STRATIGOS SECURITY

Helping EPF Mitigate Cybersecurity Risks

Presented to:
Eurasia Partnership Foundation

By:
Beau Woods
Founder/CEO
Stratigos Security
bwoods@stratigossecurity.com
+1 770 598 7486 (mobile)

Document Properties

Version Control

Draft and final document version history for Eurasia Partnership Foundation

- v1.0, published September 10, 2021

Copyright, Confidentiality, and Non-Disclosure

Table of Contents

Executive Summary

The Eurasian Partnership Foundation (EPF) leverages community activism and philanthropy to build peaceful cooperation among people in the South Caucasus region. As a part of the USAID efforts to assess and improve the security posture of their beneficiaries, USAID engaged Stratigos Security to perform a Cybersecurity Risk Assessment and to develop Cybersecurity Action Plans. The project evaluated technical systems for resilience against known adversary attack patterns, performed a risk assessment according to the SAFETAG framework, and mapped organizational cybersecurity maturity against the Center for Internet Security Top 20 Controls.

Summary of Cybersecurity Risks

Stratigos identified organizational risks based on elicitation sessions, interviews, and technical analysis. Key stakeholders voiced several concerns during an initial risk discussion, which were validated during subsequent steps. In addition, workflow analysis with individual staff members and technical testing of the internal and external network revealed other risks which are accounted for below:

- Hacking of the websites
- Hacking of corporate emails
- Unauthorized access to the organization's internal database
- Personal data about beneficiaries
- Physical security of the office

Summary of Risk Mitigation Actions

EPF has a fairly mature cybersecurity program for its size and industry, as measured by standard security benchmarks, such as the Center for Internet Security Top 20. While their size and resources limit their ability to protect against high-capability cybersecurity threat actors, it's clear they have invested in their own capabilities. EPF's cybersecurity goal is to make attacks more apparent, delay their effect, and respond quickly and effectively. To improve in several key areas, EPF should take the following actions:

- Use fully updated, supported website software
- Implement full disk encryption
- Implement Virtual Private Network (VPN) for office connectivity

Some Action Items can be implemented in parallel and improve security while the longer-term projects are underway.

- Implement Password Management Software
- Implement Multi-Factor Authentication
- Multi-User Management for Social Media Accounts

Finally, Pink will need support from an IT support specialist to implement and maintain all these actions. Full detail of these risk mitigation Action Items can be found in the **EPF - Cybersecurity Action Plan** document.

Assessment Methodology

Data Collection and Project Initiation

During this phase, we formally kick off the project, collect relevant documentation, and schedule project activities at a finer level. This ensures information and individuals are available to reduce undue delay, but with enough flexibility to accommodate inevitable changes. We will work with you to determine most relevant documents to review and personnel to meet. A kickoff meeting ensures all key stakeholders are introduced, either in person or virtually, establishes communications trees, and ensures a clear understanding of the project.

SAFETAG Framework

The Security Auditing Framework and Evaluation Template for Advocacy Groups (SAFETAG) Framework is developed by and for non-governmental organizations, civil society organizations, and non-profit cybersecurity groups. The process begins with an organizational risk assessment, which gives insight into key cybersecurity threats and concerns the beneficiary faces. Next, individual interviews provide a cross section of the people, process, and technology cybersecurity. In addition, technical scanning across the organization's entire network and set of systems provides information on software and configuration vulnerabilities.

CIS CSAT Evaluation

Our consultants led a facilitated evaluating leveraging the Center for Internet Security (CIS) Controls Self-Assessment Tool (CSAT) to gauge organizational maturity in a consistent, standardized way. This methodology takes a top-down approach to understanding organizational cybersecurity controls based on the CIS Top 20. Survey responses are mapped against industry averages to visually show how the beneficiary's cybersecurity maturity compares against a sample of other organizations.

Internal/External Network Vulnerability Assessment

An external network penetration test consists of several iterative phases. Stratigos uses the Penetration Testing Execution Standard (PTES),[1] an industry-recognized methodology, as the basis for our testing. Depending on the types of adversaries and attacks simulated, the methodology may vary from project to project.

- **Intelligence Gathering and Scope Verification** – Through open source intelligence gathering (OSINT) and other methods, the tester attempts to passively and actively gather information about the target environment. During this phase, the scope is compared against the intelligence gathered to verify that there are no gaps or misalignments.
- **Threat Modeling** – During this phase, Stratigos tailors adversarial attack patterns to your business and technical environment. This step ensures work efficiently mimics real-world threats, and that results align to business objectives.
- **Vulnerability Assessment and Analysis** – Stratigos attempts to determine vulnerabilities through automated and manual processes, by interacting with services on open ports. This includes testing known vulnerabilities, password guessing, web intrusion attempts, and other techniques.
- **Evidence Collection** – Stratigos identifies target assets and captures evidence sufficient to demonstrate findings to management.

Stratigos uses industry-leading and custom built tools to probe the network for potential vulnerabilities. The findings are analyzed to identify potential risk vectors, such as:

[1] Penetration Testing Execution Standard http://pentest-standard.org

- Potential rogue devices, including wireless clients and access points
- Common, default credentials
- Known but unmitigated software flaws
- Common configuration weaknesses
- Deviations from industry or organizational standards (such as CIS 20 Controls and OWASP Top 10 Vulnerabilities)

Technical artifacts were provided to the technical points of contact for the organization.

SAFETAG Cybersecurity Risk Assessment

The SAFETAG methodology includes conducting a cybersecurity risk assessment that captures both systemic issues and individual vulnerabilities. The initial organizational risk assessment session was attended by several key stakeholders, including the part time IT support staffer. This was followed by interviews and facilitated technical reviews with 5 employees, 5 computers, and 5 phones. In addition, technical reviews were conducted on the internal network, wifi network, website, constituent relationship management system, primary Facebook pages, and corporate email.

Hacking of the websites

Stratigos found serious problems with its 3 websites: epfarmenia.am, kronadaran.am, and hkdepo.am. Epfarmenia.am is an outdated Drupal installation on an Ubuntu 18.04 server, with an outdated version of php 7.2. The website is protected by Cloudflare's Galileo service, which has special rules for protecting Drupal, which provides a stopgap until the site can be updated to mitigate or eliminate the vulnerabilities. Kronadaran.am is running an unsupported version of Wordpress with several vulnerable plugins that could lead to defacement or attack against site visitors. Hkdepo.am is a custom written site using the PHP/Laravel framework. It is also protected by Cloudflare and outside scan didn't reveal any vulnerabilities.

Recommendation: Maintain internet-facing websites with due care by ensuring they are running supported versions and applying software security updates promptly. Develop and implement a management program to ensure that platform migrations happen with ample time to avoid going out of support.

Responsibility: EPF's management, IT manager**,** webmaster, external web developer

Hacking of corporate emails

The organization uses GSuite, which is centrally managed from the Admin Console. There is no corporate email policy, some mailboxes are accessed by more than one employee, Multi-Factor Authentication (MFA) is optional and not everyone uses it. The organization doesn't have a password management policy or system either, with some employees admitting that they use the same password for several accounts.

Recommendation: Enable MFA for all GSuite accounts, develop a corporate email policy, carry out password training for the employees and consider using password management software like 1Password or LastPass to centrally manage and enforce password policies.

Responsibility: EPF's IT manager, external digital security trainer

Unauthorized access to the organization's internal database

The organization is partly protected. The internal database is a custom written php/MySQL web application, which resides in the internal network and is usually closed for the outside world. However, due to COVID-19 it has been occasionally opened for the outside world, so that the remote workers can access it. The code is custom written and not updated, the underlying architecture is old and has a range of vulnerabilities, including some that may lead to complete system compromise.

Recommendation: In the short term the organization should consider configuring secure VPN access to the office and stop the practice of opening up the internal database to the outside

world, but instead have the work from home employees connect to the office network via VPN. In the long term, the organization should find resources to update the internal database system or invest in licensed and up to date CRM/Database system, which can serve those needs.

Responsibility: IT manager, organization's management

Personal data about beneficiaries

The organization uses a special accounting software. Since the license is very expensive, several people access it using the same password. The remaining programmatic documents: lists of participants, personal data of people involved in project, budgets and financial data are often shared via corporate email, some employees sometimes send files to their personal emails to be able to work from home. Some programmatic data is also shared via Facebook messenger.

Recommendation: Establish a data sharing policy and decide on a more suitable cloud storage solution, which would allow to secure the data and establish proper file sharing and access controls, invest in more licenses of the accounting software to accommodate the needs.

Responsibility: Chief accountant, IT manager

Physical security of the office

The organization is not protected. The computers are not encrypted, there are no security cameras in and around the office, the office doesn't have metal bars on the windows, and the server room is unprotected against physical entry.

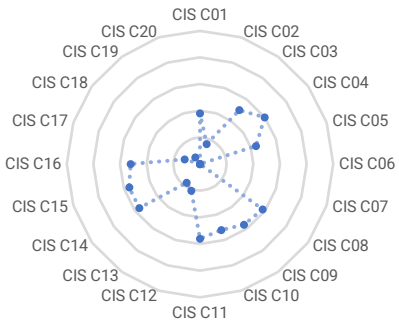
Recommendation: Encrypt all office computers and servers, and invest in security cameras. Consider investing in physical security of the building, possibly with the help of physical security consultant.

Responsibility: IT manager, organization's management

CIS Controls Self Assessment Tool Results

The Center for Internet Security (CIS) publishes a list of 20 security controls they consider to be foundational to an effective cybersecurity program. USAID beneficiaries undertaking the Digital APEX program are assessed against this list of controls using the CIS Controls Self Assessment Tool (CSAT) so they can be benchmarked against future progress, other beneficiaries, and industry averages. The tool measures the number of maturity markers for each of these controls and presents the information as a completeness percentage (0-100% of markers in place).

EPF scored very highly on the CIS CSAT for their size and level of resourcing. Notable outliers include controls around monitoring and auditing, and email and browser protections, as those are typically higher in organizations of their maturity. During the engagement Stratigos provided instructions and guidance to address these deficiencies and those recommendations appear in the Action Plans mentioned in the executive summary



Control	Score
1. Inventory and Control of Hardware Assets	38%
2. Inventory and Control of Software Assets	16%
3. Continuous Vulnerability Management	50
4. Controlled Use of Administrative Privileges	60%
5. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	44%
6. Maintenance, Monitoring, and Analysis of Audit Logs	0%
7. Email and Web Browser Protections	0%
8. Malware Defenses	58%
9. Limitation and Control of Network Ports, Protocols, and Services	56%
10. Data Recovery Capabilities	52
11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches	56%
12. Boundary Defense	21%
13. Data Protection	17%
14. Controlled Access Based on the Need to Know	56
15. Wireless Access Control	56%
16. Account Monitoring and Control	52%
17. Implement a Security Awareness and Training Program	12%
18. Application Software Security*	--*
19. Incident Response and Management	6%
20. Penetration Tests and Red Team Exercises*	--*

* Control category not assessed in the version of the CSAT used

Conclusion

It is clear that EPF values cybersecurity and its investment have paid benefits. Their personnel are knowledgeable and diligent, their technology is generally well maintained, and they have an environment of security consciousness. However some risky practices remain that the IT staff are working to resolve. With attention to these few areas, EPF can significantly raise their resilience and recoverability against accidents and adversaries.

Helping you optimize cybersecurity risk and cost through world class services.

Founded in 2012, Stratigos Security promotes strategic and holistic approaches to security for our clients. This means taking a broad view across the organization, and in the long view, to see how and where security fits into their broader context. That is different than how many information security programs are run – compartmentalized internally and isolated from the organization's value drivers. Our clients range from Fortune 100 to small businesses, and span the globe.

Stratigos Security has worked with organizations of nearly all sizes and industries, around the world. On average, our consultants have more than a decade of experience protecting organizations from information security threats, and some have been doing it for more than 20 years. Our consultants routinely present at conferences, publish papers, and release security tools.

You can contact us at **https://stratigossecurity.com** or by email **info@stratigossecurity.com**.