Archetypes: What they are and how to use them

Organizational Archetypes

Organizational archetypes are fictional profiles that pull out patterns in the circumstances of real organizations, but are not based on any single organization's experience. These archetypes capture the capacities, needs, and risks of human rights and information dissemination organizations, without putting organizations at further risk by identifying them specifically.

Organizational archetypes can serve as an educational resource within organizations, enabling staff to discuss and identify security vulnerabilities and challenges they face in order to allocate resources accordingly. In addition, they serve as a communication tool for organizations to articulate these threats and needs to funders and other community members in a safe, anonymized way.

Adversary Archetypes

Adversary archetypes illuminate the various motivations, favored means of attack, and resources being used by malicious actors without actually naming or identifying specific adversaries, which can be dangerous for at-risk organizations.

Similar to organizational archetypes, adversary archetypes can serve as both an educational resource within organizations and a communication tool for funders. Educating staff around the motives, intents, and capabilities of adversaries likely to target their organization can guide the design and adoption of security mitigations and countermeasures. Understanding threats and adversary capabilities allows organizations to be better prepared in the face of digital attacks. In addition, archetypes enable organizations to articulate to funders and other community members the type of threats they face and the need to prioritize security when allocating funding.

Icons made by Smashicons; Creaticca Creative Agency; Freepik; Eucalyp.

Human Rights Research and Advocacy Organization

This organization conducts research into human rights violations perpetrated by nation states, publishing detailed reports which it presents at international bodies like the UN. The organization experiences a high volume of phishing and other digital attacks which drain resources, put staff members and partners at-risk, and impede programmatic work.

Mission: Research, document, and publish reports on human rights violations perpetrated by nation states and conduct international advocacy

Size: 4-10 staff

Technical capacity: no IT personnel, but staff have undergone basic digital hygiene training

WHAT DOES THE ORGANIZATION WANT TO PROTECT? Records of interviews and testimony from individuals who have suffered human rights violations, including identifying names and locations; details of human rights reports and communications with international human rights institutions; and personal information of staff which could be used to target them.

WHO IS TARGETING THE ORGANIZATION? Nation state-backed cyber espionage groups, who step up attacks around periods when the organization publishes reports or press releases criticizing government activities. In addition to sending highly targeted phishing emails, these adversaries have gained access to the organization's website through brute force attacks, planting malware that infects all visitors to the site. The organization also receives regular phishing emails from financial scammers.

WHAT ARE THE SECURITY CHALLENGES? The small staff lack the time or expertise to prioritize security. Staff must retain highly sensitive information for long periods, but lack an understanding of the tools and procedures to do so securely. This is aggravated by a lack of local language resources or digital security trainings. There are no dedicated IT staff, and no one who is able to maintain the website. The organization has limited financial resources; moreover, funders insist these resources are allocated entirely to programmatic work.

WHERE ARE THE SECURITY VULNERABILITIES?

- No IT security staff
- Incorrectly configured office network
- No external backups of valuable data
- Old devices that will not allow updates
- Out-of-date software and antivirus lacking recent security updates
- High intern turnover makes safeguarding passwords difficult
- Website code not updated and vulnerable to attack
- No security system at physical office

Information Dissemination Organization

This organization conducts programs providing citizens in closed states with access to external information sources. Popular and news media content is disseminated using networks of local contacts. The organization experiences a high volume of phishing and other digital attacks which drain resources and impede programmatic work.

Mission: Provide citizens in closed information environments with access to external media content

Size: 8-15 staff

Technical capacity: One staff member with part-time responsibility for IT but no formal training in digital security

WHAT DOES THE ORGANIZATION WANT TO PROTECT? Details of the technical tools and contact networks used to transfer information in and out of the country. This includes the personal information of in-country sources who communicate with external contacts via phone. Failure to secure this information places the physical safety and lives of these individuals at risk.

WHO IS TARGETING THE ORGANIZATION? Nation state-backed cyber espionage groups who consistently seek to gain access to the organization's internal communications. The organization receives highly targeted phishing messages over email and SMS purporting to be from contacts in the civil society space or even staff members. These phishing attacks specifically target the phones of staff conducting information dissemination activities in the field in order to gain access to their networks of contacts.

WHAT ARE THE SECURITY CHALLENGES? The small staff who lack time or expertise to prioritize security. Field staff frequently have to communicate highly sensitive information with each other and headquarters-based staff, but lack an understanding of the tools and procedures to do so securely. This is aggravated by a lack of local language resources or digital security trainings. There is only one dedicated IT staff, whose main responsibility is to maintain the website. The organization has limited financial resources; moreover, funders insist these resources are allocated entirely to programmatic work.

WHERE ARE THE SECURITY VULNERABILITIES?

- Incorrectly configured office network
- Use of unencrypted messaging apps to communicate sensitive information with field-based staff
- Old devices that will not allow updates
- Out-of-date software and antivirus lacking recent security updates
- Website code not updated and vulnerable to attack
- No security system at physical office

Nation State-backed Cyber Espionage Group

This cyber espionage group is linked to repeated attacks against human rights and media groups critical of the government. In order to disrupt the activities of these organizations, they attempt to identify the identities of organization staff and deploy persistent attacks against the organization, increasing the financial cost of their operations.

Motive: Politically/ideologically-motivated

Intent: Undermine operations of organizations critical of home government

Victims: Human rights and independent media groups

Technical capacity: Professionally trained hacking team with state-funded hardware and software

WHAT IS THE GROUP'S MOTIVE AND INTENT? Defending the interests of the nation state government. To this end, the group seeks to undermine the programmatic activities of human rights and media groups perceived as critical of their government. They aim to gather intelligence on the activities and staff of these organizations, before attacking and compromising valuable data. As well as direct sabotage, they aim to shape the international media narrative by leaking strategic data to pro-government mouthpieces to employ in information campaigns.

WHAT ARE THE GROUP'S FAVOURED MEANS OF ATTACK? The group invests significant time, finances, and human intelligence into investigating target communities and individuals. Using their knowledge of the interests and networks of their targets, the group designs customized SMS and email spear-phishing attacks through which malware is implanted on the office and personal devices of organizations' staff, in order to detect and collect sensitive data. Extracted personal information is also used to threaten organizations' staff. The group targets weak passwords and outdated code on the websites of organizations, enabling them to set up watering hole attacks that compromise the devices of website visitors. Finally, the group employs Distributed Denial of Service attacks to knock the websites of high-value targets offline.

WHAT ARE THE GROUP'S CONSTRAINTS? As a criminal group working with direct support from a nation state government, the group is highly secretive and prioritizes avoiding public identification. It uses private sector infrastructure (e.g. Google, Microsoft) to perpetrate its attacks, making it vulnerable to "takedown" requests delivered to these platforms.

WHAT RESOURCES CAN THE GROUP DRAW ON?

- State-backed funding stream
- High-level software and hardware
- Staff who are experts in the field
- Access to professional training
- Time and personnel to commit to mission
- Freedom from domestic legal restraints

Commercial Phishing Group

This criminal group conducts large-scale, indiscriminate phishing operations in order to steal from or financially blackmail victims.	**Motive:** Financially/criminally-motivated **Intent:** Theft or blackmail **Victims:** Indiscriminate **Technical capacity:** Hacking team with moderate hardware and software capabilities

WHAT IS THE GROUP'S MOTIVE AND INTENT? This criminal team is focused purely on financial gain and does not target a particular type of person or organization. They distribute template phishing attacks to as wide a network of civil society and private sector targets as possible in order to steal from or gather information that may be used to blackmail them.

WHAT ARE THE GROUP'S FAVOURED MEANS OF ATTACK? The group designs template SMS and email phishing attacks which harvest credentials or implant malware and firmware on the office and personal devices of staff, gathering personal and bank account information or locking organizations out of their computer systems. The group then steals from bank accounts directly or blackmails organizations by taking control of accounts or threatening to publish sensitive information.

WHAT ARE THE GROUP'S CONSTRAINTS? Due to their relatively small size and simple mission, the group does not invest in targeting a specific profile of individual or organization. As a result, their ability to develop customized attacks that employ targeted social engineering tactics is limited, and simple trainings on identifying phishing messages dramatically reduces the effectiveness of their attacks.

WHAT RESOURCES CAN THE GROUP DRAW ON?

- Large, illicit funding stream
- Moderate software and hardware capabilities
- Time and personnel to commit to mission

Local Robbers

This local criminal group breaks into offices that they have identified as containing large amounts of high-value electronic hardware.	**Motive:** Financially/criminally-motivated **Intent:** Theft **Victims:** Small civil society organizations with weak physical security measures **Technical capacity:** Team specializes in overcoming physical security measures

WHAT IS THE GROUP'S MOTIVE AND INTENT? This criminal team is motivated purely by financial gain. The group aims to break into offices in order to steal and resell high-value electronic hardware. They most often target small, civil society organizations who have weaker physical security measures due to limited financial resources.

WHAT ARE THE GROUP'S FAVOURED MEANS OF ATTACK? The group takes advantage of poor physical security measures such as old door locks and unsecured windows to break into offices and remove hardware. They also invest time in observing target offices in order to identify infrastructure weakness as well as the staff and interns who hold keys.

WHAT ARE THE GROUP'S CONSTRAINTS? Due to their relatively small size and simple mission, the group targets the offices of organizations with visibly poor physical security. As a result, they are easily dissuaded by simple security measures such as CCTV and door and window locks. Since they aim to resell hardware rather than access data, the impact of their operations on data security is easily mitigated by external backups and secure storage of these backups.

WHAT RESOURCES CAN THE GROUP DRAW ON?

- Illicit funding stream
- Specialized tools for breaching physical security measures
- Staff who are experts in the field
- Time and personnel to commit to mission