as the basic operating system.

In the end, this study intends to highlight the issues. even though there are a number of additional aspects that are also worthy of examination but could not be mentioned or discussed. As a result this short study is meant as a starting point and motivating factor for thinking about the kind of questions which need to be asked regarding the sustained existence of Free Software products [7]

Since Gpg4win is security software, which in part requires knowledge of fairly sophisticated concepts, the circle of potential contributors is therefore limited. Alone the writing of good documentation material usually requires in-depth security knowledge. Also, in order to ensure consistent trust in the software, a corresponding quality management process is meaningful. This is not usually a fun task for most volunteers.[7]

[1] <http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm>

[2] <https://www.dhs.gov/cybersecurity-overview>

[3] <http://www.cnbc.com/2016/10/10/cybersecurity-industry-has-failed-the-market-ceo.html>

**[4]** [**http://resources.infosecinstitute.com/role-of-cryptography/**](http://resources.infosecinstitute.com/role-of-cryptography/)

[5] Mar 29, 2016

### [Cyber Security and Cryptography - Computing Concepts](http://computing-concepts.cs.uri.edu/index.php/Cyber_Security_and_Cryptography)

computing-concepts.cs.uri.edu/index.php/**Cyber\_Security**\_and\_**Cryptography**

**[6]** [**https://www.gpg4win.org/about.html**](https://www.gpg4win.org/about.html)

**[7] gpg4win study**

**[8] How to Geek: What is Encryption and how does it work?**

Part 2:

* Review the U.S. Government’s GAO Risk Assessment Report and Risk Management Case Studies Report.
* **Choose a case study in the second report and write a 2-3 page (single-spaced) summary of your review.** Describe the issues and risks identified, the assessment, impacts, and lessons learned.
* Go to the following Microsoft link: “[Microsoft Security Assessment Tool](http://www.microsoft.com/en-us/download/details.aspx?id=12273)”
* Download this program and install it on your computer. Use some simple cases to carry out a business risk profile assessment. Describe your assessment in a 1 page summary (you may include screen shots, challenges, lessons learned, etc.)

**<2-3 paged summary of reports go here…>**

Choose a case study in the second report and write a 2-3 page (single-spaced) summary of your review. Describe the

* **issues and risks identified,**

The risk assessments are associated with three types of activity—

(1) development of new computer systems,

(2) procurement of production systems from other vendors, or

(3) improvement of legacy system security features —and, generally, are limited in scope to a primary business process and supporting systems.

The supporting systems include the software, databases, and the hardware and network techno logy supporting the software, as well as the people who use and rely on these resources. Business unit

managers are responsible for executing the risk assessments associated with their unit's computer -based operations, and such responsibilities are generally documented in their performance expectations.

* **the assessment**

Although all elements of the risk management cycle are important, risk assessments

provide the foundation for other elements of the cycle. In particular, risk assessments provide a basis for establishing appropriate policies and selecting cost-effective

techniques to implement these policies. Since risks and threats change over time, it is important that organizations periodically reassess risks and reconsider the

appropriateness and effectiveness of the policies and controls they have selected

## Basic Elements of the Risk Assessment Process

Risk assessments, whether they pertain to information security or other types of risk, are a means of providing decision makers with information needed to understand factors that can negatively influence operations and outcomes and make informed judgments

concerning the extent of actions needed to reduce risk. For example, bank officials have conducted risk assessments to manage the risk of default associated with their loan

portfolios, and nuclear power plant engineers have conducted such assessments to manage risks to public health and safety. As reliance on computer systems and

electronic data has grown, information security risk has joined the array of risks that governments and businesses must manage. Regardless of the types of risk being

considered, all risk assessments generally include the following elements.

* + Identifying threats that could harm and, thus, adversely affect critical operations and assets. Threats include such things as intruders, criminals, disgruntled employees, terrorists, and natural disasters.
  + Estimating the likelihood that such threats will materialize based on historical information and judgment of knowledgeable individuals.
  + Identifying and ranking the value, sensitivity, and criticality of the operations and

asset s that could be affected should a threat materialize in order to determine which operations and asset s are the most import ant.

* + Estimating, for the most critical and sensitive assets and operations, the potential losses or damage that could occur if a threat materializes, including recovery costs.
  + Identifying cost-effective actions to mitigate or reduce the risk. These actions can include implementing new organizational policies and procedures as well as technical or physical controls.
  + Documenting the results and developing an action plan.

There are various models and methods for assessing risk, and the extent of an analysis and the resources expended can vary depending on the scope of the assessment and the availability of reliable data on risk factors. In addition, the availability of data can affect the extent to which risk assessment results can be reliably quantified. A quantitative

approach generally estimates the monetary cost of risk and risk reduction techniques based on

(1) the likelihood that a damaging event will occur,

(2) the costs of potential losses, and

(3) the costs of mitigating actions that could be taken. When reliable data on likelihood and costs are not available, a qualitative approach can be taken by defining risk in more subjective and genera l terms such as high, medium, and low. In this regard, qualitative assessments depend more on the expertise, experience, and judgment of

those conducting the assessment. It is also possible to use a combination of quantitative and qualitative methods.

## Challenges Associated With Assessing Information Security Risks

Reliably assessing information security risks can be more difficult than assessing other types of risks, because the data on the likelihood and costs associated with information security risk factors are often more limited and because risk factors are constantly

changing. For example,

* + data are limited on risk factors, such as the likelihood of a sophisticated hacker attack and the costs of damage, loss, or disrupt ion caused by events that exploit security weaknesses;
  + some costs, such as loss of customer confidence or disclosure of sensitive information, are inherently difficult to quantify;
  + although the cost of the hardware and software needed to strengthen controls may be known, it is often not possible to precisely estimate the related indirect costs,

such as the possible loss of productivity that may result when new controls are implemented; and

* even if precise information were available, it would soon be out of date due to fast- paced changes in techno logy and factors such as improvements in tools available to would-be intruders.

This lack of reliable and current data often precludes precise determinations of which information security risks are the most significant and comparisons of which controls are the most cost-effective. Because of these limitations, it is important that organizations identify and employ methods that efficiently achieve the benefits of risk assessment while avoiding costly attempts to develop seemingly precise results that are of questionable reliability.

To assist agencies in meeting this challenge and to supplement our May 1998 guide on information security management, we studied the practices of four organizations that had institutionalized practical risk assessment methods. We identified these

organizations based on recommendations from government and private sector sources. These sources recommended over 30 private and public sector organizations that were know n to have strong security programs or be actively pursuing improved risk

assessment practices. The four organizations included a multinational oil company, a financial services company, a regulatory organization, and a computer hardware and

software company. This guide describes the factors that these organizations considered critical to the success of their risk assessment processes and the benefits they cited as a result of these practices. In addition, it provides a description of the procedures they followed and examples of the tools they used to facilitate the process.

The organizations we selected had chosen risk assessment methods and developed tools that were relatively simple and, for the most part, qualitative in nature. However, one

organization used a combination of qualitative and quantitative methods. In some cases, agencies may find that it is more appropriate to use more detailed, quantitative methods to assess the risks associated with certain aspects of their computerized operations.

However, incorporating the critical success factors that we identified is likely to make any type of methodology more effective. Appendix II contains a more detailed

description of the scope of our study and the methodology we used.

* **impacts**

## Reporting and Ensuring That Agreed Upon Actions Are Taken

A series of standardized reports are produced from the risk assessment process, including a detailed risk analysis report, a report describing the application's current level of conformance to requirements, and recommendations for specific security engineering design review. One of the key reports graphically shows, for each major application, the deviation between the current controls and the controls suggested by the company’s information security policy. In addition, the reports estimate the costs for each recommended countermeasure, including costs for licenses, training, development, implementation, and recurring support.

The business unit head considers the information in these reports when deciding what new controls to implement. If the business unit head believes that certain recommendations are not cost-effective, he or she can discuss the concerns with the company’s information security managers and negotiate alternative actions.

Because business and information technology managers are being held accountable for making information security improvements, the organization has developed a number of management tools to assist them. There are over 12 management reports used to gauge the organization’s progress in achieving established information security goals. In addition, the organization has instituted audit and measurement procedures to ensure the effectiveness of actions taken and that these actions have not adversely affected system operations. Company officials emphasized the importance of managing the changes resulting from the information security risk assessments. They stressed that this requires instituting methods for monitoring the progress being made because changes can be expensive and managers are usually reluctant to implement them— especially when changes could adversely affect their business

* **lessons learned**

## Critical Success Factors

During our study, we identified a set of common critical success factors that were

important to the efficient and effective implementation of the organizations’ information security risk assessment programs. These factors helped ensure that the organizations

benefited fully from the expertise and experience of their senior managers and staff, that risk assessments were conducted efficiently, and that the assessment results led to

appropriate remedial actions. As might be expected, several of these factors are similar to the more genera l information security management practices identified in our May 1998 executive guide.

### Obtain Senior Management Support and Involvement

Senior management support was important to ensure that risk assessments were taken seriously at lower organizational levels, that resources were available to implement the

program, and that assessment findings resulted in implementation of appropriate changes to policies and controls. This support extended to participating in key aspects of the

process, such as

(1) assisting in determining the assessment ’s scope and the participants at the start of a new assessment and

(2) approving the action plan developed to respond to recommendations at the end.

For example, at the oil company we studied, business units were keenly aware of the importance of conducting risk assessments due largely to the expectations of senior executives and the related support they provided. Security was paramount in this organization and failure to comply with organizational risk assessment policy required significant justification on the part of the business owner. Also, senior

managers at the unit being assessed were actively involved in determining the scope of each assessment and in responding to final results and recommendations.

### Designate Focal Points

Groups or individuals had been designated as focal points to oversee and guide the organizations’ risk assessment processes. These focal points facilitated the planning,

performance, and reporting associated with the organizations’ risk assessment programs and helped ensure that organization wide issues were appropriately addressed. All focal points were either located at the corporate level or were members of a corporate -level

committee that coordinated the progress of the risk assessment from an organization wide view point.

D At the oil company, a corporate -level facilitator served as a focal point for

assessments throughout the company, including those pertaining to information

security. Because of familiarity with the tools and the reporting requirements, this experienced individual helped reduce the amount of training required for others involved in the process, such as those responsible for collecting and analyzing data.

D At the financial services company, each business unit had a designated individual responsible for the business unit's risk assessment activities. The facilitators

Generally met weekly as a group to discuss organization-wide risks and lessons learned from prior and ongoing assessments.

D At the computer hardware and software company, a council had been created for the purpose of improving the overall risk assessment process and reviewing the results of risk assessments.

In addition, corporate focal points were involved in developing, disseminating, and

periodically updating risk assessment guidance and often provided training to others.

The use of focal points enhanced the quality and efficiency of the risk assessments. In particular, using focal points to coordinate the planning and performance of the risk

assessments helped ensure that

* tools were used effectively under the direction of an individual who was experienced in using them,
* successful techniques were promptly applied to subsequent assessments,
* terms and methods were applied consistently,
* reports were developed quickly and according to a standardized format, and
* expectations of senior executives were met.

### Define Procedures

Each organization had defined and documented procedures for conducting risk

assessments and developed tools to facilitate and standardize the process. These, along with the use of focal points, helped institutionalize the process, ensure a level of

assessment consistency, and prevent individual business units from “reinventing the

wheel” each time a new assessment was required. To provide flexibility, business units generally could supplement or alter procedures when needed. These modifications were often shared with other units in an effort to promote the use of best practices.

Defined procedures generally specified

* who was responsible for initiating and conducting risk assessments,
* who was to participate,
* what step s were to be followed,
* how disagreements were to be resolved,
* what approvals were needed,
* how assessments were to be documented,
* how documentation was to be maintained, and
* to whom report s were to be provided.

### Involve Business and Technical Experts

Drawing on knowledge and expertise from a wide range of sources was viewed as essential to help ensure that all important risk factors were considered. Business

managers generally had the best understanding of the criticality and sensitivity of individual business operations and of the systems and data that supported these

operations. Accordingly, they were usually in the best position to gauge the business impact of system misuse or disrupt ion. Conversely, technical personnel, including

security specialists, brought to the process an understanding of existing system designs and vulnerabilities and of the potential benefits, costs, and performance impacts

associated with new controls being considered. As a result, meetings conduct ed during the risk assessment process usually included a variety of individuals from the business unit with expertise in business operations and processes, security, information resource management, information techno logy, and system operations. Others from outside the business unit might also be included, such as internal auditors and, occasionally,

contractors with specific pertinent expertise.

All the organizations relied almost exclusively on in-house personnel to perform the risk assessment rather than contractors. The computer hardware and software company initially relied on contractors to assist in conducting assessments but eventually

determined that relying on contractors deprived its own personnel of valuable experience in exploring risk.

The oil company had established a special unit to gather information on threats from outside sources, including federal agencies and organizations such as Carnegie Mellon University’s Computer Emergency Response Team Coordination Center. This helped

ensure that the organization fully understood the threat s that might affect its worldwide operations and that risk assessment teams considered this information in their analyses. Similarly, the financial services company required individuals with expertise in specific geographic areas to provide input on pertinent political and economic risk factors.

### Hold Business Units Responsible

Responsibility for initiating and conducting risk assessments, as well as following up on resulting recommendations, lay primarily with the individual business units. Business

units were considered to be in the best position to determine when an assessment was

needed and to ensure that recommendations for risk reduction techniques resulting from the assessment were implemented effectively.

D At the financial services company, the business units annually developed risk

management plans from a variety of information sources, including the results of

prior risk assessments. These plans served as a basis for establishing priorities for performing risk assessments; designating individuals to facilitate, coordinate, and execute risk assessment activities; and determining the tolerable level of risk for a given operation.

D At the computer hardware and software company, business unit managers were responsible for assessing the risks associated with their unit's computer-based operations, and such responsibilities were generally documented in their

performance expectations.

D At the oil company, the business unit was responsible for initiating a risk assessment and approving an assessment execution plan. This plan, initially drafted by a

headquarters -level facilitator, included the assessment scope, list of questions to be addressed during the process , and list of individuals that would participate in the

assessment.

### Limit Scope of Individual Assessments

Rather than conducting one large risk assessment covering all of an entity’s operations at once, the organizations generally conducted a series of narrower assessments on various individual segments of the business. As a result, the scope of each assessment was

limited to a particular business unit, system, or facility, or to a logically related set of operations.

Segmenting operations into logical units generally reduced the size of each assessment, making it more manageable to schedule and perform. In addition, segmenting operations provided organizations a means of ranking units to determine the order in which risk

assessments would be performed and which units might merit more frequent risk assessments.

* A regional office at the regulatory organization decided that, after reviewing its processes, it would do two separate risk assessments —one on its administrative operations and one on its business-related operations. Managers decided to separate the assessments because the two sets of operations relied on different systems and were subject to somewhat different risks.
* At the computer hardware and software company, risk assessment scope was generally focused on each primary business process and its supporting systems, including the software, databases, and the hardware and network technology supporting the software.

To success fully implement this unit-by-unit approach, provisions had to be made for considering shared risks and risks associated with infrastructure systems, such as

electronic mail systems and other shared resources, which supported multiple units of the organization.

* The regulatory organization centrally evaluated the controls associated with its organizationwide electronic mail system and determined that the controls over this system were adequate to support low- and medium-risk applications. Individual units subsequently used this information to determine the extent to which specific business operations should rely on the electronic mail system.
* At the financial services company, a corporate-level group of risk assessment focal points met twice weekly to consider corporatewide risks and approve actions at individual units that might affect the entire organization.

### Document and Maintain Results

Risk assessment results were documented and maintained so that managers could be held account able for the decisions made and a permanent record established. In this

way, risk assessment records were available to serve as the starting point for subsequent risk assessments and as a ready source of useful information for managers new to the

business unit. Documenting the process undertaken also permitted others, such as the internal audit department, to ensure that organizational units were complying with company policy.

All the organizations maintained databases on the results of the assessments. These

results were used as the starting point for subsequent risk assessments and to monitor the status of any open recommendations for mitigating risks identified during the

process. For example, at the financial services company, the documentation created

during a risk assessment was used as the basis for the following year’s risk management plan. At the regulatory organization, an internally developed software program was used to monitor the implementation status of assessment recommendations and to report the status to senior management.

## Tools

All of the organizations we studied had developed tools to facilitate the conduct of their risk assessments, such as tables, questionnaires, and standard report formats. These

tools helped ensure a consistent and standardized approach throughout the organization and prevented teams from “reinventing the wheel” each time a new assessment was initiated.

Such tools had been developed in-house or adapted from those used by others, and most had been computerized to speed the documentation process and to provide easy access to data and risk assessment results. Generally, the corporate offices responsible for

overseeing risk assessment activities periodically refined the tools as experience was gained and best practices were identified.

Most of these tools were relatively simple aids to assessment and reporting, although one organization had automated the majority of its analysis process.

* The oil company used a table, in the form of a matrix, that facilitated analysis of information security risks to its operations and served as an effective tool for

communicating risk assessment results to management. The matrix showed the combined effects of the probability of an undesirable event occurring and the

severity of damage or loss to key organizational assets or operations if the event were to occur.

* The financial services company used a questionnaire to document compliance or

noncom with company control objectives and the specific control techniques employed. The questionnaire was organized by specific control objectives, such as

authentication, access control, confidentiality, availability, audit, and administration.

* The computer hardware and software company had developed relatively more

sophisticated tools, including a detailed software program that had been designed to draw on large amount s of data on risk factors and automatically analyze input from the risk assessment team.

Tools used by the organizations we studied are described and illustrated in the case study descriptions included in this guide.

## Benefits

The organizations in our study told us that institutionalizing a practical risk assessment program was important to supporting their business activities and provided several

benefits. First, and perhaps most importantly, risk assessment programs helped ensure that the greatest risks to business operations were identified and addressed on a

continuing basis. Such programs helped ensure that the expertise and best judgments of their personnel were tapped to develop reasonable steps for preventing or mitigating

situations that could interfere with accomplishing the organization’s mission.

Second, risk assessments helped personnel throughout the organization better

understand risks to business operations; avoid risky practices, such as disclosing passwords or other sensitive information; and be alert for suspicious events. This

understanding grew, in part, from improved communication between business managers, system support staff, and security specialists.

Further, risk assessments provided a mechanism for reaching a consensus on which risks were the greatest and what steps were appropriate for mitigating them. The

processes used encouraged discuss ion and generally required that disagreements be

resolved. This, in turn, made it more likely that business managers would understand the need for agreed upon controls, feel that the controls were aligned with the unit’s

business goals, and support their effective implementation. Officials at one organization told us that controls selected in this manner were much more likely to be effectively

adopted than controls that had been imposed by personnel outside of the business unit.

Finally, a formal risk assessment program provided an efficient means for

communicating assessment findings and recommended actions to business unit

managers as well as to senior corporate officials. Standard report formats and the periodic nature of the assessments provided organizations a means of readily

understanding reported information and comparing results among units over time.

**<1 paged summary of tool assessment goes here…>**

The Microsoft Security Assessment Tool (MSAT) is a risk-assessment application designed to provide information and recommendations about best practices for security within an information technology (IT) infrastructure.

e Microsoft Security Assessment Tool 4.0 is the revised version of the original Microsoft Security Risk Self-Assessment Tool (MSRSAT), released in 2004 and the Microsoft Security Assessment Tool 2.0 released in 2006. Security issues have evolved since 2004 so additional questions and answers were needed to ensure you had a comprehensive toolset to become more aware of the evolving security threat landscape that could impact your organization.  
  
The tool employs a holistic approach to measuring your security posture by covering topics across people, process, and technology. Findings are coupled with prescriptive guidance and recommended mitigation efforts, including links to more information for additional industry guidance. These resources may assist you in keeping you aware of specific tools and methods that can help change the security posture of your IT environment.  
  
There are two assessments that define the Microsoft Security Assessment Tool:

* + Business Risk Profile Assessment
  + Defense in Depth Assessment (UPDATED)

The questions identified in the survey portion of the tool and the associated answers are derived from commonly accepted best practices around security, both general and specific. The questions and the recommendations that the tool offers are based on standards such as ISO 17799 and NIST-800.x, as well as recommendations and prescriptive guidance from Microsoft’s Trustworthy Computing Group and additional security resources valued in the industry.  
  
After completing an Assessment, you will gain access to a detailed report of your results. You may also compare your results with those of your peers (by industry and company size), provided that you upload your results anonymously to the secure MSAT Web server. When you upload your data the application will simultaneously retrieve the most recent data available. To be able to provide this comparative data, we need customers such as you to upload their information. All information is kept strictly confidential and no personally identifiable information whatsoever will be sent. [1]

Tracking down network security problems can be tricky and time-consuming. One tool that can help you identify and resolve security risks is the Microsoft® Security Assessment Tool (MSAT), a free utility that presents an electronic questionnaire in which you describe your security environment. Designed for mid-sized organizations with 50 to 500 computers, the MSAT poses 172 questions organized into different categories, then provides an analysis of your situation and recommendations on how to improve it.

The MSAT begins with a set of queries about your business model, which it uses to create a Business Risk Profile (BRP) that evaluates your security risk compared to others within your industry. The questionnaire typically takes two hours to complete, and you can stop and resume at any point. Here are the categories with sample questions:

Basic Information How many clients and servers are in your organization?

Infrastructure Security Do your employees work remotely? Do external contractors access your network?

Applications Security Does your company develop applications? Does it store sensitive data processed by your applications?

Operations Security Does your corporate network connect to external networks? Does your organization receive data feeds from external parties?

People Security Does your company outsource computer maintenance? Do you let employees download sensitive company data to their workstations?

Environment How many employees are in your organization? Is there high turnover in your IT department?

Next, the MSAT generates an assessment that uses a measurement called a Defense-in-Depth Index (DiDI), which focuses on the security processes you have in place. Using the same categories, typical questions are: does your organization employ firewalls at each location? Do you use custom macros in your Microsoft Office applications? Do your users have administrative rights on their workstations? Do you have a policy for deploying patches and updates to your PCs?

In response to your answers, the MSAT offers three reports. The Summary Report displays a bar graph with the results. A high score in the BRP indicates more risk, while a high score in the DiDI represents more security. As the MSAT points out, while a low BRP and a high DiDI might seem preferable, it's actually more important to examine individual areas. Thus, for each area, the Complete Report indicates whether or not you meet best practices, need improvement, or are severely lacking (see**Figure 1**).

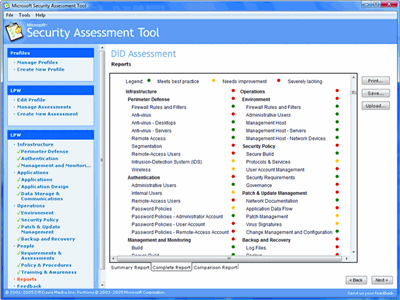


Figure 1**The complete report**(Click the image for a larger view)

Finally, the Comparison Report asks you to upload your results anonymously to a secure MSAT Web site, where you can compare your results with those of other organizations. [2]

**[1]** [**https://www.microsoft.com/en-us/download/details.aspx?id=12273**](https://www.microsoft.com/en-us/download/details.aspx?id=12273)

**[2]** [**https://technet.microsoft.com/en-us/library/2007.12.utilityspotlight.aspx**](https://technet.microsoft.com/en-us/library/2007.12.utilityspotlight.aspx)

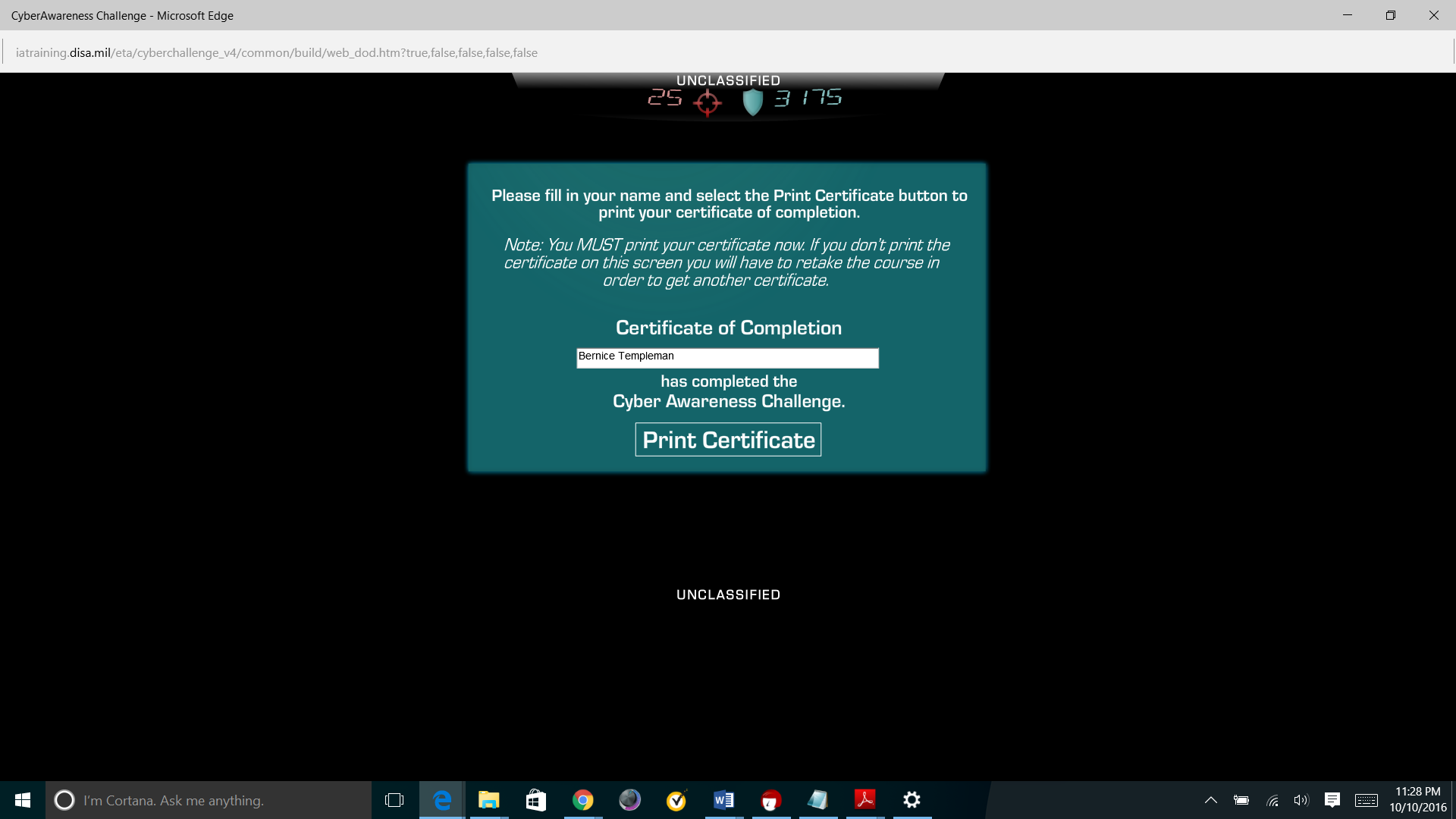
Utility Spotlight The Microsoft Security Assessment Tool

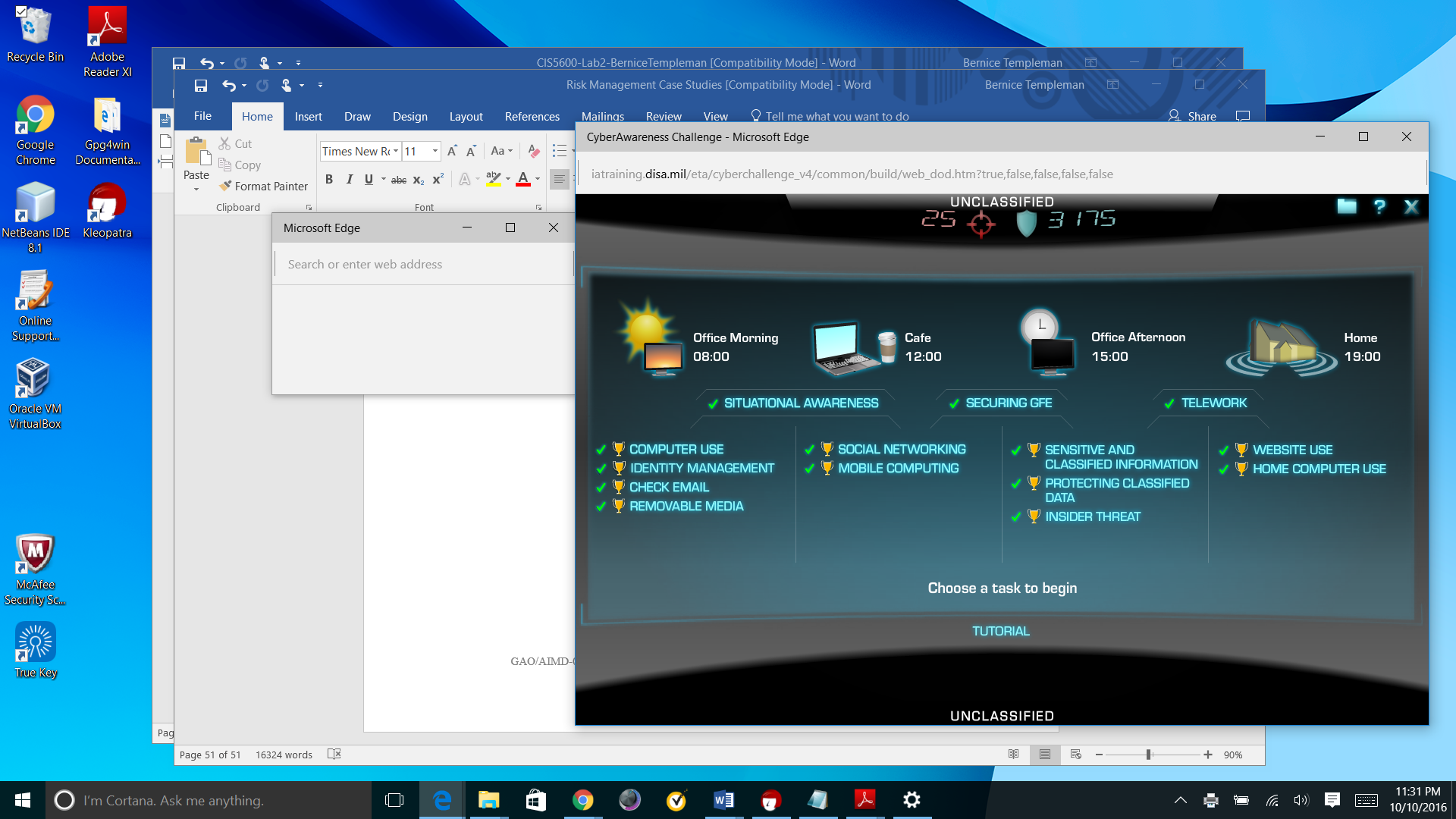
Lance Whitney

Part 3:

* Go to the following U.S. Department of Defense (DoD) Information Systems Agency web link:
  + [**http://iase.disa.mil/eta/Pages/index.aspx**](http://iase.disa.mil/eta/Pages/index.aspx)
* Click on the ***Cyber Awareness Challenge*** training module and complete the training.
* At the end of the training module, you will be asked to enter your name for a certificate of completion. Please enter your name and either print and scan your certificate, or take a screen shot of the certificate.
* Paste or embed the scanned certificate onto a MS Word document and submit as part of the assignment package. Each team member should have a certificate of completion.

**<Attach/paste images of certificates (for each member) here…>**

****

****

**References (optional)**

<Any additional references you use (either for background information or for citation) should be listed here, using the APA style>



