Montana Tavern Times
Protecting Your Assets from Cyber Criminals – July 1, 2014
By Constantine Vorobetz
Investigator – Bozeman Office, Gambling Control Division

It goes without saying that in today's world running a small to medium sized business comes with many risks. Some of those are more prevalent than others. In this article (which will be a three part series) I want to bring to the reader's attention a threat that is on the rise to small businesses, and growing at such a rapid pace that yesterday's tactics and techniques to defend against such a threat, may be expired today or tomorrow.

This is the threat of the cybercriminal. I am sure many of you have read in the media recently regarding the breach of the Target Corporations customer information. This vendor breach exposed credit card and personal data on more than a 110 million consumers and so far has cost Target over a billion dollars. Cyber criminal's accessed this data using common techniques and tactics used in the cybercriminal industry.

I want to share with all of you how this breach occurred, why it matters to your industry/business, and share some simple steps you can take to protect your businesses from the same kind of threats.

The Breach

The space allocated for this article does not provide enough space to go into the many details involving the breach at the Target Corporation. However, there are many articles regarding the issue on the web, so feel free to dig around if you would like more details. To summarize the breach, we will have to visit a couple items that some of you may or may not be familiar with.

Investigators believe the source of the Target intrusion traces back to network credentials that Target had issued to **Fazio Mechanical**, a heating, air conditioning and refrigeration firm in Sharpsburg, Pa. that Target contracted with for services. Multiple sources close to the investigation reported to "*Kreb's on Security"* (Source: http://krebsonsecurity.com/tag/target-data-breach / 02/21/2014 at 0800 hrs.) that those credentials were stolen in an ***email - malware attack*** at Fazio. This breach began at least two (2) months before thieves started stealing credit card data from thousands of Target cash registers.

What is an ***email - malware attack***? It is a Malware-laced email phishing attack. What the heck is that? A *phishing* attack by definition is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. These communications claim to be from popular social web sites, auction sites, banks, online payment processors or IT administrators, and are commonly used to lure the end-user of an electronic device.

Phishing emails may contain links to websites that are infected with malware. *Malware*, short for malicious software, is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content,

and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software.

Phishing is typically carried out by email or instant messaging. It often directs end users of computer systems to enter details at a fake website that is almost identical to the legitimate one. Phishing is an example of social engineering techniques, which are techniques cybercriminals, use to deceive users of computer systems, and discover exploits of current web security technologies. I understand how overwhelming all of this may sound. The truth is, that is how most people feel when they hear about similar terms used in cyber security. The National Cyber Security Alliance reported that in 2013, about one in five small businesses experience cybercrime every year, and of those enterprises, 60 percent shut-down within the six months following the incident. The Target Corporation incident is not isolated. It's a large corporation that made some mistakes, so it makes the headlines.

Why should you care?

The truth is, small-businesses (SMB) are more likely to fall victim to these sorts of attacks seen in the Target breach incident. Small businesses as primary targets for cybercriminals were the case for many in 2013 (these are the ones that did not make the headlines). Many small-business owners still operate under the misconception that they are not attractive targets to cyber criminals because of their limited resources.

In 2013; Verizon Enterprise's: *2013 Data Breach Investigations Report* found that, in reality, data breaches at small businesses are common and are much more likely than those at large businesses to involve hacking (72% vs. 40% of incidents). Why? I am not certain there is a single exact reason behind these attacks on small-businesses. But a couple of reasons could be for the following:

Less security: An SMB is likely to have fewer security resources with which to protect its networks and systems than a large enterprise, meaning more chance of an attack succeeding and less chance of criminals being detected, identified, and prosecuted.

More money: An SMB is likely to have more money in its bank accounts than a consumer, and more likely to be moving money around (think wire transfers, vendor payments, customer payments). While there might not be a lot of profit left at the end of the month, the amount of money circulating through an SMB is greater than for the average consumer.

With so many services switching to the world of the internet, (online reporting, point of sale systems, application renewal, etc.) small businesses in the Liquor and Gambling Industry should also recognize that they will most likely become targets of cyber criminals. This trend will only continue in the future as the next phase of technology advances to "the internet of things", which is the integration of all the technology we use in our day to day lives. We as end-users will become much more integrated with our technology, which in return, will make us more likely to become victims of cybercrime.

Why would I go through the risk of robbing a casino at gunpoint? I can pay less than $500.00 for malware software that can skim a network for credit card information, and launch an automated phishing distribution from a zombie computer. These tactics combined provide the means for the average criminal to rob a casino without exposing themselves. The risk is minimal, the reward is high, and the cybercriminal can be in and out before they are ever detected. With today's tactics,

tools and techniques; the cybercriminal does not need to be computer scientist, or a technology expert. The items and instructions are openly available and sold for affordable rates.

What can I do?

Take some time and effort to learn how to protect yourselves and your businesses. In the next two installments of this series, I will provide some suggestions. These are things I have learned on my own; I am not a certified security expert. However, I am passionate about this problem and I feel that as a criminal investigator, that it is my responsibility to help you protect your small-business, and to help protect the industry we all value. If you want to do more, then research and hunt down some professional help. Of course I will always be available to answer questions and assist you all to the best of my ability.

END OF PART ONE

Protecting Your Assets From Cyber Criminals Part II

In our previous section we discussed some techniques that cybercriminals use to bypass your computer networks; we specifically discussed phishing/malware attacks. In part II and III of this series we will discuss some good security practices to help protect you, your business, and your customers. The Internet Security Alliance recommends the following practices for small-businesses to protect themselves from cyber criminals:

Use Strong Passwords and Change Them Regularly

Passwords are an easily implemented method of limiting access to your electronic work environment. Passwords that are harder to discover will discourage many kinds of intruders. Smaller businesses often have higher employee turnover rates, which increase the need to change the passwords regularly. Since you may not know if a password has been guessed, change it at least every six months and preferably every three months, and do not allow reuse of old passwords.

For each computer and service you use (online purchasing, for example), you should have a unique password. By not reusing a password, a compromise in one area will not open access to other areas. You should not write passwords down or share them with anyone. But if you do need to write them down, store the paper in a secure location such as a locked file cabinet (not under your keyboard where anyone can find them).

A password should be complicated so it cannot be easily guessed. Do not use dictionary words, names, or minor variations of these. Consider using a combination of letters, both upper and lowercase, numbers, and punctuation marks. Lengths can vary (a minimum of six characters; longer is better). Construct the password using a pattern so that you can remember it whenever you need it without having to write it down to jog your memory. Educate employees to always change default passwords and initial access passwords as soon as possible. Policies should be established to require strong passwords and mandate a frequency of change. Employees should be educated about the need for strong passwords as soon as they are hired and reminded to change them regularly.

Look Out for Email Attachments and Internet Download Modules

Educate all e-mail users to do the following:

1. Do not use the "preview" function for e-mail contents.
2. Do not open an attachment that the anti-virus software has indicated is malicious.
3. Do not open emails (delete them instead) from someone you do not know, especially if the subject line:
- Is blank or contains strings of letters and numbers that are nonsense
- Tells you of winning a contest you never entered or money you should claim
- Describes the details of a product that you might like
- Notifies you of a problem with instructions to install software on your machine

- Notifies you of a billing or account error for a service you do not use.

4. If you know the sender or decide to open the e-mail, check to make sure the contents along with the names of attachments and the subject line make sense. Set up your browser to alert you to Internet module downloading and do not accept them from sites you do not know, especially if email from an unknown recipient has sent you to the site. Delete and do not forward chain emails (similar to chain letters) and do not use the unsubscribe function for services to which you did not subscribe initially since this only alerts an attacker that an active address has been located and makes you a more valuable target.

Deactivate the use of java scripting and Active-X in your browser and only activate them temporarily for specific web pages. When you are considering buying a software program, look for a clear description of the program and its features and make sure the source of this information is reputable.

Install, Maintain, and Apply Anti-Virus Programs

Install anti-virus software on every machine and keep the signature files current through automatic or manual updates at least weekly. Renew the automatic update capability annually as required to maintain a current virus signature file on every machine.

Install and Use a Firewall

A firewall performs much the same job as a security guard at a public building. It examines the messages coming into your system from the Internet as well as the messages you send out. The firewall determines if these messages should continue on to their destination or be stopped. The firewall "guard" can greatly reduce the volume of unwanted and malicious messages allowed into your network, but it takes time and effort to set one up and maintain it. Firewalls can also prevent many forms of undesirable access to your network.

Remove Unused Software and User Accounts; Cleanout Replaced Equipment

Remove accounts for terminated employees when they leave. When firing someone, remove the computer access before notifying them and arrange for a monitor while they are on premise. Establish a policy that unneeded software not be installed on company computers (i.e. games, free download software, music players, etc.).

Establish a process for removing data on all computers hard drives when equipment is repurposed, discarded, donated, and sold. Use a utility program to remove all information by overwriting all available disk space. Uninstall software that is no longer in use and archive data files that are no longer used. The less clutter on the system the easier it will be to manage backups and keep software on the system at a current update level.

Establish Physical Access Controls for all Computer Equipment

No matter how good the passwords and security controls on the computer, laptop, or PDA, if someone else has physical access to it they can circumvent the security and use or destroy anything on the device. Electronic devices should not be left unattended inside or outside the office, especially while a user has an account logged on and active.

End of Section II

Protecting Your Assets From Cyber Criminals Part III

Last month we discussed some practices to help reduce the risk of cyber criminals infiltrating your system. In this last part of the series we will discuss other practices to reduce your risk.

Create Backups for Important Files, Folders, and Software

If an intruder corrupted your computer systems or destroyed software programs, files and folders on the system, could you continue to operate your business effectively? Will your insurance coverage compensate for the lost business of several days, while the computer systems are repaired, and information is rebuilt manually? Many general insurance policies no longer cover cyber losses.

Backups are another form of insurance to help you recover when an intruder attacks or a disaster such as fire or flood harms your technology environment. Copying files, folders, and software onto some other media (like a disk or CD) provides a source for recovery if it is needed. Manually creating copies can be tedious, and automated options are available. You may already have some of the content in another form, such as software programs that were initially loaded from CD.

Keep Current with Software Updates

Software vendors routinely provide updates (also called patches) to fix problems and enhance functionality within their products. In addition, many of these patches fix vulnerabilities that could be used by viruses and other attacks to harm your computer and its contents. By keeping software up-to-date, software malfunctions and opportunities for system compromise are minimized.

Implement Network Security with Access Control

Good access control is critical for wireless access since use of this type of connectivity is less visible. It is not uncommon for someone sitting in a car in the parking lot to be able to access an unsecured wireless network and jeopardize everything on the entire network. You may have a wireless or remote access (dial-in) connection to your network and not realize it, since many vendors install them to provide remote support capabilities. Point-of-sales devices and inventory devices communicate to central servers via wireless.

The more access restrictions you can legitimately place on your network using blocking capabilities within the firewall and other similar services, the easier it will be to keep it secure.

Limit Access to Sensitive and Confidential Data

When access to information cannot be tightly controlled, such as e-mail or a credit card transaction over the Internet, this information can be concealed through a mathematical process called encryption. Encryption transforms information from one form (readable text) to another (encrypted or scrambled text). The encrypted text appears to be gibberish and remains so for people who don’t have the formulas (encryption transformation scheme and the decryption keys) to turn the

encrypted text back into readable text. The encryption mechanism must be sufficiently complex or someone with electronic tools could guess the formulas and defeat the encryption.

Establish and Follow a Security Financial Risk Management Plan; Maintain Adequate Insurance Coverage.

In order to be effective, security must be consistently applied across the organization. For example, the use of very tight technology controls with lax or non-existent organizational security policies does not provide protection. The best way to validate your security is through the application of a security risk management methodology. In a structured sequence of activities, participants at multiple levels of the organization work together to devise a plan that makes sense for the needs of the organization based on its use of technology. To be comprehensive, this planning process must consider the following areas:

1. Security awareness and training for all technology users
2. Organizational security policies and regulations
3. Collaborative security management (partners, third-parties and contractors)
4. Contingency planning and disaster recovery
5. Physical security
6. Network and data security

In the rush of daily activities it is easy to overlook the need for such things as employee security training, contingency planning, and disaster recovery. You may not even be aware of the level of dependency your organization has developed on technology and the potential impact that a failure of one or more components will cause. By developing a security risk management plan, these dependencies will be highlighted and mitigation steps can be identified to reduce the potential impact of technology compromise or failure.

Get Technical Expertise and Outside Help When You Need It.

Because you have a business to run and technology security is not something you can afford to have consume all or most of your time, good technical assistance can be a valuable asset. Employees, friends, and family with a technical interest can help you get started, but you need someone with security training and experience to tie all of the individual activities together into a working security protection mechanism for your organization.

Further information on these steps can be found at Internet Security Alliance website: http://www.isalliance.org/. If you become a victim of cyber-crime, contact the Gambling Investigations Bureaus or your local Law Enforcement Agency for assistance.