STRATIGOS SECURITY

Helping Eurasia Partnership Foundation Improve their Cybersecurity

Presented to:
Chuck Brackett
Digital APEX: Armenia Lead
PM Consulting Group

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

- DRAFT v1.0, published September 9, 2021

Copyright, Confidentiality, and Non-Disclosure

Table of Contents

Document Properties *1*
Version Control **1**
Copyright, Confidentiality, and Non-Disclosure **1**
Executive Summary *3*
Action Plan *4*
Use fully supported, updated website software **5**
Implement Full Disk Encryption **6**
Trusted encrypted communications platforms **7**
Implement a Virtual Private Network (VPN) for office connectivity **8**
Implement Password Management Software **9**
Implement Multi-Factor Authentication **10**
Conclusion *11*
Appendix A: VPN Selection Framework *12*

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 Findings and Recommendations

EPF operates like a small business, though it faces highly capable and motivated adversaries. 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 software
- Implement full disk encryption
- Trusted encrypted communications platforms
- Implement Virtual Private Network (VPN) for office connectivity
- Implement Password Management Software
- Implement Multi-Factor Authentication

Action Plan

Each of the pages below contains a single Action Item that will help EPF build capacity for a sustainable security program. Most of the Action Items can be implemented on a modest budget in the coming weeks or months without significant disruption to workflow. Some of the Action Items represent roadmap projects to be implemented when certain conditions and thresholds are met, as articulated in the plan.

The information provided represents an independent third-party recommendation intended to assist in justifying additional funding from donors. Where specific expertise or resources are required to implement the items, Stratigos has estimated initial implementation as well as ongoing needs.

EPF has invested in IT and cybersecurity capabilities so the list of action items is short. However, there are some key initiatives that, if undertaken, can significantly raise their security posture and improve resilience against accidents and adversaries.

The accompanying **EPF – Cybersecurity Risk Assessment** document contains detail on risks identified and the table below maps these to Action Item(s) that help in mitigating these risks. In addition, there are further recommendations specific to those risks which may partially address these issues though don't rise to the level of an Action Item. In addition, there are some Action Items which are considered effective practice and are low effort, which do not directly relate to the organization's largest risks.

Cybersecurity Risk Assessment	**Action Item(s)**
Hacking of the websites	Use fully updated, supported software
Hacking of corporate emails	Implement Password Management Software Implement Multi-Factor Authentication
Unauthorized access to the organization's internal database	Implement VPNs for office connectivity Implement Password Management Software Implement Multi-Factor Authentication
Personal data about beneficiaries	Use fully updated, supported software Implement Password Management Software Implement Multi-Factor Authentication Trusted encrypted communications platforms
Physical security of the office	Implement full disk encryption

Use fully supported, updated website software

Description
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 platform migrations happen with ample time to avoid going out of support.

Justification
Websites directly expose organizational infrastructure to adversaries over the Internet. Even sites that do not contain sensitive information or provide a direct pathway to internal systems can pose risks to reputation or site visitors if compromised.

When to initiate
Implement as quickly as reasonably possible, ideally by deploying a new server in parallel for testing, then migrate to the fully updated instance. If new sites or servers are in development, ensure that they are running the latest versions of the operating system, web platform, and any site components.

Success criteria
A recurring authenticated vulnerability or configuration scan on the organization's website can validate the action is consistently taken. In addition, uncredentialled scanning can give some insight into vulnerabilities most likely to be exploited by adversaries

Resourcing

Estimated Cost
Capital: None unless new licenses are required
Operating: Minimal

Estimated Timeline
1-2 Weeks

Required Skillset
Basic IT administration and web skillset

Implement Full Disk Encryption

Description
Full Disk Encryption (FDE) is a technology which protects information and data stored on a hard drive by converting it into unreadable code that cannot be deciphered easily. Implement FDE on computers and mobile devices.

Justification
Adversaries with physical access to a device can retrieve sensitive information that puts the organization, its employees, and its beneficiaries at risk. For instance, passwords for bank accounts or online services; personal data about clients or employees; or other protected information.

When to initiate
Organizations of all size and maturity should implement this action as soon as possible.

Success criteria
Tools like Windows BitLocker are provided by Operating System vendors free of charge. BitLocker can be trivially verified on the device or through automated configuration scanning.

Resourcing

Estimated Cost
Capital: None
Operating: Minimal

Estimated Timeline
1 week or less

Required Skillset
Basic IT administration skillset

Trusted encrypted communications platforms

Description
Protecting communications is of utmost importance when working with vulnerable populations. Train employees and constituents to use highly secure platforms, such as Signal, when sending sensitive information.

Justification
When dealing with high capability adversaries, carrying out potentially sensitive work, all due care should be taken to ensure communications are not intercepted. While Telegram is an excellent tool for reaching the public, it is not considered to be one of the more secure communications platforms, even considering the “Secret Chat” feature.

When to initiate
Organizations of all size and maturity should implement this action as soon as possible.

Success criteria
Select platforms that enforce strong end-to-end encrypted communication, with the ability to verify identity and authenticity, and that have had extensive, publicly available security auditing. Stratigos recommends Signal, which meets these criteria.

Resourcing

Estimated Cost	Estimated Timeline	Required Skillset
No Costs	N/A	No special skillset required

Implement a Virtual Private Network (VPN) for office connectivity

Description
Virtual Private Networks (VPNs) can help avoid censorship and evade eavesdropping. VPNs can also allow organizations to restrict access to sensitive or highly critical resources on internal networks. Many network border devices provide VPN capabilities to allow secure access to internal network resources.

Justification
Sensitive resources and databases on the internal network exposed to the Internet pose an unacceptably high risk. VPNs significantly mitigate these risks, especially when combined with multifactor authentication.

When to initiate
Organizations that need to provide remote access to internal network resources should implement this action as soon as possible, provided they have basic IT administration skills to implement and maintain it.

Success criteria
Stratigos has developed a VPN evaluation framework (Appendix A) to help decisionmakers select VPN options.

Resourcing

Estimated Cost
Capital: None
Operating: Low

Estimated Timeline
1-2 weeks

Required Skillset
Basic IT administration skillset

Implement Password Management Software

Description
Password management applications automatically generate, store, and use strong, unique credentials for each internal or cloud-based system. Provide password management software for all employees and enforce its usage.

Justification
Credential attacks are the largest security threat most organizations face, in large part because authentication mechanisms are designed to work well for computers and not people. Password management software makes it easy and inexpensive to generate, maintain, and use high security credentials for internal and cloud-based systems. Their low cost and ease of use may improve employee productivity and efficiency. Central management further improves management control over IT assets.

When to initiate
Organizations of all size and maturity should implement this action as soon as possible. Organizations with a basic IT skillset can take advantage of central management capabilities.

Success criteria
Select password management software that provides local language support, centralized management, and multi-platform integration. Many password managers flag credentials that have been recently breached and automate updating passwords.

Resourcing

Estimated Cost
Capital: Minimal, especially for non-profits
Operating: Minimal, especially for non-profits

Estimated Timeline
1-3 weeks

Required Skillset
No special skillset

Implement Multi-Factor Authentication

Description
Multi-Factor Authentication (MFA) greatly increases account protection, especially for cloud-based services. By augmenting password authentication with physical tokens or temporal codes, adversaries that acquire a password are still prevented from gaining access to a system. Implement MFA on compatible systems, including email, website, and cloud based data storage.

Justification
Credential attacks are the largest security threat most organizations face. Adding a second factor of authentication reduces this risk by at least an order of magnitude. Multi-Factor Authentication (MFA) is relatively inexpensive, low friction, and low implementation cost for most systems.

When to initiate
Organizations of all size and maturity should implement this action as soon as possible on Internet-facing services that make the capability available.

Success criteria
Select technologies that are easy to use and low or no cost, and that provide app-based or token-based authentication. High capability adversaries can easily intercept or tamper with SMS-based authentication factors, so avoid those.

Resourcing
Estimated Cost
Capital: Low to none
Operating: Minimal

Estimated Timeline
2-3 weeks

Required Skillset
Basic IT administration skillset to implement, no special skillset to use

Conclusion

It’s clear that EPFs executives and staff are concerned about cybersecurity and have used a share of their limited resources to build up infrastructure, employ IT personnel and train their staff in cybersecurity practices. It is also clear that the organization would benefit from more investment in their infrastructure and up to date, licensed software improve their security posture to counter the high capability adversaries they face.

Appendix A: VPN Selection Framework

The virtual private network (VPN) selection framework was developed by Stratigos Security to facilitate decision-making by management when evaluating alternatives, whether self-hosted or commercial services.

Management

- **Implementation** - Difficulty and cost in implementing the VPN server or service, given the organization's financial and technical capabilities.
- **Operating expense** - Ongoing cost (per month, per seat) for the VPN, including employee training (if necessary).
- **Provisioning** - Ease of adding new accounts onto the platform.
- **Scalability** - How many total or concurrent accounts the server can support.

Ease of Use

- **Acceptability** - Ease of use for employees and others utilizing the VPN day-to-day.
- **Client availability** - Whether the VPN has clients to support all platforms that the organization uses.
- **Language support** - Whether VPN clients support all the languages in use within the organization.

Supply Chain

- **Proximity** - Relative location of the VPN server or service to resources and individuals using the VPN, which can affect speed and integrity of the connection.
- **Legal policies** - National or local policies on data interception, individual surveillance, or others, which may compel the service provider to degrade the integrity or confidentiality of the VPN connection.
- **Code and component transparency** - How transparent is the software or service provider about third-party and open source code, and partnerships (for instance, their cloud and VPN provider).
- **Logging** - Whether the software or service keeps connection logs or other information which could uniquely identify individual or organizational traffic.

Security assurance

- **Third-party attestation** - Whether the software or service provider have regular third-party security assessments with attestation, from reputable security firms.
- **Protocol security** - Security of the encryption protocol selection and implementation.
- **Network detection avoidance** - Difficulty for local network providers to detect (and potentially block) VPN traffic.
- **Disconnect security** - Whether the VPN prevents data leakage before it is connected or when the connection terminates.
- **Tenant isolation** - The degree to which accidents and adversaries affecting one host, region, or IP address will affect all VPN tunnels.

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**.