# CYBER SECURITY REPORT


## Media Impact International

MII™

Revised February 14, 2017

# TABLE OF CONTENTS


1. **Executive Summary** 2

2. **Introduction: Cyber Security in the Missional Context** 5

3. **Cyber Threats** 7

4. **Cyber Security Survey** 15

5. **Cyber Risk Assessment** 20

6. **Cyber Risk Mitigation** 26


This overview provides the highlights of MII's Cyber Security Report. Please contact MII for a copy of the full report, along with the extensive Appendix, featuring additional cyber security recommendations and resources.



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 these 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, 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 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 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

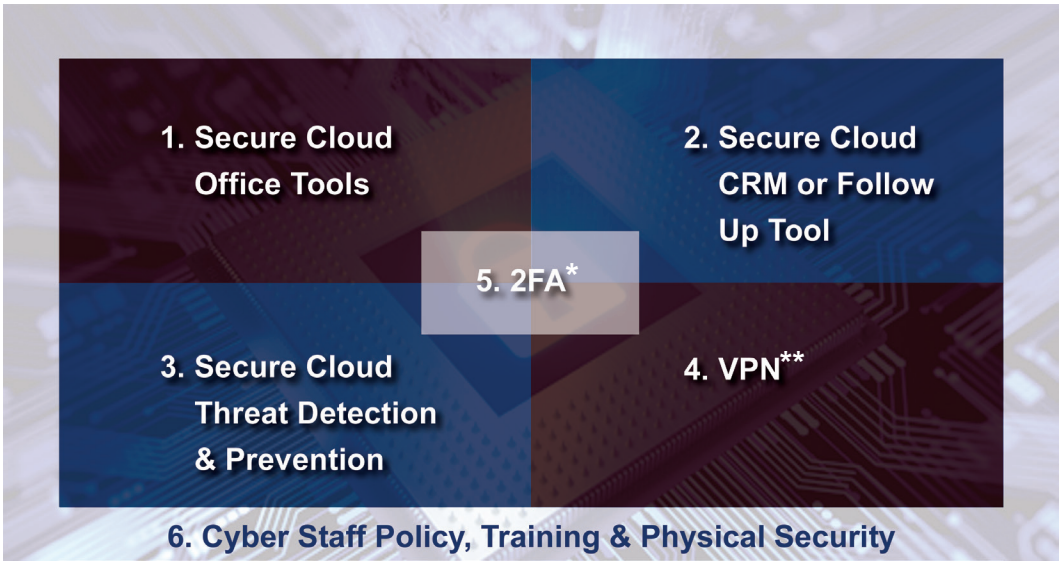
environment for field ministry, when the message and mission of an organization is opposed by a state actor.

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. This report uses a framework 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. 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 full report's appendix also includes sample policies in the areas of passwords, communication, and the reduction of sensitive information. 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 fulfill a baseline Cyber Safety Profile.

### CYBER RISK MITIGATION MODEL / STEPS




* Two Factor Authentication

**Virtual Private Network

## 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. 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 pre-existing networks that need to be secured and a detailed “cookbook” has been provided (in the appendix of the full report), that has a step-by-step procedure on how to lock down a network.

Large entities have much more complex network architectures and often many legacy systems. It is not possible to recommend a single course of action that will implement a cyber safety profile for large organizations. However, the report provides a cloud-based proposal similar to the one for small- and medium-sized organizations (along with cost estimates in the full report).

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.

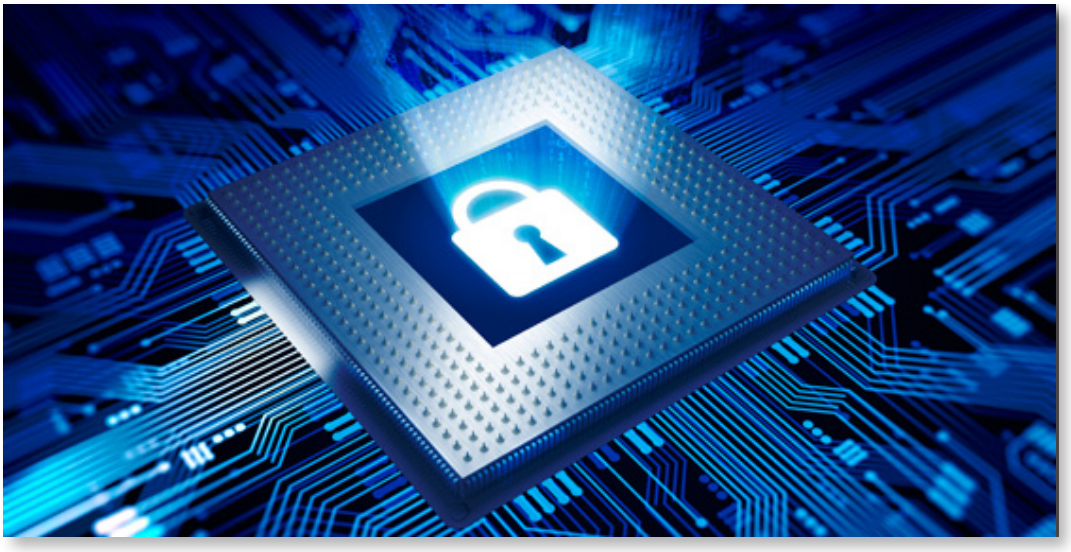
## A Final Word

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 or 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, mission leaders seldom consider the full implications of the rapid adoption of so many electronic devices and online services. 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 address this challenge.



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 the death of disciples, imprisonment, expulsion, loss of funding and organizational reputation, and other negative outcomes.

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 significant 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 along with full-time staff. 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 is the first five Critical Security Controls of the Center for Internet Security (CIS)[i], as the starting place for any mitigation effort. This report is also focused primarily on the cyber risk in the MENA region. 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?" In the missions world not only is there no reporting, but there are seldom any internal valuations attached to 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 – reduce 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 breaches, as well as the current practices, attitudes and aspirations about cyber security. The results of this survey indicate that cyber breaches are having a deep and costly impact on many organizations.

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 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 of the full report, additional resources are provided including a list of useful products and vendors.

> ***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**

i https://www.sans.org/security-resources/posters/special/20-critical-security-controls-55

# CYBER THREATS

In order to effectively protect an organization, relevant and realistic Cyber Threats and Threat Actors must be identified. Once these have been identified, a Risk Assessment can be conducted and Cyber Safety Profiles developed. Then appropriate mitigations can be put in place to fulfill 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 a genuine Cyber War.[1]

## PROBABILITY OF CYBER SECURITY BREACH

In a global study of more than 380 companies, it was determined that there was a 31%[2] chance in the MENA region that 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.

## 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).

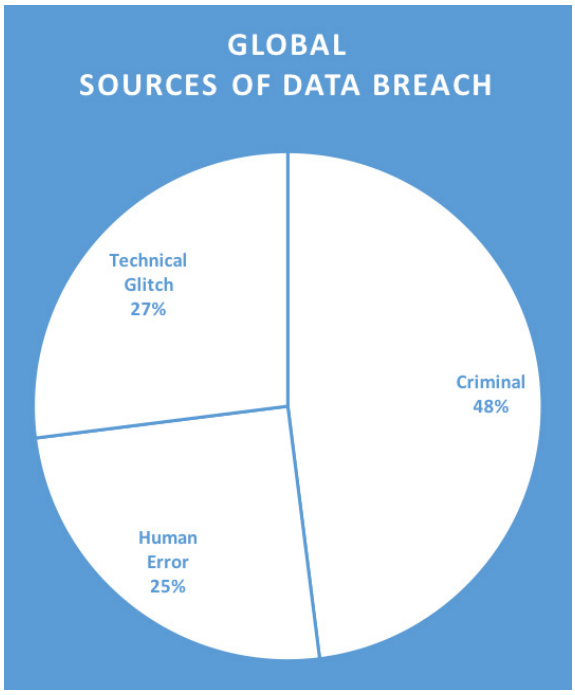
1 'Cyberwar' Is Over Hyped: It Ain't War Til Someone Dies
2 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute Research Report, p 22

## 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.[3] The Mean Time To Contain (MTTC) is 70 days.[4] 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.

## 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 or do harm to the organization. This second threat is also called an "insider threat." In this study we have cited data that 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%[5], 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.




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

## 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.

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

3 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute Research Report, p 23
4 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute Research Report, p 24
5 http://www.prnewswire.com/news-releases/employee-errors-cause-most-data-breach-incidents-in-cyber-attacks-300342879.html

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


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

## SS7 GLOBAL TRACKING

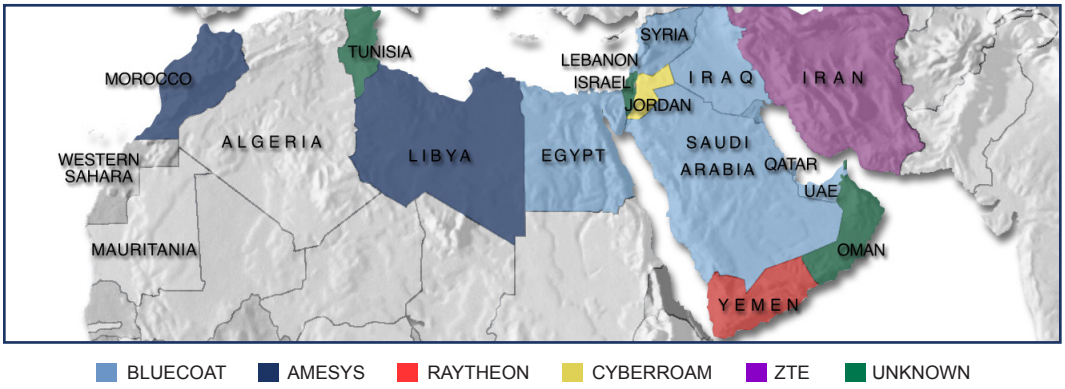
SS7 is a global locator system for phones that are roaming in networks other than their own. It allows a telecom to determine what network the phone belongs to, and whether it has a way to bill that user for the use of the local phone network. SS7 is available to all cell phone networks. The system can also be misused to track individuals on a global scale.[6] 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. 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.

## DEEP PACKET INSPECTION (DPI)

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

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

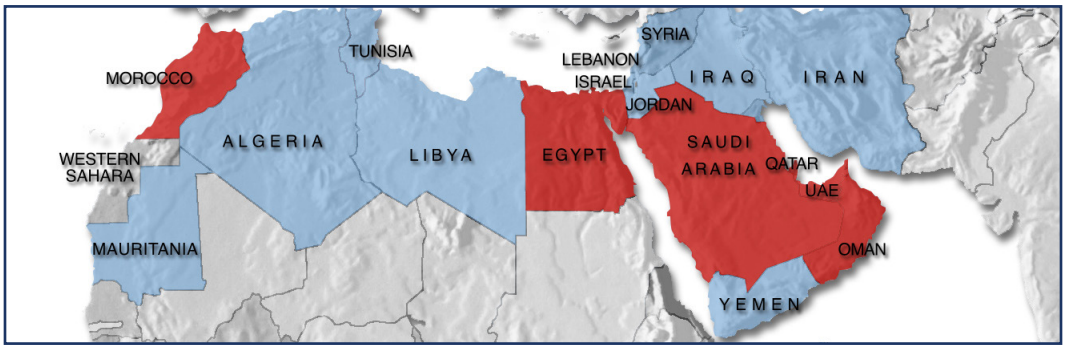
MENA region are documented as having DPI technology in place. Vendors are Bluecoat,[7] Amesys,[8] Raytheon,[19] Cyberroam,[10] Narus,[11] and ZTE.[12]




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

## THE HACKING TEAM

The Hacking Team[13] 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.[14]***

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

## *MENA Cyber Threats*

[ The following is a condensed sampling of 7 of the 20 country profiles that are covered in the full report. Each full-length profile includes a list of likely threats specific to each country.]

### 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."[15] 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.[16]

### 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. By 2015, the government of Egypt had Finfisher[17] software in place,[18] 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.[19] It is also publicly documented that Egypt has Lawful Interception Gateway (LIG) and DPI technology,[20] as well as tools from the Hacking Team.

15 https://freedomhouse.org/report/freedom-world/2016/algeria - see section D.
16 https://www.osac.gov/pages/ContentReportDetails.aspx?cid=19075
17 https://en.wikipedia.org/wiki/FinFisher
18 https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/
19 http://www.al-monitor.com/pulse/en/originals/2015/01/egypt-cyber-security-council-privacy.html
20 http://www.huffingtonpost.com/timothy-karr/congress-urges-state-depa_b_821949.html

## 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.[21] In February 2014, Iran was considered to be a first-tier cyber warfare threat to the USA.[22] 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.[23] In August 2015, Iran was caught high-jacking two factor authentications of a Gmail account[24] (two factor authentication is considered a best practice in cyber security). 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.[25]

Iran has a very strong hacker capability[26] with many groups aligned with state purposes.[27] 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 actor. It has also treated missional work and church planting as a national security threat.

## 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

21 http://arstechnica.com/tech-policy/2010/03/how-nokia-helped-iran-persecute-and-arrest-dissidents/
22 http://foreignpolicy.com/2014/02/18/forget-china-irans-hackers-are-americas-newest-cyber-threat/
23 Personal conversation with ministry leaders
24 https://citizenlab.org/2015/08/iran_two_factor_phishing/
25 http://www.theregister.co.uk/2016/03/08/us_trade_ban_on_zte
26 https://en.wikipedia.org/wiki/Iranian_Cyber_Army
27 http://uk.businessinsider.com/what-its-like-to-be-a-hacker-in-iran-2016-2?r=US&IR=T

social media.[28] They have also conducted “false flag” attacks where they produce anti-ISIS media to attract their most ardent opponents.[29] This content is delivered with exploits that allow ISIS hackers to trace the physical location of the person who accessed the media, and then trace who the media was shared with. The central government of Iraq has advanced cyber attack and monitoring tools.[30] 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.[31]

## SAUDI ARABIA


Saudi Arabia conducts raids on private Christian meetings on a regular basis.[32] These raids are reported to be initiated by anonymous tips, but could be the result of surveillance.[33] 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.[34] The government is thought to employ a “Social Media Army”[35] to monitor, interact with and subvert online discussions. The government also seeks to block or monitor all VOIP traffic.[36] All web use is monitored and many sites are blocked.[37] 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.[38] With a virtually unlimited budget for cyber security and top-end surveillance technology,[39] 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.

28 http://www.al-monitor.com/pulse/originals/2015/04/iraq-social-media-convey-battle-against-islamic-state.html
29 http://www.bbc.co.uk/news/technology-28418951
30 https://sii.transparencytoolkit.org/search?utf8=✓&utf8=✓&q=Iraq
31 https://sii.transparencytoolkit.org/search?utf8=✓&utf8=✓&q=Iraq
32 https://www.jihadwatch.org/2016/09/saudi-arabia-27-christians-arrested-and-deported-for-conducting-christian-prayers-in-private-residence
33 http://www.dailymail.co.uk/news/article-2756134/Dozens-Christians-including-women-children-arrested-Saudi-Arabia-tip-state-s-Islamist-police-force.html
34 http://www.oxfordbusinessgroup.com/news/saudi-arabia-strengthen-defences-against-cyberattacks
35 https://freedomhouse.org/report/freedom-net/2015/saudi-arabia
36 Ibid
37 https://en.wikipedia.org/wiki/Censorship_in_Saudi_Arabia
38 http://www.economist.com/blogs/pomegranate/2014/07/internet-monitoring-gulf
39 https://www.issworldtraining.com/ISS_MEA/index.htm

## SYRIA


At the time of this study, Syria is an active war zone that involves regional and 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. There are reports that the SEA receives help and training – not just from the central government – but also from Russia and Iran.[40] 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 for intelligence purposes.[41] 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.[42] There is public information that Syria has LIG and DPI technologies, and advanced Internet surveillance and monitoring tools.[43] 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.

## UNITED ARAB EMIRATES (UAE)


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.[44] The public record indicates that the UAE is investing in world class surveillance and cyber attack tools.[45] It has been reported 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.[46]

40 http://www.aljazeera.com/programmes/peopleandpower/2015/06/syria-electronic-armies-150617151503360.html
41 http://europe.newsweek.com/syria-grants-free-internet-access-so-it-can-snoop-230442?rm=eu
42 http://www.aljazeera.com/programmes/peopleandpower/2015/06/syria-electronic-armies-150617151503360.html
43 https://sii.transparencytoolkit.org/search?utf8=✓&utf8=✓&q=syria
44 https://home.kpmg.com/ae/en/home/media/press-releases/2015/12/kpmg-uae-cyber-security-survey-2015.html
45 http://www.middleeasteye.net/news/exclusive-uae-elite-task-force-security-secret-surveillance-state-135285760
46 https://sii.transparencytoolkit.org/search?utf8=✓&utf8=✓&q=UAE

# 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.[47] Thirty respondents completed the on-line survey utilizing Survey Monkey.[48]

## 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.

## 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.

[ This overview only provides findings on adverse impacts and aspirations. For complete survey results, please see a copy of the full report.]

## ADVERSE IMPACTS OF CYBER SECURITY BREACHES

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

47 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.

48 Https://www.surveymonkey.com

## 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

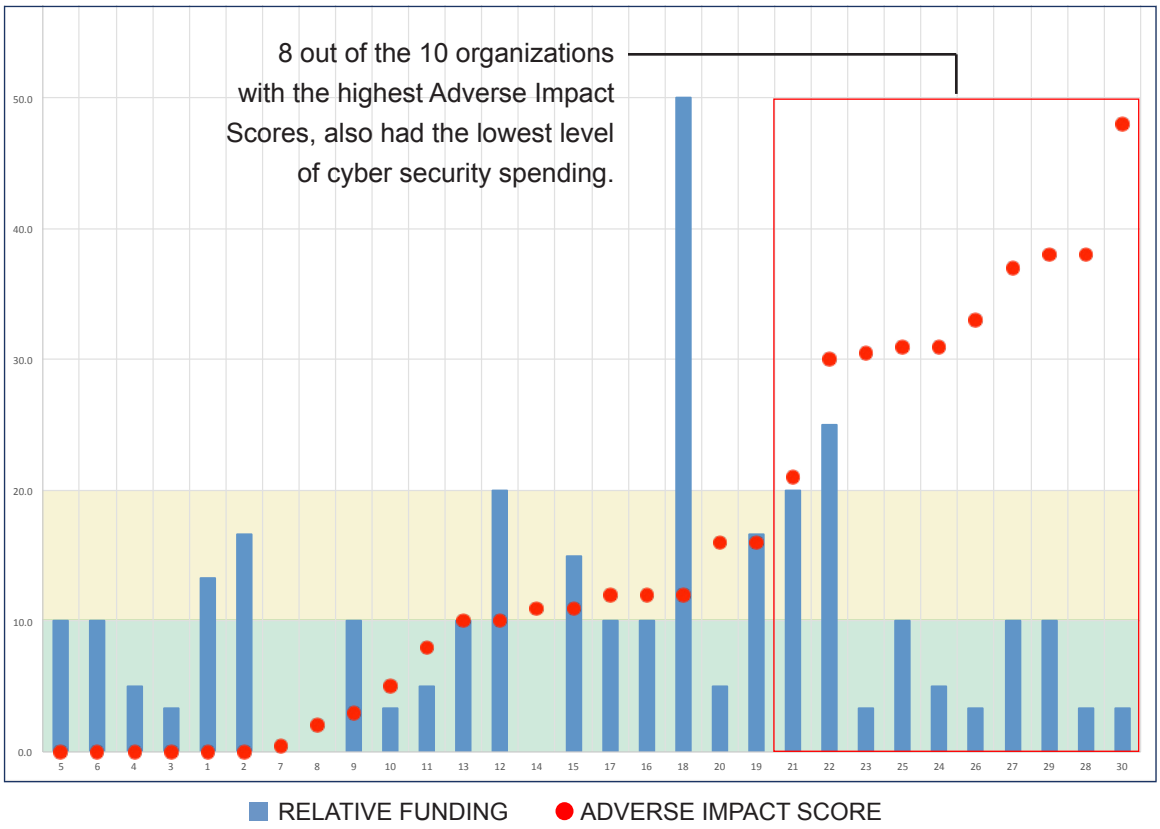

47% reported that they had experienced a loss of time and resources due to a breach of Cyber Security.

## ADVERSE IMPACT SCORE

To analyze the overall impact of cyber security breaches, we constructed a weighted scoring system based on the severity of adverse impacts. The purpose was to provide a single score that indicated how deeply an organization had been impacted. From this analysis, the graph below shows the relationship between the Adverse Impact and the Cyber Security Funding Levels. The 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 Scores. The higher the Adverse Impact Score, the worse the result for the organization. The taller the column, the more that was spent on cyber security. For data points with no column, the organization did not disclose 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.

**Adverse Cyber Impact vs. Relative Funding for Cyber Security**



## CYBER SECURITY ASPIRATIONS

Following are the key findings from the organizations 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 Survey 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.

> ***Overall, organizations aspire to have good cyber security, yet the clear majority do not currently have good practices in place.***

# CYBER RISK ASSESSMENT

One of 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 *Vulnerability Assessment.*[49] This type of assessment identifies areas where an organization *might* be attacked.[50] 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.[51]

An alternative to vulnerability assessment is *Threat Assessment,*[52] 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.

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

These are 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.

49 https://en.wikipedia.org/wiki/Vulnerability_assessment
50 https://en.wikipedia.org/wiki/Vulnerability_(computing)
51 Expat Digital Resources, Threat Centric Digital Security, Presentation 2015, p3
52 https://en.wikipedia.org/wiki/Threat_assessment

## *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 overall Threat Actors[53] 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<br>• Opportunistic theft of information<br>• Malicious Software (Malware)<br>• Password Guessing<br>• Social Engineering<br>• Collecting Public Information |
| **Organizational Staff** | • Poor Passwords<br>• Use of apps which steal data<br>• Clicking on links on suspect sites and emails<br>• Opening suspect attachments<br>• Careless handling of equipment<br>• Careless handling of sensitive information<br>• Inappropriate use of Social Media<br>• Failure to follow good security practices<br>• Failure to secure servers |
| **The Curious**<br>*This is in the field context: Neighbors, Friends, Local Co-Workers, Host Government* | • Overhearing conversations<br>• Passive monitoring of unencrypted email<br>• Passive monitoring of Social Media<br>• Passive monitoring of calls and SMS<br>• Passive monitoring of web usage<br>• Notice use of finances<br>• Notice attitude toward local government and religion |
| **The Suspicious**<br>*This is in the field context: Neighbors, Friends, Local Co-Workers, Host Government* | • Eavesdropping on conversations<br>• Active monitoring of unencrypted email<br>• Active monitoring of Social Media<br>• Active monitoring of calls and SMS<br>• Active monitoring of web usage<br>• Scrutinize use of finances<br>• Scrutinize attitude toward local government and religion<br>• Attempts to access accounts |
| **Militant Groups** | • Watch for activity that looks like spying<br>• Watch for activity that appears threatening<br>• Watch for activity that is oppositional |
| **State Actors** | • Targeted Monitoring<br>• Active Surveillance<br>• Targeted Interventions |

53 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.[54] 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 is 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.[55] 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.

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.

54 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute Research Report, p 11
55 Expat Digital Resources, Threat Centric Digital Security, Presentation 2015, p6

**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."
  (RPD – Reduce / Protect / Detect – see the full report for an overview of this strategy)

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.

## TECHNICAL MITIGATIONS

Technical Mitigations involved a wide range of technical actions like having a firewall to protect a network and individual machines, using Anti-Virus and Anti-Malware software, hardening 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.

> ***It is critically important to understand that technical mitigations without behavioral mitigations will fail to improve cyber 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.

| DIGITAL SAFETY PROFILE – BASELINE | |
|---|---|
| **Threat Profile**<br>**Opportunistic Criminals & Organizational Staff** | **Mitigations** |
| Opportunistic theft of devices<br>Careless handling of equipment | Security Cable for laptops – lock down and remote wipe of devices; Full disk encryption of laptops |
| Opportunistic theft of information<br>Careless handling of sensitive information<br>Collecting Public Information | Sensitive Information – Reduce, know yourself, trim down; Encrypted communication |
| Malicious Software (Malware) | Anti-Malware; Patch software and firmware |
| Password Guessing /<br>Poor Passwords | Password Policy; 2 Factor Authentication;<br>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 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)

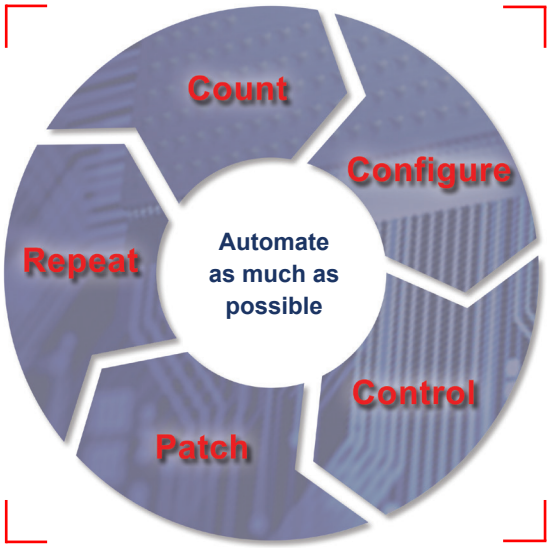
Clearly there is no "one size fits all" solution for cyber risk mitigation. However, we will present possible approaches for each category of organization. For each one, the goal is to provide a starting place that is sound and as low cost as possible. In the previous section, we developed a Baseline – 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[56] can be overwhelming for an organization just starting a cyber risk mitigation program. To foster early "wins" that any organization can benefit from, it is important to focus on the first five Critical Security Controls as the starting point.

**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)

56 See Appendix C in the full Cyber Security Report




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**[57]

## *Cyber Risk Mitigation for Small and Highly Distributed Groups*

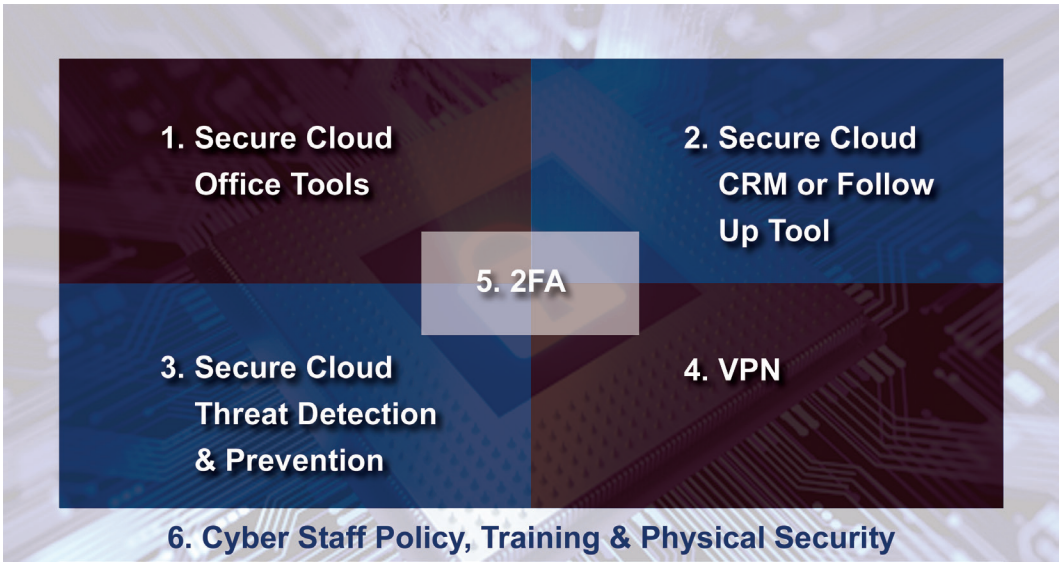
About one-third of the organizations that participated in our survey had less than 50 staff members. Such organizations typically have tight budgets and seldom have dedicated IT staff. They are often highly distributed and do not have a central server infrastructure. They also tend toward BYOD (Bring 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:

57 https://www.sans.org/security-resources/posters/special/20-critical-security-controls-55




## 1. SECURE CLOUD OFFICE TOOLS

The two main options are Google G-Suite and Microsoft Office 365 Live.[58] 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 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

G-Suite or Google Suite is a cloud-based service offered for businesses. The suite includes email, calendar, internal communication tools, 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.[59] G-suite was designed to work with the low-cost Chromebook[60] 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[61]

58 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.
59 https://support.google.com/work/answer/6056693?hl=en&ref_topic=6055719
60 https://www.google.com/chromebook/9 https://www.google.com/intl/en_uk/chromebook/about/
61 https://gsuite.google.com/products/admin/mobile/

app that allows protection of all mobile devices in an organization (including BYOD), and incorporates a centrally-managed remote wipe, as well as an overall organizational control panel. Standard Chromebooks can be purchased for $200 - $300 each, and present a lower risk of theft than standard laptops.

**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 is more expensive than G-suite.

## 2. SECURE CLOUD CRM OR FOLLOW-UP TOOL

Most missional 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[62] 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[63] make it possible to have key security tools across a distributed organization that are centralized.

62 https://www.echoglobal.org
63 https://www.webroot.com/us/en/business

### 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 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.

### 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[64] or special mobile app.[65] The web resource requires that you provide the correct password and a time-limited secure token to gain access.

### 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 of the full report. A new online cyber security training service for religious non-profits, Expatdigital.com,[66] is offering an introductory rate of $25 a year per household, with volume pricing for organizations (see Appendix E in the full report). 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.

## *Cyber Risk Mitigation for Medium-Sized Groups*

In our survey, about one-third of the respondents were from medium-sized organizations. In this group, one organization that reported the highest level of negative consequences due to cyber breaches, 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

64 https://www.rsa.com/en-us/products-services/identity-access-management/securid/hardware-tokens
65 https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2
66 https://expatdigital.com

organization has little in place. Overall, the best starting point 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 in the full report for model policies).

## *Cyber Risk Mitigation for Large-Sized Groups*

In our survey, about one-third of the respondents were from large-sized organizations. Of these organizations, 55% reported spending less than $25,000 a year on cyber security. Additionally, all of the large entities 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.

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. Certain large organizations will need a cyber security specialist, but that is beyond the scope of this study. Overall, for entities 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.

## *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 entity that needs to put in place 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 address 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 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 of the full report. Media Impact International is also available to provide direction and referrals to address this important area.