GAINING MONITORING CAPABILITIES AND INSIGHTS INTO RESPONSES FROM PHISHING DATA

Thesis

Presented in Partial Fulfillment of the Requirements for Master of Science in the Graduate School of The Ohio State University

By

Alah Raqab, CSSGB

Graduate Program in Industrial and Systems Engineering

The Ohio State University

2014

Master's Examination Committee:

Theodore T. Allen, Advisor

Cathy Honghui Xia
Copyright by

Alah Raqab

2014
ABSTRACT

Cyber-attacks are considered the greatest domestic security threat in the United States and among the greatest international security threats. In the recent past, phishing and “denial of service” attacks are starting to become the most relevant forms of cyber intrusion, even while they can involve exploiting system vulnerabilities. Specifically, phishing attacks are reaching the level at which many large organizations are seriously considering purchasing technology and adopting mitigating practices. Therefore, data-driven decision support technology relating to mitigating or avoiding phishing and denial of service attacks are increasingly relevant.

A key element of the proposed approach is to treat management of phishing and denial of service cyber-attacks in a manner similar to quality management in production systems. Phishing control charting can become critical tools in both moving target (MT) decision-making and metric development, just as similar techniques are already in manufacturing and service operations. In this thesis, we explore the case study application of design for six sigma to create a proposed integrated system response to phishing email attacks.

Specifically, we used a CTQ flow diagram to clarify the relevance of CTQ characteristics including the number of phishing emails and the number of suspended
accounts. In Chapter 3, we describe the observed autocorrelations in time series corresponding to both CTQ characteristics. This motivated the use of moving centerline demerit (MCD) charts from a standard reference.

From developing an interrelationship diagram, we identified several important interrelationships including the relationship between phishing emails and organizational password policies. Clear seasonality was observed in the data suggesting that responsiveness in certain months (January and summer months) are months are more critical than other months.

Strong patterns were identified in that selected sub-populations were much more prone to being tricked by the emails and giving away their information. We omit the specific populations and organizational details for security reasons but the Pareto 80-20 rule was observed to be highly relevant in formulating system responses. We developed a simple charting method based on word frequencies to provide recent information summarizing the nature of phishing attacks. By integrating previous conclusions, we formulated a recommended system response that targets sub-populations, uses the proposed text series charts, and actually reduces password changing requirements on several sub-populations.
To my Parents, Mohammad and Sumayya, who have raised me to be the person I am today and because whatever I am is due to their hard work, prays, and love.

To my siblings, Raed, Hisham and Nidaa, who are my first best friends in life and best supporters.

To my best friends, Zeina and Wala’a, who are never too busy to encourage me and give me good advices.
ACKNOWLEDGMENTS

I would like to express my gratitude to my Advisor, Dr. Theodore Allen, for his generous advice and guidance through my master degree study at the Ohio State University. This thesis could not been completed without his generous and professional collaboration. The key results here are co-authored with him. I would also thank Dr. Cathy Xia, for her constructive comments and recommendations. My gratitude is also extended to Dr. Anthony Afful-Dadzie for his help and instructions.

Moreover, I owe great debt of gratitude to the Mr. Steven Romig and Ms. Helen Patton for their patience and expert support.
VITA

Jan., 2006 .................................................................B.S. Industrial Engineering, University of Jordan, Jordan
Jan., 2006 to July, 2012 ....................................Consultant, TAG Consulting Amman, Jordan
Dec., 2012 to present .........................................Graduate Research and Teaching Associate, Department of Integrated and Systems Engineering, The Ohio State University

Publications


FIELDS OF STUDY

Major Field: Industrial and Systems Engineering

Primary Area: Quality and Statistic Engineering

Secondary Area: Operation Research
# TABLE OF CONTENTS

ABSTRACT ........................................................................................................................................... ii
ACKNOWLEDGMENTS .................................................................................................................... v
VITA .................................................................................................................................................. vi
TABLE OF CONTENTS ...................................................................................................................... ix
LIST OF TABLES ............................................................................................................................... xi
LIST OF FIGURES ............................................................................................................................. xii

## Chapter 1 Introduction .................................................................................................................... 1

1.1 Plan .............................................................................................................................................. 1
1.2 Problem Statements and Outline ................................................................................................. 3
1.3 References .................................................................................................................................. 4

## Chapter 2 Background Quality Methods and Concepts ............................................................... 6

2.1 Introduction ................................................................................................................................. 6
2.2 Phishing Datasets ....................................................................................................................... 7
2.3 Relevant Cyber Monitoring Literature ...................................................................................... 8
2.4 Description of Control Chart Methods ..................................................................................... 11
2.5 References .................................................................................................................................. 13

## Chapter 3 Reducing The Number of Suspended Accounts From Phishing Attacks .................. 16

3.1 Introduction ................................................................................................................................. 16
3.1.1 Problem ............................................................................................................................ 17
3.1.2 Approach .......................................................................................................................... 17
3.1.3 Results .............................................................................................................................. 18
3.1.4 Design For Six Sigma ....................................................................................................... 18
3.2 Define .......................................................................................................................................... 18
3.1 Measure ...................................................................................................................................... 22
3.1.1 Autocorrelation Evaluation for Chart Selection ................................................................. 22
3.1.2 Moving Centerline Demerit Chart ..................................................................................... 24
3.2 Analyze ....................................................................................................................................... 26
3.2.1 Interrelationship Diagram ............................................................................................... 27
LIST OF TABLES

Table 2.1. Eight phishing emails from the phishing corpus (2014).................................9
Table 3.1. Performance indicator (PI) and key performance indicator (KPI) for 27
months........................................................................................................................................21
Table 3.2. The AR(1) parameters for the three data set #1......................................................24
LIST OF FIGURES

Figure 2.1 Depiction of a control chart with the reference population (distribution of the charted quantity if there are no assignable causes) ..................................................12
Figure 3.1 Critical to Quality (CTQ) characteristics flow down. ......................................20
Figure 3.2 Numbers of phishing emails and suspended accounts by year..........................21
Figure 3.3 (a) Autocorrelation function and (b) partial autocorrelation function for the number of phishing emails by month.................................................................23
Figure 3.4 (a) Autocorrelation function and (b) partial autocorrelation function for the number of accounts suspended by month. ...............................................................23
Figure 3.5 MCD control chart for counts of phishing emails. ............................................25
Figure 3.6 MCD control chart for counts of suspended accounts ......................................26
Figure 3.7 Interrelationship diagram for phishing emails ..................................................28
Figure 3.8 Plot of counts of phishing emails by month in the year ..................................28
Figure 3.9 Pareto chart of counts of suspended accounts by type of stakeholder ..............29
Figure 3.10 Proposed procedure to generate “word frequency series” charts ..................32
Figure 3.11 Word frequency series chart for three months of phishing emails ...............33
CHAPTER 1

INTRODUCTION

1.1 Plan

Phishing emails are weaknesses that potential hackers can exploit on devices ranging from personal computers to personal mobiles. Phishing is a relatively new internet crime in comparison to viruses and hacking, but it is becoming increasingly common. Its rampant occurrences and technique advancements are posing big challenges for researchers in both academia and the industry (Purkait, 2012). EMC reported that phishing remains an ominous threat to consumers and businesses around the world. 2013 has proven to be yet another record year in the number of phishing attacks launched globally. With nearly 450,000 attacks and record estimated losses of over USD $5.9 billion (EMC Report, 2013). As we mark the 10th annual National Cyber Security Awareness, the most common and effective cyber-attack method is spear phishing (Hawthorn, 2013). Clarke (2012) reported that cyber-attacks currently are or soon will be considered the number one domestic security threat by the United States Federal Bureau of Investigation, greater than terrorism. Similarly, Clarke and Knake (2010) and others reported that the United States Department of Defense considered cyber warfare and intrusions to be among the type five international security threats.
Many view phishing and cyber threats as being related primarily to computer science and electrical engineering. However, there are many “enterprise-level” or “system-level” responses that can mitigate or even eliminate threats. These include educating the populations of system stakeholders who are prone to phishing attacks about their nature and what to expect.

Part of the issue, in practice, that the locations of people and devices that can be attacked is so widespread. Derek (2011) called cyber security the “everywhere threat” partly because computers are already woven into all of our production, delivery, and usage systems. Industrial engineering and operations research (IEOR) are an area of research and practice related to making systems more efficient (Salvendy, 2007). Despite industrial and operations engineers constituting the third largest population of engineers in the United State according to the Department of Labor, it might be said that IEOR receives relatively little attention among policy makers and is not associated with cyber security among the general public. Current, United States laws require only a “reasonable effort” to defend against phishing and cyber-attacks (National Strategy to Secure Cyberspace, 2003). These vague rules might be caused by a lack of awareness as to how IEOR techniques related to quality engineering address similar evaluation and monitoring challenges in other contexts.

Data on phishing emails and cyber vulnerabilities are difficult to obtain partly because organizations are hesitant to reveal their own weaknesses (Chang, Jain, Slade, and Tsao, 1999). Therefore, confronting data limitations is a major challenge if IEOR techniques are to be applied to support systems level decision-making related to cyber vulnerabilities.
Another important issue related to phishing and cyber vulnerabilities is their exponential growth (Alhazmi and Malaiya, 2005). This growth clearly complicates the evaluation of the quality level of local responses because it might seem appropriate to expect them to fall behind in train people to identify and avoid phishing messages.

The goals of this thesis include investigating the relevance of quality engineering and operations research (IEOR) techniques to combat the phishing emails threat. As a tangential issue, we seek to create a simple charting method to help populations prone to phishing attacks become better prepared by viewing, at-a-glance, the nature of the recent attacks.

1.2 Problem Statements and Outline

This thesis will address the following problems.

1. What are the potential critical to quality (CTQ) measures that an organization can use to measure its response level to phishing attacks?

2. What is appropriate control charting technique to establish the quality level of the system phishing response that addresses the nature of the available data which could have autocorrelation?

3. What are the key interrelationships in the system that can be exploited to improve outcomes for stakeholders?

4. Are there patterns in the incidence of phishing emails that can be exploited in designing the system response?
5. Are there sub-populations of stakeholders who are more prone to phishing emails that the system response can focus on to improve the quality level?

6. Can we develop a data-driven charting method to help educate the selected sub-population so that they are more aware of the nature of recent phishing scams?

7. Can a data-supported standard operating procedure (SOP) be developed to create an integrated system for improving organizational response to phishing emails?

Once the above questions can be answered, a follow-up to this thesis involves recruiting ideas and support including “verification of concept” from the administrators in the chosen case study organization. The remainder of this thesis is organized as follows. Chapter 2 reviews literature and describes basic technology including control charts to provide background for non-quality experts. Chapter 3 addresses the problem statements in the form of a case study using the design for six sigma (DFSS) organization (Allen, 2010, pp. 511-518). Chapter 4 collects the solutions to the problem statements as conclusions.

1.3 References


CHAPTER 2

BACKGROUND QUALITY METHODS AND CONCEPTS

2.1 Introduction

Cyber-attacks are considered the greatest domestic security threat in the United States by the Federal Bureau of Investigation and among the top four international security threats by the Department of Defense (Clarke, 2012 and Clarke and Knake, 2010). Some 92 percent of targeted attacks in 2012 started with spear phishing, according to research by Trend Micro (Hawthorn, 2013). A study of 51 companies in the United States about the financial impact, customer turnover, and preventive solutions related to breaches of sensitive information concluded that (on average) organizational costs of a data breach in 2010 increased to $7.2 million, up 7 percent from $6.8 million in 2009 (Ponemon Institute, 2011). 2013 has proven to be yet another record year in the number of phishing attacks launched globally. With nearly 450,000 attacks and record estimated losses of over USD $5.9 billion (EMC Report, 2013)

In the recent past, more than 90% of actual attacks have exploited known vulnerabilities such that technologies which could have prevented the attack were easily
available but not applied (Cockburn, 2009 and Legard, 2002). Yet, according to Clarke and Knake (2010), phishing and “denial of service” attacks are starting to become the most relevant forms of cyber intrusion, even while they can involve exploiting system vulnerabilities. Specifically, denial attacks are reaching the level at which many large organizations are seriously considering purchasing technology and adopting mitigating practices. Therefore, data-driven decision support technology relating to mitigating or avoiding phishing and denial of service attacks are increasingly relevant.

A key element of the proposed approach is to treat management of phishing and denial of service cyber-attacks in a manner similar to quality management in production systems. Like maintenance problems and defects in production, phishing and adversarial attacks are negative events that occur sporadically. Phishing control charting can become critical tools in both moving target (MT) decision-making and metric development, just as similar techniques are already in manufacturing and service operations.

2.2 Phishing Datasets

In this research, we have used three data sets for phishing emails; the first data set is 40 phishing sent to individual account in 2005. The second data set is emails sent to big size individuals working inside large organization between 2011 and 2013, the needed information from this data set are the number of phishing emails received and the number of suspended accounts. The third data set is also coming from the same large organization but for in data set two but it is for year 2014, the needed information from this data set
are the number of phishing emails received and the emails’ contents (Email subject and body).

### 2.3 Relevant Cyber Monitoring Literature

Previous authors have developed monitoring techniques relating to cyber data but based on different sources and/or different objectives. For example, Ahmed, Al-Shaer, and Khan (2008) and Abedin, Nessa, and Al-Shaer (2006) both proposed novel rating metrics relating to cost data, current and past vulnerabilities, and the probability of an attack. However, if the attack probability was constant at 0 or 1, their methods would provide little insight about system changes and whether anything unusual or assignable was occurring. Furthermore, the data requirements for these rating metrics exceed what is in a typical vulnerability report or phishing dataset and include costs that are generally difficult to estimate (Dowdy, 2012).

In relation to phishing emails, denial of service attacks, or cyber vulnerabilities, there are different levels of severity. For example, a phishing email in a spam folder is much less of a negative event than a phishing email in an inbox. Also, phishing that succeeds on a critical host is much more severe than phishing on an ordinary host. Weightings of counts or “demerits” and the associated “demerit charting” techniques are potentially relevant (e.g., see Nembhard and Nembhard, 2000).

However, unlike in manufacturing, the same negative phishing event can identically occur on separate days because the adversary involved resends the same email. For example, Table 2.1 shows actual phishing emails (2014, phishingcorpus). See
the two identical emails supposedly from Southtrust Bank. Also, the hosts (or units) with cyber vulnerabilities (or nonconformities) are not newly generated each period. Instead, these hosts might be personal computers which are used for multiple time periods and might likely have the same vulnerabilities for an extended time. On-going “patching” eliminates a fraction of the vulnerabilities each month, but far fewer than 100%. These occurrences particular to cyber security induce high levels of “autocorrelation” or correlation in period-to-period counts.

<table>
<thead>
<tr>
<th>Date</th>
<th>Subject</th>
<th>Body</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/12/2005</td>
<td>Update Your Account Information</td>
<td>We are glad to inform you, that our bank has a new security system. The new updated technology will ensure the security of your payments through our bank. Hoping you understand that we are doing this for your own safety we suggest you update your information, to maintain your account updated.</td>
</tr>
<tr>
<td>6/13/2005</td>
<td>Security Update</td>
<td>Please follow this link to verify security update installation.</td>
</tr>
<tr>
<td>6/16/2005</td>
<td>IMPORTANT ACCOUNT NOTICE FROM SOUTHTRUST BANK</td>
<td>This is a multi-part message in MIME format. In 1841 stars battle in the Tour de France in 1872 in 1923.</td>
</tr>
<tr>
<td>6/26/2005</td>
<td>eBay account verification!</td>
<td>After fraud complaints from the eBay members, the eBay Inc. had developed a security program against the fraudulent attempts of accounts hefts. Please click the link below and sign in into your account: We are performing maintenance, which may interfere with access to your Online Services. Due to these technical updates your online account has been flagged and we …To Confirm Your Identity click the link below…</td>
</tr>
<tr>
<td>6/26/2005</td>
<td>KeyBank Customer Confirm Your Identity</td>
<td>We recently received a report of unauthorized credit card use associated with this account. As a precaution, we have limited …please visit the Resolution Center by following the link below: We recently have determined that different computers have logged into…please follow the link below:…</td>
</tr>
</tbody>
</table>

Table 2.1. Eight phishing emails from the phishing corpus (2014).
Autocorrelation can cause false alarms for certain types of control charts and/or worsen their ability to detect assignable causes (Montgomery and Mastrangelo, 1991, and Loredo, Jearkpaporn, and Borror, 2002). Yet, among the most desirable approaches in the published literature include methods from Runger and Willemain (1995) who recommend using batch sizes such that detection with levels of autocorrelation of 0.78 is not possible with fewer than 20 periods. With each period being 1 week, 20 weeks is almost one half of a year making the methods inadequate for calling attention to urgent problems such as the one that occurred at Target in late 2013.

An additional complication is that phishing and vulnerabilities are influenced by external causes including continual discoveries of new vulnerabilities for the software in use. These phenomena cause an increase in vulnerability counts over time on many systems (Alhazmi and Malaiya, 2005).

Despite the fact that many of the relevant methods proposed in the past have unacceptable responsiveness (“average run lengths”) and are potentially not adapted to trending external environments, it is helpful to review the associated models to clarify the foundation for new methods. Charting based on autoregressive moving average modeling seeks to eliminate the negative effects of autocorrelation and trending because the model residuals are generally uncorrelated and de-trended (Montgomery and Mastrangelo, 1991, and Runger and Willemain, 1995). A possible benefit for autoregressive (AR) moving average residual charting is simplicity because, unlike regression residual charting, there is no need to involve data about worldwide vulnerabilities or local patching activities. Perhaps the simplest of the relevant schemes is based on the first autoregressive or “AR(1)” model. Authors have noted the ability of such approaches to address
autocorrelation as well as underlying trends (Runger and Willemain, 1995). An important purpose of the proposed research relates to “demerit difference” charting methods which are similar to AR(1) residual charts but might seem even simpler and tailored to charting cyber vulnerabilities. Once the residuals or period-to-period differences are derived using any of these methods, “individuals” charting methods from Alwan and Robert (1988) can be applied for monitoring (Loredo, Jearkpaporn, and Borror, 2002 and Runger and Willemain, 1995).

### 2.4 Description of Control Chart Methods

In general, statistical process control has been proven in manufacturing to be an effective method for improving a firm's quality and productivity (Saniga, 1989). Perhaps the primary tool of statistical process control is the control chart (Mcgourty and Swart, 1998). The charted quantities in control charts are often called “quality characteristics”. The control chart is a graphical display of quality characteristics used for monitoring and system evaluation. Control charts were introduced by Shewhart in the 1920s while working for Western Electric and Bell Labs and, since then, they have been routinely used in manufacturing. For detailed descriptions of these charts and extensive annotated examples, see Juran and Gryna (1999), Montgomery (2008), and Allen (2010).

In general, a control chart contains a center line (CL) that represents the mean value for the in-control process of the charted statistic, which could be the average value of a “subgroup” or an individual value. Subgroups are sets of observations that are generally chosen to be representative of performance during a time period.
Two other horizontal lines, called the upper control limit (UCL) and the lower control limit (LCL) are also shown on the chart. These control limits are chosen so that, if there is nothing unusual shifting the process, the charted quantities will usually remain between the limits. Conversely, if there is an assignable cause shifting the process, a signal will likely occur because the charted quantity will go outside the control limits.

Figure 2.1 illustrates the related concepts including charted quantities outside the limits representing “out-of-control” signals.

Note that assignable causes sometimes require the attention of local authority or might simply indicate mistakes in the data collection system which could make all assessments misleading.

Also, the overall quality level of the process might not relate in a simple way to monitoring using control charts because the monitoring intent is primarily for the
identification of assignable causes that might be fixable by local authority, e.g., the instructor or department chair, without major investment. The chart in Figure 2.1 could hypothetically indicate that there might be an assignable cause that affected the last two subgroups plotted (e.g., an instructor might need assistance).

Alternative types of control charts have been reviewed in Leydens et al. (2004). The most popularly used one is from Shewhart (1931). Often, in Shewhart charting, the subgroups include only 4 or 5 data points. For example, an academic program might randomly sample five students and pay them to take a test to obtain a subgroup for program evaluation. In general, so-called “three sigma” control limits are used so that the chance that a signal will signal that the process is out-of-control wrongly is approximately 0.0026. Shewhart charting actually involves making two separate charts of the subgroup average value and the range of observations.

2.5 References


CHAPTER 3

REDUCING THE NUMBER OF SUSPENDED ACCOUNTS FROM PHISHING ATTACKS

3.1 Introduction

Cyber-crime worldwide is a massive problem and growing more serious. The Center for Strategic and Internal Studies report (2013) put global costs at up to $500B per year. Individual successful intrusions cost millions of dollars on average according to Ponemon (2010). Nelson (2014) describes many of the challenges and cites President Obama for saying that cybercrime is one of the most serious economic and national security threats faced by the U.S. Clarke and Knake (2010) and Clark (2012) discuss many types of threats and conclude that so-called “phishing” emails are likely more effective than other types of exploits and pose arguably the greatest security threat in the near future. Phishing attacks relate to emails asking for click-through and account information. The obtained account information can be directly exploited to gain privileges, steal intellectual property, launch attacks from compromised accounts, and even change the targets back account information to steal direct deposits.
Here we focus on the roles for quality technology in addressing threats from phishing attacks. This contrasts with Afful-Dadzie and Allen (in press) which focused on vulnerabilities which accumulate on hosts and computers through usage. Recent experiences at Target and other major companies remind us that there can be interactions between phishing email attacks and vulnerabilities already on host computers which have not been patched or repaired.

3.1.1 Problem

A large organization is facing serious security problems: stakeholders are being attacked phishing emails and a fraction of them are giving away personal account information. Further, a fraction of the compromised accounts are becoming sources for further phishing attacks and being suspended by the organization, causing losses of productivity and good will.

3.1.2 Approach

We investigated 27 months of reported phishing email counts and 2,446 actual emails (text) from the most recent four months. We also interviewed experts from the organization and developed a text-based charting technique called “word frequency time series” charting. Using a design for six sigma (DFSS) approach, we designed a system for reducing the effectiveness of phishing emails and the need for suspending accounts.
3.1.3 Results

It is shown that specific populations among organizational stakeholders are particularly prone to phishing email attacks. Therefore, the proposed system focuses on those populations. A recommended benefit for stakeholders not in the prone populations is a reduction in the frequency of required password updates.

3.1.4 Design For Six Sigma

Standard Design for Six Sigma employs a so-called DMADV roadmap (Allen, 2010). It involves the five phases: define (D), measure (M), analyze (A), Design (D), and Verify (V). This roadmap is used to design from scratch a new system such as the integrated phishing response system which is the primary objective here. In each the phases, statistical quality control and engineering techniques were applied such as control charts and interrelationship diagrams.

3.2 Define

In this phase, we seek to define the objective of the system in terms of measurable characteristic values and determine objectives for these measures. A common technique to identify critical to quality characteristics (CTQ) or system outputs is the CTQ flowdown diagram (Does, Vermaat, Verver, Bisgaard, and Heuvel (2009).

The primary stakeholder in our case study is the sponsoring organization. For the purpose of protecting security, we omit the identity of this organization which could be a
private company, a portion of a state or federal government, a hospital, or a university. The information flow starts externally from this organization as represented in the CTQ flow diagram in Figure 3.1 by the “attacker” in upper left-hand-corner. The attacker sends emails to targets who are stakeholders of the organization, e.g., employees, patients, or students. The “*” in Figure 3.1 indicates that the raw emails to all stakeholders may not be easily obtainable but, in our case, an on-going stream of voluntarily forwarded phishing emails is a critical information source.

A percentage of the targets respond by following phishing hyperlinks to websites. Then, these unfortunate individuals proceed to give their confidential account information to the attacker. One aspect of this system is that the number of compromised individuals is generally not easily quantities by organizational officers. However, if the attacker uses the compromised accounts to launch further attacks on other targets or create a fault condition in the intrusion detection system of the organization, the employer will generally suspend the compromised accounts. Because this suspension causes the target distress and because it is a symptom of system failure, we propose that the number of suspended accounts is the key performance indicator (KPI) of the system. Further, while the incidence of phishing emails is largely uncontrollable by the organizational administrators, a non-negligible portion of these emails derives from the compromised accounts. Therefore, the number of phishing emails forwarded to the information office is itself a performance indicator (PI).

We did not have information about compromised bank accounts or information about intrusions other than the number of suspended accounts. In other situations, these
data sources might be available and permit additional key performance indicators to be identified.

Figure 3.1 Critical to Quality (CTQ) characteristics flow down.

Our team was given access to 27 months of count data summarizing the KPI and PI values as shown in Figure 3.2 and Table 3.1. The reported numbers were only a tiny fraction of all phish received by stakeholders of the organization. Moreover, not all of the emails forwarded were actual phishing emails. For simplicity, we take the number of
forwarded emails as the PI and and refer to all as phishing emails even while a fraction were mis-reported.

![Figure 3.2 Numbers of phishing emails and suspended accounts by year.](image)

<table>
<thead>
<tr>
<th>Period</th>
<th>Period Start Date</th>
<th>Phishing Count</th>
<th>Accounts Suspended</th>
<th>Period</th>
<th>Period Start Date</th>
<th>Phishing Count</th>
<th>Accounts Suspended</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10/2011</td>
<td>209</td>
<td>11</td>
<td>15</td>
<td>12/2012</td>
<td>171</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>11/2011</td>
<td>185</td>
<td>12</td>
<td>16</td>
<td>1/2013</td>
<td>245</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>12/2011</td>
<td>92</td>
<td>5</td>
<td>17</td>
<td>2/2013</td>
<td>371</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>1/2012</td>
<td>397</td>
<td>17</td>
<td>18</td>
<td>3/2013</td>
<td>196</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>2/2012</td>
<td>259</td>
<td>31</td>
<td>19</td>
<td>4/2013</td>
<td>325</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>3/2012</td>
<td>205</td>
<td>9</td>
<td>20</td>
<td>5/2013</td>
<td>359</td>
<td>17</td>
</tr>
<tr>
<td>7</td>
<td>4/2012</td>
<td>130</td>
<td>33</td>
<td>21</td>
<td>6/2013</td>
<td>256</td>
<td>5</td>
</tr>
<tr>
<td>8</td>
<td>5/2012</td>
<td>77</td>
<td>0</td>
<td>22</td>
<td>7/2013</td>
<td>310</td>
<td>18</td>
</tr>
<tr>
<td>9</td>
<td>6/2012</td>
<td>83</td>
<td>2</td>
<td>23</td>
<td>8/2013</td>
<td>244</td>
<td>78</td>
</tr>
<tr>
<td>10</td>
<td>07/2012</td>
<td>47</td>
<td>0</td>
<td>24</td>
<td>9/2013</td>
<td>232</td>
<td>42</td>
</tr>
<tr>
<td>11</td>
<td>8/2012</td>
<td>77</td>
<td>1</td>
<td>25</td>
<td>10/2013</td>
<td>125</td>
<td>48</td>
</tr>
<tr>
<td>12</td>
<td>9/2012</td>
<td>146</td>
<td>0</td>
<td>26</td>
<td>11/2013</td>
<td>137</td>
<td>68</td>
</tr>
<tr>
<td>13</td>
<td>10/2012</td>
<td>234</td>
<td>4</td>
<td>27</td>
<td>12/2013</td>
<td>131</td>
<td>19</td>
</tr>
<tr>
<td>14</td>
<td>11/2012</td>
<td>243</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 3.1. Performance indicator (PI) and key performance indicator (KPI) for 27 months.
3.1 Measure

Our measure phase involves evaluating the system quality using statistical control charting and process capability. Through statistical control charting (see Section 2.4) data that is associated with assignable causes which were permanently addressed are removed since it is often regarded as unfair to include these data in system measurements. For chart selection, we first investigated the degree of autocorrelation in the associated time series.

3.1.1 Autocorrelation Evaluation for Chart Selection

By examining the autocorrelation function (ACF) and partial autocorrelation function (PACF), we determined that autocorrelation is significant for both the PI and KPI time series. Figure 3.3 shows the ACF and PACF for the PI (the number of phishing emails by month). Figure 3.4 shows the ACF and PACF for the KPI (the number of suspended accounts by month). Therefore, both time series can be approximately modeled using autoregressive models with a single autoregressive term (AR1).
Figure 3.3 (a) Autocorrelation function and (b) partial autocorrelation function for the number of phishing emails by month.

Figure 3.4 (a) Autocorrelation function and (b) partial autocorrelation function for the number of accounts suspended by month.
The autoregressive (AR) model of the demerits per host \( y_i \) with a single lag can be written for period \( i \):

\[
y_i = \mu + \varphi y_{i-1} + \epsilon_i
\]  

(1)

where \( \epsilon_i \) is assumed to be \( N(0, \sigma^2) \). While the same AR(1) model form in equation (1) applied to our case, the degree of autocorrelation represented by the coefficient \( \varphi \) and the mean \( \mu \) and standard deviation \( \sigma \) varied. Table 3.2 summarizes the coefficients for our case from AR(1) modeling.

<table>
<thead>
<tr>
<th></th>
<th>Phishing By Month</th>
<th>Accounts Suspended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coefficient ( \varphi )</td>
<td>0.465</td>
<td>0.523</td>
</tr>
<tr>
<td>Mean ( \mu )</td>
<td>203.20</td>
<td>16.48</td>
</tr>
<tr>
<td>Sigma ( \sigma )</td>
<td>93.83</td>
<td>20.49</td>
</tr>
</tbody>
</table>

Table 3.2. The AR(1) parameters for the three data set #1.

### 3.1.2 Moving Centerline Demerit Chart

In the previous section, we describe data indicating that both the KI and KPI time series are autocorrelated. Here, we describe the application of moving centerline demerit (MCD) charts from Nemhbad and Nemhbad (2000). While there are multiple options for control charting autocorrelated data, we select the MCD method for at two reasons. First, the charted quantity is the PI or KPI making the chart relatively easy to understand. Second, the MCD method is reasonably simple to implement since it involves only fitting a exponentially weighted moving average (EWMA) series and using that fitted series as the chart centerline. The exponentially weighted moving average (EWMA) model
includes only a single adjustable parameter, $\lambda$. Therefore, they based the centerline ($\text{CL}_i$) of their moving centerline demerit (MCD) chart on the following EWMA formula:

$$\text{CL}_i = \hat{y}_{i+1} = \lambda y_i + (1 - \lambda)\hat{y}_{i-1}$$

(2)

Then, the MCD control limits are:

$$\text{UCL}_{i+1}, \text{LCL}_{i+1} = \hat{y}_i \pm M\sigma$$

(3)

where $M$ is a potentially adjustable parameter given in Nembhard and Nembhard (2000), and $M = 3.0$. Nembhard and Nembhard (2000) proposed two procedures for estimating $\lambda$ and $\sigma$. The first which we use for illustration involves selecting $\lambda$ to minimize the sum of squared residuals and $\sigma$ as the root mean squared residual.

The values derived for $\lambda$ and $\sigma$ are also given in Table 3.2 for both the PI and KPI. The value for the PI (number of phishing emails) is $\lambda = 0.498$. The resulting MCD chart is given in Figure 3.5. The chart indicates only a single out-of-control subgroup. However, with no assignable cause found, we retain this data point and use the average number of emails as the process capability which is 203.2 emails per month.

![Figure 3.5 MCD control chart for counts of phishing emails.](image)
Similarly, the value for the KPI (number of suspended accounts) is \( \lambda = 0.282 \).

The resulting MCD chart is given in Figure 3.6. The chart shows no out-of-control signals. Therefore, we retain all the data and the average number of suspended accounts (16.5 per month) is our process capability.

![MCD control chart for counts of suspended accounts](image)

Figure 3.6 MCD control chart for counts of suspended accounts.

### 3.2 Analyze

The next phase of the DMADV is to analyze the process to identify relationships between controllable system inputs (Xs) and system outputs (Ys). We describe three analysis activities: the development of an interrelationship diagram, scatter plotting email counts by month, and Pareto charting suspended account numbers by target type. Each of these activities yielded insights. We then assembled these insights to develop an integrated system response in the design phase.
3.2.1 Interrelationship Diagram

By interviewing an expert from the organizations information office, the interrelationship diagram was generated. We brainstormed the system issues. We arranged the issues by type and systematically studied the interrelationships. Starting from the upper-left-hand corner of Figure 3.7, we learned that a significant fraction of all internet communication is spam email and a significant fraction of that is phishing email. Therefore, bandwidth is, to a limited extent, lost because of phishing. Also, spam filters often miss phishing emails because of their continual evolution filling inboxes. We also learned that the compromised accounts have, in rare instances, resulted in payrolls stolen as the attacker transfers the direct deposits away from the target.

Further, it has been reported that literally over 1 trillion of U.S. intellectual property is being stolen by foreign hackers, particularly in the People’s Republic of China. There was a reported instance in which a Chinese internet business literally used the access from a compromised account to provide arguably the main service to their Chinese customers. Interesting, the password renewals are related to compromised accounts. This follows because the primary reason for forcing timely password updating is that the updating process often uncovers the compromised accounts. Further, the targets are often upset at the organization for suspending their account even while they were the people tricked by the phishing email.
3.2.2 Scatter Plotting Numbers of Phishing Emails By Month

To understand how much a process varies from time to time in which the data experiences regular and predictable changes which recur every calendar year. Seasonality analysis conducted as shown in Figure 3.8. The analysis suggests that, there is a pattern that is correlated with the 4 months (July, August, September and October).
3.2.3 Pareto Charting Numbers of Suspended Accounts by Sub-Population

Figure 3.9 shows a Pareto chart of the numbers of suspended account by sub-population. We omit the details of this dataset for security reasons. Yet, sub-populations could relate to employee types or levels of seniority in a private corporation or patient types in a hospital. Interestingly perhaps, two sub-populations exhibited far greater than average susceptibility to phishing attacks. We believe that this concentration represents a significant opportunity to leverage existing resources in the integrated system response. This follows because there is a possibility of focusing attention on these (relatively) small populations while addressing over 80% of the suspended accounts.

![Pareto Chart of Holder Types](image)

Figure 3.9 Pareto chart of counts of suspended accounts by type of stakeholder.
3.3 Design

In the analysis phase, we uncovered the relationship between phishing and password renewal (Figure 3.7). In particular, if phishing attacks could be avoided, it might appropriate to reduce the intervals between required password renewals for at least some of the sub-populations. The standing renewal policy for the organizations was that all stakeholders must renew their passwords every 90 days and select so-called “strong” passwords. This policy generates widespread dissatisfaction and has been known anecdotally to backfire as select individuals pick weak but memorable passwords. We tentatively propose a system design in which individual not within the susceptible sub-populations are permitted 120 intervals (instead of 90) for renewals while the susceptible sub-populations remain at 90 day intervals. Also, we suggest greater publicity for the motivations behind renewal as many stakeholders are unaware of the reasons.

Also, the timing of the phishing arrivals potentially suggests a tailored response (Figure 3.8). We propose that additional educational materials prepare individuals within susceptible sub-populations both in late December and in late May. Such notices would precede the periods of high phishing email incidence.

Relating to the sub-populations most susceptible (Figure 3.9), we propose additional efforts to educate those individuals about the nature of the threat. As is typical, emails should urge those individuals to never give out their personal information as prompted by an email. Further, we suggest that providing non-trivial information about the nature of recent attacks might likely inspire behavioral changes. Next, we propose a
so-called “word frequency time series” charting method which attempts to familiarize the viewer with the recent content the concept of continually evolving phishing email threats.

3.3.1 Word Frequency Time Series

Our team only had access to approximately three months of actual email that had been referred to the information office. The previous emails had been destroyed by a standing policy. The dataset include 2,446 emails of which only 353 were either phishing emails or similar emails. The remaining 2,093 emails were from a known issue in which spam was repeatedly sent by a denial type attack. Removing those emails, we were able to tabulate the word counts and analyze these counts.

A standard “word cloud” seemed not appropriate since the spatial dimensions are generally random and only the word size has an interpretable meaning. To provide additional nontrivial information including about time evolution, we propose the method shown in Figure 3.10. A desirable property of the proposed method is that it is fairly easy to implement in that available free software (e.g., “wordle”) can be used for all the needed frequency counts.
1. Divide the overall corpus into sub-corpora by time.

2. Tabulate the most frequently used words in each period.

3. Tabulate for the words in step 2 the frequencies in the overall corpus.

4. List the words by frequency from Step 2 with font size inversely proportional to the frequencies in Step 3 for each period in a time sequence.

5. Use colors to distinguish between verbs, nouns and proper names, green, red and blue respectively.

Figure 3.10 Proposed procedure to generate “word frequency series” charts.

The result of applying the proposed method to our corpus is shown in Figure 3.11. We believe that emails from the information office to the susceptible subpopulations containing a brief description of the nature of phishing attacks and word frequency series charts such as Figure 3.11, but based on up-to-date data, are a key part of an integrated system response.
3.4 Verify

This thesis is not intended to offer a fully complete case study. An important objective for future research is to improve, verify with management, and implement an integrated system response to the phishing email threat. The objective of this work is largely to exemplify the possible benefits of applying quality and a systematic design for six sigma approach. For at least, the case study organization, we hope that the proposed integrated response described in the last section will be improved and implemented.
3.5 References


CHAPTER 4

CONCLUSIONS AND FUTURE WORK

4.1 Introduction

In this chapter, we review the problem statements and collect the answers from the preceding chapters. The main future work items is completing the design for six sigma (DFSS) case study and obtain verification and implementation from the case study organization mentioned in Chapter 3.

4.2 Conclusions

The problems addressed and solutions provided in this thesis are summarized as follows with all results derived in Chapter 3.

1. What are the potential critical to quality (CTQ) characteristics? We used a CTQ flow diagram to clarify the relevance of CTQ characteristics including the number of phishing emails and the number of suspended accounts.
2. What are appropriate control charting techniques for the identified characteristics? In Chapter 3, we described the observed autocorrelations in time series corresponding to both CTQ characteristics. This motivated the use of moving centerline demerit (MCD) charts from Nembhard and Nembhard (2000).

3. What are key interrelationships? From developing an interrelationship diagram, we identified several important interrelationships including the relationship between phishing emails and organizational password policies.

4. What are patterns in phishing email incidence? Clear seasonality was observed in the data suggesting that responsiveness in certain months (January and summer months) are months are more critical than other months.

5. What are patterns in sub-populations prone to phishing emails? Strong patterns were identified in that selected sub-populations were much more prone to being tricked by the emails and giving away their information. We omit the specific populations and organizational details for security reasons but the Pareto 80-20 rule was observed to be highly relevant in formulating system responses.

6. Can a data-driven charting method be developed to educate? We developed a simple charting method based on word frequencies to provide recent information summarizing the nature of phishing attacks.

7. Is there a recommended system response? By integrating previous conclusions, we formulated a recommended system response that targets sub-
populations, uses the proposed text series charts, and actually reduces password changing requirements on several populations.

4.3 References


REFERENCES


39


National Strategy to Secure Cyberspace (2003),


