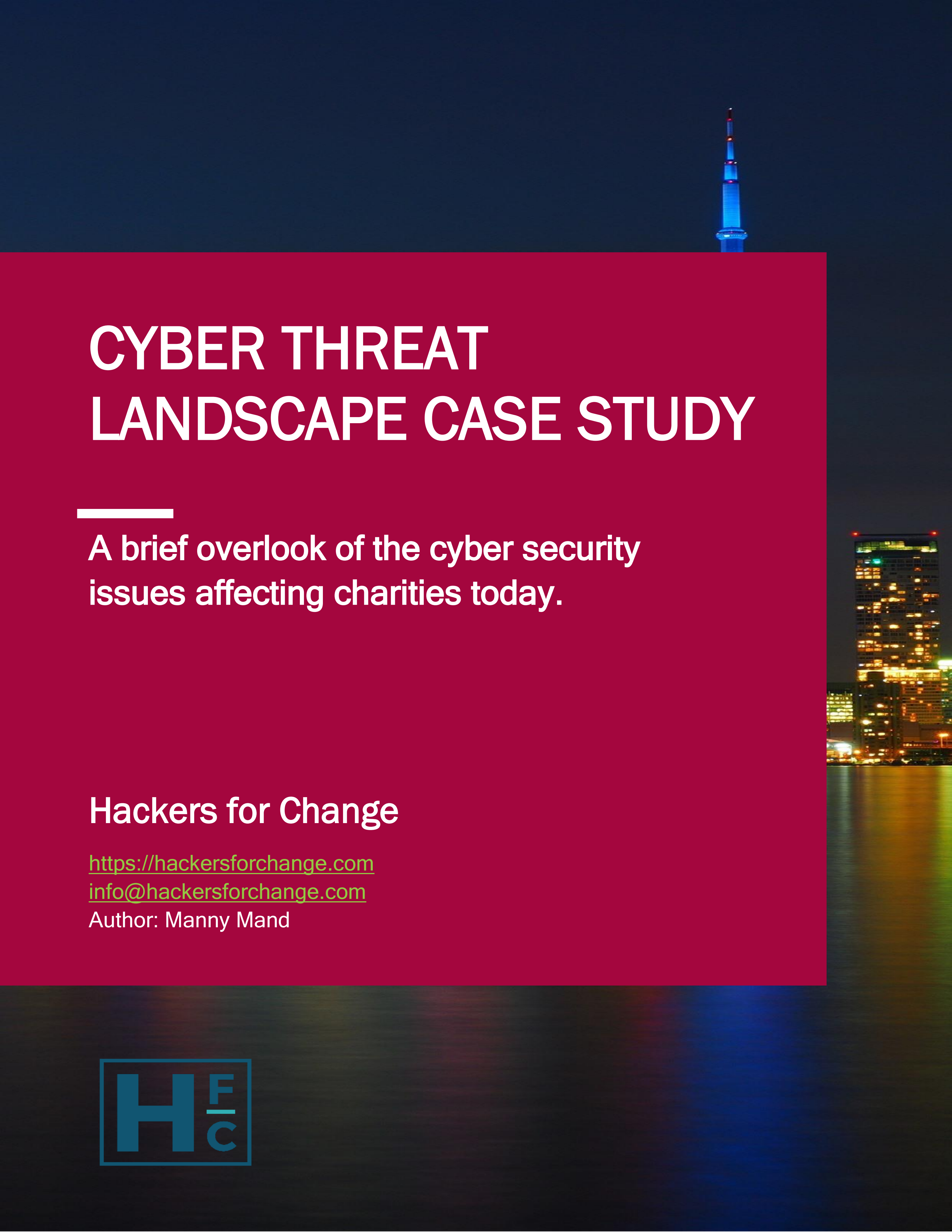


CYBER THREAT LANDSCAPE CASE STUDY

A brief overlook of the cyber security issues affecting charities today.

Hackers for Change

https://hackersforchange.com
info@hackersforchange.com
Author: Manny Mand

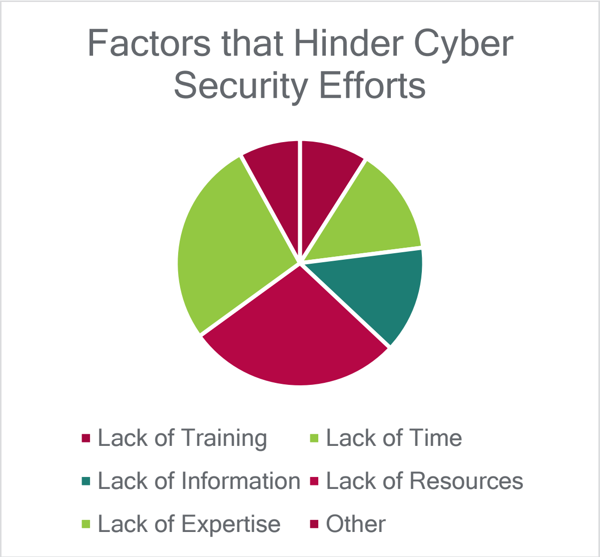
Threat Landscape Case Study

Introduction

In 2019 over 4.1 billion consumer records were compromised (Norton). There is an undeniable need for cyber security services to stay ahead of malicious hackers; to protect organizational and customer data. However, the issue is cyber security services are expensive and most small to medium charities/NPO's organizations do not have the financial resources to pay exorbitant amounts to secure their network. Hackers for Change is a not-for-profit organization that addresses this gap by rendering cyber security services for charitable organizations at a nominal fee. Services rendered by Hacker's for Change include assistance from industry experts and students getting relevant experience in their respective industry.

THREAT LANDSCAPE OVERVIEW

A Clark School study at the University of Maryland quantified that a cyber-attack occurs every 39 seconds. With the unprecedented amount of cyber-attacks, it is evident that there is an undeniable need for cyber security to safeguard sensitive information against hackers. With services rendered by security companies often too costly; this leaves small charitable organizations in a tough, and oftentimes insecure position. Hackers for Change intends to leverage its powerful volunteer network to offer low-cost cyber security services to the charities/non-profits allowing them to focus on maximizing their social impact.



The importance of cyber security can be grouped into three categories; customer protection, availability of data and reputation. Organizations may be held liable in the event of a data breach. Acts such as PIPEDA require certain industries (such as healthcare non-profit/charity ventures) to implement safeguards to protect their data. Successful cyber-attacks can also affect the availability of client facing services. In 2017 Little Red Door, a small US healthcare charity received an email from a group of hackers that had blocked access to client files and financial data and were demanding money for its release. The hackers were asking for

$43,000 USD in exchange for the data. As they did not pay the ransom it took them months rebuilding client data. Finally, reputational damage usually arises during cyber-attacks and there can be a severe loss of trust between the public and organizations. A study by DataBreachToday concluded that 54% of companies believe it can take 10 months to two years to restore an organization’s reputation after a data breach.

CHARITY CYBER ATTACK I - ST. JOHN AMBULANCE

Overview

St. John Ambulance is the UK's leading first aid charity. They provide training courses, advice, and volunteering opportunities related to first aid. In July 2019, a group of cyber criminals temporarily disabled their systems by installing ransomware on their server. A ransomware is a form of a malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the previously encrypted files. Information compromised included client names, invoice details and driving license data.

What went wrong?

An employee of the organization had fallen for a phishing email which installed ransomware on the St John Ambulance network. Phishing is a method of trying to gather personal information or infect a system with malware by using deceptive email techniques.

What went right?

St. John Ambulance had an effective incident response strategy which enabled them to recover from the attack in thirty minutes. On average the number of days a ransomware incident lasts is 16.2 days. St John's effective incident response strategy allowed them to recover quickly.

Post Mortem Evaluation

St. John Ambulance had an effective incident response which allowed them to recover quickly. Although they had a plan in place, The Global Cybersecurity Index (GCI) 2017 report revealed that 69% of non-profits/charities did not have a cyber security response plan in place. It is vital to have an effective cyber security plan to ensure your organization can recover from any incident. In addition to this, performing security awareness training can significantly reduce the risk of employees falling victim to phishing attacks.

Mitigation Strategies

St John Ambulance should have performed routinely cyber security awareness training to ensure the employees can identify and effectively respond to phishing attempts. Hackers for Change provides Security Awareness Training with interactive training to ensure your volunteers are prepared to deal with any cyber security threats.

CHARITY CYBER ATTACK II – PEOPLE INC.

Overview

People Inc. is Western New York’s leading non-profit human services agency. In 2019 nearly one thousand current and former clients of People Inc. have been notified of a security breach which exposed their personal and health information. The attacker gained access to personal private information such as social security numbers, drivers licenses and government information.

What went wrong?

An employee of the organization had their email account hacked. This led to a hacker gaining access to loads of sensitive information. There are a number of ways an attacker could have gotten this employee’s information, such as finding the information in previous data breaches or utilizing a brute force technique to ascertain the password. Hackers for Change helps mitigate this issue by searching for all employee information across the internet and the dark web. In addition to this, we review password policies to ensure brute force .

People Inc

Where your world opens up.

Post Mortem Evaluation

People Inc. did not have an effective policy that prevented the transmission of sensitive information over email. In addition to this, they did not have multi factor authentication configured which could have also prevented the unauthorized access of the email. From NTEN’s State of Nonprofit it reveals that 68.2% of respondents do not have documented policies and procedures for when they get attacked.

Mitigation Strategies

People Inc. should have had password policies in place as well as policies related to the transmission of sensitive information. Hackers for Change can provide policies tailored to password management, sensitive information handling, etc. In addition to this, we will set up secure mediums for you to safely exchange files over the internet.

CHARITY CYBER ATTACK III - SAVE THE CHILDREN

Overview

The Save the Children foundation was established to improve the lives of children through better education, health care, and economic opportunities. In December 2018 cyber criminals were able to steal over $1 million dollars of capital from the organization. The cyber criminals had compromised an email account and drafted a number of fake invoices which the charity approved. The money was sent to a company in Japan which was eventually dispersed by the cyber criminals.

What went wrong?

An employee of the organization had their email account hacked. This led to a hacker being able to draft a number of fake invoices that totaled more than 1 million dollars. There are a number of ways an attacker could have got this employees information such as finding the information in previous data breaches or brute forcing the password.

What went right?

Save the Children had cyber insurance in place which covered a large extent of the losses. They only ended up having to pay a little over 100,000 as the insurance had covered the rest.

Post Mortem Evaluation

The Save the Children foundation did not have any password policies or secure configuration settings enabled on their email provider. This resulted in the loss of $1 million dollars which funded cyber criminals.

Mitigation Strategies

The Save the Children foundation should have had password policies in place as well as policies related to the transmission of sensitive information. Hackers for Change can provide policies tailored to password management, sensitive information handling, etc. In addition to this, we will set up secure mediums for you to safely exchange files over the internet.