**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 :**

**Dear Bernice,**

**Congratulations!!! You have successfully decrypted this message using PGP encryption technology.**

**With this new found knowledge, you are now a step closer to becoming an IT security professional.**

**Your team's special password is: Watermelon**

**Please copy and paste this entire message into your Lab #2 submission document.**

**Thank you,**

**-Dr. Lanman**

**…>**

**<Summary of Cryptography and GPG4Win**

Cryptography is part of Cybersecurity andis important to us because of the increasing numbers and sophistication of cyber-attacks, the ongoing requirements to protect sensitive business and personal information, as well as safeguarding national security.*[1]* According to the Homeland Security website,

*“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 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. [9] 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. Therefore, cryptography is also an art. [4]

*According to* [*Webopedia.com*](http://www.webopedia.com/term/e/encryption)*, “Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or passwords that enables you to decrypt it. Unencrypted data is called plain text. encrypted data is referred to as cipher text*.” [5] By using open standards, encryption is available to the general public.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. [6]

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). [7]

A study of the GPG4win,

*“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.*

*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]*

I found GPG4Win easy to download, install and use. This tool can help people encrypt messages easily and protect them. It uses a Two-Key Method. According to PCMag.com,

*Gpg4win uses a public key and a secret key. The sender and receiver of encrypted messages each have their own unique secret keys that do not need to be shared while also relying on a publicly visible key. The public key is used to encrypt messages. Since it’s publicly visible, anyone can use it to send you encrypted messages. Only you can decrypt them, however, using your secret key. Even the person who sent you a message encrypted with your public key can’t decrypt it, so the system is virtually unbreakable.*

*Your secret key is stored on your computer. Someone could theoretically steal it if they were to steal your computer, so it’s protected with two layers of security. The first way it is protected is that no one can write to the file or alter it in any way, not even system administrators or Trojan horse viruses. The second way it is protected is with an unguessable passphrase.*

*A passphrase works like a password, but it’s based on a sentence instead of a word. It’s not something easily “guessable.” A passphrase is a string of letters and numbers that mean something only to the person who created it. Passphrases are created in two steps. Start by thinking of a personal and easy to remember sentence, such as “I was born three years after my sister Annie in 1977.” Then take the first letters of each word in your sentence and run them together, which in this case is IwbtyamsAi1. That’s your passphrase. You aren’t likely to forget it, but it’s virtually impossible for anybody to guess it*. [10]

**References**

[1] Cyber Security Primer. (2016). Retrieved from <http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm>

[2] Cybersecurity Overview. (2016, September 27). Retrieved from <https://www.dhs.gov/cybersecurity-overview>

[3] Cybersecurity industry has failed the market: CEO. (2016, October 10). Retrieved from <http://www.cnbc.com/2016/10/10/cybersecurity-industry-has-failed-the-market-ceo.html>

[4] Chapter 7: The Role of Cryptography in Information Security. (2012, June 11). Retrieved from <http://resources.infosecinstitute.com/role-of-cryptography/>

[5] Encryption. (2016). Retrieved from <http://www.webopedia.com/TERM/E/encryption.html>

[6] [Cyber Security and Cryptography - Computing Concepts](http://computing-concepts.cs.uri.edu/index.php/Cyber_Security_and_Cryptography). (2016, March 29). Retrieved from [computing-concepts.cs.uri.edu/index.php/Cyber\_Security\_and\_Cryptography](http://computing-concepts.cs.uri.edu/index.php/Cyber_Security_and_Cryptography)

[7] About Gpg4win. (2016). Retrieved from <https://www.gpg4win.org/about.html>

# [8] Short Study: Sustainable Free Software: From project to permanent activity, using the example Gpg4win. (2008, September 30). Retrieved from <https://www.gpg4win.org/ShortStudy-Sustainable-FS-example-Gpg4win.html>

[9] How to Geek: What is Encryption and how does it work?. (Retrieved 2016). Retrieved from <http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/>

[10] Gpg4win. (2016). Retrieved from http://www.pcmag.com/business/directory/encryption/1119-gpg4win

**…>**

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**

In my review of the Software Company in the Risk Management Case Studies report, the issues and risks I identified are associated with three activity types:

(1) development of new computer systems

(2) procurement of production systems from other vendors

(3) improvement of legacy system security features

The supporting systems include:

* software
* databases
* hardware
* network technology supporting the software
* 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.

In the assessment I found that even though all elements of the risk management cycle are important, risk assessments provide the foundation for other elements of the cycle. Risk assessments provide a basis for establishing appropriate policies and selecting cost-effective techniques to implement these policies.

## The basic elements of the Risk Assessment Process usually include:

* + 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 assets that could be affected should a threat materialize in order to determine which operations and assets 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 different ways for assessing risk. 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

(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.

I found the following 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.
* 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.

The 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.

The impacts I found are:

## 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

**The lessons learned from the case studies include:**

## Critical Success Factors

### Senior Management Support

### Designate Focal Points

### Define Procedures

### Involve Experts

* Hold Business Units Responsible
* Limit Scope

### Document and Maintain Results

## Tools

## Benefits

1. 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.
2. 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.
3. 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.
4. 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.

**…>**

**<Summary of the tool assessment**

I downloaded and installed the MSAT. I ran the application and answered the questions not based on a real company. I also did some research on the tool and found the following:

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.  
  
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

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 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]

I also found the following:

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.

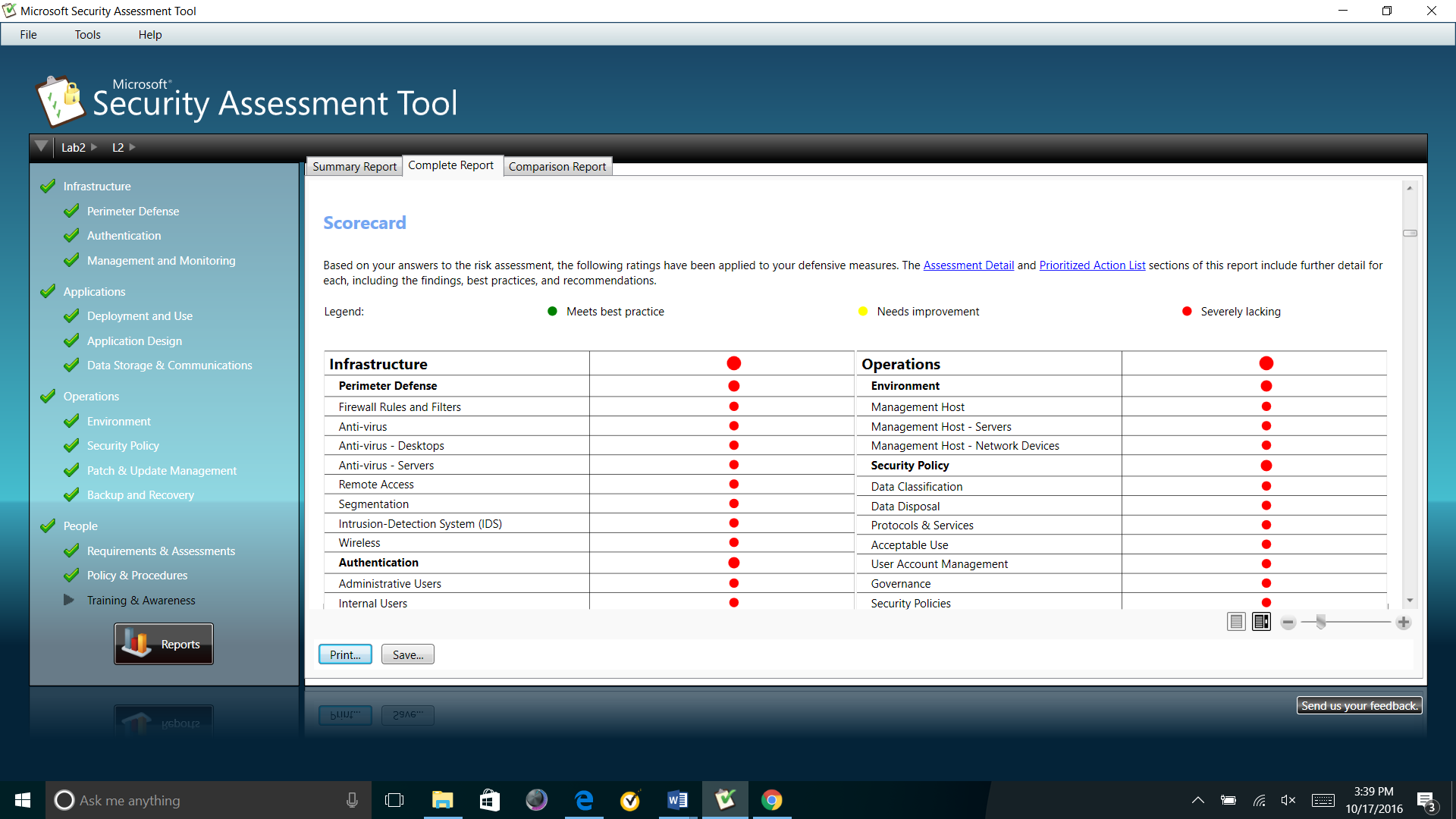
Using the same categories, typical questions are:

* 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.

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]



**Screenshot from the complete report**

# [1] Microsoft Security Assessment Tool 4.0. (2016). Retrieved from <https://www.microsoft.com/en-us/download/details.aspx?id=12273>

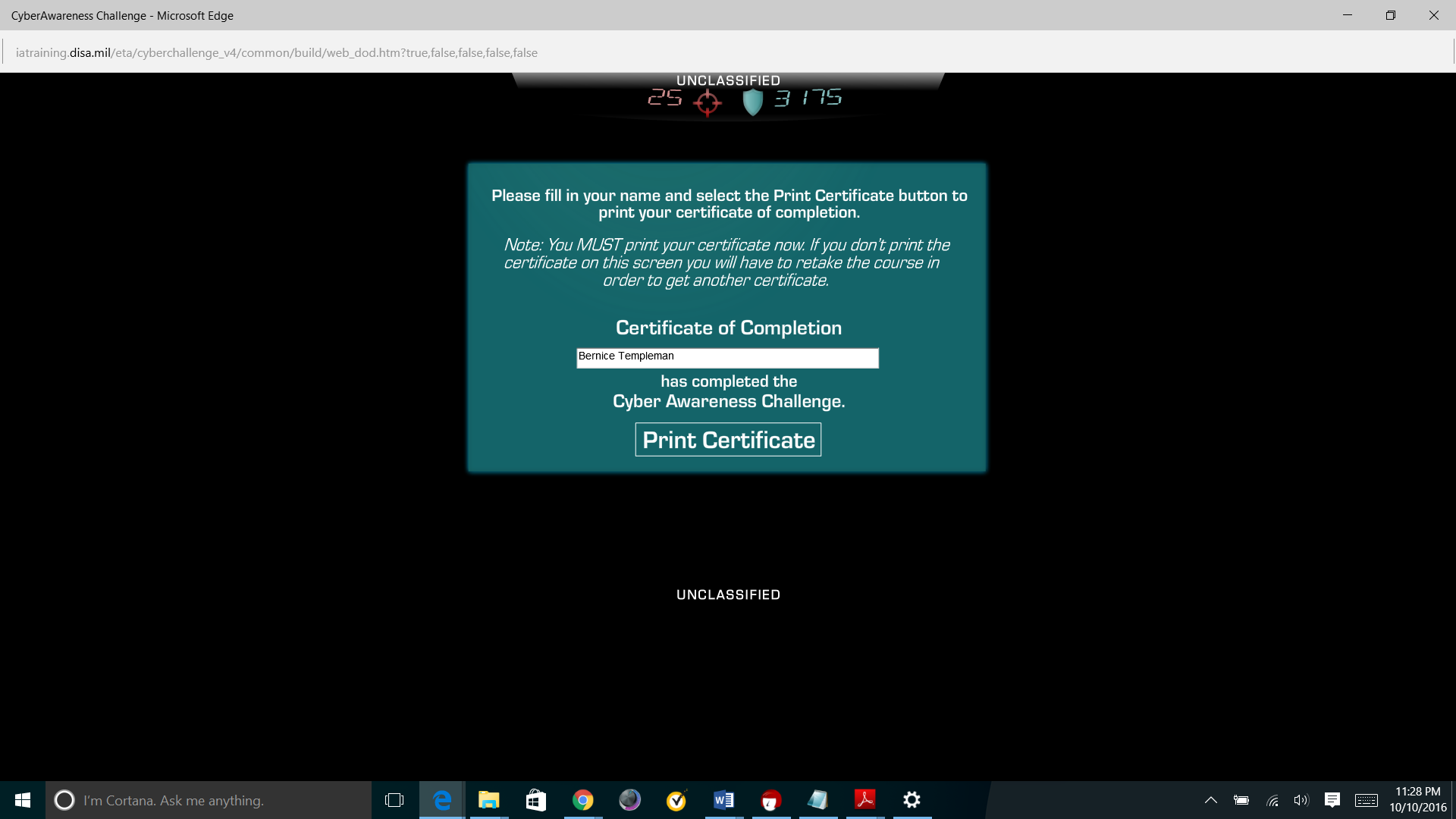
[2] Utility Spotlight: The Microsoft Security Assessment Tool. (2008). Retrieved from <https://technet.microsoft.com/en-us/library/2007.12.utilityspotlight.aspx>

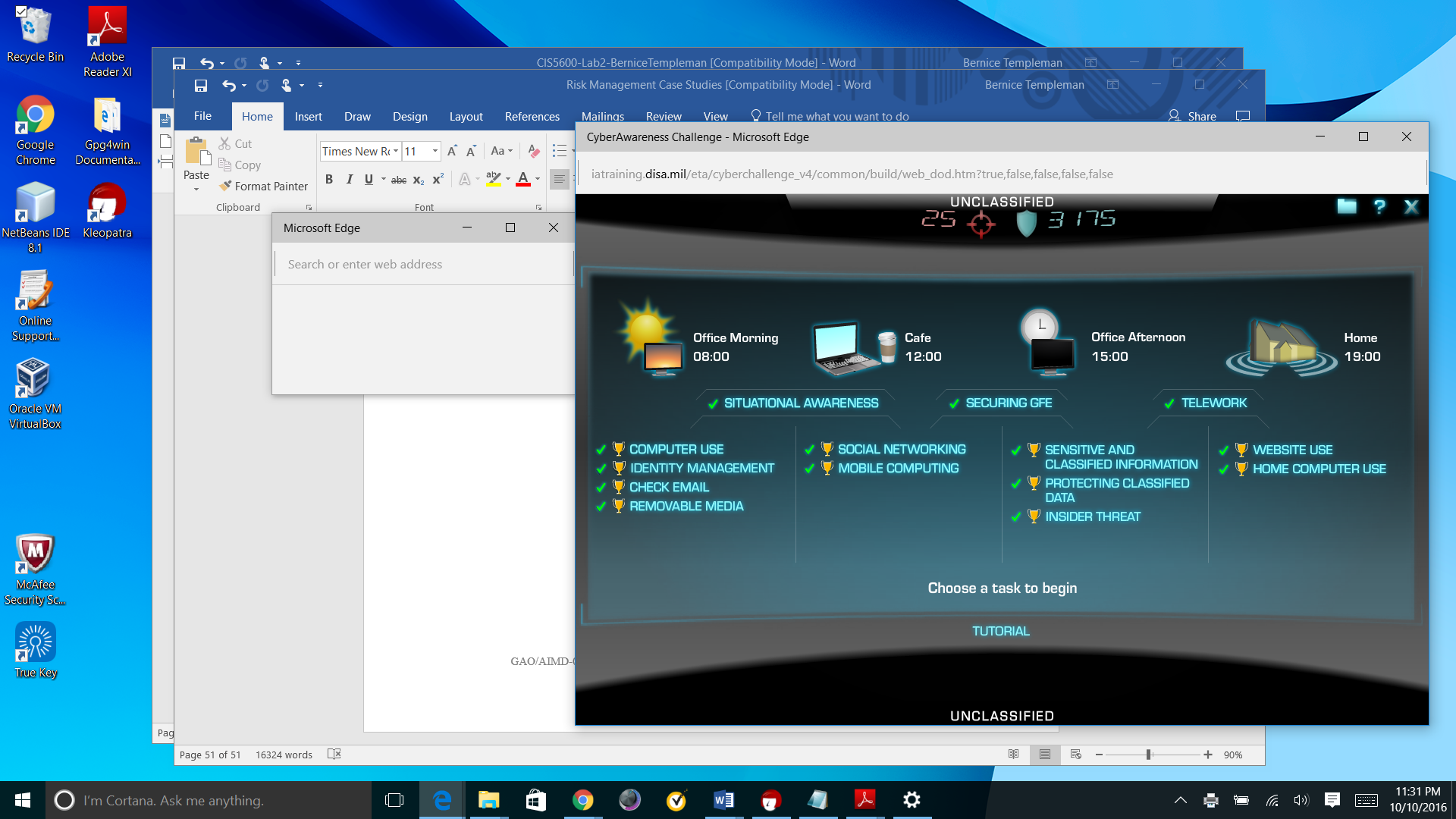
**…>**

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>