ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

Cybersecurity in Non-Profit and Non-Governmental Organizations

Results of a Self-Report Web-Based Cyber Security Survey with Non-Profit and Non-Government Organizations

February 2017

Authors:

Stan Mierzwa (ICIT Fellow and Director, Information Technology, Population Council)

James Scott (Senior Fellow, Institute for Critical Infrastructure Technology)

Contents

Cybersecurity in Non-Profit and Non-Governmental Organizations

February 2017

Authors
Stan Mierzwa, ICIT Fellow and Director, Information Technology, Population Council
James Scott, Sr. Fellow, ICIT

Upcoming Event

Join us at the 2017 Critical Infrastructure Forum to learn about the findings in this and other ICIT research publications.

The 2017
Critical Infrastructure Forum
Rise of The Machines
June 7, 2017
The Four Seasons - Washington D.C.

www.ICITForum.org

Visit the ICIT Library to view additional research and publications

https://www.amazon.com/James-Scott/e/B01IPLQKSQ/ref=dp_byline_cont_pop_ebooks_1

Abstract

Non-Profit and Non-Government Organizations (NGOs) rely greatly on the use of information technology for both their operations and innovative strategic program initiatives. In a sense, they are no different than any small, medium or large-scale enterprise with regard to computing. Keeping information confidential and free from integrity and privacy challenges as well as ensuring their systems are available are as important to a Non-Profit and NGO as they are to any other entity and because of this they need to ensure they are protecting themselves, staff and systems against cybersecurity vulnerabilities. This paper will discuss results from a survey conducted with international NGOs and Non-Profit organizations, including what type of cybersecurity programs, staffing, controls, and assessments are being employed, planned or considered. In addition, several modest suggestions to consider are provided to help the Non-Profit and NGO sector better prepare themselves to protect their organizations against cybersecurity threats within the broad computing paradigm found.

Introduction

The for-profit, healthcare and government sector have available to them industry specific guidelines to follow specific to information security. Many of these guidelines are provided by larger governing bodies, such as the National Institute of Standards and Technology, which has issued the 800-53, NIST Cybersecurity Framework and other 800-series special publications, the International Standards Organization (ISO) through its 27001:2013 as well as other institutes which provide subject matter expertise. In certain industries, such as banking and healthcare, many of the guidelines are requirements that must be fulfilled. For example, US government organizations need to comply with the Federal Information Systems Management Act (FISMA), which includes protection of government-owned information technology and systems. Executive Order 13587, issued by the United States President in 2011 mandated that every U.S. government agency that has classified information – in effect, all of them – must have an insider threat program in place [1]. This mandate was followed by the Cybersecurity Strategy and Implementation Plan in late 2015. The guidelines that do apply or could be implemented (such as NIST 800-53) are all often quite long and comprehensive, and complicated for small and medium-sized business (SMB), Non-Profits, and NGOs to implement. Non-Profits, NGOs and others would greatly benefit from simplifications or short implementation summaries of NIST and other frameworks. Larger organizations, outside the Non-Profit sector, often have more resources, which may include specialized departments that focus on cybersecurity. Organizations with Non-Profit budgets may not have the funding available to create information technology and/or controls assessment units to work towards better protection, and in many cases may not have staff in their IT unit who can provide some cybersecurity specialty functions. A primary goal for a Non-Profit is to exist to serve specific goals, work towards a mission, and focus efforts on obtaining funding and reducing costs. Ownership, management, and staff all work towards these goals, as their entire incentive structure is built on them. Unfortunately, good cybersecurity generally does not accomplish or align with these goals [10]. Without a true cyber security strategy, it may only be a matter of time before an organization becomes victim to security vulnerabilities. Non-Profit employees often think cybersecurity is not very important, as the employees do not view their organizations as valuable targets for cyber-crime [2]. There is no guarantee that a cyber security strategy including routine security assessments will thwart dangerous threats, but with a strategy, there is a greater chance that planning, reviewing, testing and evaluating weaknesses can limit exposure and thus security incidents should they occur.

Methods

A ten-question survey was created and circulated to several listserves that focus on technology leadership in Non-Profit organizations, as well as an information technology group focused on international Non-Government Organizations (NGOs). The number of questions in the survey was kept short in order to get as many completed organizational surveys as possible, and recipients were also told ahead of time it would be brief so that it would not disturb their workday. The survey was created using a popular web-based tool and made available for completion on any computing device that supports web browser functionality with Transport Layer Security (TLS) security. The recipient groups were asked to voluntarily complete the survey and also that the survey results would be shared with them. The survey allowed for participants to complete one questionnaire per device, and participants were asked not to complete the survey more than once per organization. Participants were not asked to provide any identifying information so as to keep the responses anonymous. A timeframe of several months was provided to allow participants to complete the survey at their convenience. Fifty-three surveys were completed.

Results

Overall, 50% of the participants responded that they had experienced a ransomware event in their organization. Ransomware is a form of computer malware that is covertly installed and causes one's system to be encrypted or locked so that the files and contents are inaccessible until payment is made.

When recipients were asked if their organization has a formal cyber security unit or staff member(s) responsible and assigned to protecting the computing environment from cyberattacks, 51% said they did have such a focus, and 49% did not. Given that these organizations rely on purpose-specific donor funding that often does not extend to infrastructure support, it is not too surprising to see that about half of them are not able to hire or create a special department or unit to focus on cyber-related security tasks and issues.

For those organizations who answered no to having a formal cyber security unit or focus, and whether there is a plan to incorporate one in the next 6-12 months, 11% of organizations said they did have such a plan, but an overwhelming 86% said they do not have a plan in place.

For a question pertaining to whether cybersecurity frameworks are currently employed in the NGO or Non-Profit organization, 51% said there is one and 47% said there is not.

In response to a question regarding what framework they are utilizing, 56% of the organizations responded that they are using an internally developed framework, followed by 32% which are using NIST guidelines, such as the 800-53a, followed by 24% of the organizations using another solution and 20% using SANS Top 20 Critical Security Controls.

When asked if the controls established in the employed cybersecurity framework are routinely tested, 52% said they are not.

Regarding staff training on cybersecurity issues, 53% of the organizations polled said they do provide routine training, followed by 43% who did not and 4% who declined to answer. In the same training vein, when asked if the organizations require cybersecurity training for staff, 56% said they did, followed by 41% did not require cybersecurity training and 4% declined to answer the question.

As Ransomware is a growing trend, 50% of the organizations responded that they had been hit by ransomware followed by 50% who have not been hit, yet.

When organizations that had been infected or compromised by ransomware were asked what they did to recover from the damaging attacks, 87% of the organizations responded that they restored data from backups, followed by 13% who did something else to recover, and 0% said they would pay the ransom. Although restoring from backups can be effective, there is always a risk in that the backups may not be fully up to date, causing true data loss. In addition, restoring from backup does present downtime while users cannot access information.

Discussion

The key take-away from the short cybersecurity survey demonstrates that there is ample opportunity and a critical need for Non-Profit and non-governmental organizations to improve their approach to securing their assets, information, staff and systems.

Of the nearly half of the respondents who said they did not have a staff person or department fully assigned to tackling cybersecurity, only 11% responded that they have a plan in place to create one in the next 6-12 months. This is a very low percent when in technology services cybersecurity is currently viewed as a strategic priority. The reasons can be many, including budget constraints, since there may be restrictions on using donor funds for overhead projects, such as cybersecurity, instead of programmatic efforts which contribute to the core value they provide to their donors and constituents.

The Non-Profit and non-governmental sectors do have the opportunity to put a focus on their cybersecurity approaches perhaps without much of a budget and limited spending. Cyber-hygiene controls, which include a set of practices and behaviors designed to minimize the impact of possible breaches, such as segmentation of duties, segmentation of privileges, access policies, and the like are free to adopt. The primary limitations to their implementation are awareness, training, and discipline. There are a number of incremental efforts and techniques that can be implemented despite constraints that may be helpful. Some of these to consider are: 1) For those organizations who are hosting web applications or publicly available websites in the cloud or on-premises, referring to the Open Web Application Security Project (OWASP). The OWASP provides guidelines, articles, and methodologies freely for organizations to employ. 2) Ensuring that IT systems are updated routinely for operating system updates, and employing adequate end-point protection software. 3) Create a cybersecurity awareness program that allows staff to be continually educated on steps they can take to contribute to securing their access to systems. 4) If the organization has an enterprise risk management program, it should include cybersecurity concerns. 5) Develop a plan for what steps you should take if and when the possibility of a serious security concerns arises. 6) When developing or using Android or iOS device applications, only download from trusted sources that are verifiable and link to trusted websites. 7) Make the best use of existing hardware, software and firewall capabilities, such as enabling Geo-IP filtering. 8) Even if you cannot get certified, follow one of the recognized security frameworks such as ISO 27001, COBIT, NIST Cybersecurity Framework or NIST 800-53a. The NIST documents offer much backed cybersecurity research that is freely available. 9) Consider if it is possible to add cybersecurity coverage to the organizations existing insurance policy.

Given that the overwhelming method used by organizations to recover from ransomware was from backup restore, it would be prudent to ensure that backups are routinely tested and working properly. Keeping redundant backups would be advised. A single backup is useless if it suddenly does not work or if it is also infected by ransomware. Converting single purpose servers to virtual machines will also provide a mechanism for quicker recovery from ransomware. Performing at least one disaster recovery drill per year within an IT department would provide a documented track record that proves the system works and put into place a routine for system administrators in case such an attack occurs. Setting up basic operating system (OS) event monitoring will also put in place a way to quickly identify when a ransomware attack is underway. Many Non-Profits and NGOs may not be aware of what devices are on their network or what access to the devices is present. An increase in cyber-hygiene and improvements to endpoint security can be accomplished by mapping the network and controlling access based on need. Mapping and need-only access policies are free and can be simple to implement. Testing the endpoint device security, as the last line of defense should be done quarterly as a spot check to ensure devices are protected.

When infected with ransomware, the majority of organizations response was to restore from data and file backup to recover from the resulting attack. Although the backup restores are usually effective, it would have been good to know why organizations in this the sector will not pay the ransom. In a recent ransomware attack on a local police department in Massachusetts the police network started to become slow and inconsistent for a short period of time, and then a message popped up onto computer screens in the department reading “Your personal files are encrypted. File decryption costs $500” [3] [4]. The police chief of the department attempted to decrypt the files without paying the ransom with assistance from federal and state agencies as well as two private cyber security firms [3] [4]. The encryption from the ransomware proved too challenging to be solved by these combined efforts, resulting in the police department having to pay the ransom five days later. This can make you wonder if when you are in this situation you should just pay the ransom. Paying the ransom is a less optimal idea and should only be used as a very last resort. There is no guarantee that the threat actor will send the decryption key. Further, the ransom hacker might remain on your network to spread ransomware or to re-infect the system, or even exfiltrate data. Finally, by paying the ransom, the victim is demonstrating that ransomware is a profitable cybercrime. That ransom paid to free your system directly contributes to the threat actor's future attack campaigns, and it signals to potential threat actors that the ransomware market is still viable for entry.

Limitations

The brief survey did not fully capture the reasons for why there appear to be areas for improvement in cybersecurity defenses within this organization sector. Open responses were captured in certain questions, and although some reasons were offered, the survey would have been stronger had we asked for specific reasons for certain variable questions.

The response that 51% of the organizations can have a staff member or department assigned to the role of technology security brings up the question of the size and budget of the organizations able to do so, which was not posed in the survey.

Nearly 47% of the organizations responded they were not using a standard available framework for their security controls. An obvious next question would be to probe and ask why not and if there is a general awareness of standard frameworks. In many larger organizations and industries, awareness is governed by oversight agencies and risk management departments where the use of a framework may be mandatory, and this would tend to increase knowledge and awareness of the frameworks. 56% of those organizations which are employing a framework responded that the framework is an internally developed model, which reinforces the question about the awareness of frameworks.

Organizations which reported that they were infected by ransomware in the past year were not questioned as to how the ransomware entered their environments. The Verizon 2016 Data Breach Report stated that 30% of targeted Phishing emails were opened, and that 12% of users went on to click the malicious link or attachment [6]. Although it may be difficult to obtain, knowledge of the source of ransomware would be valuable in future like surveys.

Conclusion

In many cybersecurity seminars and conferences, the topic of products, be they hardware or software, are often promoted as a method to protect organizations from threats. It’s true that technology can provide layers of protection to minimize cyber issues. Non-profits and Non-Government Organizations do employ the basic tools to help protect their technology and staff environments, including both perimeter protection and endpoint security. The more advanced tools which permit for logging of events to be centralized and analyzed, even with artificial intelligence, are not possible in many of the organizations discussed in this paper. There are however opportunities to further protect an organization’s environment, without large capital purchases. Behavioral research and approaches provide an opportunity to help provide protection for organizations, without large purchases; however, this would require staff level focus. If humans using computer systems are given the tools and information they need, taught meaningful and responsible use, and trusted to behave appropriately with respect to cybersecurity, desired outcomes may be obtained without security procedures being perceived as troublesome or onerous [5]. It's well known that despite technical cybersecurity efforts, the employee remains the most vulnerable target for cyber-criminals [5]. Therefore, providing more education to staff, may not require a large capital purchase but could yield substantial benefits.

Framework awareness for Information Technology staff could be further enhanced to help bring about cybersecurity activities at organizations. With little budgets for tools, being knowledgeable of the landscape would bring an advantage. One possible consideration is for IT groups to pursue standard body certifications such as the Systems Security Certified Practitioner (SSCP) and Certified Information Systems Security Professional (CISSP) both offered by ISC^2. Such certifications bring a common body of knowledge for security and can be approached without taking formal classes but by having substantial background knowledge, experience, and books available on standard best practices. The certifications cover a broad range of topics and domains and apply to most any organization. In addition to staff training certifications, pursuing or learning more about the NIST and ISO 27001 series documents, guidelines and frameworks will only enhance one's confidence in their information security management systems.

Although many questions were answered to help provide a sense of cybersecurity preparations, planning, and management activity in the Non-Profit and NGO sector, as discussed in the limitations, more demographic data about them would have provided further insight into the responses and answer further the why. Future such research should include more comprehensive survey questions. The cybersecurity ransomware issue remains a threat, as the FBI reported that such attacks have cost organizations $209 million in the first three months of 2016, based on a tally of complaints received, this compared to $24 million for all of 2015 [7] [8]. The goal of this research effort was to get a general sense and bring forward the fact that further attention on cybersecurity needs to be brought to the Non-Profit and NGO sector.

ICIT Contact Information

Phone: 202-600-7250 Ext 101

E-mail: http://icitech.org/contactus/

ICIT Websites & Social Media

www.icitech.org

https://twitter.com/ICITorg

https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-

https://www.facebook.com/ICITorg

Acknowledgements

We would like to acknowledge Irene Friedland, at the Population Council for her contributions to the thorough edit she has provided to this paper. A hearty acknowledgment to James Scott and Parham Eftekhari, founders of the Institute for Critical Infrastructure Technology (ICIT) that avails itself to writing focused material on cybersecurity, hosting venues such as think tank sessions, and for promoting the knowledge exchange of cybersecurity frameworks, particularly the NIST special publications. An additional acknowledgment to Dan Waddell, Managing Director at ISC^2, who has helped to provide valuable information on the varied ISC^2 security certification programs available to all industries, including the Non-Profit and NGO community.

References

1 – Lemmon, Kevin K.; "Meeting the Present and Future Demands of Cybersecurity", National Cybersecurity Institute Journal, Volume 3, No.2, 2016

2 – Zackal, J. "Cyber security Q&A: Non-Profits at Risk", http://thirdsectortoday.com/2014/07/30/cyber-security-qa-nonprofits-at-risk/ , 2014

3 – Choi, KS; Scott, TM; LeClar, DP; "Ransomware Against Police: diagnosis of Risk Factors via Application of Cyber-Routine Activities Theory", SciDoc Publishers, ISSN 2332-287X, 2016

4 – Bray, H.; "When hackers cripple data, police departments pay ransom", Boston Globe, 2015

5 – Hu, Q.; Dinev, T.; Hart, P.; Cooke, D.; "Managing employee compliance with information security policies: The critical role of top management and organizational culture", Decision Sciences Journal, 43, 615-659, 2012

6 -- Verizon 2016 Data Breach Investigations Report, 2016

7 – Chandler, Adam; "How Ransomware Became a Billion-Dollar Nightmare for Businesses", The Atlantic, September, 2016

8 – Finkle, Jim; "Ransomware: Extortionist hackers borrow customer-service tactics, Reuters, Technology News, April 12, 2016

9 – Ray, John Randy; "Training Programs to Increase Cybersecurity Awareness and Compliance in Non-profits", University Of Oregon, Capstone Report, 2014

10 – Holt, Thomas, J.; "Cybercrime Through an Interdisciplinary Lens", ISBN: 978-1-138-66883-6; Routledge, 2017