SOHO: Information Security Awareness in the Aspect of Contingency Planning

Jason Maurer
College of Arts & Sciences
Regent University
Virginia Beach, Virginia U.S.A.

Brandon Clark
College of Arts & Sciences
Regent University
Virginia Beach, Virginia U.S.A.

Young B. Choi
College of Arts & Sciences
Regent University
Virginia Beach, Virginia U.S.A.

***Abstract*—This paper seeks to take general security awareness information for home and small business owners and make it understandable and accessible by looking at practical ways to keep valuable information accessible after an incident or disaster according to current methods. This paper will first review select general security awareness information, then take a look at some aspects of contingency planning and look at some basic practical techniques to use in order to protect systems and information from complete loss after an incident. Finally, the ground work for implementing an individualized plan for a small business office or home office will be laid and some practical steps to take will be recommended.**

Keywords—SOHO; Information Security; Contingency Planning; Small Office; Home Office

I. Introduction

It is recognized that cybersecurity is important but until recently has been neglected by many [1]. When a computer virus, power outage, loss of Internet access, vandalism, theft, hacker, fire, or some other disaster or incident occurs, will you be ready? When your computer shut down permanently or your hard drive malfunction, will you lose all your valuable information? If your filing cabinet and backed up files on the external hard drive in your desk drawer are under water, is all that information gone for good? If you anger an employee with access to your files stored in the cloud and they are all gone the next day, are you prepared to recover and continue with your business processes? These are just a few common scenarios that happen but are often ignored when it happens to someone else. Now is the time to prepare. Now is the time to plan. Our research seeks to inform you about an aspect of information security that is often avoided because of the time and resources it takes to do, with no obvious immediate results, and that is contingency planning. The goal of information system security is to maintain accessibility, confidentiality, and integrity [2] and information security in general encompasses of all your information, whether databases, files, or even printed papers and images, etc. Once you realize that you would be in a bad situation if you lost everything in your office, you need to know what to do and where to start. Our research is intended to get you thinking ahead and planning for the event that gets through all your layers of prevention and disrupts your operations and give a good foundation for you to start planning how to protect your information beginning with basic information security review.

II. Information Security Review

As first stated earlier, the goal of information security is to maintain accessibility, confidentiality, and integrity of all your information. This means electronic and physical information must remain at the determined level of privacy while also having accuracy and accessibility [2]. This is a very simple statement but a challenging goal. Information can be protected easily if it is not readily available and can be easily made available if it is not protected and can easily maintain accuracy if no one accesses it. Finding a good balance of these things if the goal of Information Security as shown in Figure 1 where you see examples of various imbalances and in the middle you see a balanced situation where only authorized users can access the information. Contingency planning is thinking ahead and preparing to maintain accessibility, confidentiality, and integrity of all your information so that you can continue operations with minimal down time in the event of an incident or disaster. Figure 2 shows the secure, accessible and accurate information being destroyed by incident or disaster. This triggers the recovery of the information using the contingency plan that was put in place for the specific type of event and restoring it to the original state of being secure, accessible and accurate. This begins with an assessment of the risks that your home or office might be susceptible to and then doing as much as possible to prevent or mitigate those risks and make a plan in case those preventions fail or don't work as expected.

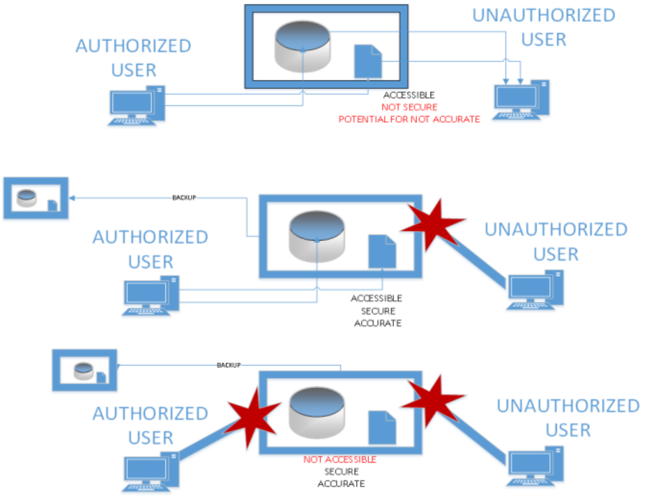

Fig. 1. Various Information Access Balances

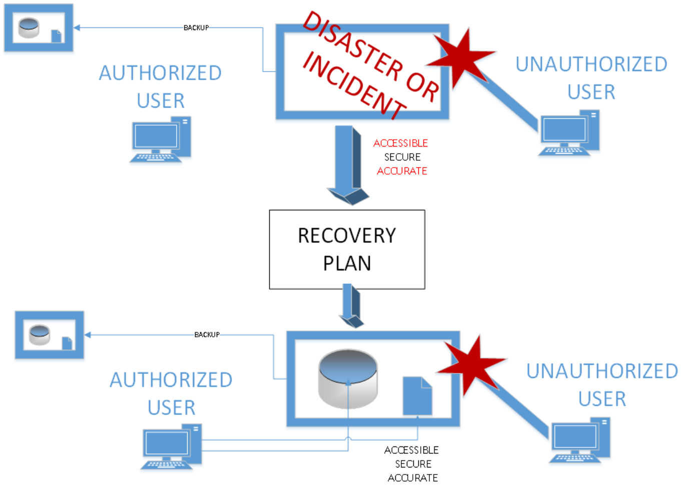

Fig. 2. Secure, Accessible, and Accurate Information Being Destroyed by Incident or Disaster

III. PLANNING

Planning is critical to maintaining a small office or home office for when incidents happen or disaster strikes. Having an insurance policy covering your home or business location is not enough. Contingency planning could be thought of as a form of self-insurance. It will cost time and resources to plan and prepare, as an insurance premium does, but when an incident happens, you will spend much less money to get things operational when it is all said and done because you have prepared and developed an appropriate plan. Contingency planning is not just about planning for major disasters such as fire, flood or Hurricane, but about recovering from situations that negatively affect operations such as suppliers going bankrupt, an important delivery being delayed, or even the entire office staff getting food poisoning at an office party [3]. "The goal of a resilient organization is to continue mission essential functions at all times during any type of disruption [4]."

A. Why Plan?

The security and continuity of your business processes is very important to any business or organization manager, especially in Small Office/Home Office (SOHO) setups. However, the authors speculate that most people either do not think that security is important, or think that it is second to everything else and often never get around to putting a plan in place. Putting planning in second place is flawed thinking as security and preparedness for incidents should be the first priority when setting up any information system. The threats to businesses and other organizations are growing and require great attention to information security technology to combat both people threats and the seeming increased occurrence of natural disasters [5].

Chris Stock, Director, Security Programs, TM Forum says, "I think there are still people out there who think, 'I don't have too much to worry about… They are just going to risk it and take the consequences if they are hacked [6]." More than 75% of the responders to a survey done for 100 small businesses in New York, New Jersey, and Connecticut after Hurricane Sandy did not have disaster recovery plans in place and "…on average, Staten Island small businesses lost more than $83,000 in revenues in the month that it took them to reopen. Annual revenues were reduced by approximately $200,000 to $500,000 following Sandy [7]." While this is just one specific incident of large scale, if those business had put the time and effort into creating a plan, they may have opened their doors much quicker and not lost nearly as much revenue. The damage from a disaster impacts more than the buildings, equipment, and processes. In certain situations, it also affects revenue, reputations, and can simply put people out of business.

B. Why People Don't Plan

As mentioned previously, the information published in Contingency Planning and Disaster Recovery by Cynthia Scarinci [7] uses a series of surveys from various sources to identify various shortfalls and issues that were experienced by accounting firms and small businesses in the aftermath of hurricane Sandy. In the article, the author shows where the responding business managers fell short and what hindered them from having plans in place. The top reason was that they simply did not know how. It can also be seen how much immediate losses were while recovering from Hurricane Sandy and that there was a general reduction in annual revenue after the disaster. There are two major issues to be addressed from the results of this survey. The first is that there are business owners that do not appreciate the importance of planning for the unexpected, often because of the time and cost commitment. Secondly, it is essential to educate these business owners on "how a plan can facilitate their recovery process [7]." This is exactly what our research seek to do, educate those people working in small offices and home offices and show how and where to start with contingency planning.

IV. TYPES OF PLANNING

There are several types of contingency plans that are beneficial for an organization to have as contingency planning can be broken into several different areas. Many of these are talked about in National Institute of Standards and Technology (NIST) publication SP 800-34 which covers the topic of contingency planning. Some of the plan types that apply to Contingency planning include Business Continuity Plan (BCP), Continuity of Operations (COOP) Plan, Disaster Recovery Plan (DRP), and the Information System Contingency Plan (ISCP). Each of these will be mentioned briefly to see how they fit into contingency planning. The majority of the information covered in this section is from the NIST SP 800-34 document.

A. Business Continuity Plan

The main purpose of creating a Business Continuity Plan (BCP) is to have information that will sustain the mission/business processes of an organization during and after a disruption. The examples in the NIST documentation given for these types of processes is the organization's payroll process or customer service process. This plan has information that keeps you going after a disaster. They say that a BCP "may be written for mission/business processes within a single business unit or may address the entire organization's processes" and the scope can be only priority functions [4].

B. Continuity of Operations Plan

Continuity of Operations (COOP) focuses on mission essential functions performed at an alternate site for up to 30 days. This typically includes items such as risk management, budgeting and acquisition of resources, order of succession, delegation of authority, vital records management, human capitol, and reconstitution. Our research does not go into depth on this type of planning as it is usually only used by organizations that are federally mandated to use them. Non-government organizations typically use a BCP described above [4].

C. Disaster Recovery Plan

Disaster recovery is just what it sounds like. It is used when an event happens and services are majorly disrupted, which are usually physical disruptions to a company's services that deny staff access to the primary facility and infrastructure for an extended period of time [4]. "A DRP is an information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency [4]." There can be multiple contingency plans that all involve steps in recovery of many individual systems once an alternate location has been established [4]. Practically speaking, this is a pre-thought through plan of what you are going to do to restore your entire business if something happens that completely removes you from your current facility and disables many or all of your resources. It may seem overwhelming and impossible, and it is a large project but it can be done one step at a time.

D. Information System Contingency Plan

As mentioned above, the DRP can be made up of many contingency plans. Creating an Information System Contingency Plan (ISCP), established procedures to assess and recover a system following a disruption [4]. "The ISCP has key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of a system [4]." One can distinguish this type of plan as being different from a DRP in that ISCP's can be implemented no matter the location. The same steps will be followed to restore a system where the DRP is about establishing an alternate site for operations [4].

E. Other Important Terms

NIST contingency planning documents also contains information on other important terms you will need to know and think about when working on your contingency plans. Maximum Tolerable Downtime (MTD) is the maximum acceptable amount of time a system can be down. This gives direction on recovery methods and detail of recovery procedures [4]. Critical operations with very low tolerable down time will require more resources and in depth planning to support a quick recovery time. Recovery Time Objective (RTO) "defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD." This is important for selecting the best methods suited to stay within the MTD [4]. Recovery Point Objective (RPO) basically determines how much data can be lost during the recovery. There is typically a point in history where the data can be restored from with the last backups. This determines the amount of data loss or how far back the restore point is allowed to be [4].

V. Starting to Plan

It is thought that the root cause of 80% of security incidents could be avoided by "doing the basics well [8]." To begin, you need to know what you do and how you do it. Start by developing a list of all the important or critical processes you have in place [3].

A. Processes

This can be a difficult task as everything from taking orders and delivering a product or processing payroll to purchasing paper for the copy machine has a standard process and can seem important. Distinguish between the processes that are critical to operations, payroll, payment processing, sales, customer support, etc. This is a good place to start. Take each one and list them out from most critical to the least critical.

B. Resources

Next determine what resources or systems are involved with each process. Use this information to determine the most important resources. If all your processes involve the Internet, then the Internet is going to be a critical resource along with making sure you have a working computer. "Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records [4]."

C. Risks

Next, a manager will want to identify the risks applicable to their small businesses. This is done by doing a risk analysis. A Risk analysis is very involved if it is done comprehensively. You will "draw on detailed information such as project plans, financial data, security protocols, marketing forecasts, and other relevant information. However, it's an essential planning tool, and one that could save time, money, and reputations [9]." You need to determine what could harm or disrupt your business, such as file deletion, viruses, hackers, theft, hurricane, fire, etc. It is important to prioritize them or you will be overwhelmed. You don't want to start by making a plan for each threat. Start with those that will have the most impact and are the most likely to happen. At the same time you will be considering what you already have or will have in place to mitigate the risk. Looking at the threat of theft in a high crime area, the risk is high. If you mitigate the threat by installing a comprehensive top of the line security system along with armed security guards and 24/7 surveillance, the risk of theft is lower than the threat of a hacker if you have no firewall installed. "A good plan identifies all critical business functions, and it outlines ways to minimize losses [3]." The website for MindTools gives a list of well said guidelines for keep in mind while developing your plan. This list can be seen in the reference [3].

VI. Practical Steps

In this section, practical considerations of the planning process are discussed. Simple things like keeping a list of important contacts in a purse or wallet and making sure all employees have one also can make a huge difference on how contingency plans go. An alternate location, alternate internet access, as well as the cost versus benefit of everything will need to be considered. Backing up files is a huge part of recovering from disasters and certain incidents and will be emphasized a little more.

A. Alternate Internet Access

An area that is very standard for most business' staff to rely on is their Internet connection. It is a good idea to look into an alternate Internet option. It may be a hot spot that is compatible with cell towers or simply a different vendor that supplies an alternate site with service. Even if an alternate Internet Service Provider (ISP) is considered in the event that your standard provider's service ceases to operate, there is no guarantee that the alternate provider will not also be affected by the same conditions.

B. Alternate Location

Consider where you will go if your building is destroyed. Where will your new office location be until the current location is rebuilt or renovated? How far away will it be? If it is too close it may be affected by the same disaster, if it is too far you may not get all your employees there or be able to service the customers in your normal area. Do you need a hot site where all your data and systems are already on and running and fully staffed or do you need an empty room that you and a couple employees can go to for internet access on their laptops? These things need to be considered.

C. Weigh Cost versus Benefits

Throughout the process, when it comes time to make decisions, you will need to weigh the cost versus the benefit. This is where your impact analysis and risk assessment are valuable. If there is a critical process that your business cannot function without, then spare no expense to keep it running smooth. If a process is not needed to survive, do not invest a lot of time and money into having a plan B for it.

D. Virus Protection

Mitigate the threat of computer down time due to malware with virus protection. Many people do not know the benefit of having protection on each machine or do not know how or which solution to use. This is where a large company would have a large team of employees to address each question or issue. For small business or home offices those running the office will need to seek out a professional, or be educated.

E. Scan Paper Files

A simple method to backup information stored on paper, usually stored in file cabinets, is to scan in your papers and store them in searchable PDF format. It may take time to catch up, but integrating this step into your processes can save a lot of trouble in the future if a fire burns all the paper in your file cabinet. There are machines that can scan directly to a network storage device with no computer needed to scan the document making it simple and swift.

F. Backup Digital Data

Data is one thing that is very important in today's business world. It is important to have a plan in place in the event that a disaster, incident, or other event takes place. The thing is, many people and small businesses do not have any kind of backup solution [6]. It cannot be stressed enough that you must have multiple copies of your information backed up on different systems and even off site. Use either on an external server with RAID (Redundant Array of Independents Disks) options, on an external hard drive or the cloud to back up your data. Having multiple external hard drives that can be rotated is very beneficial. Even if you already backup your data in "the cloud" you may still want to have an offline copy of critical data that would cause severe problems and keep it in a location away from your office or home, even if it is just for peace of mind [10]. It is even wise to think about the situation of a disgruntled employee or even someone making a genuine mistake who deletes all the data out of the cloud or off a server. Being able to recover and restore data after an incident, whether a malware incident or a natural disaster, is critical to the continuity of a small office, whether at home or at a small business. The best policy is to have backups done at regular intervals to make sure the latest data is backed-up. An article by Santos and Bernadino called *Open Source Tools for Remote Incremental Backups on Linux* describes the easiest way to do a back-up is to copy an entire disk to a back-up disk [6]. This helps to prepare against drive failure. Luckily there are several free open-source utilities to help make back-ups more accessible [6]. The ones mentioned in the article are all Linux tools, but can be used to back-up other types of systems. The most popular tools include Rsync, Rdiff-backup, Duplicity, Areca Backup, and Link-Backup. The various tools are then tested to compare the performance of the various tools. After testing was complete, the authors determined that Rsync was the best if encryption and compression were not needed. If those where needed, Duplicity performed the best. However, Rsync was determined to be the most efficient tool to make simple back-ups [6]. There are also many cloud based vendors in existence that backup multiple versions of every file. They will even take a snapshot of an entire drive, operating system and all and can then restore it to that state if disaster strikes a machine.

VII. Conclusion

The topic of Information Security include many topics. In our research, several areas of information to get a small office started with contingency planning efforts for emergencies, incidents, and disasters were discussed. There will always be threats to the security of computer systems, but having a plan in place will help keep data secure, accurate, and accessible and keep a small office successful. Get a plan in place and maintain it, practice it and make it familiar to every employee so there are few questions during an incident or disaster.

References

[1] Fourie, L. et al. (2014). THE GLOBAL CYBER SECURITY WORKFORCE – AN ONGOING HUMAN CAPITOL CRISIS. Global Business and Technology Association.

[2] OIT Communications Group. (2014). definition-information-security. Retrieved 11 29, 2014, from oit.unlv.edu: https://oit.unlv.edu/network-and-security/definition-information-security

[3] Mind Tools Ltd. (n.d.). Contingency Planning. Retrieved 02 21, 2015, from mindtools.com: http://www.mindtools.com/pages/article/newLDR_51.htm

[4] Swanson, M. et al. (2010). Contingency Planning Guide for Federal Information Systems. SP 800-34. Retrieved from

http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

[5] Williamson, J. (2014). Privacy & Security: Locking Value into the Digital Economy. TM Forum.

[6] Santos, A., & Bernardino, J. (2014). Open Source Tools for Remote Incremental Backups on Linux: An Experimental Evaluation. Journal Of Systems Integration (1804-2724), 5(3), 3-13

[7] Scarinci, C. A. (2014). Contingency Planning and Disaster Recovery after Hurricane Sandy. The CPA Journal, 60-63.

[8] Schreiner, S., Carpenter, M., Hamerstone, A., Coffey, C., Webb, N., & Rottinger, J. (2013). CyberOps Quick Start Guide: Human Factors, Version 1.2. Retrieved from TMForum: http://www.tmforum.org/GuideBooks/GB968CyberOpsQuick/50365/article.html

[9] Mind Tools. (n.d.). *Risk Analysis and Risk Management*. Retrieved 2015, from minddtools.com: http://www.mindtools.com/pages/article/newTMC_07.htm

[10] Brinson, L. C. (2014). backup cloud storage. Retrieved from how stuff works: http://computer.howstuffworks.com/backup-cloud-storage4.htm