CYBER SECURITY REPORT

Media
Impact
International

MII™

Revised February 14, 2017

TABLE OF CONTENTS

MII would like to acknowledge and thank 100fold and its Director for serving as the lead researcher for this report, and the countless hours committed to this important project. MII also appreciates the many cyber professionals – inside and outside of the missional world – that provided counsel and expertise for this report.

EXECUTIVE SUMMARY

Overview

While Cyber Security breaches are often in the news, the impact of cyber security breaches on field ministry is often kept secret. In our survey of 30 key MENA ministries, we found that mission organizations were not only experiencing financial loss (perhaps in the millions of dollars), but more than 50% had staff or seekers that experienced arrest or harassment, prison, expulsion – and even death – due to cyber security breaches. These adverse impacts raise cyber risk from a technical issue to be solved by the IT department, to an organization's board and executive team that need to put in place cyber risk mitigation strategies.

The survey also found that a third of responding organizations were being deeply impacted by cyber security breaches, and did not appear to know what to do to improve their situation. Another third were impacted, but had implemented a plan to improve their cyber security profile. The last third reported almost no cyber security problems, but often lacked the means to even detect a cyber breach.

MENA Cyber Risks

A review of the cyber risks present in the MENA region shows that both state and non-state actors have access to – and use – increasingly sophisticated cyber attack tools. In addition, network-wide tools that are common in the West for monitoring terror organizations and criminal activity (Deep Packet Inspection and Lawful Interception Gateway) are being deployed across the MENA region. These

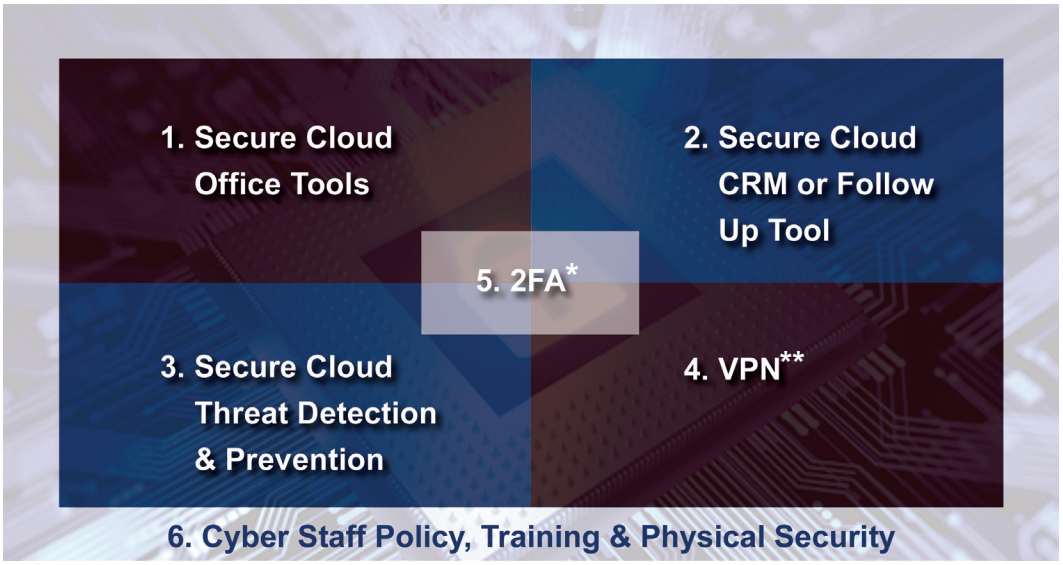
tools allow for the monitoring of all phone calls and a great deal of online activity. This creates a very challenging environment for field ministry, when the message and mission of an entity is opposed by a state actor.

The knowledge of the threats and actors in the region – and what actions they are most likely to take – makes it possible to do rational Cyber Risk Assessment. A rubric is suggested in the report that considers likely risks and matches that with appropriate mitigation steps. This process is designed to be flexible and allows organizations to have a sensible level of response based on actual risks. This in turn reduces cost and complexity of implementing a Cyber Risk Reduction program.

Cyber Risk Mitigation

A key point is that technical interventions alone will not solve cyber risk issues. Appropriate policies and strong cyber security training are crucial to a successful cyber risk reduction program. In fact, addressing staff behavior is the single most important factor in reducing cyber risk. Flexible and low-cost training tools have been identified, and the report also includes sample policies in the areas of passwords, communication, and the reduction of sensitive information to assist in this area.

CYBER RISK MITIGATION MODEL / STEPS



* Two Factor Authentication

**Virtual Private Network

In the last section of the report, Cyber Risk Mitigation steps are proposed that are based on the baseline cyber risk assessment conducted in section five. These mitigation steps involve policy, training and technical interventions that fulfil the Baseline Cyber Safety Profile.

Cyber Response By Size of Organization

In our survey of MENA organizations, we found that roughly a third of respondents were from small organizations, with less than 50 staff. About a third were from medium-sized organizations, with more than 50 but less than 500 people. And a third were from large organizations with 500 or more staff. Each of these different-sized organizations have specific challenges, so the report proposes possible next steps with cost projections for each type. We also recognize that "one size does not fit all" and that each organization must address their unique situation and safety profile.

Small entities typically have tight budgets, highly distributed teams and little IT support. So the report proposes new cloud-based tools and training that can be implemented in stages, and that greatly improve the cyber security profile of an organization.

Medium-sized entities may have preexisting networks that need to be secured and a detailed "cookbook" has been provided (in the appendix) that has a step-by-step procedure on how to lock down a network. A cost estimate for implementing this has also been provided. An alternative proposal – similar to the one for small entities is also provided – along with cost estimates.

Large entities have much more complex network architectures and often many legacy systems. So it is not possible to recommend a single course of action that will implement a cyber safety profile for a large organization. However, the report provides a cloud-based proposal similar to the one for small and medium sized organizations, along with cost estimates for implementation. For those organizations with very little in the way of cyber security, it is recommended that a Cyber Risk Assessment be conducted, and that the organization begin logging adverse impacts that are the result of cyber breaches. These two tools can then be used to inform and prioritize next steps.

A Final Word

At every step in this study, effort has been made to simplify the process and reduce cost. Missional organizations are often resource limited, so the question will often be asked "Can I afford this?" As was noted earlier, some of the negative impact that organizations reported included the loss of reputation, death of workers and seekers, and the shutdown of programs due to cyber breaches. The cost of these adverse impacts far exceeds those of implementing a baseline Cyber Safety Profile. Therefore, the question really becomes, "How can I afford NOT to do this?"

INTRODUCTION

Cyber Security in the Missional Context

It is clear that technology has strengthened the work of Christian ministries around the world. However, missiologists and missions leaders seldom consider the full implications of the rapid and pervasive adoption of so many electronic devices and online services, often by workers with little understanding of the underlying technologies. This study will focus on one aspect of the use of technology in the missional context – that of cyber security. It is important to note that this is a "point in time" report and that the whole area of cyber security is changing rapidly – both in terms of the types of risks and the potential solutions to mitigate this challenge.

Cyber security is just one piece of the over-arching security context of missional work. From the start of the Church, physical security was a recognized concern of the missional effort. This can be seen in decisions to inform local military authorities of a plot to kill a missionary (Paul), avoid a riot situation (in Ephesus), scatter away from places of intense physical persecution, as well as many other situations.

Cyber security deals with unauthorized or unexpected access to data and electronic devices. Such access can expose identities of seekers, field workers, budgets, methods, and physical locations. This can lead to death of disciples, imprisonment, expulsion, loss of visa status, counter movements, negative impact on organizational reputation, loss of funding, and other negative outcomes. Another way to consider this is to look at cyber security as a significant risk that every organization should evaluate and seek to mitigate.

When we began this study, we could find no existing data on the impact of cyber breach on missional organizations. Additionally – while there are many sources for standards and best practices in cyber security – the level of detail, high technical level and high cost required to implement them appeared to have been overwhelming to many small- and medium-sized organizations.

Therefore, we have sought to help organizations reduce their cyber risk in an approachable and affordable way. This report is not a comprehensive work on cyber security in all its technical detail – such a report would be hundreds of pages long and incomprehensible to all but specialists.

There are also vast differences in context and technologies employed by missional organizations. Some small organizations are totally distributed with members using personal devices with no IT staff, much less cyber security staff. Some large organizations are utilizing cloud-based central services, are well developed and have implemented cyber security policies and full-time cyber security staff. We have chosen to focus most closely on those areas that can help the least protected improve their cyber security risk profile.

> ***We have chosen to focus most closely on those areas that can help the least protected improve their cyber security risk profile.***

The core cyber security profile we have chosen for this study are the first five Critical Security Controls of the Center for Internet Security (CIS)[i], as the starting place for any cyber risk mitigation effort.

This study is also focused primarily on the cyber risk in the MENA region – how organizations can evaluate that risk and what they can do to mitigate it. However, our findings should be applicable to mission organizations in many contexts outside the MENA region.

One question that all organizations must ask – even if they don't want to ask it openly – is "what is the compelling reason for us to invest a lot of resources in this problem?" For very large corporations, it is often cheaper to deal with the adverse impacts from a cyber security breach than to implement a comprehensive and robust cyber security plan.[ii] In the corporate world there is public accountability for a financial loss that comes from cyber security breaches, so there is some ultimate accountability. However, in the mission world – not only is there no reporting – but there are seldom any internal valuations attached to

i https://www.sans.org/security-resources/posters/special/20-critical-security-controls-55
ii http://www.cbsnews.com/news/the-reason-companies-dont-fix-cybersecurity/

adverse impacts due to cyber security breaches. This can make the problem invisible to senior leaders, boards and donors who all have an interest in – and a duty to – mitigate organizational risk.

Since there is no existing data on the cost of cyber security breaches in missional organizations, we have researched the cost for businesses as a surrogate. We also conducted a direct survey of 30 MENA missional organizations to gather information about the impact of cyber security breaches, attitudes and aspirations about cyber security, as well as a snapshot of current practices. The results of this survey indicate that cyber breaches are having a deep and costly impact on many organizations.

As all cyber risk originates from some threat source, it is important for organizations to identify the threats they face and seek to develop a risk mitigation strategy. To aid this process, this report provides information on known cyber risks in the MENA region as well as a flexible risk assessment tool. While it is not possible to provide comprehensive cyber risk mitigation guidance in this report – as each organization has many different issues and contexts – a section has been included on basic cyber risk mitigation. The suggestions in that section are relatively low in resource requirements, and have the potential to greatly improve the cyber security profile of an organization that is struggling with "where to start." In the appendix, additional resources are provided including a list of useful products and vendors.

It is clear from the survey we conducted with MENA ministries, that cyber security is a very significant issue for at least two-thirds of the organizations that responded. Not only are organizations suffering financial losses, but also the death and imprisonment of workers due to cyber security breaches. This is coupled with a sense in several organizations of not knowing what to do to improve their cyber security situation.

This report seeks to illuminate the need, as well as provide practical information and help for missional organizations wrestling with cyber security.

> ***A wise man is full of strength, and a man of knowledge enhances his might, for by wise guidance you can wage your war, and in abundance of counselors there is victory.*** **Proverbs 24: 5-6 ESV**

CYBER THREATS

In order to effectively protect an organization, relevant and realistic Cyber Threats and Threat Actors must be identified. Once threats and threat actors have been identified, a Risk Assessment can be conducted and Cyber Safety Profiles developed. Then appropriate mitigations can be put in place to fulfil the profile.

In the survey of MENA ministries conducted for this study, a number of adverse impacts were reported due to cyber security breaches. These included:

1. Death of national workers or disciples
2. Imprisonment of national and expat workers
3. Arrest of national and expat workers
4. Expulsion of expat workers
5. Shut down of programs
6. Loss of organizational reputation
7. Loss of time and resources

The loss of life and imprisonment of personnel is a far greater adverse impact than is typically experienced by a for-profit company. This type of loss actually meets the definition of genuine Cyber War.[1]

What was not collected in the survey was the financial impact of cyber security breaches for missional organizations. In this study we will use data from breaches in for-profit companies as a surrogate for the financial impact in missional organizations.

PROBABILITY OF CYBER SECURITY BREACH

In a global study of more than 380 companies, it was determined that there was a .256 probability of a Cyber Security Breach that involved at least 10,000 data records.[2] In the MENA region this was calculated at 0.31.[3] Another way to state this is that between 1 in 4 and 1 in 3 organizations would experience a cyber security breach that involved 10,000 data records or more (over any 2-year period).

In the survey conducted for this report, 23 out of 30 (or 76%) of respondents reported some type of cyber security breach. However, the time frame for those breaches was not collected in the survey.

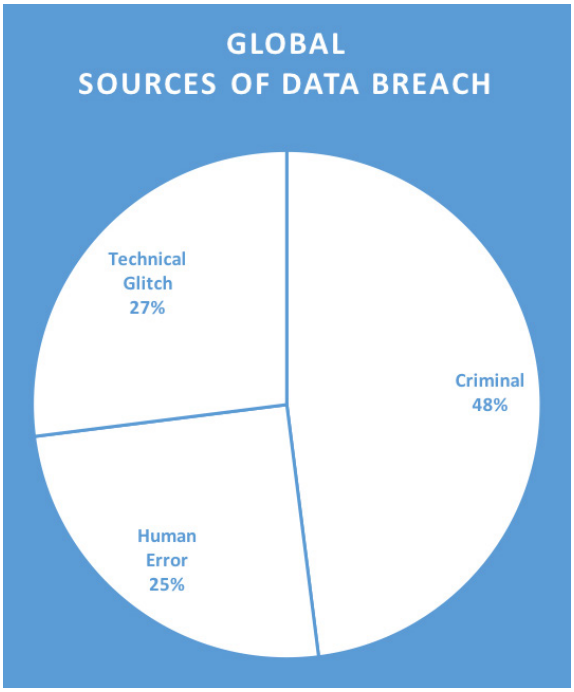
1 'Cyberwar' Is Over Hyped: It Ain't War Til Someone Dies
2 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute Research Report, p 21
3 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute Research Report, p 22

FINANCIAL LOSS DUE TO CYBER SECURITY BREACH

Financial loss for cyber breach was calculated on a cost per record basis. This cost incorporates the total cost to the entity. This differs by industry and region. The low-end cost was $61 per record and the high-end cost was $221 per record (over a 3-year span). For a loss of 10,000 records, this would range from $610,000 to $2.2 million per organization. If we model this using the eight mission organizations in the survey that had an Adverse Impact Score of 30 or above, that would yield a range of $4.8 million to $17.6 million in financial loss. Based on Adverse Impacts like Loss of Organizational Reputation, Shut Down of Programs, Expulsion of Expats and Death of National Workers, it appears likely that real financial losses experienced by missional entities could easily fall within this range.

TIME NEEDED TO IDENTIFY & CONTAIN A CYBER SECURITY BREACH

Mean Time To Identify (MTTI) represents the average time it takes a company to identify that they have had a cyber security breach. Currently, among for-profit companies the MTTI is 210 days or roughly 7 months.[4] The Mean Time To Contain (MTTC) is 70 days.[5] It is not known what the MTTI and MTTC are for missional organizations. However, based on the low level of spending on cyber security by a third of the survey respondents, it is likely that the MTTC and MTTI are greater for those entities.



Globally, at least 25% of Cyber Breaches are due to human error.

ORGANIZATIONAL STAFF

Organizational staff can present two main types of threats to an organization. The first is due to negligence and error that results in a cyber security breach. The second is malicious actions that seek to steal from the organization or do harm to the entity. This second threat is also called an "insider threat." This second type of threat is considered targeted criminal behavior. In this study we have cited data that

4 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute Research Report, p 23
5 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute Research Report, p 24

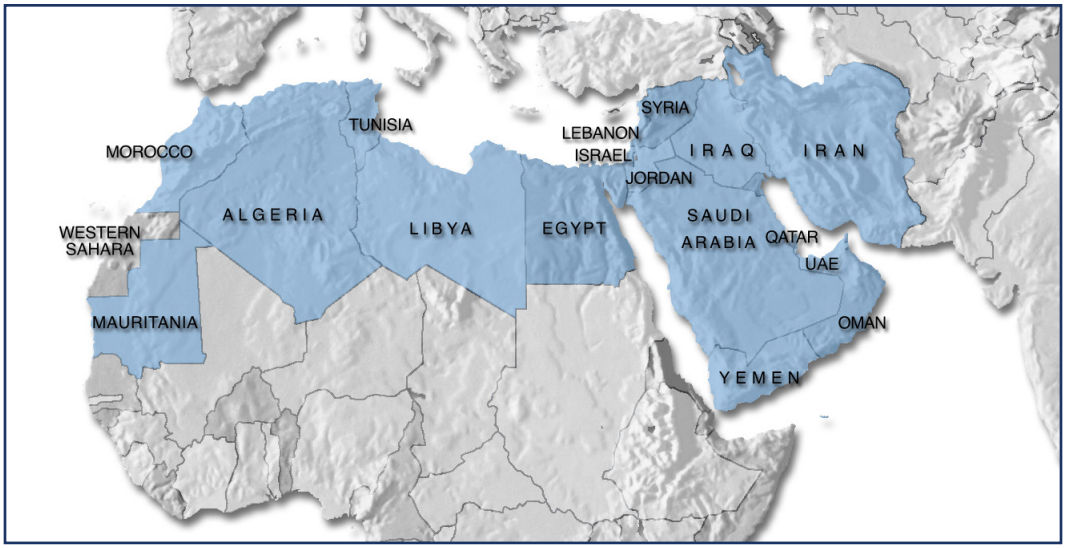
indicates that at least 25% of cyber breaches can be directly attributed to staff actions. There are multiple online sources that claim this to be as high as 90%[6], however the bulk of these claims were not substantiated with data. In any case, organizational staff training and compliance is a key factor in a successful risk mitigation program.

OPPORTUNISTIC CRIMINALS

Opportunistic Criminals use a variety of un-targeted physical and cyber attacks to steal information, equipment, funds, personal identities, hold information ransom and a range of other criminal actions.

LAWFUL INTERCEPTION GATEWAYS (LIG)

Lawful Interception Gateways are technologies built into the telecom infrastructure that allow telecoms to monitor, intercept, record and analyze all phone call and SMS traffic. This technology has become standard globally and is intended to be used to counter terrorism and criminal activity. However, the extensive invasive capabilities of these systems are only limited by the legislation of any specific country.



All MENA countries have some version of the Lawful Interception Gateway capacity.

When built out extensively, it is possible to monitor all call and SMS traffic simultaneously and in real time. Because this monitoring can be automated it greatly reduces the “hide in the long grass” privacy defense. Lawful Interception Gateways can be configured to access GPS and telecom user location data – so that not only can the system monitor a call or SMS – but it can pinpoint the location of the person receiving the call and the person making the call (if they are both in the network). Additionally, user location data can be accessed for people within a specific distance of either caller if they have phones.

6 http://www.prnewswire.com/news-releases/employee-errors-cause-most-data-breach-incidents-in-cyber-attacks-300342879.html

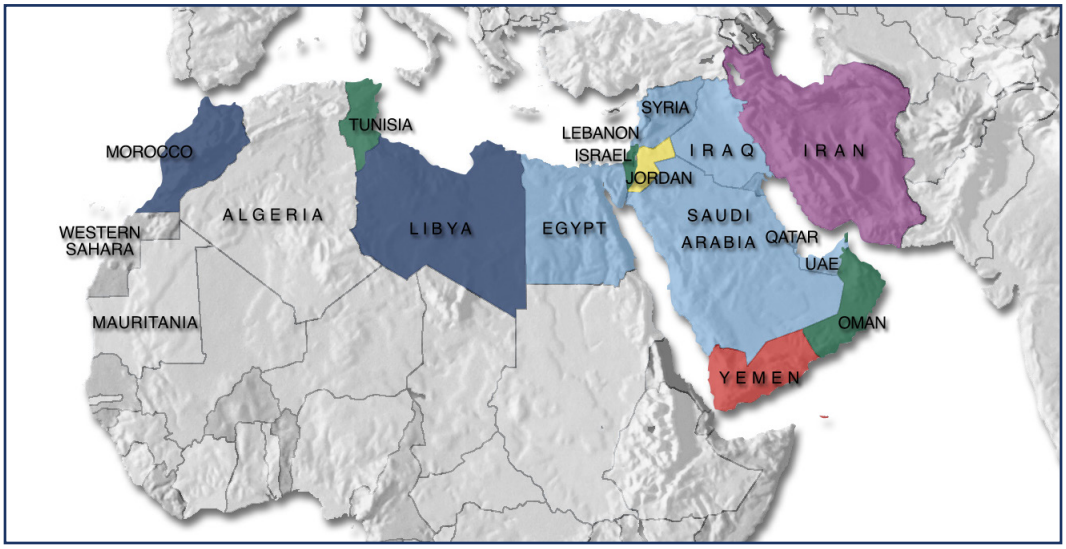
Systems can also be configured to report who a caller received a call from, and who that caller telephoned after receiving a specific call, and who each of those people called after contacted by the first caller.

SS7 GLOBAL TRACKING

SS7 is a global locator system for phones that are roaming in networks other than their own. It allows a telecom to determine what network the phone belongs to, and whether it has a way to bill that user for the use of the local phone network. SS7 is available to all cell phone networks. The system can also be misused to track individuals on a global scale.[7]

For example, if someone from France was visiting the UAE and was "roaming," the telecom in the UAE would recognize that this phone was from outside its network and would query SS7 as to where the phone was from, and if its home telecom had a roaming agreement with it. If the agreement existed, the person from France would be able to make calls without having to buy a local SIM chip. However, once the local telecom in the UAE made a record of the phone's unique equipment ID number, it would be possible to query the SS7 system in the future and request location information on that phone, even if it was back in its home network in France, or any place they were located around the globe. Therefore, if someone on the UAE telecom network traveled to another country and *even changed their SIM card*, the phone would still be trackable on the SS7 network based on the unique hardware ID number.

DEEP PACKET INSPECTION (DPI)



Countries using DPI Technology in the MENA region – DPI vendors identified for each country.

7 Webinar by Silent Circle - https://www.youtube.com/watch?v=JaxHk-QUsnE&feature=youtu.be

Deep Packet Inspection (DPI) is a technology that allows an Internet Service Provider (ISP) to examine in great detail all of the Internet traffic from an Internet user. All unencrypted traffic can be monitored, including usernames and passwords. DPI can also be used to identify and block specific content and services. Many governments in the MENA region are documented as having DPI technology in place. Vendors are Bluecoat,[8] Amesys,[9] Raytheon,[10] Cyberroam,[11] Narus,[12] and ZTE.[13] DPI systems can be programmed to identify specific users and services automatically, defeating in part the "hide in the long grass" privacy defense.

THE HACKING TEAM

The Hacking Team[14] is a company that specializes in producing tools that can invade a mobile device and use it to remotely monitor the user. The software is typically undetectable by the device owner and gives access to all data and communication on the device, and avoids encryption tools that allow privacy in communication. The Hacking Team typically sells their tools to governments. There are confirmed incidents of The Hacking Team tool being used to monitor human rights advocates by governments they oppose.

Map of countries in the MENA region (highlighted in red) that are known to have purchased The Hacking Team tools.[15]

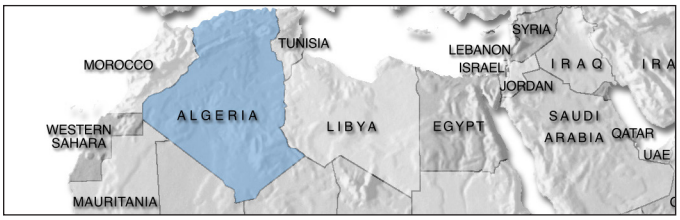
8 https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/
9 https://malwaretips.com/threads/access-denied-crazy-internet-censorship-in-morocco.19319/
10 http://www.deepacketinspection.com/dpi/AS51140
11 https://lwn.net/Articles/506337/
12 http://www.pcworld.com/article/218142/article.html
13 Reuters News , 25 May 2012, U.S. probes China's ZTE over tech sales to Iran
14 https://en.wikipedia.org/wiki/Hacking_Team
15 http://mashable.com/2014/02/18/controversial-government-spyware-hacking-team/#Uj7MvVCwPEqD

MENA Cyber Threats

SUNNI, SHIA, JEWISH CYBER WAR

In the MENA region there is an active cyber war between Iran, Egypt / Saudi Arabia and Israel.[16] Initially, this consisted of website defacements and DDOS attacks of various sites. However, it has now escalated to attacks on core infrastructure and industries. This cyber war likely involves state and non-state actors with more than 30 non-state hacker groups involved. While the focus of all of these resources is the other belligerents, it is important to note that any perception that a missional group or its staff was in some way aligned with the goals of any of the attacker's interests, that missional group could be subjected to a targeted attack by the other two belligerents.

ALGERIA



While there is no public record of Algeria acquiring DPI (Deep Packet Inspection) technology, the country does have centralized systems to monitor Internet traffic and the legal power to block websites "contrary to public order and decency."[17] We did not receive specific reports of cyber attacks on ministries by Algeria, however press and government sources have reported attacks on websites and social media increased 300% – with over 500 cases – in 2015.[18] Algeria has a small but vibrant software development segment and thus a skilled pool of people that could engage in cyber activities. There have been numerous attacks on French websites by Algerian hackers.[19] The capacity of these hackers was shown in 2013 with the development of the "SpyEye" financial fraud malware package by Hazma Bendelladj. "SpyEye" was considered the most widely used financial fraud malware package in the world.[20]

Currently the most likely threats are:

1. Petty theft.
2. Government monitoring of web and phone activity.
3. Website defacement and destruction if targeted by Algerian hackers.

16 http://www.bluekaizen.org/CSCAMP2012/CONFHpdfs/EbrahimHegazy/Cyber-Warfare-in-the-middle-east.pdf
17 https://freedomhouse.org/report/freedom-world/2016/algeria - see section D.
18 https://www.osac.gov/pages/ContentReportDetails.aspx?cid=19075
19 http://www.huffingtonpost.com/2015/01/13/charlie-hebdo_n_6464318.html
20 http://arstechnica.com/tech-policy/2013/05/alleged-mastermind-behind-spyeye-botnet-tools-extradited-to-us/

EGYPT

The national network in Egypt has had a low level of security in general, which led to widespread infestation with botnets and other criminal software. In 2010, there were hundreds of thousands of machines that were infected.[21] By 2015, the government of Egypt had Finfisher[22] software in place,[23] which is a commercial "botnet" that is used for surveillance. In the same year, the Cyber Security Council of Egypt was formed as a national-level effort to improve cyber security. However, many groups see the CSC as a means of national surveillance and suppression.[24] It is also publicly documented that Egypt has Lawful Interception Gateway (LIG) and DPI technology,[25] as well as tools from the Hacking Team. In December 2016, Egypt began to block the use of "Signal," an encrypted communications app at the network level.[26] As part of the new Cyber Security Infrastructure, Egypt has signed agreements to share cyber intelligence with South Korea, Oman, Malaysia, Uganda, Tunisia, India, Tanzania and the U.S.[27] With nine different terrorist organizations operating within the borders of Egypt[28] (ISIS being one of them) – and thirteen hacking groups[29] – Egypt presents a complex environment with many physical and cyber security challenges.

There have been no specific reports of cyber attacks targeted at missional organizations, however the well equipped and antagonistic government,[30] as well as hostile militant groups are viable threat actors. Currently the most likely threats are:

1. Monitoring of unencrypted email, SMS, VOIP, and phone calls.
2. Monitoring of unencrypted web and social media usage.
3. Untargeted malware and phishing attacks.
4. Exposure of personal information by radical Muslim hackers who operate in Egypt.
5. Petty theft.

21 https://en.wikipedia.org/wiki/Virut
22 https://en.wikipedia.org/wiki/FinFisher
23 https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/
24 http://www.al-monitor.com/pulse/en/originals/2015/01/egypt-cyber-security-council-privacy.html
25 http://www.huffingtonpost.com/timothy-karr/congress-urges-state-depa_b_821949.html
26 http://english.alarabiya.net/en/media/digital/2016/12/21/Egypt-blocks-encrypted-messaging-app.html
27 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Egypt.pdf
28 http://thehill.com/blogs/congress-blog/foreign-policy/239566-terror-attacks-skyrocket-in-egypt-and-across-the-globe
29 http://www.bluekaizen.org/CSCAMP2012/CONFHpdfs/EbrahimHegazy/Cyber-Warfare-in-the-middle-east.pdf
30 http://www.nytimes.com/2016/12/22/opinion/egypts-cruelty-to-christians.html?_r=0

For those that are engaged in high profile activities, work among suspect populations, or have drawn the attention of the government or radical groups, the following are likely threats:

1. Targeted malware and phishing attacks – which could lead to kidnapping.
2. Targeted malware and phishing attacks – which could result in exposure of a network of contacts.
3. Targeted cyber attack on personal devices.
4. Targeted network attacks.
5. Active monitoring of all communications – phone, SMS, VOIP, Chat, email, etc.

IRAN

In April 2010, there was public evidence that Nokia sold LIG equipment to Iran that could be used to monitor all calls and texts – especially mobile communications.[31] In February 2014, Iran was considered to be a first-tier cyber warfare threat to the USA.[32] In April 2014, Viber – the most popular chat app in Iran at the time – was shown to have stored communications in unencrypted form,[33] and thus gives credence to claims by Iran of monitoring communications on Viber.[34] In September 2014, the Iranian high court issued orders to block Viber. This occurred after there was evidence that Viber had an opportunity to fix the security issues.[35]

In September 2014, there were reports from a media ministry serving Iran that phone numbers had been blocked and high-jacked. Security personnel in Iran have also impersonated ministry counselors to gather intelligence on seekers that called a high-jacked phone number.[36] In August 2015, Iran was caught high-jacking two factor authentications of a Gmail account[37] (two factor authentication is considered a best practice in cyber security). In Winter 2015, it was reported that Psiphon VPN service was widely disrupted in Iran.[38] At the time of the attack, Psiphon was one of the most widely used VPNs in Iran. In Spring 2016, it was reported that a device in the West was compromised and data ex-

31 http://arstechnica.com/tech-policy/2010/03/how-nokia-helped-iran-persecute-and-arrest-dissidents/
32 http://foreignpolicy.com/2014/02/18/forget-china-irans-hackers-are-americas-newest-cyber-threat/
33 http://thehackernews.com/2014/04/vibers-poor-data-security-practices.html
34 https://www.iranhumanrights.org/2014/09/viber-company-refutes-tapping-claims-by-iranian-officials/
35 http://www.al-monitor.com/pulse/originals/2014/09/iran-internet-communication-viber-whatsapp-judiciary.html
36 Personal conversation with ministry leaders
37 https://citizenlab.org/2015/08/iran_two_factor_phishing/
38 Bulletin from Psiphon Feb 2016

filtrated that resulted in the arrest of more than a dozen people inside Iran.[39] This appears to have been a targeted cyber attack. In March 2016, the company ZTE was banned from trade in the U.S. over selling DPI and other technologies to Iran. The investigation provided public proof of long suspected capabilities to use DPI to monitor Internet use in Iran.[40] Iran is also a major sponsor of Hamas and would be able to share information gained via cyber breach with them.[41] Additionally, Iran has a very strong hacker capability[42] with many groups aligned with state purposes.[43] This has resulted in attacks on high profile Western targets and the ability of Iran to project cyber power on a global scale.

Iran is a very well equipped and aggressive state threat actor. It has also treated missional work and church planting as a national security threat. Any organization seeking to work in Iran – or partner with those who work there – needs to be diligent in their cyber security preparations. Currently the most likely threats are:

1. Targeted theft.
2. Targeted cyber attacks on personal devices.
3. Targeted network attacks.
4. Active monitoring of all communications – phone, SMS, VOIP, Chat, email, etc.
5. Exploits against two factor authentication.
6. Blocking VPN at the network level.
7. Arrest, imprisonment and possible torture of nationals in country that are exposed in a cyber breach.

IRAQ

Iraq is an active war zone with fighting between ISIS and Western powers. The Cyber Caliphate has emerged as a hacking group aligned with ISIS. The Cyber Caliphate is very social media savvy and has a large number of members monitoring and engaging with social media.[44] They have also conducted “false flag” attacks where they produce anti-ISIS media to attract their most ardent opponents.[45] This content is delivered with exploits that

39 Personal conversation with ministry leaders
40 http://www.theregister.co.uk/2016/03/08/us_trade_ban_on_zte
41 http://www.al-monitor.com/pulse/originals/2016/06/gaza-hamas-resume-relations-iran.html
42 https://en.wikipedia.org/wiki/Iranian_Cyber_Army
43 http://uk.businessinsider.com/what-its-like-to-be-a-hacker-in-iran-2016-2?r=US&IR=T
44 http://www.al-monitor.com/pulse/originals/2015/04/iraq-social-media-convey-battle-against-islamic-state.html
45 http://www.bbc.co.uk/news/technology-28418951

allow ISIS hackers to trace the physical location of the person who accessed the media, and then trace who the media was shared with. This information can then be used for targeted kidnapping,"hit lists" (for ISIS sympathizers to kill if the person lives outside Iraq), or cyber exploits to gather intelligence. As a pure hacking force, ISIS has received a good deal of publicity, but a recent analysis has determined that ISIS hackers are currently deploying standard open-source hacking tools and well-dated exploits.[46] This implies that missional workers can build a Cyber Safety Profile that will protect them against the vast majority of ISIS hacking efforts.

The central government of Iraq has advanced cyber attack and monitoring tools.[47] There is public information that Iraq has LIG and DPI technologies, as well as advanced Internet surveillance and monitoring tools. They also utilize over-the-air surveillance systems that allow for the interception, monitoring and physical tracking of cell phone calls in real time.[48] The Iraqi central government also receives cyber training and support from the U.S. and NATO.[49] The most likely threats are:

1. Monitoring of unencrypted email, SMS, VOIP, and phone calls.
2. Monitoring of unencrypted web and social media usage.
3. Untargeted malware and phishing attacks.
4. Exposure of personal information by radical Muslim hackers who operate in and outside of Iraq.
5. Social engineering on social media with attempts to identify those opposed to ISIS.
6. Petty theft.

For those that are engaged in high profile activities, work among suspect populations, or have drawn the attention of the government or radical groups, the following are likely threats:

1. Targeted malware and phishing attacks – which could lead to kidnapping.
2. Targeted malware and phishing attacks – which could result in exposure of a network of contacts.
3. Targeted social media malware attacks – which could lead to kidnapping or execution.
4. Targeted cyber attacks on personal devices.
5. Targeted network attacks.
6. Active monitoring of all communications – phone, SMS, VOIP, Chat, email, etc.

46 Hacking for ISIS: The Emergent Cyber Threat Landscape. Flashpoint. 2016
47 https://sii.transparencytoolkit.org/search?utf8=✓&utf8=✓&q=Iraq
48 https://sii.transparencytoolkit.org/search?utf8=✓&utf8=✓&q=Iraq
49 http://www.nato.int/cps/en/natohq/news_139179.htm

JORDAN

There are reports of Internet scams and identity theft as an ongoing concern in Jordan.[50] Petty theft and untargeted break-ins against expatriates are also reported.[51] Jordan has been attacked by elements of ISIS and there appears to be a significant ISIS presence in some areas of the country.[52] There is public evidence that Jordan has DPI, LIG, FinFisher surveillance software, and remote access tools from The Hacking Team. They also have over-the-air surveillance systems that allow for the interception, monitoring and physical tracking of cell phone calls in real time.[53]

There were no reports of cyber attacks against a missional organization by Jordan. The government has a reputation of being tolerant of Christianity. Most incidents of persecution originate at the personal and family level.[54] Currently the most likely threats are:

1. Monitoring of unencrypted email, SMS, VOIP, and phone calls.
2. Monitoring of unencrypted web and social media usage.
3. Untargeted malware and phishing attacks.

For those that are engaged in high profile activities like work among refugees, or have drawn the attention of the government or radical groups, the following are likely threats:

1. Targeted malware and phishing attacks.
2. Targeted malware and phishing attacks – which could result in exposure of a network of contacts.
3. Targeted cyber attacks on personal devices.
4. Targeted network attacks.
5. Active monitoring of all communications – phone, SMS, VOIP, Chat, email, etc.

50 https://www.osac.gov/pages/ContentReportDetails.aspx?cid=19208
51 Ibid
52 http://www.middleeasteye.net/news/enemy-within-jordans-battle-stop-home-grown-terrorism-481722991
53 https://sii.transparencytoolkit.org/search?utf8=✓&utf8=✓&q=jordan
54 https://www.vomcanada.com/jordan.htm

LEBANON

Lebanon does not have a central policy nor a legislative framework for cyber security.[55] It is reported that Lebanon is subject to significant cyber crime.[56] Although on the surface Lebanon does not appear to have much cyber security capacity, there is evidence that the country and non-state actors like Hezbollah have significant surveillance and cyber warfare capability. In 2015, a large and long-term cyber espionage campaign was identified as originating out of Lebanon, under the control of Hezbollah.[57] This cyber espionage campaign was considered to be advanced and representative of a high level of internal capability.[58] There is public evidence that Lebanon has DPI, LIG, FinFisher surveillance software, and remote access tools from The Hacking Team. They also have over-the-air surveillance systems that allow for the interception, monitoring and physical tracking of cell phone calls in real time.[59] Petty theft, targeted theft, and kidnapping are all present risks.[60] Militant groups like ISIS, Hezbollah and at least seven other extremist groups operate within Lebanon.[61] They have specifically targeted Christians[62] in Lebanon and many have been tortured and killed.[63]

The lack of political stability, the high influx of Syrian refugees, the unrestrained presence of militant groups with proven cyber espionage capability, and the use of very sophisticated surveillance and cyber attack tools by the state, presents a very complex and challenging environment for missional organizations. Special precautions should be taken to encrypt and compartmentalize sensitive data. The most likely threats are:

1. Petty theft.
2. Monitoring of unencrypted email, SMS, VOIP, and phone calls.
3. Monitoring of unencrypted web and social media usage.
4. Untargeted malware and phishing attacks – criminal.

---

55 http://www.tra.gov.lb/Cybersecurity-in-Lebanon
56 http://www.executive-magazine.com/economics-policy/lebanon-cyber-security-telecommunications-regulatory-authority
57 http://www.csmonitor.com/World/Passcode/2015/0601/Cyberattack-tied-to-Hezbollah-ups-the-ante-for-Israel-s-digital-defenses
58 http://www.csoonline.com/article/2904396/data-protection/lebanese-cyberespionage-campaign-hits-defense-telecom-media-firms-worldwide.html
59 https://sii.transparencytoolkit.org/search?recipient_country_facet=Lebanon
60 https://www.osac.gov/Pages/ContentReportDetails.aspx?cid=19280
61 https://www.osac.gov/Pages/ContentReportDetails.aspx?cid=19280
62 http://www.foxnews.com/opinion/2016/07/02/after-fallujah-isis-moves-to-lebanon-and-targets-christians.html?refresh=true
63 Private report of converts being tortured and killed for position of Christian media, 2016.

For those that are engaged in high profile activities – especially with refugees – or have drawn the attention of the government or radical groups, the following are likely threats:

1. Targeted theft.
2. Targeted cyber attack on personal devices.
3. Targeted network attacks.
4. Active monitoring of all communications – phone, SMS, VOIP, Chat, email, etc.
5. Exposure of personal information by radical Muslim hackers to hostile militant groups.
6. Possible kidnapping, torture and death of nationals in country that are exposed in a cyber breach.

LIBYA

The government of Libya is publicly known to have LIG and DPI Technology. During the unrest in 2011, the government shut down the Internet for the entire country. After that total shut down, there have been multiple partial shutdowns,[64] demonstrating total control of the Internet by the central government. Additionally in 2011, ten Libyan hacking groups were identified that were aligned with the central government, and at least one hacking group that was engaged in cyber jihad against the West.[65] This cyber jihad group was found to be creating viruses that were used against major corporations. A wide-ranging analysis of the national network of Libya also showed a poor state of cyber security standards, meaning that the compromise of national systems was likely.[66] This makes for a ripe environment of botnets and other cyber attack tools. In 2016, there were reports that in the active Libyan war zone, non-state actors were engaged in cyber espionage against high-profile Libyans using the remote access trojan (RAT) “AlienSpy.” Using a combination of targeted phishing and social engineering, a Telegram account of a target was taken over and used to pass malware to contacts of the target. Researchers said this software – while not sophisticated – could allow the tracking and monitoring of individuals for possible kidnapping and assassination.[67]

64 Project Cyber Dawn v1.0, The Cyber Security Forum Initiative. P. 8
65 Ibid. p 21
66 Ibid. p 25
67 http://news.softpedia.com/news/libyan-scorpions-cyber-espionage-group-targets-high-profile-lybians-508664.shtml

No reports have been received of direct cyber attacks on missional organizations operating in Libya. However, the most likely threats are:

1. Monitoring of unencrypted email, SMS, VOIP, and phone calls.
2. Monitoring of unencrypted web and social media usage.
3. Untargeted malware and phishing attacks.
4. Exposure of personal information by radical Muslim hackers who operate in Libya.
5. Petty theft.

For those who are engaged in high profile activities – such as work among suspect populations or ministries that have drawn the attention of the government or radical groups, the following are likely threats:

1. Targeted malware and phishing attacks – which could lead to kidnapping.
2. Targeted malware and phishing attacks – which could result in exposure of a network of contacts.

MOROCCO

The government of Morocco is publicly known to have LIG and DPI technologies, and to have purchased tools from The Hacking Team.[68] Conversations with local workers indicated that the government has monitored the use of VPNs by nationals, especially in rural areas.[69] In 2010, the government of Morocco expelled scores of Christian workers.[70] Some Christian workers reported that phone calls are being monitored, SMS messages are being hijacked, email and web usage is being monitored, and this information is used in identifying other expat workers and national Christians.[71] In 2012, 2013 and 2014, the government of Morocco used tools from The Hacking Team to gain control of mobile phones, computers, webcams, email accounts, and social network accounts of journalists and "civil society advocates."[72] Hacking groups have also been very active in Morocco. In 2013 and 2014, there were reports of cyber attacks on the Israeli government, academic and infrastructure sites by Moroccan hackers.[73] There were also ISIS-aligned radical

68 Their Eyes On Me – Stories of surveillance in Morocco, Privacy International, 2015. P 10
69 Private conversation with local worker.
70 http://www.christianpost.com/news/morocco-begins-large-scale-expulsion-of-foreign-christians-44271/
71 Debrief with Christian worker who was expelled. Unpublished paper 2010.
72 https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/
73 https://www.moroccoworldnews.com/2015/02/152136/moroccan-hackers-behind-cyber-attacks-on-israeli-targets/

Muslim hackers that attacked media outlets in 2014.[74] After more than 100 workers were expelled in 2010, those who attempt to work in Morocco should be using sound cyber security practices. Currently the most likely threats are:

1. Monitoring of unencrypted email, SMS, VOIP, and phone calls.
2. Monitoring of unencrypted web and social media usage.
3. Untargeted malware and phishing attacks.
4. Exposure of personal information by radical Muslim hackers that operate in Morocco.
5. Petty theft.

For those that are engaged in high profile activities, work among suspect populations, or have drawn the attention of the government or radical groups, the following are likely threats:

1. Targeted malware and phishing attacks.
2. Monitoring of encrypted email and VOIP.
3. Monitoring of encrypted web and social media usage.
4. Remote entry to computers and mobile devices, allowing access to encrypted files, webcam and microphones on those devices.
5. Physical search of premises.
6. Targeted effort to circumvent VPN protections.

SAUDI ARABIA

Saudi Arabia conducts raids on private Christian meetings on a regular basis.[75] These raids are reported to be initiated by anonymous tips, but could be the result of surveillance.[76] Expats caught up in raids are expelled, while local people can be arrested, imprisoned, tortured and killed. The government of Saudi Arabia spends more than $37 billion a year on cyber security.[77] The country has one of the most active social media environments in the world.[78] Because of its prevalence, the government is thought to employ a “Social

74 http://themoroccantimes.com/2014/09/10779/cyber-attacks-isils-new-deadly-weapon
75 https://www.jihadwatch.org/2016/09/saudi-arabia-27-christians-arrested-and-deported-for-conducting-christian-prayers-in-private-residence
76 http://www.dailymail.co.uk/news/article-2756134/Dozens-Christians-including-women-children-arrested-Saudi-Arabia-tip-state-s-Islamist-police-force.html
77 http://www.oxfordbusinessgroup.com/news/saudi-arabia-strengthen-defences-against-cyberattacks
78 http://www.economist.com/news/middle-east-and-africa/21617064-why-social-media-have-greater-impact-kingdom-elsewhere-virtual

Media Army"[79] to monitor, interact with and subvert online discussions. The government also seeks to block or monitor all VOIP traffic.[80] All web use is monitored and many sites are blocked.[81] There is also public evidence of government capability to circumvent the encryption of SSL connections, as well as most "secure" chat apps.[82] There is public information that Saudi Arabia has LIG and DPI technologies, as well has tools from The Hacking Team for taking over mobile devices.[83] The most common cyber crime in Saudi Arabia is cyber blackmail – where compromising details are acquired through a cyber attack and used as leverage to receive a payment.[84]

With a virtually unlimited budget for cyber security and top-end surveillance technology,[85] as well as a close partnership with the U.S. in intelligence, Saudi Arabia presents a very challenging environment for Christian workers. Special precautions should be taken to encrypt and compartmentalize sensitive data. Currently the most likely threats are:

1. Targeted theft.
2. Targeted cyber attack on personal devices.
3. Targeted network attacks.
4. Active monitoring of all communications – phone, SMS, VOIP, Chat, email, etc.
5. Exploits against two factor authentication.
6. Cyber blackmail.
7. Arrest, imprisonment and possible torture of those in country who are exposed in a cyber breach.

SYRIA

At the time of this study, Syria is an active war zone that involves not just regional, but global powers. The same is true for the cyber war that is being waged there. The Syrian Electronic Army (SEA) is a hacker group that is aligned with the central government. It has hijacked social media accounts of the opposition, gathered critical intelligence, and changed the outcome of military campaigns. To do this it has used RAT's (Remote Access

79 https://freedomhouse.org/report/freedom-net/2015/saudi-arabia
80 Ibid
81 https://en.wikipedia.org/wiki/Censorship_in_Saudi_Arabia
82 https://moxie.org/blog/saudi-surveillance/
83 http://www.economist.com/blogs/pomegranate/2014/07/internet-monitoring-gulf
84 http://www.arabnews.com/online-blackmail-main-cyber-crime
85 https://www.issworldtraining.com/ISS_MEA/index.htm

Trojan) software as well as spear phishing (targeted phishing), and social engineering techniques.[86] There are reports that the SEA receives help and training not just from the central government, but also from Russia and Iran (both of which are major cyber warfare powers).[87] The central government, while possessing the capacity to heavily filter or cut off the Internet, chooses to lightly filter – but heavily surveil – Internet and social media usage, and gathering user names and passwords of Facebook accounts so that it can access those for intelligence purposes.[88] There are also reports that Russia has sent technical resources that allow it to tap into the core sub-oceanic fiber optic cable that feeds more than 60% of the Internet access for Syria.[89]

It has also been reported that surveillance technology was used to discover the IP addresses of activists opposed to the central government, and that these people were arrested and tortured.[90] The opposition also has a significant cyber warfare capability, and some elements of that opposition received training and funding from the U.S. and other Western powers opposed to the central government of Syria. Other elements of the opposition – ISIS and al-Qaeda – are not aligned with any Western governments and have their own cyber attack capabilities.

There is public information that Syria has LIG and DPI technologies, and advanced Internet surveillance and monitoring tools.[91] There is also evidence that they utilize satellite phone interception and tracking technology as well. The combination of both active physical and cyber warfare – along with the involvement of major militant groups and global cyber warfare powers – makes for an extremely hazardous and complex environment. Currently the most likely threats are:

1. Monitoring of unencrypted email, SMS, VOIP, and phone calls.
2. Monitoring of unencrypted web and social media usage.

For those that are engaged in high profile activities, work among suspect populations, or have drawn the attention of the government or radical groups, the following are likely threats:

1. Targeted malware and phishing attacks.
2. Targeted malware and phishing attacks – which could result in exposure of a network of contacts.
3. Targeted cyber attack on personal devices.
4. Targeted network attacks.
5. Active monitoring of all communications – phone, SMS, VOIP, Chat, email, etc.

---

86 http://www.aljazeera.com/programmes/peopleandpower/2015/06/syria-electronic-armies-150617151503360.html
87 Ibid
88 http://europe.newsweek.com/syria-grants-free-internet-access-so-it-can-snoop-230442?rm=eu
89 https://www.alaraby.co.uk/english/news/2016/10/20/syrian-regime-internet-network-repairs-guise-for-more-surveillance
90 http://www.aljazeera.com/programmes/peopleandpower/2015/06/syria-electronic-armies-150617151503360.html
91 https://sii.transparencytoolkit.org/search?utf8=✓&utf8=✓&q=syria

TUNISIA

The government of Tunisia is publicly known to have LIG and DPI technologies. In 2011 during the Arab Spring uprisings, the government was stealing Facebook users' IDs and passwords on a massive scale through ISPs (Internet Service Providers). This resulted in counter actions by Facebook to restore control of accounts to their rightful users.[92] Some Tunisian hackers have been identified as aligned with ISIS, and have attacked U.S. government websites as well as banking and infrastructure sites in 2014.[93] The Falaga hacking group from Tunisia is also engaged in attacking targets in France and Israel.[94]

While the government of Tunisia has significant cyber attack capabilities – and radical Islamic hacker groups have a history of operating in the country – there have been no direct reports of missional organizations being directly attacked by either group. Currently the most likely threats are:

1. Petty theft.
2. Government monitoring of web, social media and phone activity.
3. Website defacement and destruction if targeted by Tunisian hackers.
4. Possible DDOS attacks on websites.
5. Exposure of identity information by radical Islamic hackers who operate in Tunisia.

92 http://www.theatlantic.com/technology/archive/2011/01/the-inside-story-of-how-facebook-responded-to-tunisian-hacks/70044/

93 http://www.hstoday.us/briefings/daily-news-analysis/single-article/exclusive-tunisian-hackers-announce-cyber-jihad-against-us-banks-airport-computer-systems/7c3d2373e69fa9319e521816ce539b7d.html

94 http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/fallaga-team-tunisian-hacker-group-engages-in-jihadi-hacktivism-active-on-twitter-facebook-youtube/

UNITED ARAB EMIRATES (UAE)

The UAE recently upgraded their laws concerning the use of VPNs. Many missional workers in Dubai stopped using VPNs out of concern that the use would make them subject to heavy fines or expulsion. However, at least one legal opinion holds that their core law is no different from a year ago, only the level of fine has changed. Therefore it is likely that missional workers would not be charged under this law for normal use of a VPN. However, until there is a test case on the matter it remains uncertain.[95]

VOIP services are "unlicensed" and the use of them is subject to heavy fines.[96] There is evidence to indicate that the UAE monitors all communications and web usage. The cyber crime law also contains punishments for offending the state, its rulers, its symbols, or for insulting Islam and other religions. Violating this law can result in arrest. Imprisonment, expulsion, and harsh physical punishment can also be applied.[97] A KPMG cyber survey of UAE in 2015, showed the country to be one of the top ten global locations for cyber crime, with over a third of those surveyed indicating they had been hacked in the last 12 months.[98]

The public record indicates that the UAE is investing in world class surveillance and cyber attack tools.[99] There is additional public information that the UAE has LIG and DPI technologies, advanced video surveillance and facial recognition technology, as well as tools from The Hacking Team for taking over mobile devices.[100] No reports have been received of direct cyber attacks on missional organizations operating in the UAE. The most likely threats are:

1. Monitoring of unencrypted email, SMS, and phone calls.
2. Monitoring of unencrypted web and social media usage.
3. Untargeted malware and phishing attacks – criminal.

For those that are engaged in high profile activities, like work among refugees, or have drawn the attention of the government or radical groups, the following are likely threats:

95 http://www.lexology.com/library/detail.aspx?g=60307f30-2f86-4aae-88fe-0cdae6c427dc
96 https://freedomhouse.org/report/freedom-net/2015/united-arab-emirates
97 Ibid
98 https://home.kpmg.com/ae/en/home/media/press-releases/2015/12/kpmg-uae-cyber-security-survey-2015.html
99 http://www.middleeasteye.net/news/exclusive-uae-elite-task-force-security-secret-surveillance-state-135285760
100 https://sii.transparencytoolkit.org/search?utf8=✓&utf8=✓&q=UAE

1. Targeted malware and phishing attacks.
2. Targeted malware and phishing attacks – which could result in exposure of a network of contacts.
3. Targeted theft.
4. Targeted cyber attack on personal devices.
5. Targeted network attacks.
6. Active monitoring of all communications – phone, SMS, Chat, email, etc.

For additional Country Profiles, please see Appendix N.

CYBER SECURITY SURVEY

The Cyber Security Survey was conducted in July and August of 2016. It sought to determine if cyber security breaches were having a detrimental impact on missional organizations – especially those working in the MENA region. The survey was conducted as an anonymous assessment and no identifying information was collected on respondents. The anonymous survey was chosen to increase the likelihood that organizations would report adverse impacts.[101] The survey was "advertised" through a cyber security affinity group in the missions community and via a private mailing list of participants in a regional ministry conference. Thirty respondents completed the on-line survey utilizing Survey Monkey.[102]

SURVEY LIMITATIONS

Before the survey was conducted, we sought out existing data on cyber security breaches in missional organizations to help establish a baseline, but we didn't find any. As in any survey, we were somewhat limited by the perceptions of the respondents. It is possible for two organizations to have cyber security programs that are vastly different technically, yet both report that they have effective programs. We sought to mitigate this through questions about outcomes and spending that helped to identify gaps in effectiveness.

While preparing the survey, we received feedback from potential survey participants that long and detailed surveys would be rejected or only answered in part. Therefore, we endeavored to keep the survey concise, thus limiting its scope. We also recognized that it was possible for survey respondents to be unaware of cyber attacks that had penetrated their organization, and have a false sense of security. This issue could not be resolved in the survey as it was an "unknown unknown" for the respondents. We did seek to address this gap in the section of the report on risk mitigations.

SURVEY DATA

The survey collected data about the following issues:

- Adverse impacts of cyber security breaches
- Details about the cyber security program of the organization
- Attitudes about cyber security / cyber risk
- Felt needs in cyber security
- Organizational demographics
- Additional cyber security needs

101 Multiple anecdotal reports of adverse impacts have been shared with the author "off the record," thus indicating that adverse impacts are occurring and that organizations typically don't disclose them.

102 Https://www.surveymonkey.com

A list of all of the survey questions can be found in Appendix J.

ADVERSE IMPACTS OF CYBER SECURITY BREACHES

In this section of the survey, respondents were asked to indicate Yes, No, Not Sure or NA for various adverse impacts. The purpose of the “Not Sure” response was to capture data about “possible” adverse impacts. In the case of cyber security, the respondent may not be ‘certain’ that specific adverse impact was caused directly by a cyber security breach, or they may know institutional lore about an adverse impact that cannot be verified. In this part of the survey, we viewed “Not Sure” responses as indicating that a specific adverse impact may have happened as a result of a cyber security breach.

Following are the key findings about the adverse impacts that missional organizations have experienced due to a breach of cyber security.

DEATH

4% reported the death of a local disciple / local worker / expat worker due to a breach of Cyber Security.

IMPRISONMENT

39% reported that local disciples / workers were imprisoned due to a breach of Cyber Security.

LOSS OF ORGANIZATIONAL REPUTATION

10% reported that there had been a loss of organizational reputation due to a breach of Cyber Security.

ARREST AND HARASSMENT

40% reported that local disciples / workers had been arrested or harassed due to a breach of Cyber Security.

EXPULSION

30% reported that an expat worker had been expelled from the country due to a breach of Cyber Security.

SHUT DOWN OF MINISTRY / PROGRAM

30% reported that they had a ministry or program shut down due to a breach of Cyber Security.

LOST TIME AND RESOURCES

47% reported that they had experienced a loss of time and resources due to a breach of Cyber Security.

ADVERSE IMPACT SCORE

To facilitate analysis of the overall impact of cyber security breaches, we have constructed a weighted scoring system based on the severity of adverse impacts that an organization has experienced. The purpose is to provide a single score that indicates how deeply an organization has been impacted due to a cyber security breach.

Weighted Scoring:

- Death of a worker or disciple is the most severe adverse impact and is scored as a 10, for both the impact on the family and colleagues of that worker, and the organization and ministry work as a whole.
- Imprisonment of a worker is scored as an 8, for the impact on the worker, their family, the organization and ministry work as a whole.
- Loss of organizational reputation is scored as an 8, for the broad impact on an organization in recruiting, fund raising and field operations.
- Shut down of a ministry or program is scored as a 7, for the impact on the local ministry and the loss of resources invested in the work by the larger organization.
- Arrest and harassment of a worker is scored as a 5, for the impact on the worker, their family and the local ministry.
- Expulsion of an expat worker is scored as a 5, for the impact on the local work and the larger organization.
- Lost time and resources are scored as a 3, as it represents the least impact on the workers and the work of an organization.

Maximum Adverse Impact Score:

1. Death of national worker – 10 points
2. Death of expat worker – 10 points
3. Imprisonment of national worker – 8 points
4. Imprisonment of expat worker – 8 points
5. Loss of organizational reputation – 8 points
6. Shut down of ministry program – 7 points
7. Arrest or harassment of national worker – 5 points
8. Expulsion of expat worker – 5 points
9. Lost time and resources – 3 points

The total is 64 points for a maximum adverse impact score.

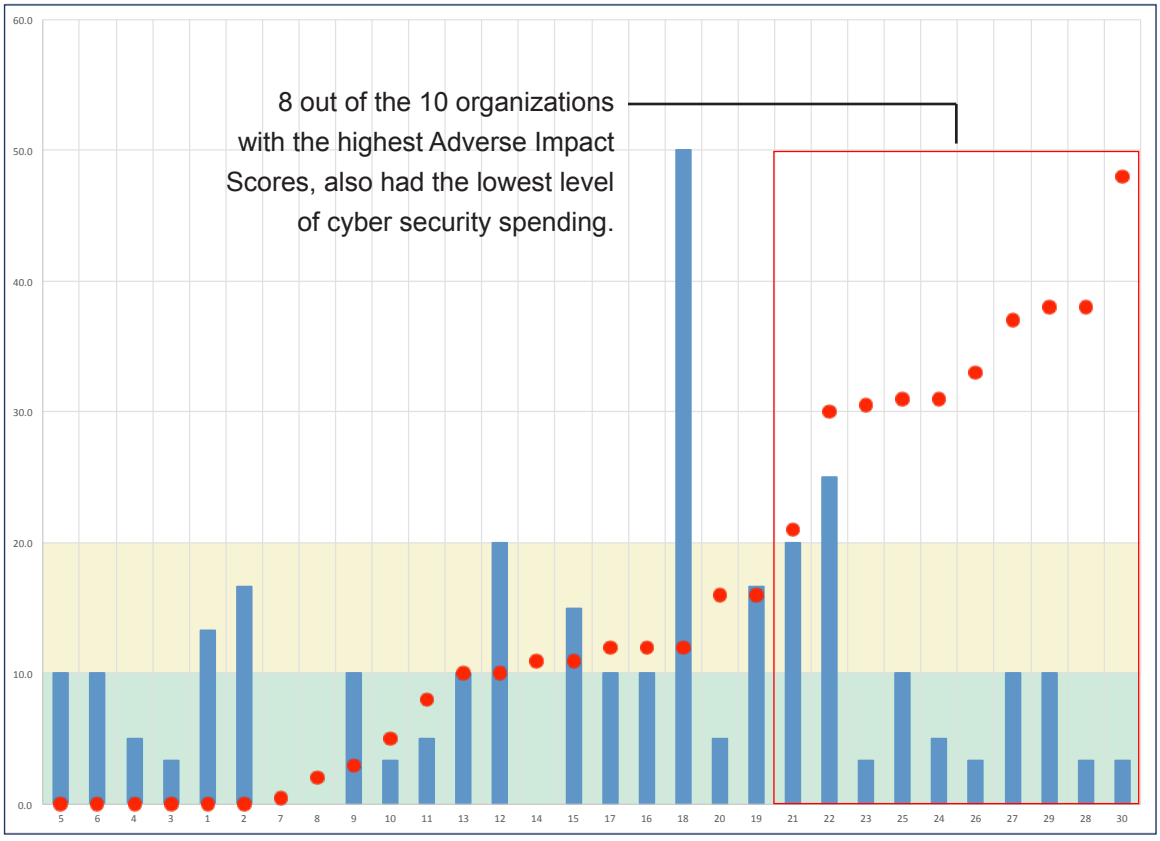
Because “not sure” responses represent possible impact, those were scored at 25% of the category score to capture the impact load for an organization.

After initial scoring, the data was reviewed to determine whether or not those organizations with low scores actually represented highly adverse impacts. For example, if an organization with a total score of 10 – which would be considered “low” over all – had reported a death due to a cyber security breach (a score of 10), this would indicate that the scoring system was actually down-grading the impact of that death. Review of the data showed that the scoring system was rational and was not downgrading or hiding highly adverse impacts.

The scored data fell into three main groupings:

Scores less than 10 – **low level** of adverse impact (9 respondents)
Scores of more than 10 but less than 20 – **medium level** of adverse impact (11 respondents)
Scores above 20 – **high levels** of adverse impact (10 respondents)

Adverse Cyber Impact vs. Relative Funding for Cyber Security



This graph represents the relationship between the Adverse Impact and the Cyber Security Funding Level. The vertical blue columns represent the amount of money spent on cyber security in proportion to the size of the organization. The red dots represent the Adverse Impact Score for the organization. The higher the Adverse Impact Score, the worse the result for the organization. The taller the vertical column, the more that was spent on cyber security. For data points with no column, the organization did not disclose Cyber Security Funding levels.

The horizontal lines represent both Relative Cyber Security Funding levels and Adverse Impact Score. A ranking of 10 or below is the lowest level of funding – where small organizations that spent $25K or less received a 10, medium-sized organizations with that level of spending received a 5, and large organizations with that level of spending received a 3. A ranking of 10 or below for Adverse Impact Score (shaded green) is a low level of adverse impact. A ranking between 10 and 20 (shaded yellow) is a moderate Adverse Impact Score. A ranking above 20 (not shaded) is a high Adverse Impact Score.

The most striking result from this graph is the following: 8 out of the 10 organizations with Adverse Impact Scores above 20 (see red box), also had the lowest level of relative cyber security spending.

Not all organizations with low cyber security spending had high levels of adverse impact, but **80% of those organizations with the highest levels of adverse impact had the lowest level of cyber security spending**.

CURRENT STATUS OF CYBER SECURITY PROGRAM

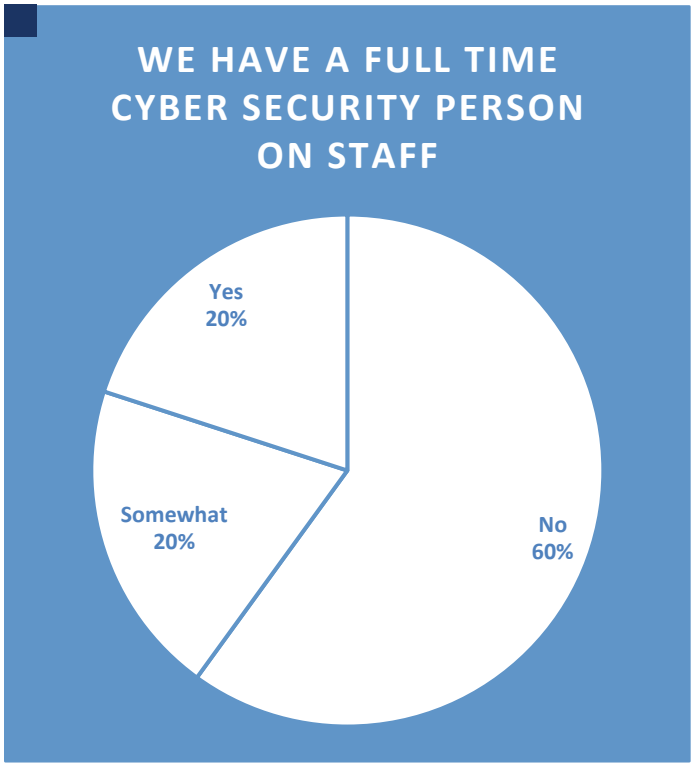
Five questions were asked to gain an understanding of the current cyber security programs utilized in the missional organizations:

1. Do you have a full time cyber security person on staff?
2. Do you have a cyber security advisor or consultant?
3. Have you conducted a cyber security risk assessment?
4. Have you implemented a cyber security risk reduction plan?
5. Have you implemented a cyber security risk reduction training for staff?

Responses were Yes, No and “Somewhat.” The “Somewhat” answer was allowed to capture partial efforts or informal relationships. For example, an organization may not have a full time cyber security professional on staff, but they may have someone part time in that role or at least have a staff member with cyber security as part of their job description.

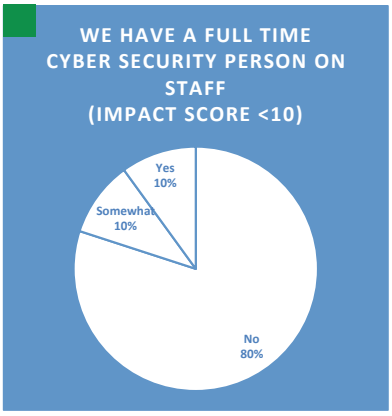
Following are the responses from the responding missional organizations.

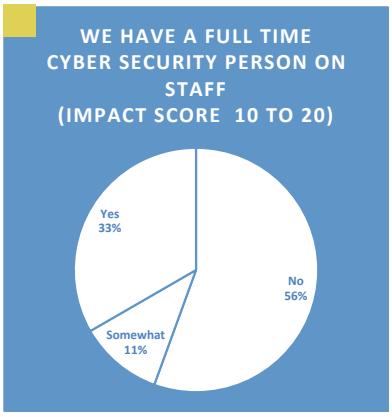
CURRENT STATUS OF CYBER SECURITY PROGRAM: Question #1

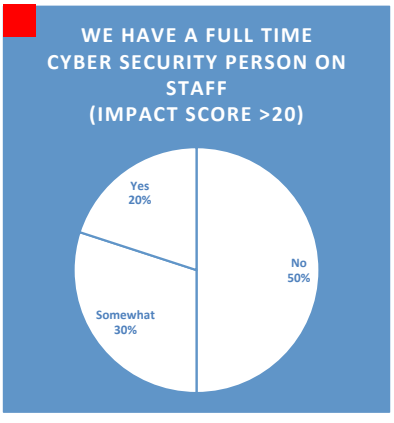


In response to the first question, 60% of all respondents reported that they did not have a full time cyber security professional on staff. Interestingly, large organizations (with more than 500 staff members) had only a slightly higher rate, with 50% reporting that they did not have a full time cyber security professional on staff.

When we break out the responses to this question based on the Adverse Impact Score, we find that those organizations with moderate scores (10 to 20), were more likely to report they had a full time cyber security professional on staff.

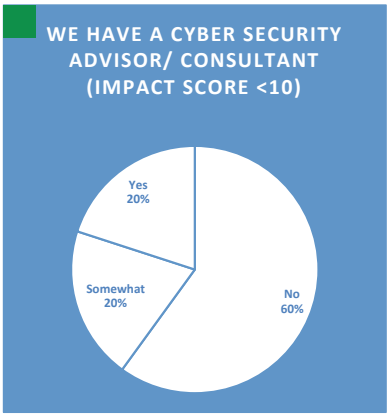


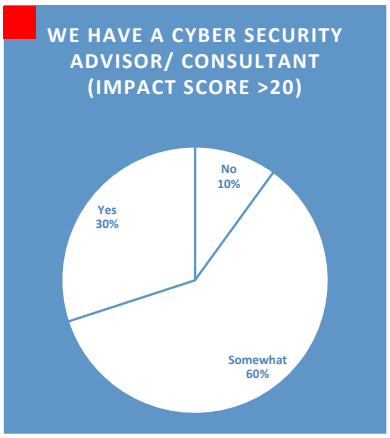




Low Impact Score
Medium Impact Score
High Impact Score

CURRENT STATUS OF CYBER SECURITY PROGRAM: Question #2

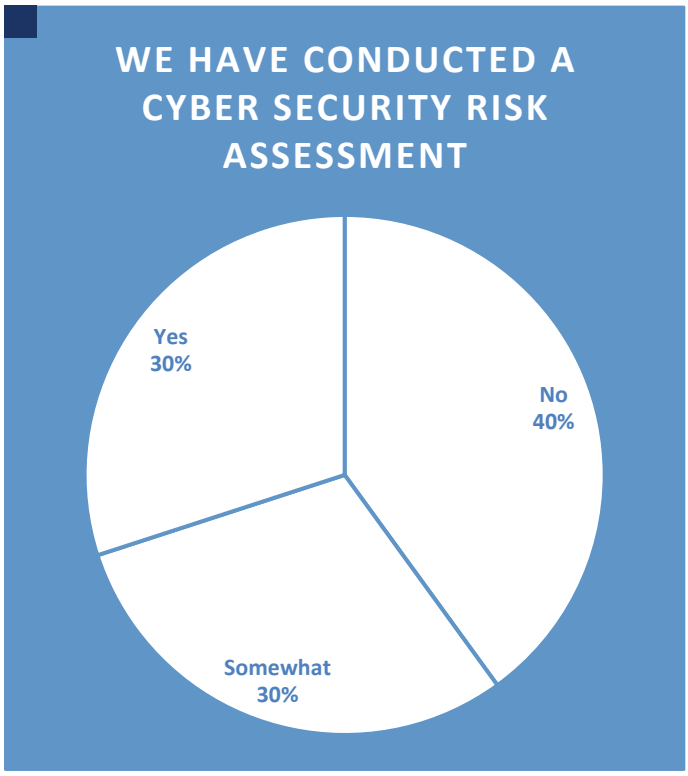


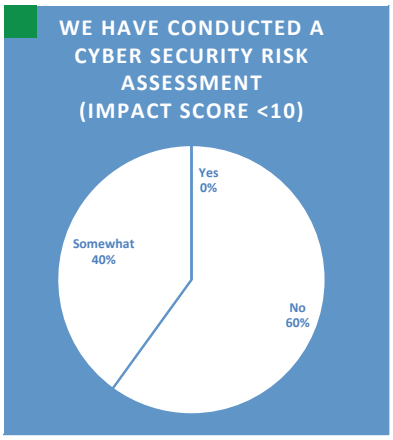


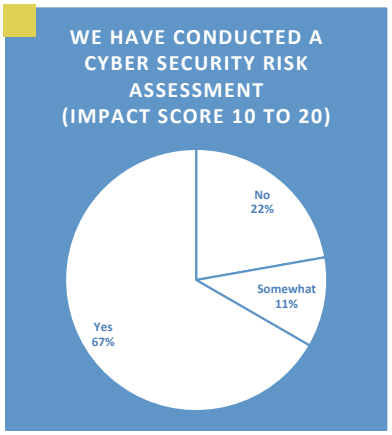
In response to the second question, 77% of all respondents said they had some type of cyber security advisor or consultant. However, when we break out the responses based on Adverse Impact Scores we get a very different picture. Among those organizations with moderate scores (10 to 20) almost 90% said that they definitely had a cyber security advisor or consultant. In contrast to this, among the organizations with the highest levels of Adverse Impact Scores, only 30% reported that they definitely had an advisor. Of those organizations with the lowest scores, 60% reported that they did not have an advisor. In the previous question about full time cyber security staff, 80% of these organizations reported that they did not have full time staff.

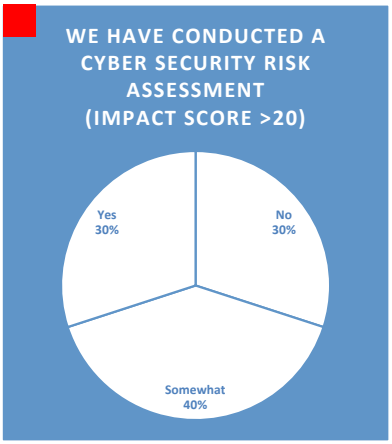
Low Impact Score
Medium Impact Score
High Impact Score

CURRENT STATUS OF CYBER SECURITY PROGRAM: Question #3







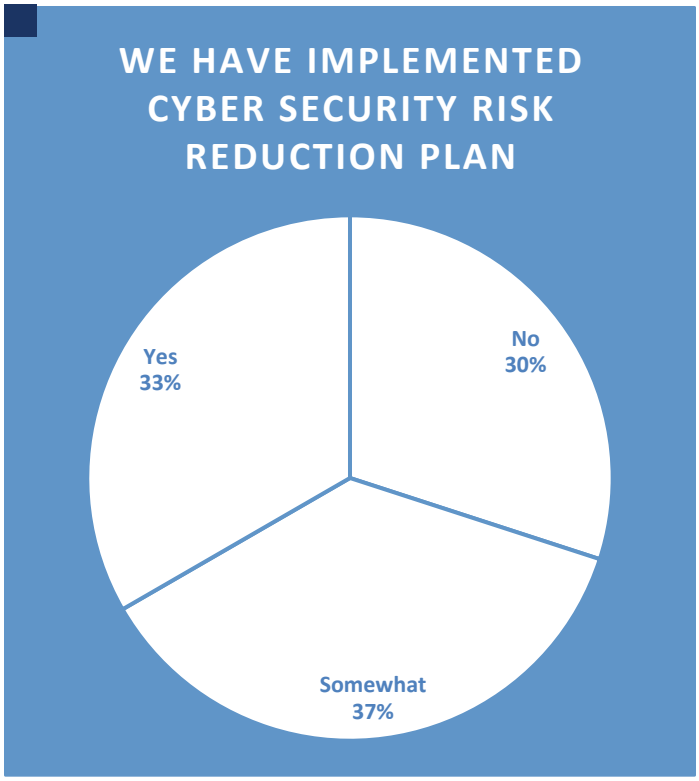


Low Impact Score
Medium Impact Score
High Impact Score

For the third question, 60% of all respondents indicated that they had done some type of cyber security risk assessment and 30% saying they had definitely conducted an assessment. Some 40% of organizations reported that they had not done any risk assessment at all.

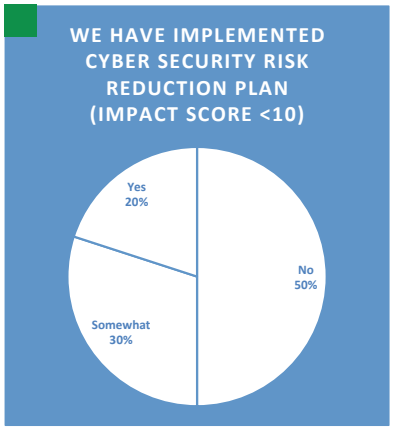
Breaking out the results based on Adverse Impact Scores, those organizations with mid-level impact scores (10 to 20), 67% reported a definite cyber risk assessment rate, which is 37% higher than the average rate. Among those organizations with the highest Adverse Impact Scores, (>20), only 30% of entities reported that they had definitely done an assessment.

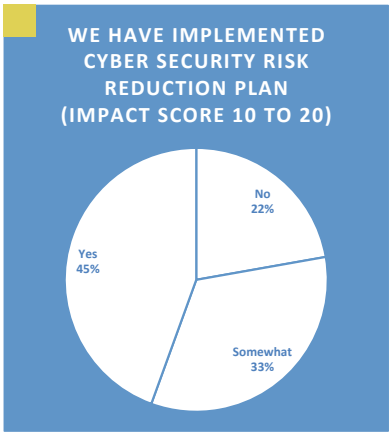
CURRENT STATUS OF CYBER SECURITY PROGRAM: Question #4

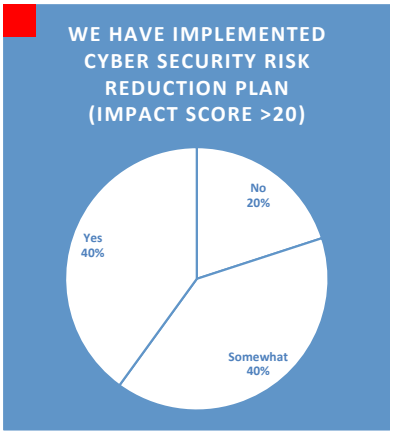


On question four, some 70% of respondents reported that they were implementing some type or cyber risk reduction plan. This was 10% more than those who reported having a cyber risk assessment.

When breaking the results out by Adverse Impact Scores, organizations with mid-level and high levels of adverse impact reported a nearly 80% rate for implementing some type of cyber risk reduction plan.





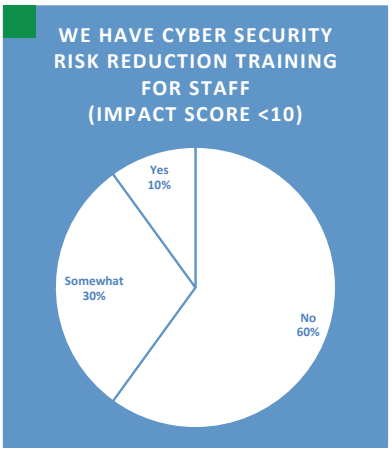


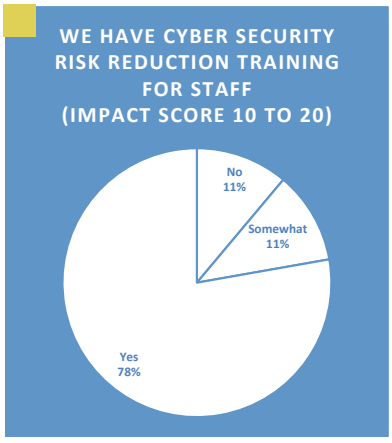
Low Impact Score
Medium Impact Score
High Impact Score

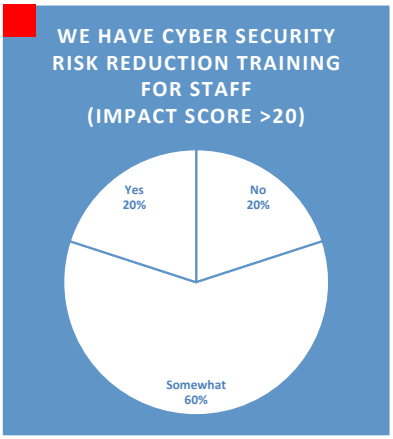
CURRENT STATUS OF CYBER SECURITY PROGRAM: Question #5

On question five, 70% of all respondents reported some type of cyber risk reduction training.

When we break out the results based on Adverse Impact Scores, we find that 78% of organizations with mid-level scores reported having definitely implemented cyber risk reduction training for staff. This is more than three times the level (20%) reported by those organizations with high adverse impact scores.







Low Impact Score
Medium Impact Score
High Impact Score

In analyzing the response to the five questions, it was important to break out the results by Adverse Impact Scores to get a more accurate picture of the importance the organizations place on cyber security.

For those organizations with low Adverse Impact Scores, it appears that cyber security is a low organizational priority as the majority did not have cyber risk assessments, cyber risk reduction plans or training. These organizations are therefore at risk of highly adverse cyber security breaches. It is also possible that these organizations have undetected cyber security breaches and unrecognized adverse impacts.

For organizations with mid-level Adverse Impact Scores, cyber security appears to be a high priority as almost 80% reported having cyber risk reduction training, almost 70% reported having a cyber risk assessment, and almost 90% reported having a cyber security advisor or consultant. The only gap in this reporting was in the development of a cyber risk reduction plan, with less than 50% reporting definite plans.

Overall, the data suggests that these organizations are aware of negative impacts, have invested in assessment and mitigation and are seeking to improve their risk profiles. In the case of organizations with high levels of Adverse Impact Scores, the profile is dominated by the response “somewhat.” This appears most strongly when comparing the results of organizations with mid-level Adverse Impact Scores and those with high Adverse Impact Scores.

Cyber Risk Mitigation	Mid-Level Score Response	High Level Score Response
Cyber Security Advisor	“Somewhat” 11%	“Somewhat” 60%
Cyber Risk Assessment	“Somewhat” 11%	“Somewhat” 40%
Cyber Risk Training	“Somewhat” 11%	“Somewhat” 60%

Because the “somewhat” answer indicates a partial or incomplete action as opposed to a “yes” response, it appears that those organizations with high Adverse Impact Scores are less engaged with cyber security issues than the organizations with Mid-Level Adverse Impact Scores. This might be explained in a couple of ways. The first would be that organizations with high Adverse Impact Scores are “playing catch up” in the face of multiple breaches. As this survey is a snapshot in time, these organizations might be much more focused on their cyber risk in a few months.

The second possibility is that the leadership of these organizations are not well informed – or do not take seriously – the adverse impacts that their organization is experiencing. The fact that 8 out of 8 of the organizations with high Adverse Impact Scores (in excess of 30) all have low relative cyber security spending levels, indicates that these organizations are not engaging with their cyber security breach issues in a focused and effective way.

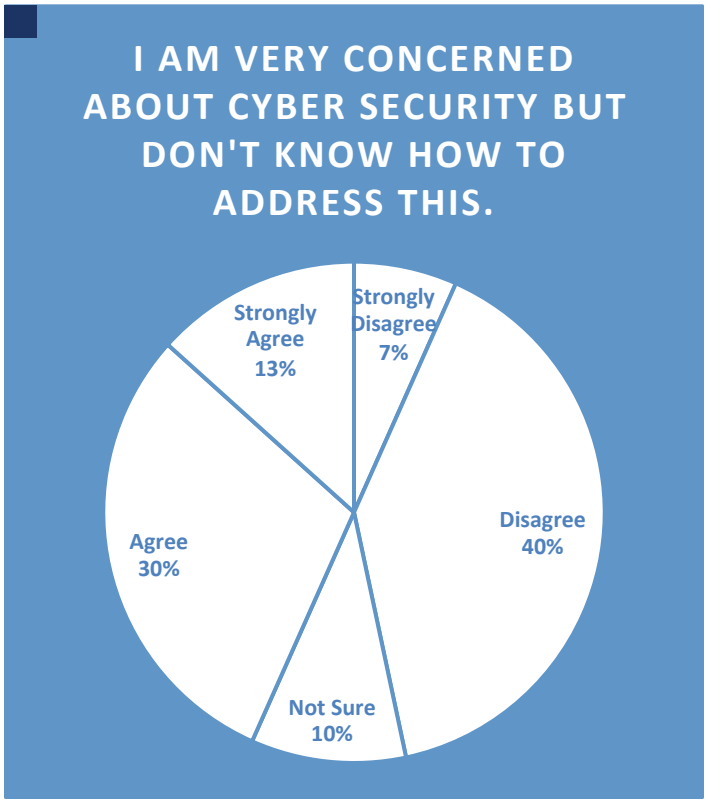
ATTITUDES ABOUT CYBER SECURITY

Six questions were asked that sought to measure organizational attitudes about cyber security risk. These were presented as statements with the response range of Strongly Agree, Agree, Not Sure, Disagree, Strongly Disagree:

1. I am very concerned about Cyber Security but don't know how to address this.
2. Cyber Security is important but not in our top ten list.
3. We lack personnel and specialty knowledge to address Cyber Security risk.
4. Our biggest hindrance to dealing with Cyber Security risk is lack of budget.
5. Cyber Security risk is the last thing I want to talk to a donor about.

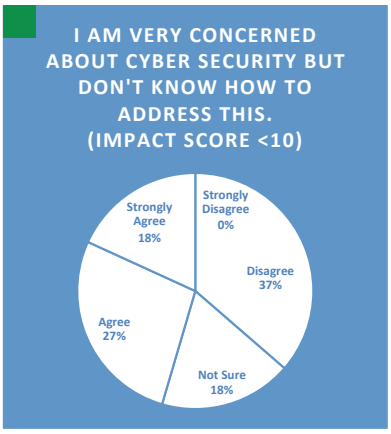
Following are the responses from the responding missional organizations.

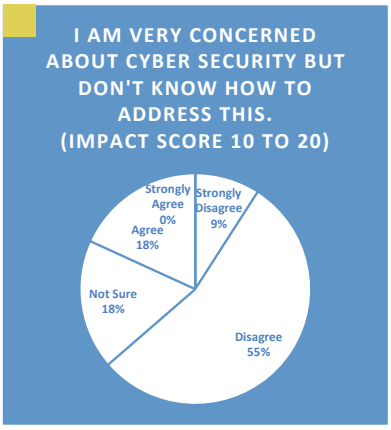
ATTITUDES ABOUT CYBER SECURITY: Question #1

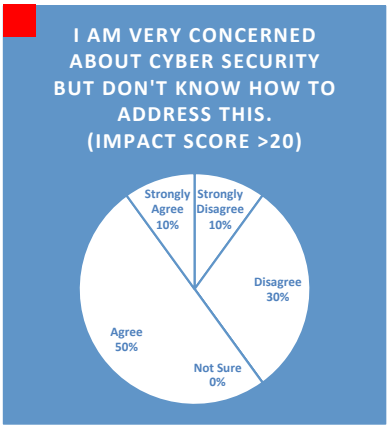


Of all respondents, 43% felt they did know how to address cyber security issues while 47% did not feel they knew how to address these issues.

When breaking responses out by Adverse Impact Scores we find some very important differences. Among those organizations with the highest Adverse Impact Scores, 60% felt they did not know how to address their cyber security issues. In contrast, 65% of those with mid-level Adverse Impact Scores (10 to 20) felt they did know how to address their issues. This fits with the trends we found in the last series of questions that appeared to show this group actively engaged in improving their cyber security profile.

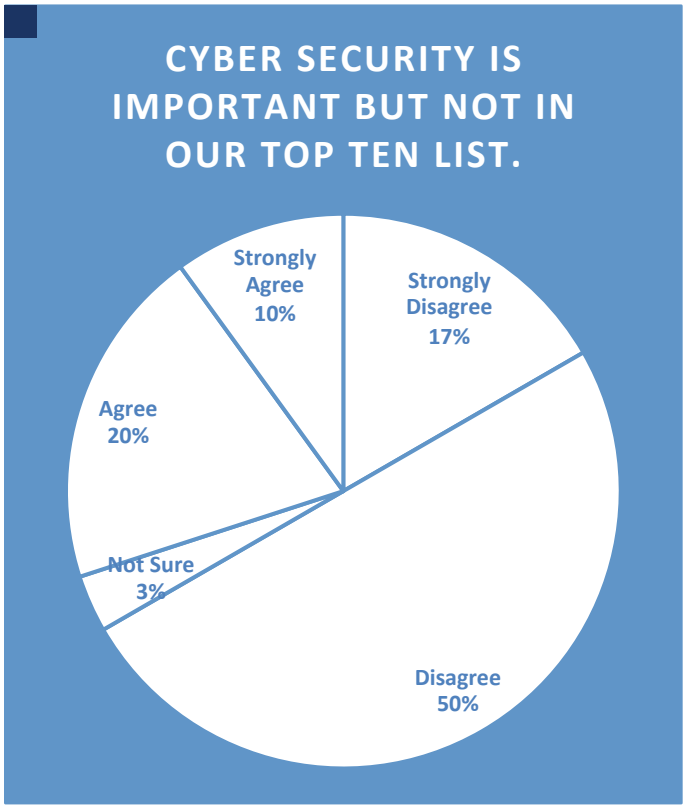






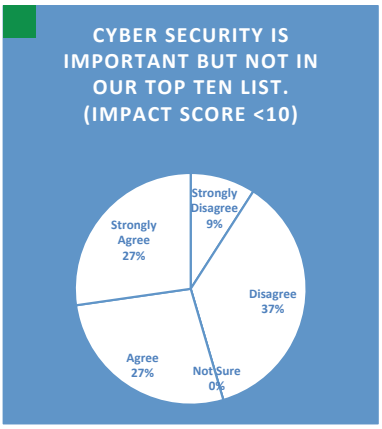
Low Impact Score
Medium Impact Score
High Impact Score

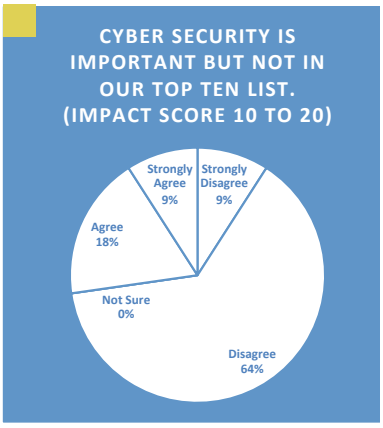
ATTITUDES ABOUT CYBER SECURITY: Question #2

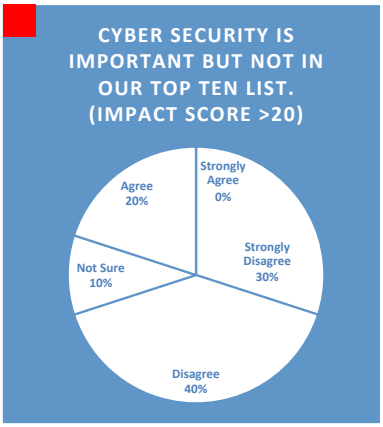


The goal of the second statement is to detect the level of urgency that an organization has about cyber security. Among all respondents, 30% indicated that cyber security was not a high priority.

When we break out results based on Adverse Impact Scores, we find that 54% of those organizations that currently experience a low level of adverse impact from breaches do not consider cyber security to be a high priority.

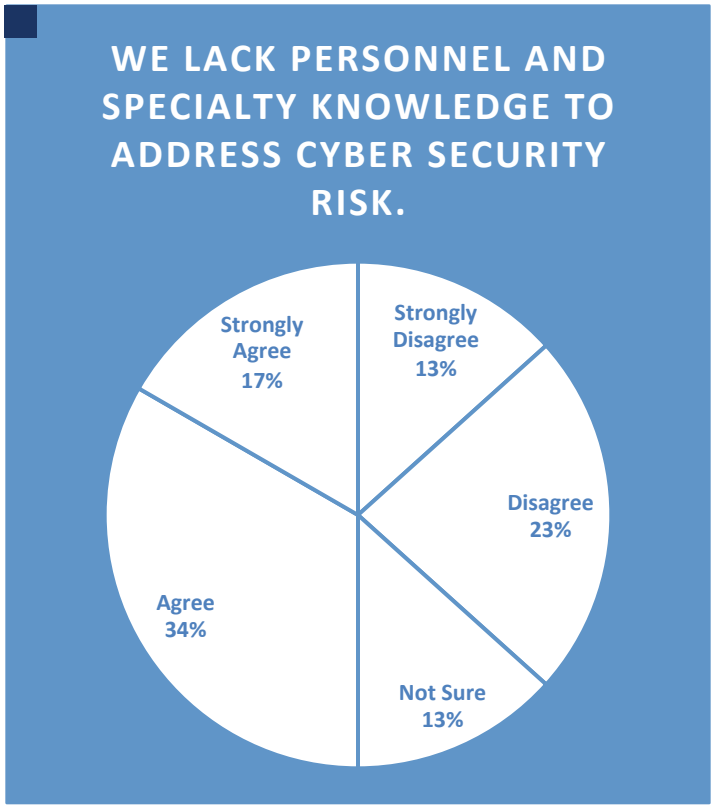






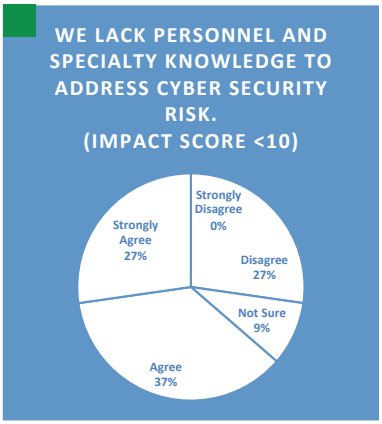
Low Impact Score
Medium Impact Score
High Impact Score

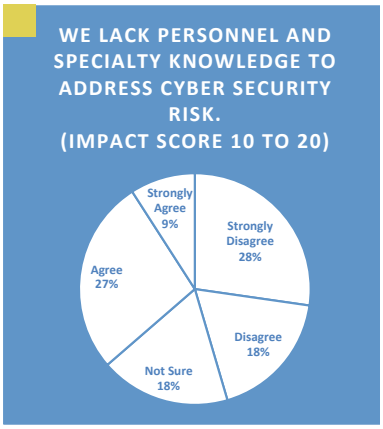
ATTITUDES ABOUT CYBER SECURITY: Question #3

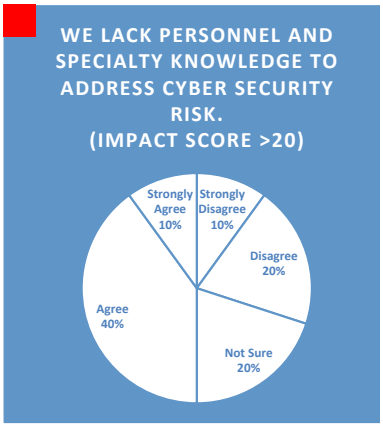


Among all respondents, over 50% felt they lacked the specialty personnel and knowledge to address their cyber security issues.

When breaking out the results based on Adverse Impact Scores, we find that only 36% of those with mid-level scores felt they lacked the specialty personnel and knowledge to address their cyber security issues. This appears to affirm the general finding that these entities are investing in and engaging to address cyber security risk.

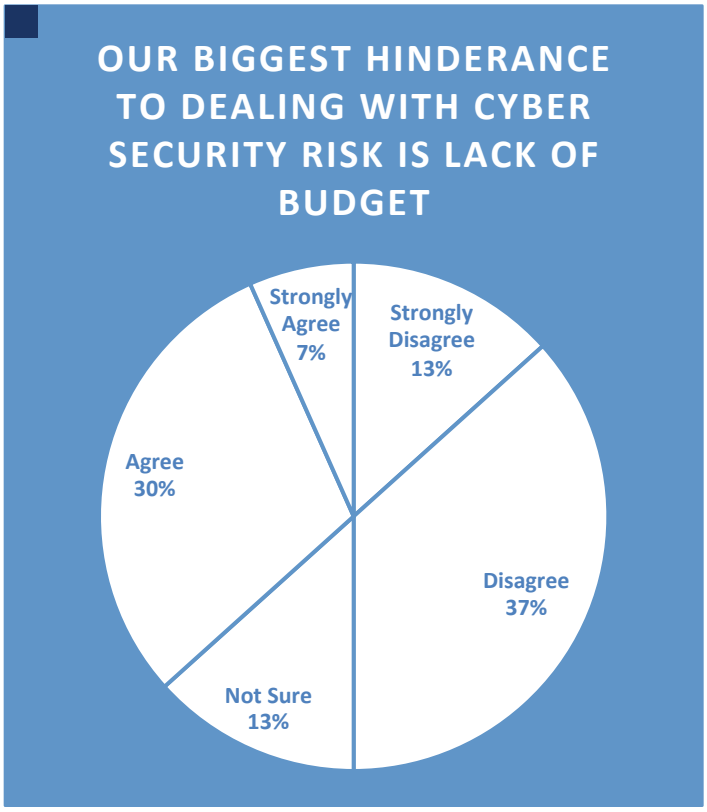






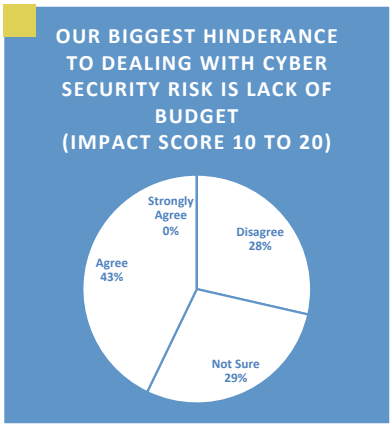
Low Impact Score
Medium Impact Score
High Impact Score

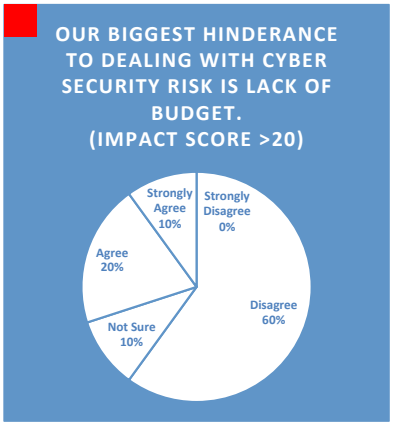
ATTITUDES ABOUT CYBER SECURITY: Question #4



Among all respondents, 50% felt that budget was not the greatest hindrance to dealing with their cyber security issues while 37% felt it was the single biggest challenge.

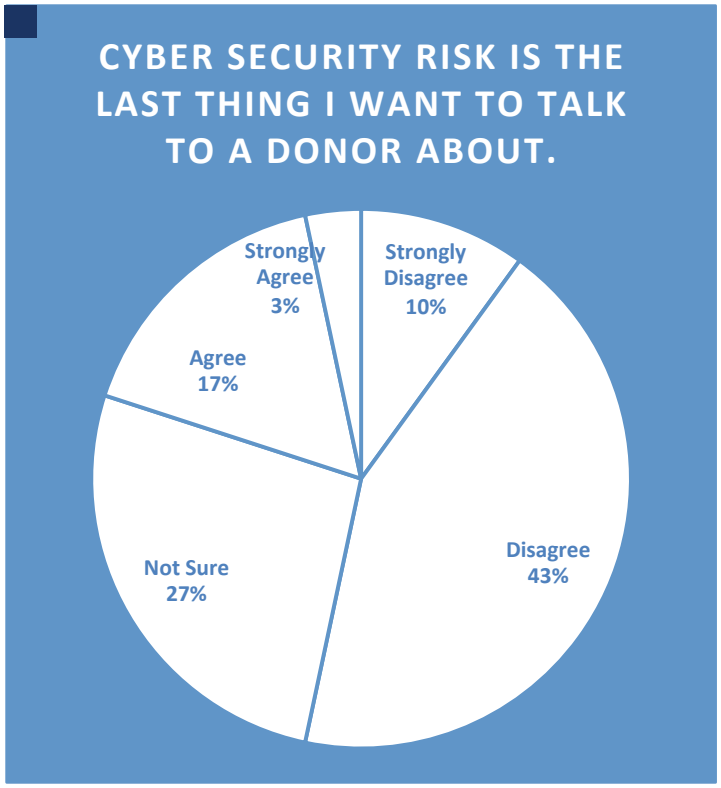
When breaking out the results based on Adverse Impact Scores, 60% of those with high scores (over 20) stated the budget was NOT their biggest hindrance. This group has some of the lowest levels of relative spending for cyber security. This appears to indicate that for these organizations, lack of funding does not control the level of expenditure for cyber security.

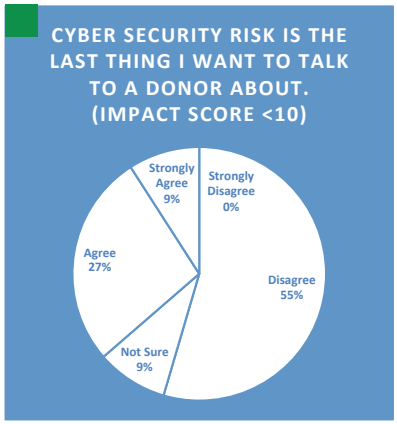


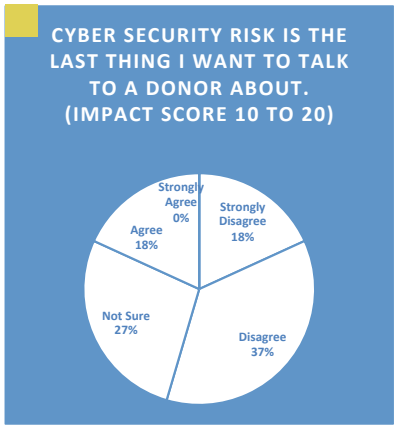


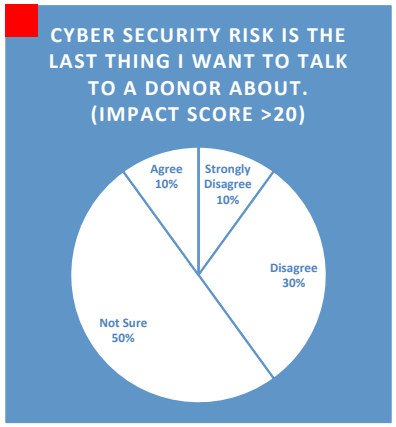
Low Impact Score
Medium Impact Score
High Impact Score

ATTITUDES ABOUT CYBER SECURITY: Question #5





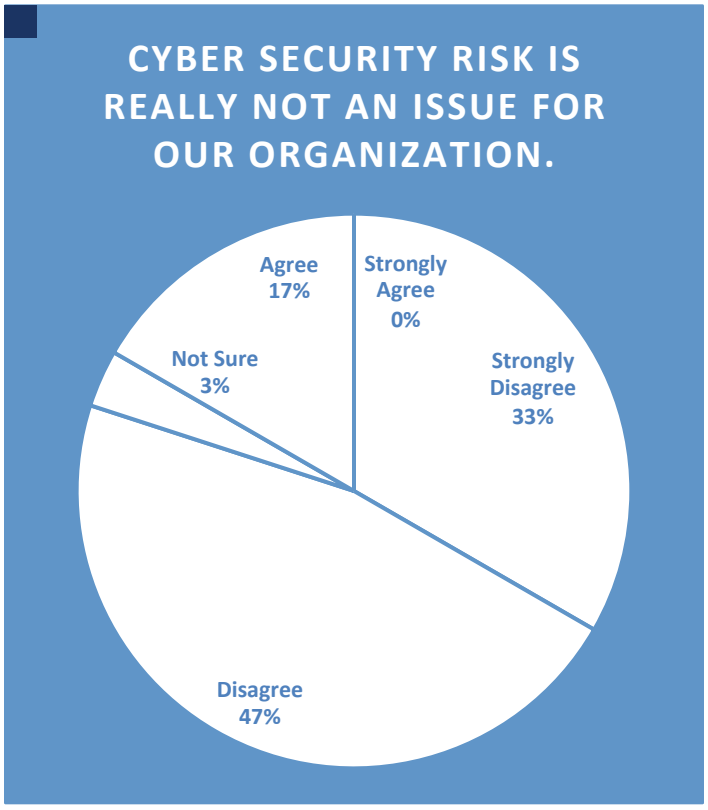




Among all respondents, 20% indicated they did not want to discuss these issues with donors (potentially cutting themselves off from funding for this very area). However, when taking into account "not sure" responses, 47% of all respondents were either unwilling or reluctant. When breaking out results based on Adverse Impact Scores, we found that entities with high scores were the most reluctant. It is worth noting that among those with high scores, they also indicated that budget was not the key factor holding back their response to cyber security needs. Additionally, 60% of this same group also responded that they "somewhat" had a cyber security advisor or consultant. There appears to be a correlation between the reluctance to discuss issues with donors and a reluctance to fully engage with a Cyber Security advisor or consultant.

Low Impact Score
Medium Impact Score
High Impact Score

ATTITUDES ABOUT CYBER SECURITY: Question #6



This statement attempts to capture attitudes about cyber security in general. Among all respondents, only 17% state that cyber security is not an issue for their organization.

When we break out the responses based on Adverse Impact Scores, only 8% of the Mid-level group indicate that cyber security is not an issue for their organization.

Low Impact Score
Medium Impact Score
High Impact Score

CYBER SECURITY ASPIRATIONS

The next set of statements are intended to capture the aspirations of organizations toward Cyber Security. Respondents were asked “Would any of these things help you in dealing with Cyber Security Risk?” The items were:

1. Cyber security risk assessment
2. Cyber security risk reduction plan
3. Cyber security training for technical staff
4. Cyber security training for field staff
5. Trusted vendors that can help them
6. Funding for cyber security expertise, equipment and software
7. Cyber security network which shares threats and information

Following are the key findings about their cyber security aspirations:

RISK ASSESSMENT

Over 80% of all respondents felt that a Cyber Security Risk Assessment would improve their cyber risk profile.

RISK REDUCTION PLAN

Over 80% of all respondents felt that a Cyber Risk Reduction Plan would improve their cyber risk profile.

CYBER SECURITY TRAINING

Cyber Security Training for technical staff *and* field staff was desired by over 70% of all respondents.

TRUSTED VENDORS

63% reported that utilizing Trusted Vendors that could help them would improve their cyber security profile.

FUNDING

69% indicated that Funding for Cyber Security Expertise, Equipment and Software would be helpful in improving their cyber security profile.

CYBER SECURITY NETWORK

The perceived usefulness of a Cyber Security Network (which shares threats and information) was overall positive with 81% of all respondents indicating this would help them improve their cyber security profile.

Overall Findings

The respondents to the survey came from a nearly equal number of small, medium and large organizations. The most important result from the survey was the reporting of adverse impacts due to a cyber security breach. Currently there is no clearinghouse for such reports and typically missional organizations don't publicize these breaches. By computing an Adverse Impact Score for each entity, it was possible to filter the survey results in ways which revealed important insights into current cyber security programs, attitudes about cyber security, and cyber security aspirations of missional organizations – especially those with active work in the MENA region.

Overall, organizations aspire to have good cyber security, yet the clear majority do not currently have good practices in place and about half of the entities appear to feel they lack the personnel, knowledge, budget and strategy to address cyber security. Additionally, about half of the organizations that responded to the survey are unwilling or reluctant to talk to donors about cyber security needs.

When breaking out the data by Adverse Impact Scores, a much more nuanced picture is formed. Each Adverse Impact Score group has a profile that can be helpful in identifying key needs and attitudes.

Low Adverse Impact Group

This group has experienced very few or no known adverse impacts from cyber security breaches. One respondent in this group wrote that they have never suffered a cyber security breach. This group has generally low levels of spending on cyber security and has the lowest level of readiness. Even the bright spot of implementing a cyber risk reduction plan is brought into question when there were no entities that had conducted a full cyber risk assessment.

Organizations in this group aspire to have a good cyber security profile and recognize it as an important issue. They would welcome funding and outside expertise to assist them in improving their cyber security program, and more than half are willing to talk to donors about their needs in this area.

It is not clear if the organizations in this group are aware of the cyber security breaches which may have occurred, as they likely lack the capacity to monitor and report such incidents.

Mid-Level Adverse Impact Group

This group has experienced significant adverse impacts and is actively engaged in improving their cyber security profile. They are investing resources in cyber security and do not see outside funding as the key to their success in this area. They appear to have the best level of readiness of any of the Adverse Impact Groups. Most of this group feels it has a strategy, personnel and technical resources to improve their current cyber security status.

High Adverse Impact Group

This group is experiencing the more extreme adverse impacts – deaths, imprisonment, expulsion and shutting down programs. Yet the eight entities with Adverse Impact Scores of 30 or above have the lowest reported level of spending on cyber security. This group also exhibits low levels of cyber security readiness.

Just as with the low Adverse Impact Score group, they report that 40% of the organizations have implemented a cyber risk reduction plan, yet only 30% report having done a full assessment, which brings this response into question.

Most of this group feels that it does not know how to address their cyber security issues, and only 40% feel they have the needed knowledge and personnel to deal with this risk. Most of this group are unwilling or reluctant to discuss their cyber security issues with donors.

Taken together it appears that organizations in this group could benefit from:

1. An experienced cyber security advisor.
2. A cyber risk assessment.
3. Cyber risk training.

Due to the extreme level of the Adverse Impacts experienced, it appears there is need for leadership in these organizations to have regular cyber breach and adverse impact reports to assist in prioritizing a response to this critical problem.

CYBER RISK ASSESSMENT

One of the key steps in the process of improving an organization's cyber risk profile is performing a Cyber Risk Assessment. Traditionally, this assessment was focused around a *Vulnerability Assessment.*[103] This type of assessment identifies areas where an organization *might* be attacked.[104] This results in mitigation efforts that produce best practices that can appear to be disconnected from the core mission of the organization. This can also produce mitigations that don't closely match the actual threats that an organization faces.[105]

An alternative to vulnerability assessment is *Threat Assessment,*[106] which comprises strategies or pathways used to determine the credibility and seriousness of a potential threat, as well as the likelihood that it will be carried out in the future. Performing a Threat Assessment allows an organization to clearly identify threat sources and the risk that each presents to the organization. This makes it possible for the organization to assess which risks are acceptable and where to focus limited resources to gain the best improvement for their cyber security profile.[107] Additionally, threat assessments can be granular – having different levels of mitigation depending on the context – even if in the same organization.

A Cyber Threat Assessment as envisioned in this report entails three major components:

1. THREAT PROFILES

Threat Profiles seek to identify who the Threat Actors are and what Actions they will take. These Actors and Actions are not theoretical, but based on the specific work of the organization and the Actors who are likely to engage with the organization and what Actions those Actors would take.

2. MITIGATIONS

Technical solutions and behavioral changes that are implemented to mitigate the risk presented in the threat profiles.

3. DIGITAL SAFETY PROFILES

These are contextual and practical profiles that match up specific Threat Actors and their most likely Actions with the appropriate technical solutions and behavioral changes needed. Digital Safety Profiles are clearly tied to the work processes of the organization. Thus, compliance with the safety profile "makes sense" to staff members as they can understand the rationale for the mitigations and the importance of the protection offered. These profiles are also tailored for each context within an organization.

103 https://en.wikipedia.org/wiki/Vulnerability_assessment
104 https://en.wikipedia.org/wiki/Vulnerability_(computing)
105 Expat Digital Resources, Threat Centric Digital Security, Presentation 2015, p3
106 https://en.wikipedia.org/wiki/Threat_assessment
107 https://www.sans.org/reading-room/whitepapers/auditing/overview-threat-risk-assessment-76

Developing Threat Profiles

Threat Profiles are made up of two components: Threat Actors, and Actions that those Actors may take. The identification of Threat Actors is specific to the work and context of each organization. However, for missional entities working in the MENA region, there are six Threat Actors[108] which can be identified as a starting place for organizations. In the table below, each Actor is matched with potential risk Actions:

Threat Actors	Actions
Opportunistic Criminals	• Opportunistic theft of devices • Opportunistic theft of information • Malicious Software (Malware) • Password Guessing • Social Engineering • Collecting Public Information
Organizational Staff	• Poor Passwords • Use of apps which steal data • Clicking on links on suspect sites and emails • Opening suspect attachments • Careless handling of equipment • Careless handling of sensitive information • Inappropriate use of Social Media • Failure to follow good security practices • Failure to secure servers
The Curious *This is in the field context: Neighbors, Friends, Local Co-Workers, Host Government*	• Overhearing conversations • Passive monitoring of unencrypted email • Passive monitoring of Social Media • Passive monitoring of calls and SMS • Passive monitoring of web usage • Notice use of finances • Notice attitude toward local government and religion
The Suspicious *This is in the field context: Neighbors, Friends, Local Co-Workers, Host Government*	• Eavesdropping on conversations • Active monitoring of unencrypted email • Active monitoring of Social Media • Active monitoring of calls and SMS • Active monitoring of web usage • Scrutinize use of finances • Scrutinize attitude toward local government and religion • Attempts to access accounts
Militant Groups	• Watch for activity that looks like spying • Watch for activity that appears threatening • Watch for activity that is oppositional
State Actors	• Targeted Monitoring • Active Surveillance • Targeted Interventions

108 Expat Digital Resources, Digital Threat Profiles, Presentation, Rev 2016.02

Developing Mitigations

Mitigations to the Actions of Threat Actors are of two types – Behavioral and Technical. Behavioral mitigations are very important, as at least 25% of all cyber breaches are due to human error or negligence.[109] However, in the case of the Threat Profiles for missional organizations in the MENA region, **almost 70%** of the Threat Actions can be eliminated or greatly reduced by behavioral changes.

BEHAVIORAL MITIGATIONS

Behavioral mitigations are focused on organizational staff. Properly training staff, along with compliance and successful implementation, are critical. This will be the single most important factor in cyber risk reduction.

There are two core behavioral areas or mindsets that need development. The first is a SIR Mindset and the second is a Security Mindset. The SIR Mindset involves awareness of context, identity and reputation. The SIR Mindset is of critical importance for field workers. The Security Mindset involves awareness of secure and insecure actions and the impact of those actions.

1. SIR Mindset

SIR stands for Strategic Intercultural Relations.[110] A SIR Mindset involves three key elements:

- **Legitimacy** – Cultivating an appropriate identity
- **Awareness** – Understanding yourself and those around you
- **Respect** – Behavior that leads to an honorable reputation

Two quick negative examples can help:

> Suppose an expat Christian worker is in a country of focus with a local identity as a small business owner. However, this worker seldom seems to attend to their business and seems to have a disposable income several multiples greater than other owners of similar businesses. This worker casually makes jokes about the local religion and political leadership on social media. This worker also seems to have few local relationships.
>
> Suppose a local Christian worker has a local identity as a school teacher. Yet they have a laptop and mobile phone far more expensive than their peers. Somehow they seem to have more money than their peers and they travel internationally once or twice a year for personal reasons in a context where that would be rare. They also have multiple international phone calls and texts to their mobile phone from non-relatives.

109 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute Research Report, p 11
110 Expat Digital Resources, Threat Centric Digital Security, Presentation 2015, p6

When we place these behaviors in our Threat Profile we find that it would incite high levels of scrutiny and suspicion by The Curious, The Suspicious, Militant Groups and State actors.

A SIR Mindset is not about deception, but rather actions and attitudes that are consistent with an identity within a culture. If there are communications or actions that are part of a Christian worker's purpose – yet would be incompatible with their cultural identity – those should be considered "sensitive information" and handled with a Security Mindset.

2. Security Mindset

A Security Mindset as used in this report consists of two key elements:

- Appropriate actions in response to known threats
- Using an RPD strategy to reduce the risk of "sensitive information"

Appropriate actions in response to known risks involves practices like: not sharing passwords, not clicking on suspect links and attachments, appropriate use of social media, safeguarding equipment, and other baseline behavioral practices.

RPD Strategy

Using an RPD strategy to reduce the risk of "sensitive information" involves three core concepts:

1. **Reduce** – Reduce the amount of "Sensitive Information" you create.
    - Communication Guidelines for how to communicate in this context.
    - Educate partners and constituents about what to communicate to you and about you – drawing from principles of the Communication Guidelines.
    - Know yourself and how you tend to communicate, choose wisely the form of communication and content.
    - Trim Down by reviewing sensitive communication and content and see what you can reduce or eliminate.
2. **Protect** – Protect the Information that you store and share using C3 Method (see Appendix K, L and M for C3 guidelines on VPN's, email, messaging)
    - COVER – to obscure the fact that there is anything to hide. When it is known that there is something of value hidden, scrutiny increases and it becomes much more difficult to keep that information concealed. Cover is tied closely with the SIR principle of Legitimacy – the cover should enable consistent legitimacy, not hinder it. The goal of cover, just like Legitimacy, is to avoid closer scrutiny.

RPD Strategy (continued)

- CONCEAL – If Cover has been compromised, concealment attempts to disguise and encrypt the sensitive information and communication. Concealment, while necessary, is less ideal than cover, because operating under scrutiny is an order of magnitude more difficult.
- COMPARTMENTALIZE - This is the concept that information and communication should be divided such that if it is compromised, it does not expose the entire life of a worker, team and other teams working in the host country or region. When all else fails, compartmentalization helps to limit the fallout.

3. **Detect** – Online Situational Awareness. This attempts to monitor – as close to real time as possible – any information which can compromise personnel or operations. One tool used for this is Google Alerts.

TECHNICAL MITIGATIONS

Technical Mitigations involve a wide range of technical actions – like having a firewall to protect a network and individual machines, using Anti-Virus and Anti-Malware software, hardened network configurations, keeping software and firmware patched and many other interventions.

The following table shows the most important behavioral mitigations, along with whether or not a technical mitigation is possible. It is important to note that in some threat profiles there are no technical mitigations. This table also illustrates that typically *both* behavioral and technical mitigations are needed.

It is critically important to understand that technical mitigations without behavioral mitigations will fail to improve cyber security. As the threat actors become more capable and threatening, behavioral mitigations become more critical for maintaining security.

THREAT PROFILE		MITIGATIONS	
Threat Actors	**Actions**	**Behavioral**	**Technical**
Opportunistic Criminals	• Opportunistic theft of devices	Appr. Actions	Yes
	• Opportunistic theft of information	Appr. Actions	Yes
	• Malicious Software (Malware)	Appr. Actions	Yes
	• Password Guessing	Appr. Actions	Yes
	• Social Engineering	Appr. Actions	No
	• Collecting Public Information	Appr. Actions	Yes
Organizational Staff	• Poor Passwords	Appr. Actions	Yes
	• Use of apps which steal data	Appr. Actions	Yes
	• Clicking on links on suspect sites and emails	Appr. Actions	Yes
	• Opening suspect attachments	Appr. Actions	Yes
	• Careless handling of equipment	Appr. Actions	Yes
	• Careless handling of sensitive information	Appr. Actions	Yes
	• Inappropriate use of Social Media	Appr. Actions	Yes
	• Failure to follow good security practices	Appr. Actions	No
	• Failure to secure servers	Appr. Actions	Yes
The Curious	• Overhearing conversations	SIR+RPD	No
	• Passive monitoring of unencrypted email	SIR+RPD	Yes
	• Passive monitoring of Social Media	SIR+RPD	Yes
	• Passive monitoring of calls and SMS	SIR+RPD	Yes
	• Passive monitoring of web usage	SIR+RPD	Yes
	• Notice use of finances	SIR+RPD	No
	• Notice attitude toward local gov. and religion	SIR+RPD	No
The Suspicious	• Eavesdropping on conversations	SIR+RPD	No
	• Active monitoring of unencrypted email	SIR+RPD	Yes
	• Active monitoring of Social Media	SIR+RPD	Yes
	• Active monitoring of calls and SMS	SIR+RPD	Yes
	• Active monitoring of web usage	SIR+RPD	Yes
	• Scrutinize use of finances	SIR+RPD	No
	• Scrutinize attitude toward local gov. and religion	SIR+RPD	No
	• Attempts to access accounts	SIR+RPD	Yes
Militant Groups	• Watch for activity that looks like spying	SIR+RPD	Yes
	• Watch for activity that appears threatening	SIR+RPD	Yes
	• Watch for activity that is oppositional	SIR+RPD	Yes
State Actors	• Targeted Monitoring	SIR+RPD	Yes
	• Active Surveillance	SIR+RPD	Yes
	• Targeted Interventions	SIR+RPD	Yes

SIR – Strategic International Relations; RPD – Reduce, Protect, Detect

Now that we have a Threat Profile and Mitigations we can build a Digital Safety Profile and develop a scoring system to help us to monitor progress in improving cyber security. Each Digital Safety Profile in this paper builds on the one before. Because of that, the first profile is actually the most critical to put in place as all the others – the more challenging profiles – build upon it.

DIGITAL SAFETY PROFILE – BASELINE	
Threat Profile **Opportunistic Criminals & Organizational Staff**	**Mitigations**
Opportunistic theft of devices Careless handling of equipment	Security Cable for laptops – lock down and remote wipe of devices; Full disk encryption of laptops
Opportunistic theft of information Careless handling of sensitive information Collecting Public Information	Sensitive Information – Reduce, know yourself, trim down; Encrypted communication
Malicious Software (Malware)	Anti-Malware; Patch software and firmware
Password Guessing / Poor Passwords	Password Policy; 2 Factor Authentication; Password Manager
Social Engineering	Training
Use of Apps which steal data	Training; Device level App approval
Clicking on links on suspect sites and emails	Training
Opening suspect attachments	Suspect link blocker
Inappropriate use of Social Media	Communication policy; Training
Failure to follow good security practices	Training
Failure to secure servers	Secure Servers, or move to secure cloud services

Once each mitigation(s) has been identified, they should then be listed and scored as to how much progress has been made in each area. This should be updated on a quarterly basis to help staff see the progress being made against goals.

CYBER RISK MITIGATION

One of the greatest challenges faced in implementing a cyber risk mitigation program is the question of where to start.

In our survey we found that respondents fell into 3 categories:

- **Small** – Organizations of less than 50 people (usually highly distributed and without a central computer network)
- **Medium** – Organizations of 50 to 500 people (often has a central computer network – at least in the main office)
- **Large** – Organizations over 500 people (usually has a central IT infrastructure)

Clearly there is no "one size fits all" solution for cyber risk mitigation. However, we will present possible approaches for each category of organization. For each one, the goal is to provide a starting place that is sound and as low cost as possible. In the previous section, we developed a Baseline – Digital Safety Profile – that identified base level threats and mitigations. The baseline profile is central to all other profiles. Therefore, effort and resources invested in this profile will improve the cyber risk level of any organization.

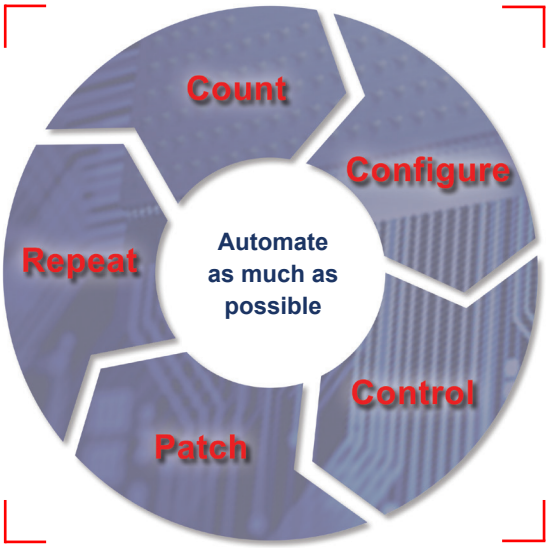
The SANS Institute has produced a guide for cyber risk mitigation that is called Center for Internet Security Critical Security Controls (CSC). However the full CSC[111] can be overwhelming for an organization just starting a cyber risk mitigation program. To focus on early "wins" that any organization can benefit from, the Center for Internet Security has launched a National Campaign for Cyber Hygiene[112] that focuses on the first five Critical Security Controls as the starting point.

NATIONAL CAMPAIGN FOR CYBER HYGIENE

Five core questions that all organizations should be able to answer:

1. Do we know what is connected to our systems and networks? (CSC 1)
2. Do we know what software is running (or trying to run) on our systems and networks? (CSC 2)
3. Are we continuously managing our systems using "known good" configurations? (CSC 3)
4. Are we continuously looking for and managing "known bad" software? (CSC 4)
5. Do we limit and track the people who have the administrative privileges to change, bypass, or over-ride our security settings? (CSC 5)

111 See Appendix C
112 https://www.cisecurity.org/cyber-pledge/



These questions can be further summarized by five key words that identify the main actions that need to take place (and to automate this process as much as possible):

- **Count**
- **Configure**
- **Control**
- **Patch**
- **Repeat**[113]

While these five Critical Security Controls are the most common ones that are recommended, to achieve the Baseline Digital Safety Profile these will need to be supplemented with the following:

1. Security cable for laptops
2. Full disk encryption for laptops
3. Password manager software (see Appendix E for recommended products)
4. Security policies
    - Password policy (see model policy in Appendix G)
    - Communication policy (see model policy in Appendix F)
    - Sensitive information reduction (see model in Appendix I)

While the above actions are certainly more helpful than the full list of 20 core CIS Critical Security Controls, the actual implementation of mitigations can present a bewildering array of technologies that need to be evaluated, cost compared and then implemented. Also, cyber security staff can cost between $75,000 - $175,000[114] a year. To reduce cost and complexity, there are suggested paths forward (starting on page 60) for small, medium and large organizations to reduce cyber risk.

MOBILE DEVICES

Mobile devices dominate most organizations and present a prevailing security risk. In the recommendations that follow in this section of the report, the focus is on tools that lock down phones and prevent the installation of unapproved apps. They also allow leadership to remotely wipe the device of someone who is arrested or their device is stolen. We also recommend services that proxy all web browsing, allowing an organization to set content

113 https://www.sans.org/security-resources/posters/special/20-critical-security-controls-55
114 https://gooroo.io/analytics/skill/CISSP/#

access policies as well as block the activation of malware links that may be inadvertently clicked on by users.[115]

There is one recommendation that we can make to entities of any size regarding mobile, and that is migrating to iOS devices for greater security. In 2015, it was widely reported that 97% of malware for phones was targeted at the Android platform / apps.[116] In 2016, there were some well reported exploits for iOS, but these were mitigated quickly.[117] iOS phones don't provide perfect security, but they are much more secure than stock Android phones.

INTRUSION MONITORING

The widely reported penetration of the U.S. Office of Personal Management shows that having a well-funded cyber security program – with full-time cyber security professionals – does not assure cyber safety.[118] Continuous monitoring for intrusion is required to give assurance that systems are indeed safe. This type of monitoring is called Network Security Monitoring (NSM). NSM requires specialized software and specific technical skills to set up and monitor. One of the vetted vendors in Appendix E provides this service for missional organizations. However, this expense is often outside the budget of small organizations. To meet this need, a new low-cost service is in development by Expat Digital. This new service is expected in Q4, 2017. Inquiries can be sent to info@expatdigital.com.

SECURE SOCIAL CHAT

There is an abundance of social chat apps that claim to be secure. This often presents a confusing landscape for missional organizations, as the consequences of insecure communications can be imprisonment or even death. At this time, there are only two social chat apps that were recognized by the Electronic Frontier Foundation as reliably secure – Signal and WhatsApp.[119] However, the Signal app is generally associated with social change advocates[120] and it not widely used. Therefore, as of the date of this report, the pervasive WhatsApp would be our single recommendation for secure social chat.

SECURE CLOUD STORAGE

A number of organizations now share team resources on group cloud storage. However, this storage is often not encrypted – and even if it is – there can be other issues that put the information at risk, or the identity of those using it at risk. There are two services we recommend for secure cloud storage: https://spideroak.com, an audited and certified supplier, and https://tresorit.com, a very promising competitor.

115 http://info.publicintelligence.net/DHS-FBI-AndroidThreats.pdf
116 https://www.scmagazineuk.com/updated-97-of-malicious-mobile-malware-targets-android/article/535410/
117 http://www.zdnet.com/article/the-state-of-mobile-device-security-android-vs-ios/
118 https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/
119 https://www.eff.org/secure-messaging-scorecard
120 https://www.wired.com/2016/10/signal-cypherpunk-app-choice-adds-disappearing-messages/

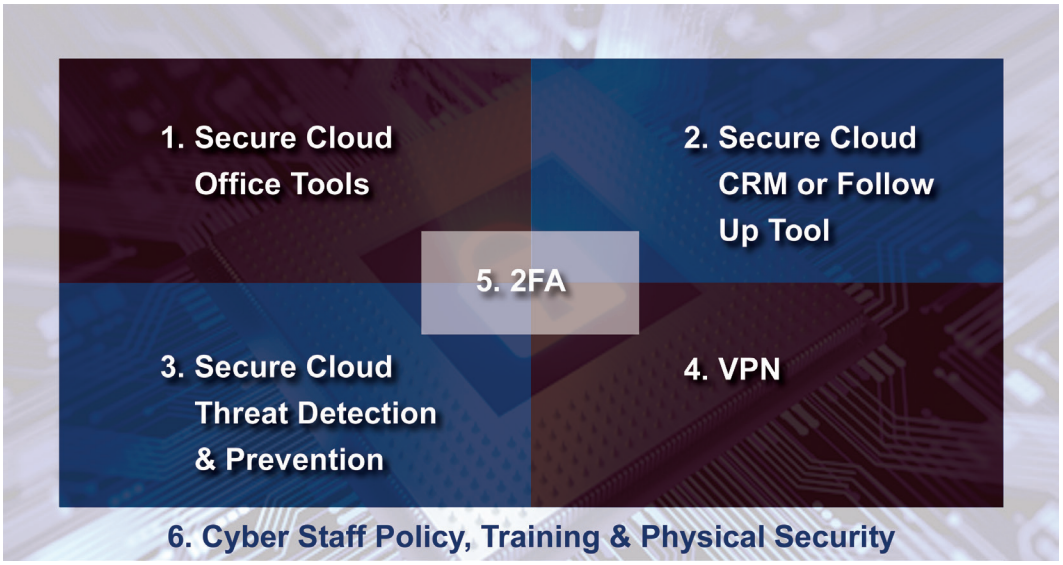
Cyber Risk Mitigation for Small and Highly Distributed Groups

About one-third of the organizations that participated in our survey had less than 50 staff members. Such organizations typically have tight budgets and seldom have dedicated IT staff. They are often highly distributed and do not have a central server infrastructure. They also tend toward BYOD (Bring Your Own Device) for most endpoints (laptops, tablets and phones) in their organization.

This profile presents five core problems for developing a cyber risk mitigation strategy:

- Resource constraints
- Low level of IT support
- No centralized infrastructure to leverage for automating controls
- Securing one endpoint does not scale across the organization
- Lack of training for staff members on security processes and procedures.

To address these problems, we propose that small and highly distributed entities implement a secure cloud-based workflow and cloud-based security tools, along with physical security changes and policy implementations. This approach has six main elements:



1. SECURE CLOUD OFFICE TOOLS

The two main options are Google G-Suite and Microsoft Office 365 Live.[121] Both of these systems have SSL protected access to online resources and data, and have granular group policies that allow control over how access is used and how data is shared. In using these tools, the vast majority of documents created reside on the secure cloud, yet allow

121 Amazon WorkSpace is another potential solution, however at the time of this report there was not enough independent information to add it to our recommendations.

local work without access to the internet. This moves the concentration of sensitive data away from endpoints (laptops, tablets and phones) and concentrates them in the secure cloud.

G-Suite Option

G-Suite or Google Suite is a cloud-based service offered by Google for businesses. The suite includes email, calendar, internal communication tools (both audio and video), documents, spreadsheets, custom forms, presentations, internal websites and file storage. These services differ from the consumer apps, in that Google provides privacy and security guarantees for G-Suite clients.[122] G-Suite also allows users to benefit from Google security research and professionals. G-suite was designed to work with the low-cost Chromebook[123] computer, which has a custom operating system (Chrome OS) that is constantly updated against virus and malware attacks. G-Suite also provides a Mobile Management[124] app that allows protection of all mobile devices in an organization (including BYOD), and incorporates a centrally-managed remote wipe. For organizations with full or part time IT staff, G-Suite offers an organizational control panel. For those without IT staff, a registered service provider can supply needed support remotely and very cost effectively.

Standard Chromebooks can be purchased for $200 - $300 each, and present a lower risk of theft than standard laptops. The Business Suite of G-Suite is $10 a month per user,[125] and provides the needed security controls for in-house IT staff. If an organization lacks IT staff, a registered service provider or reseller can provide the support required remotely.

For a small and distributed organization the G-suite with a Chromebook – and using the Mobile management app – would cover the core issues addressed in the CIS five core requirements, and is an affordable and scalable solution.

122 https://support.google.com/work/answer/6056693?hl=en&ref_topic=6055719
123 https://www.google.com/chromebook/9 https://www.google.com/intl/en_uk/chromebook/about/
124 https://gsuite.google.com/products/admin/mobile/
125 https://gsuite.google.com/pricing.html

Office 365 Option

Microsoft Office 365 offers a comprehensive set of tools for any size office – including MS Word, Excel, Power Point, Skype for Business, SharePoint, Voice and Video calling, file storage and many other office tools. The Enterprise Level 5 Package comes with the control panels needed to have admin and central security control for all users. Microsoft also offers Enterprise Mobility + Security that provides for mobile security and control.

MS Office 365 works on normal PCs and laptops that are more expensive than the average Chromebook. Also, normal PCs and laptops are subject to a range of intrusions that are much less common on the Chromebook. However, MS Office 365 Services can be used in a mixed environment with existing Microsoft Server networks. This allows organizations that already have a network – which is critical to their central office operations – to continue to use that, while flexibly increasing their security profile. They can utilize Office 365 for those areas that do not need to access the central office network.

MS Office 365 is more expensive than G-suite. The Enterprise Grade E5 service is $35 per user per month, plus $8.75 a month for Enterprise Grade E3 for Mobility + Security, for a total of $43.75 per month per user. For a staff or 50 people, this would be $2,187.50 a month. This is much less than the cost of a full time IT person, and certainly less than a staff security person.

However, Microsoft offers a discounted license to religious organizations that are not churches, but are registered 501c3 entities. This make it possible to acquire the license for Office 365 Enterprise E5 for $10 per user per month[126] and the Microsoft Mobility + Security E3 is available for $1.65 per month per user[127] at the time of this report. This takes the price to $11.65 per month per user – which is quite close to the G-suite pricing. An organization can apply for religious[128] and non-profit pricing through Techsoup,[129] a non-profit organization that helps non-profits get free and discounted software.

126 https://products.office.com/en-us/nonprofit/office-365-nonprofit-plans-and-pricing
127 https://www.microsoft.com/en-us/philanthropies/product-donations/products/enterprise-mobility
128 Microsoft has a non-discrimination policy that must be adhered to in order to qualify for reduced price and free software. However, currently Microsoft recognizes that religious entities are exempt from non-discrimination policy. This means that an organization that holds to a Biblical view of gender expression, for example, would be eligible for discounted and free software.
129 http://www.techsoup.org

2. SECURE CLOUD CRM OR FOLLOW-UP TOOL

Most mission organizations in this study are engaged in evangelism, discipleship and church planting. To support this focus, they need some way to keep track of personal details about people they are engaging. Many organizations will use Salesforce or some product built upon Salesforce. For end users, Salesforce can be accessed through a browser. Therefore, it can be accessed on a Chromebook running Chrome OS as well as on a PC or a Mac. This makes it possible for a small and distributed team to utilize a core technology in a secure cloud-based approach.

For organizations that need a distributed secure cloud-based solution for follow-up, ECHO[130] is designed to be browser-based and works very well on a Chromebook. It allows follow-up volunteers to engage those responding to ministry, without giving the volunteers access to the organization's internal network.

3. SECURE CLOUD THREAT DETECTION & PREVENTION

For small and distributed groups, it is difficult to have central antivirus and malware protection. However, new cloud-based services like Webroot[131] make it possible to have key security tools across a distributed organization that are centralized. Webroot provides three core offerings that would be very useful for small and distributed organizations:

WEBROOT®
Smarter Cybersecurity

- **Endpoint Protection** – this is for computers and it protects against virus, malware and emerging threats to your computer.
- **Mobile Security** – this provides security similar to the Endpoint security but for mobile devices.
- **Secure Web Gateway** – this is a service that allows an organization to have all web browser usage done through the Webroot cloud-based system, providing for the deployment of web use policies, and monitoring usage. Additionally, the secure web gateway protects users who click on emails that take them to cyber-attack sites (and offer cyber-attack downloads), which are a major cause of security breaches.

  Webroot Endpoint Protection is not compatible with Chromebooks running Chrome OS, and is seen as unnecessary by the security model of Chrome OS. However, Webroot Endpoint Protection would be compatible with Office 365.

130 https://www.echoglobal.org
131 https://www.webroot.com/us/en/business

Webroot Mobile protection would have overlap with both G-suite Mobile and Office 365 Mobility + Security, but it would function without conflicts. Testing would need to be conducted to see if there is any security gain from "doubling up" Webroot Mobile Security and the mobile security offerings by Office 365 and G-suite.

Webroot Secure Web Gateway is compatible with Chromebooks running Chrome OS as well as PC and Mac platforms. This would be a good tool to implement organizational web usage controls and a critical layer of protection from phishing attacks.

Webroot Endpoint Protection costs $25 per user per year. Non-profit pricing is available, but has to be negotiated directly with Webroot sales. Webroot Mobile Protection is $15 per device per year, and this is much more expensive than the G-suite Mobile Security and Office 365 Mobility + Security, which are licensed by user rather than device. Again, non-profit pricing is available but has to be negotiated directly with Webroot sales. Webroot Secure Web Gateway is $33 a year and also has non-profit pricing.

4. VPN – VIRTUAL PRIVATE NETWORK

Virtual Private Network (VPN) software can provide an encrypted path from an endpoint machine (computer, tablet or mobile phone) to another endpoint. That second endpoint can be a private server owned by the ministry – in which case it would be a closed private connection – or it can be to a server owned by a third party that provides access to the Internet. This second use is now a very common way to protect mobile endpoints (laptops, tablets and mobile phones) from having their web traffic monitored or hijacked when using public Internet access. VPNs can also allow users to bypass firewalls of countries that seek to limit access to online resources, and it protects the user from having their Internet usage monitored. However, not all VPNs are secure. This is especially true for third-party VPNs used to access the Internet. Third-party VPNs can log your Internet usage, sell your personal details (and browsing history), or push ads to you while using the system. Some third-party VPNs are free to use to the end-user, while others charge monthly or yearly fees. For the purpose of this study, we are primarily focused on the use of VPNs to avoid having Internet access monitored or hijacked.

There are a large number of third-party VPN services and it can be very difficult to decipher the sales jargon to compare vendors. A good resource for an independent evaluation of VPNs is: thatoneprivacysite.net[132] Once a VPN has been chosen for an organization, it should be installed on all mobile endpoints (laptops, tablets and mobile phones).

132 https://thatoneprivacysite.net/choosing-the-best-vpn-for-you/

It should be noted that Chromebooks with Chrome OS do allow VPN usage, but they only work with a limited number of VPN products. Therefore, is it important for those using Chromebooks with Chrome OS to confirm that their VPN of choice will work with that platform.

5. 2FA TWO FACTOR AUTHENTICATION

Two Factor Authentication or Multifactor Authentication uses more than a single password to access an Internet resource. The second factor is often a security code that is generated by a stand-alone device[133] or special mobile app.[134] The web resource requires that you provide the correct password and a time-limited secure token to gain access.

Some implementations of 2FA have used SMS to the phone of the user to provide the time limited token, however this has proven to be subject to attack by countries that control the national telecom.[135] Therefore, it is wise to avoid SMS-based 2FA.

G-Suite, Office 365, and many other secure cloud services support 2FA. It provides a significant layer of protection and helps to assure that only the authorized user is accessing a resource.

6. CYBER STAFF POLICY, TRAINING & PHYSICAL SECURITY

For the purpose of this study, we will be handling baseline policies, training and physical security under this heading. Core model policies for passwords and communication are provided in Appendix F and G. Cyber security training has typically been expensive and not very well focused on the needs of ministries. It has also been difficult to deliver the training to a distributed workforce. However, a new online cyber security training service for religious non-profits, Expatdigital.com,[136] is offering an introductory rate of $25 a year per household, with volume pricing for organizations (see Appendix E). This cloud-based service can provide the ongoing training needed to mitigate the human risk factor that untrained staff present. To round out the baseline profile, the most critical physical security component is a laptop cable lock.

By implementing all six of the above components, a small and distributed organization can greatly improve their cyber risk profile and establish a cost-effective foundation on which to build future improvements.

133 https://www.rsa.com/en-us/products-services/identity-access-management/securid/hardware-tokens
134 https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2
135 https://citizenlab.org/2015/08/iran_two_factor_phishing/
136 https://expatdigital.com

COST ESTIMATE FOR IMPLEMENTATION

G-Suite Option

- G-suite for 50 staff @ $10.00 per month or $500 a month and $6,000 a year.
- Chromebooks for 50 staff @ $300 each is $15,000, one time cost.
- The ECHO CRM/Follow-Up solution is $475 a month for 5 concurrent users with a $1,995 set up fee, for a first year cost $5,700 + $1,995 = $7,695.
- Webroot Gateway for 50 staff is $1,650 a year. Multi-year discounts available.
- Computer lock for 50 staff @ $20 each is $1,000.
- High quality VPN for 50 staff @ $132 a year each is $6,600 (assumes totally distributed staff).
- Cyber Security Training with Expat Resources for 50 staff @ $25 a year is $1,250 for the first year and $500 a year thereafter.

Labor

- Once implemented the system must be monitored. It is estimated that this would take a staff network admin about 5 hours a week on average (or 1/8 of a network admin's time) at an average salary of $77,000 a year. This would come to $9,235 a year of admin time.

Total cost for 50 Staff: $38,595 first year cost
Total cost for 50 Staff: $19,850 each year afterward

Office 365 Option

This option assumes the use of existing computers.

- Office 365 E5 + Mobile Security (non-profit pricing) for 50 staff @ $11.65 a month or $139.80 each a year ($6,990 for all 50 staff).
- The ECHO CRM/Follow-Up solution is $475 a month for 5 concurrent users with a $1,995 set up fee, for a first year cost $5,700 + $1,995 = $7,695.
- Webroot Endpoint protection (for computers) for 50 is $1,380 a year for the group.
- Webroot Gateway for 50 staff is $1,650 a year.
- Computer lock for 50 staff @ $20 each is $1,000.
- High quality VPN for 50 staff @ $132 a year each is $6,600 (assumes totally distributed staff)
- Cyber Security Training with Expat Resources for 50 staff @ $25 a year is $1,250 for the first year and $500 a year thereafter.

Office 365 Option (continued)

Labor

- Once implemented the system must be monitored. It is estimated that this would take a staff network admin about 5 hours a week on average or 1/8 of a network admin's time at an average salary of $77,000 a year. This would come to $9,235 a year of admin time.

First Year Cost: $35,800
Second Year Cost: $32,055

Cyber Risk Mitigation for Medium-Sized Groups

In our survey, about one-third of the respondents were from medium-sized organizations (50 - 499 people). In this group, one organization that reported the highest level of negative consequences due to cyber breach, spends more than $250,000 a year on cyber security. The organization that reported the second-highest level of negative consequences spends less than $25,000 a year. While it was outside the scope of this study to determine what type of attacks each organization was experiencing, it would be likely that the first organization has good basic cyber risk mitigation practices in place and is subject to targeted attacks, while the second organization likely has few cyber risk mitigation practices in place.

The best starting place is implementing the first 5 CIS Critical Security Controls and adding Cyber Staff Policy, Security Training and Baseline Physical Security (see Appendix F, G, H and I for model policies). For an organization that does not have a lot of key resources for their members on an internal network, moving towards G-suite with mobile security or Office 365 with Mobility + Security could greatly improve their security profile. However, if an organization already has a central server configuration, then securing that server infrastructure and all the end points (computers, tablets and phones) that access those servers would be the most important next step.

A practical – yet very helpful – approach is proposed in a study[137] that identified the same key elements as the National Campaign for Cyber Hygiene, but in the context of a small business implementation. This study weighs various technologies with an eye to cost control and ease of implementation / maintenance and provides a "cookbook" (SBI Cookbook) for implementation.[138]

The SBI Cookbook assumes that most small to medium-sized businesses will have a Microsoft Windows Network. If that is not the case, the SBI Cookbook will still be of use, but it will need to be supplemented with other tools and skilled advice. A recommended vendor list can be found in Appendix E.

For organizations that are MS Windows Network centric, the following tools were used in the SBI Cookbook to implement the five Critical Security Controls that are the foundation of every cyber risk mitigation program. These tools are not the most sophisticated but were selected for their low cost and ease of use, while providing solid performance.

- **Spiceworks**[139] – Inventory tool to perform an automated inventory of a network including the software installed on each machine. This can also be set up to monitor all the mobile devices and installed software on those devices as well when used in conjunction with the MaaS360 app. Cost: Free – ad supported
- **OpenSSH**[140] – (for accessing Linux-based systems) – provides remote login with the SSH protocol. Cost: Free (open source)
- **MaaS360 app**[141, 142] – provides security control for mobile devices, both Android and iOS. Cost: $18 a year per device.
- **Microsoft Security Compliance Manager (SCM)**[143] – provides centralized security baseline management, a baseline portfolio and has customization capabilities. Cost: Free
- **Windows Deployment Services (WDS)**[144] – enables remote deployment of Windows operating system and also supports custom images. Cost: Free
- **Microsoft Deployment Toolkit (MDT)**[145] – provides a unified collection of tools, processes and guidance for automating desktop and server deployments. Also offers improved security and configuration management. Cost: Free

137 Small Business Implementation of the Critical Security Controls – Cookbook Style.
138 See Appendix A and B
139 http://www.spiceworks.com/free-pc-network-inventory-software/
140 http://www.openssh.com
141 https://play.google.com/store/apps/details?id=com.fiberlink.maas360.android.control
142 https://itunes.apple.com/us/app/maas360-for-ios/id459732007?mt=8
143 https://technet.microsoft.com/en-us/library/cc677002.aspx
144 https://technet.microsoft.com/en-us/library/cc771670(v=ws.10).aspx
145 https://technet.microsoft.com/en-us/windows/dn475741.aspx

- **Group Policy (GP)**[146] – feature built into the Active Directory Domain Services (AD DS) and allows centralized configuration control across all Windows PCs that are attached to the AD DS. Cost: Free
- **Enhanced Mitigation Experience Toolkit (EMET)** – EMET helps protect against new and undiscovered threats even before they are formally addressed through security updates or anti-malware software. Cost: Free
- **Windows Server** – Cost: $882 standard price[147] (non-profit pricing available through TechSoup,[148] $66)
- **Kaspersky Endpoint Security for Business (Select)**[149] – $21.99 per user for one year for 200 licenses (non-profit pricing available through negotiation with sales).

While these tools are low cost, they are not all free and there is also the cost of the hours needed to set up and manage the system once in place. Organizations that have a staff IT person should be able to put this cyber risk mitigation plan in place with mostly internal resources. However, it is a good idea to contract with an outside cyber security professional for review and advice (see Appendix E for recommended vendor list). By far, the largest cost involved will be the hours of skilled labor to install and configure the tools recommended in the SBI Cookbook.

A key concern of organizational leaders is how much time will it take to implement the cyber risk mitigation plan? That really depends on several factors:

- Size and complexity of the network
- The number of devices that have to be configured
- Whether or not the organization is currently using active directory
- How experienced the IT staff or consultant is with these tools
- How much troubleshooting is required to get the system in place.

Any Cyber Risk Mitigation project will have at least three main phases:

- Phase I – Implementing the CSC1 – CSC5 Controls
- Phase II – Monitoring, updating and tweaking the system
- Phase III – Cyber security training for staff.

While it is nearly impossible to predict the full cost involved – due to the number of factors that are unique to each entity – an estimate has been calculated for an organization with

146 https://technet.microsoft.com/en-us/library/hh147307(v=ws.10).aspx
147 https://www.microsoft.com/en/server-cloud/products/windows-server-2016/default.aspx
148 http://www.techsoup.org/search/products/microsoft%20server/
149 https://www.cdw.com/shop/products/Kaspersky-Endpoint-Security-for-Business-Select-subscription-license-re/2938515.aspx?

200 people that each have one mobile device. This organization would have a central IT center and have its own network server running MS Windows Server.

COSTS PHASE I:

Software

- Kaspersky Endpoint Select – 200 licenses - $4,400 per year
- MaaS360 – 200 licenses - $4,000 per year
- Spiceworks – Free
- MS Windows Server - $890 (but non-profit pricing is lower) per year.
- MS network tools (EMET, GP,MDT, WDS and SCM) – Free
- Open SSH – Free

Total Minimum Estimated Software Cost Phase I: $9,290

Labor

- For internal IT staff, estimates range from 700 to 1000 hours to implement the Cyber Risk Mitigation plan (SBI Cookbook). This would be 1/3 to 1/2 of a full time IT person for a year. Assuming a network admin salary of $77,000[150] this would come to $25,000 to $39,000 of admin time.
- If an experienced external consultant were engaged it could take 320 hours @ a median cost of $125.00 per hour or approximately $40,000.

Total Minimum Estimated Labor Cost Phase I: $40,000

Total Minimum Estimated Cost for Phase I: $49,300

COSTS PHASE II:

Software

- Renewal - Kaspersky Endpoint Select – 25 licenses - $4,400 per year
- Renewal - MaaS360 – 25 licenses - $4,000 per year
- Renewal - Spiceworks – Free
- Renewal MS Windows Server - $890 (non-profit pricing is lower) per year.
- MS network tools (EMET, GP,MDT, WDS and SCM) – Free
- Open SSH – Free

Total Minimum Estimated Software Cost Phase II: $9,300

150 https://gooroo.io/analytics/skill/Network_administrator/united-states#

COSTS PHASE II (continued):

Labor

- Once implemented, the system must be monitored, updated and patched to maintain viability. It is estimated that this would take a staff network admin about 5 hours a week on average or 1/8 of a network admin's time at an average salary of $77,000 a year. This would come to $9,235 a year of admin time.
- If an experienced external consultant were engaged it could take 10 hours a month at a median cost of $125.00 per hour or approximately $15,000.

Total Minimum Estimated Labor Cost Phase II: $12,000[151]

Total Minimum Estimated Cost Phase II: $23,300

While it is possible that the cyber risk mitigation plan could be implemented and maintained for less than this, it would certainly be possible for it to cost a great deal more. These estimates are provided as a starting place for planning and budgeting.

The third phase is training and it has typically been expensive and not very well focused on ministry's needs. However, a new online cyber security training service for religious non-profits, Expatdigital.com, is offering an introductory rate of $25 a year per household, along with volume pricing for organizations.

COSTS PHASE III:

Training

- 250 member licenses for Expat Resources @ $1,500 for the first year and $500 each year after.

Labor

- 1 hour a week to manage the process at ~$2,000 a year

Total Minimum Estimated Cost Phase III: $3,500 a year

151 Average of staff admin cost and consultant cost

Cyber Risk Mitigation for Large-Sized Groups

In our survey, about one-third of the respondents were from large-sized organizations (greater than 500 people). Of these large organizations, 55% reported spending less than $25,000 a year on cyber security. Additionally, all of the large organizations that reported they had a project shut down due to a breach in cyber security, also spend less than $25,000 a year. And, 80% of the large organizations that reported arrests, imprisonment and possible deaths of workers, spent less than $25,000 a year on cyber security.

> ***Organizations that were poorly funded and staffed reported almost all of the negative outcomes.***

Our study, with one exception, shows a dichotomy between the poorly funded and staffed cyber security efforts, and the well funded and staffed cyber security efforts. The organizations that were well funded and staffed, reported almost no negative outcomes for cyber security breaches. Those that were poorly funded and staffed, reported almost all of the negative outcomes for their size category.

There was one area where both groups had negative outcomes, and that was with the expulsion of expat workers. It is likely that these situations may be due more to operational security – like inappropriate social media postings – rather than a cyber security breach of a server or endpoint. This will be addressed in Cyber Security Training.

For those organizations that are well funded and staffed, the additional training of personnel – like that provided by expatdigital.com – could improve already solid cyber risk mitigation programs. For those organizations that are poorly funded and staffed, it appears there is a need to educate organizational leaders about the high monetary, program and human costs that their organizations are experiencing.

While large organizations are more complex to secure – and tend to have a mixed cyber risk profile – the basics are still the same as those for small to medium-sized ones. A focus on the top five Critical Security Controls (along with policy, baseline physical security and cyber security training), are excellent places to start. Even a large enterprise could implement the guidance for small and highly distributed organizations in their remote and field locations, and implement the guidance for medium-sized organizations at their central offices. Certain large organizations will need a cyber security specialist, but that is beyond the scope of this study.

Overall, for organizations that are experiencing significant negative outcomes due to cyber security breaches, even moderate first steps can greatly improve the effectiveness of the whole organization, and the safety of their staff and partners.

COST ESTIMATE FOR IMPLEMENTATION

Office 365 Option

This option assumes the use of existing computers. At this volume, additional discounts can usually be negotiated.

- Office 365 E5 + Mobile Security (non-profit pricing) for 1,000 staff @ $11.65 a month or $139.80 each a year and $139,800 for all 1,000 staff (ask for volume discounts –there are significant discounts when asked for individually).
- The ECHO CRM/Follow-Up solution is $900 a month for 9 concurrent users with a $1,995 set up fee, for a first year cost $10,800+ $1,995 = $12,795.
- Webroot Endpoint protection (for computers) for 1,000 is less than $25,096 (ask for volume discount for lower price).
- Webroot Gateway for 1,000 staff is less then $28,884 a year (ask for volume discount for lower price).
- Computer lock for 1,000 staff @ $20[152] each is $20,000.
- High quality VPN for 1,000 staff @ $132[153] a year with hubs and individual users, 200 licenses @ $132, for a total of $26,400.
- The cost of training with Expat Resources for 1000 people is $5,000 the first year and $1,500 a year thereafter. Labor: 4 hours a week to manage the process at ~$8,000 a year in labor cost. Total Estimated Training Cost: $13,000.

Labor

- Once implemented the system must be monitored. It is estimated that this would take a staff network admin about 30 hours a week on average or 3/4 of a network admin's time, at an average salary of $77,000 a year. This would come to $57,750 a year of admin time.

Total First Year Cost: $ 323,725 a year
Total Second Year Cost: $298,235 a year

This breakout does not cover servers and services for a large organization.

152 https://www.amazon.com/Kensington-64068F-MicroSaver-Laptop-Business/dp/B00000K4KH
153 http://www.jungl.me/#pricing

Conclusion

Overall, it is clear that Cyber Security is a serious issue for missional organizations. The adverse impacts that are currently being experienced require organizations to raise cyber risk from a technical issue for the IT department, to the leadership of each organization that needs to put in place cyber risk mitigation strategies.

Please note that this is a “point in time” report and the whole area of cyber security is changing rapidly – both in terms of the data, types of risks, and the potential solutions to mitigate this challenge. And while technical interventions are important, they alone will not solve cyber security issues. Appropriate policies and strong cyber security training are crucial to a successful cyber risk reduction program, as addressing staff behavior is the single most important factor to reduce cyber risk.

This report has focused on how to simplify the cyber security process and reduce the cost for missional organizations, no matter the size. Additional resources and more complex solutions and recommendations are located in the Appendix. Media Impact International is also available to provide direction and referrals to address this important area, so that . . .

. . . more people in unreached areas are brought into God’s Kingdom and growing in their faith, through the effective utilization of media.

APPENDIX

A – Small Business Implementation of the CSCS Part 1

B – Small Business Implementation of the CSCS Part 2

C – Critical Controls Poster 2016

D – IBM MaaS360 Bundles

E – Vetted Service Providers

F – Models of Social Media / Communication Policies

G – Model of Password Policy

H – Phishing Training Model

I – Sensitive Information Reduction

J – Survey Questions

K – C3 Guidelines for Email

L – C3 Guidelines for VPN

M – C3 Guidelines for Messaging

N – Additional Country Profiles