**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**

***Cybersecurity*** *Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction* [1]

It is important to us because

*Governments, military, corporations, financial institutions, hospitals and other businesses collect, process and store a great deal of confidential information on computers and transmit that data across networks to other computers. 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.*

*During a Senate hearing in March 2013, the nation's top intelligence officials warned that cyber attacks and digital spying are the top threat to national security, eclipsing terrorism.[1]*

*Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. A range of traditional crimes are now being perpetrated through cyberspace. This includes the production and distribution of child pornography and child exploitation conspiracies, banking and financial fraud, intellectual property violations, and other crimes, all of which have substantial human and economic consequences.*

*Cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks. Of growing concern is the cyber threat to critical infrastructure, which is increasingly subject to sophisticated cyber intrusions that pose new risks. As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend. 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]

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. [4]

# Cryptography

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. [5]

## **About Gpg4win**

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

## **What is Gpg4win?**

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]

* GPG4Win website and download the open source software at: <http://www.gpg4win.org/documentation.html>
* 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 (Open Source; among other things free of charge for all commercial and non-commercial purposes).
* After installation, review the documentation, examples, and perhaps check out some YouTube videos that describe how to use GPG4Win.

[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] 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**

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

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

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 assessment, impacts, and lessons learned.
* **Case Study 4:**
* **Computer Hardware and Software Company**

## Distinguishing Characteristics

D Used expert system to analyze data and develop recommendat ions.

D Conduct ed extensive quality review of data.

D Included risk assessment as part of employee performance expectat ions.

This organization uses a defined risk assessment process to ensure that informat ion secur ity contro ls in place comply with estab lished requirements . The risk assessment process was initiated due to the compan y’s efforts to pursue more secure electron ic commerce and increased integration of informat ion systems within the compan y and

with its cust omers, suppliers, and stockho lders. Using a combination of qualitative and quantitative methods , the process is designed to take advantage of the compan y’s expert knowledge of its applications and related secur ity requirements , scale results in such a way as to minimize unreasonab le recom mendations, and establish the minimum

adequate amount of secur ity across the company. The execut ion of the process

identifies and documents the current secur ity contro ls in place for the operat ions under assessment , identifies the current risks to the systems , and identifies additional contro ls needed to provide an appropr iate level of risk mitigation.

As a hardware /software compan y, the organization provides its customers with network hardw are and software, support services, and consu lting services. The company

conducts business in over 110 countr ies and operates its netw ork in over 68 of those count ries. It uses thousands of systems to execut e the day-to-day functions of the

company, including numerous network connect ions to cust omers, suppliers, and part ners. Prot ecting the information resources that support these operat ions is espec ially challenging at this compan y because its engineering culture thrives on openness and sharing of data.

The key steps of the process are shown in the following diagram and discussed in greater detail in subse quent pages.

### Figure 9: Risk Assessment Process Diagram 4

Step Individuals Involved

|  |  |
| --- | --- |
| **Data Gathering Phase**  Determine controls currently in place  Identify business concerns & potential loss | |
| **Information technology & business team** | |
|  |  |

Complete questionnaire

|  |  |
| --- | --- |
| **Analysis Phase**  Identify deviations between current controls & established control objectives  Determine the adequacy of the current controls  Determine recommendations for additional controls  Quantify gap between current controls  & desired policy  Create security specifications | |
| **Software program** | |
|  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | |
| d | Perform quality review | | |
| **Quality review team** | | |
|  | | |  |

Final Questionnaire

Reports

|  |  |
| --- | --- |
| Decide what actions to take to close gap | |
| **Business unit manager & information**  **Technology manager** | |
|  |  |

Register plan

## Initiating a Risk Assessment

At this compan y, organizational policy requires the corporate informat ion secur ity group to initiate risk assessm ents based on the import ance of the operat ions and the time

lapse from the last assessment . Business unit managers assist in determ ining what the most import ant operat ions are within their business units. The genera l expect ation is that risk assessm ents are to be performed on import ant operat ions annua lly. In

instances where the operat ion is extreme ly critical or has changed significantly, risk assessm ents could be performed more often. In addition, at any time, business unit managers can request that a risk assessment be performed .

The risk assessments are assoc iated with three types of activity—(1) development of

new computer systems, (2) procurem ent of product ion systems from other vendors , or

(3) improvement of legacy system secur ity features —and, genera lly, are limited in scope to a primary business process and support ing systems. The support ing systems include the software, databases , and the hardw are and network techno logy support ing the

software , as well as the people who use and rely on these resources . Business unit

managers are respons ible for execut ing the risk assessm ents assoc iated with their unit's computer -based operat ions, and such respons ibilities are genera lly documented in their performance expect ations.

Once a decision is made to perform a risk assessment , the business unit manager forms a team of information techno logy and business expert s to conduct the first part of the assessment , which entails collecting data. The size of the team depends on the number of business and technical people involved in the operat ion being assessed . Often 12 to

14 people are part of the team, but the number can vary. In addition, the organization

uses a cadre of other individuals to perform risk assessm ent tasks, including performing quality reviews, analyzing the results using a software tool, and facilitating the process

across the organization.

## Conducting and Documenting the Assessment

The organization's risk assessm ent process involves (1) using a questionnaire to compile informat ion on the value of critical operat ions and assets , policies and contro ls in place, and other system attr ibutes and (2) compar ing this informat ion with predeterm ined

policy and contro l requirements . The compan y has developed a software program that automat ically performs this compar ison. When the analysis identifies an area that does not meet the estab lished contro l requirements , the software program automat ically

accesses a database of suggested contro l solutions that has been developed by compan y experts . These contro l solutions form the basis of recommendat ions generated by the

analysis.

### Data Gathering Phase

During this phase , the team completes a questionnaire, developed by the organization for the risk assessment process , to determ ine what contro ls are current ly in place over the operat ions being assessed . An individual exper ienced in applying the questionnaire assists the team and helps ensure greater quality and consistenc y of the answers and

greater certa inty that the team members provide accurate answers .

At the time of our study, the questionnaire, which is continually subject to change, had 260 multiple choice questions divided into the following categories:

D valuation of the operat ion,

D policy implementat ion,

D training,

D authorization process , D authent ication process , D identification process , D disaster recovery,

D physical secur ity,

D confidentiality/integrity/nonrepud iation,

D audit,

D detection,

D incident response ,

D configuration criteria,

D configuration management , and

D graphical inventor y of the systems architecture

The multiple choice questions have been designed to precisely capture a descr iption of existing operat ions and cont rols. Exam ples of the types of questions included are

show n in the following box.

### Figure 10: Questionnaire Items Related to Authorization

1. Estimate the percenta ge of user population access ing this application regularly from the following sites. From those sites with access , enter the percenta ge value for the appropr iate site. (Total of all answers may exceed 100%.)
   1. from primary organization campuse s,
   2. from private home s,
   3. from kiosks,
   4. from contractor, partner, or supp lier sites with whom there is a written contract to manage info-security,
   5. from customer sites,
   6. from sites with nomad ic accounts ,
   7. from executive suites,
   8. from anywhere,
   9. from contractor, partner, or supp lier site without info-security contract, and/or
   10. unknow n.
2. Estimate the number of administrators and other key staff listed below for this application system. [Comment : The purpose of this question is to determ ine the number of people who are in key positions to effect the secur ity of the system.

Please be sure to count the number of staff assoc iated with this application from all organizations involved.]

* 1. database administrators,
  2. application administrators,
  3. system administrators ,
  4. access contro l and account administrators ,
  5. technical support operations,
  6. security administrators or coordinators,
  7. IT developers, and/or
  8. unknow n.

The company treats the “valuation of the operat ion” section of the questionnaire as a

separate phase of the risk assessment . During this phase , the team determ ines (1) what conse quences need to be protected against, assum ing an attack or other damaging event occurs and (2) what the likely damage to the compan y would be as a result of such

events. Because these valuations are considered very subjective, the team relies on the assistance of additional experts with specific finance related knowledge, who are

typically from the compan y contro ller’s office. The informat ion developed during this phase is critical to determ ining the significance of any contro l deficiencies that may be identified later in the analysis.

The team first determ ines what conse quences could occur . The compan y has defined

potent ial damage as including fraud, operat ional outage, embezzlement , extort ion, theft of intellectual propert ies, regulatory violations, or diminishment of the organization's

image. Although the questionnaire is intended to be comprehens ive, the compan y recognizes that additional types of damage may need to be considered .

Once it is determined what conse quences apply to the operat ions under assessm ent, the team estimates the level of damage that could result from these conse quences by

considering the potential cost s of rest oration and recovery, as well as secondar y effects, such as embarrassment and loss of credibility. Estimating the cost of secondar y effects is espec ially difficult because of the uncerta inty assoc iated with the ultimate impact on such intangible factors . For examp le, the cost of restor ing a damaged web site is much easier to estimate than the cost of recovering from the embarrassment and loss of

credibility from such damage.

Usually, the team can complete the entire questionnaire in 1 to 2 hours . In cases where the team members are less familiar with the application, it can take up to 12 hours or

more because people with additional expert ise are contacted to assist in completing the questions. Once the questionnaire is completed, additional individuals perform an

extens ive quality review that analyzes the answers for completeness , reasonab leness and consistenc y. Often, it takes as many as five reviews to attain the required quality.

The time taken to complete the quality review varies by assessment from a few hours to several days to even weeks in rare cases . The quality review benefits the process by

ensur ing that (1) the data used are complete and the best available and (2) the questions are consistently applied and interpret ed. Redundanc y is also built into the questions to help the quality review determ ine if the team thorou ghly considered the questions.

### Analysis Phase

After the quality review is completed, the analysis group input s the information about the current cont rols, as derived from the questionnaire’s answ ers, into a software

program. The software program compares these contro ls to contro l requirements

documented in the compan y’s informat ion secur ity policies. The database of over 400 informat ion secur ity contro l requirements , which is referred to as a “policy library” by

the organization, represents a consensus of the exper ience and best judgment of a broad group of business and information techno logy expert s organizationwide. The analysis

performed by the software identifies instances where existing contro ls do not meet the compan y’s suggested contro l requirements .

Using the results of this comparison, additional information from the questionnaire, and a defined list of 180 contro l techn iques, the software automat ically proposes contro l

techn iques to achieve compliance with the contro l objectives. Each contro l techn ique, or countermeasure , can have up to five different stren gth levels, which genera lly depend on the specific type of contro l techn ique chosen and the rigor of assoc iated enforcement efforts. Examp les of stren gth levels for informat ion secur ity training are shown in the following box.

**Figure 11: Example of Five Strength Levels for Security Training**

Level 1

No specific training requirement exists, so compliance with the requirements

is not measured.

Level 2

Security training requirements exist, and business unit managers record

completion of the training, but complianc e is not independently verified.

Level 3

Security training requirements exist, and the business unit managers

determ ine in advance the required percenta ge of compliance among the

individuals involved in that operation. During the periodic risk assessme nt, a compa rison is done to assure complianc e with the

estab lished percentage.

Level 4

Same as Level 3.

Level 5

Security training requirements exist, and the business unit manager is

respons ible for tracking and verifying that all individua ls involved in the operation are compliant.

Next, the analysis group reviews and further refines the proposed recom mendations using a software tool that considers a number of factors , such as the number of users , number of access paths , and effects on other systems . The organization has also

designed the software tool to consider detailed requirements for individual

circumstances . For examp le, systems with more than 150 users require more rigid account management procedures to be in place than do systems with fewer users .

Accord ing to this compan y's policy, the attr ibutes of these procedures for systems with over 150 users should include:

D formal procedures for revocation or modification of terminated or inactive account s;

D cent rally assigned and monitored passw ords;

D a unique password for each user, with 90-day mandator y password changing; and

D screen ing of new passwords for suitability prior to being accepted by system.

Based on the determinations made during the analysis, the analysis group finalizes the recommendat ions. When necessar y, systems engineers are brought into the process from the information techno logy area of the business unit to perform an engineering

review of the assessment ’s output and recommendat ions. The purpose of this review is to determine the feasibility of the reco mmen dations and to resolve any open issues

identified, such as the need for a detailed design review. The precise techn ical method of implementing the recom mended improvement is left to the judgment of personne l in the business unit.

## Reporting and Ensuring That Agreed Upon Actions Are Taken

A series of standard ized reports are produced from the risk assessment process , including a detailed risk analysis report , a report descr ibing the application's current level of conformance to requirements , and recommendat ions for specific secur ity

engineering design review. One of the key reports graphically shows , for each major application, the deviation between the current contro ls and the contro ls suggested by the compan y’s informat ion secur ity policy. In addition, the reports estimate the costs for each recommended countermeasure , including costs for licenses , training,

development , implementat ion, and recurr ing support .

The business unit head considers the informat ion in these reports when deciding what new contro ls to implement . If the business unit head believes that certa in

recommendat ions are not cost-effective, he or she can discuss the concerns with the compan y’s informat ion secur ity managers and negotiate alternat ive actions.

Because business and informat ion techno logy managers are being held accountab le for making informat ion secur ity 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 estab lished informat ion secur ity goals. In

addition, the organization has instituted audit and measurem ent procedures to ensure the effectiveness of actions taken and that these actions have not adversely affected system operat ions. Compan y officials emphas ized the importance of managing the

changes resulting from the informat ion secur ity risk assessments . They stressed that this requires instituting methods for monitoring the progress being made because

changes can be expens ive and managers are usually reluctant to implement them— espec ially when changes could adversely affect their business.

**<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**).

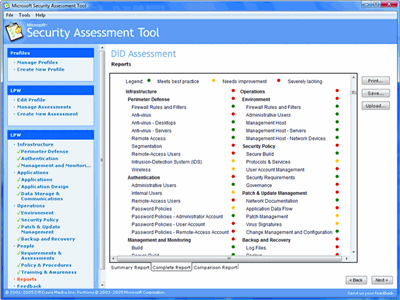


Figure 1**The complete report**(Click the image for a larger view)

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)

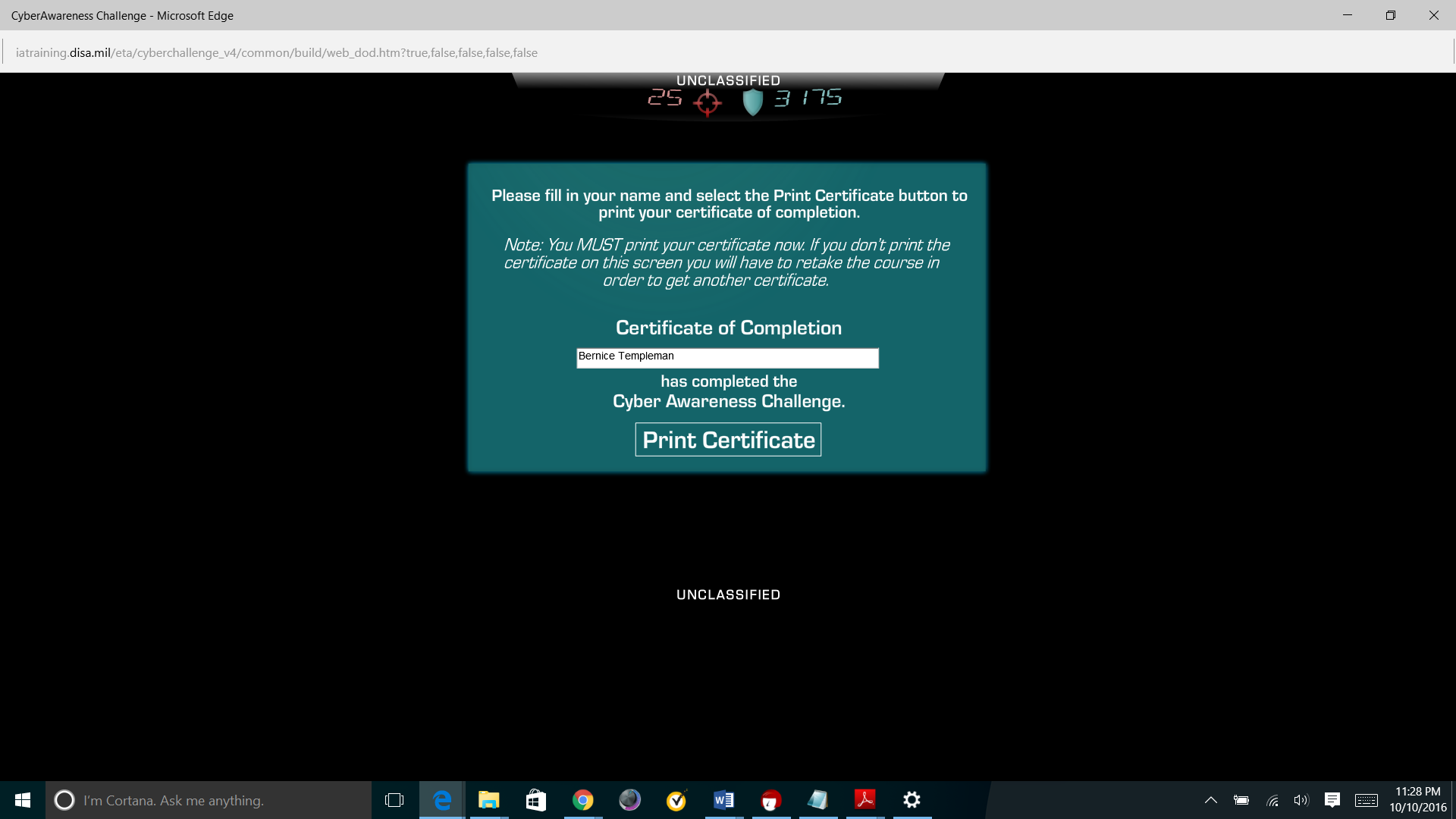
Utility Spotlight The Microsoft Security Assessment Tool

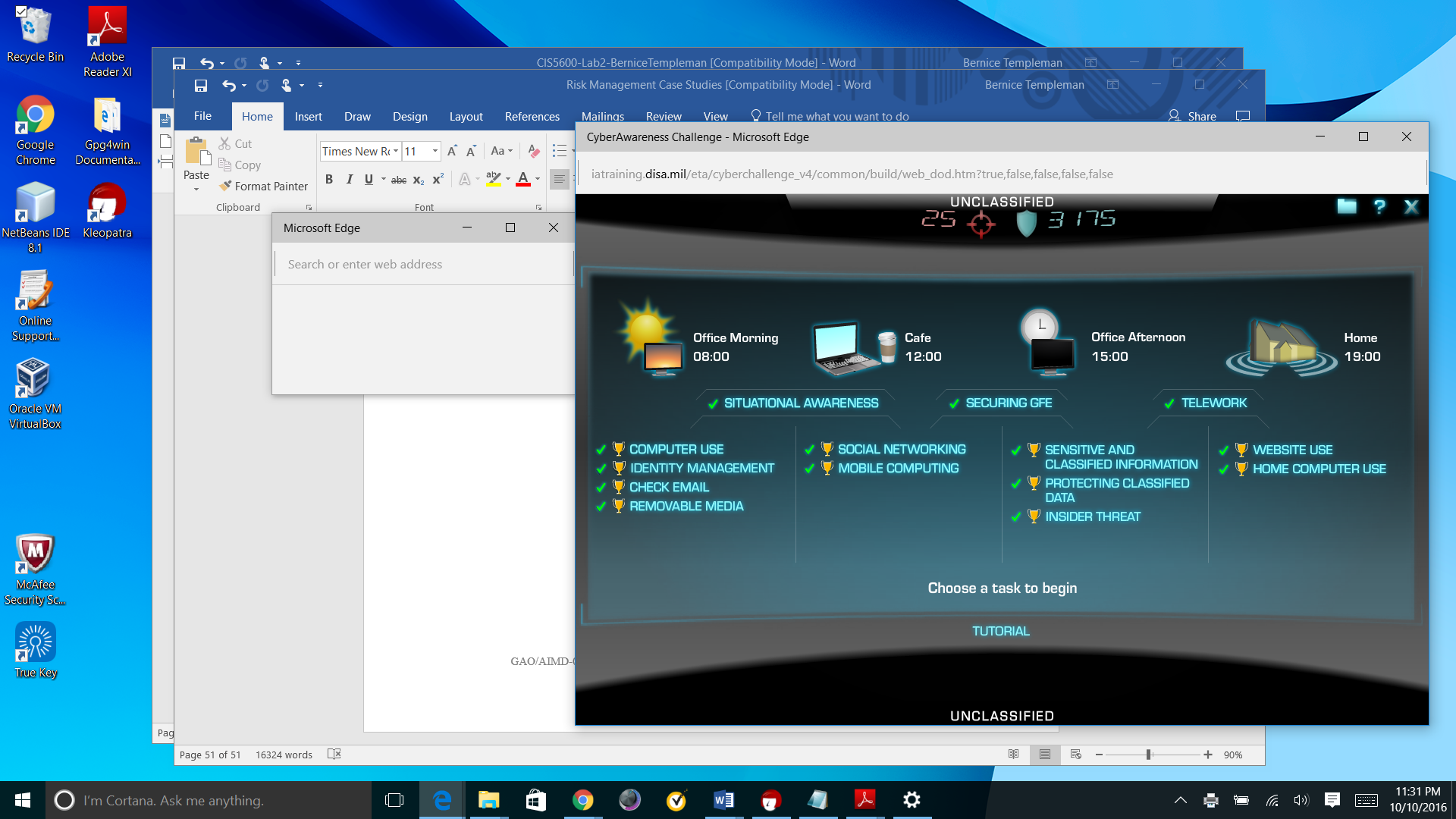
Lance Whitney

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>