KIRSCH GROUP

# UNDERSTANDING OUR ONLINE EXPOSURE - IDENTIFYING, ASSESSING & MITIGATING OUR DIGITAL RISKS.

Many inquiries about online exposure and digital risk focus on the methods and tools for finding exposed data on the open as well as deep and dark web. But that is only part of the equation. Digital risk reports that are simple lists or catalogues of an individual's information available online is only useful, to a point.

A complete assessment includes mitigating risk as well as the act of identifying it. What are we looking for, what does the information we find mean in terms of risks and what should we do about it?

At Kirsch Group we have developed a standard methodology to instruct our researchers and help our clients interpret and action the results into a security plan that is right for them.  We serve corporate security teams with executive protection responsibilities, law firms or the individuals themselves.

Please feel free to look, use, and share – to protect yourself, your clients, or anyone to whom you have a duty of care. We are also very open to feedback and suggestions. Let's work together to keep each other safe.

## This guide includes the following sections:

### 1: What should we look for when we conduct open-source research on an individual

### 2: How we interpret the risk of what we find (OSINT risk ratings)

### 3: Recommendations to mitigate identified risk based on the findings

*I hope you find this helpful for your own assessments. If you would like assistance, please get in touch and we'd be happy to scope a project*

**Protect what's important to you.**

# WHAT WE LOOK FOR WHEN WE CONDUCT OPEN SOURCE CHECKS ON AN INDIVIDUAL

## 1: What is the subjects physical security threat surface?

Definition: Any physical place identified in connection to or association with the subject that would provide a possible opportunity for an attacker to confront the individual. This includes associations with known activities that would reveal the subject's future identifiable movements and whereabouts.

### Looking for evidence of static private and public locations associated to individual:

- **Personal Home, Office, Cottage, Vacation home**
- **Spouse and Children: Home, Office**
- **Children school**
- **Religious institution affiliation**
- **accounts.**

### Hobbies that can be associated to a physical location:

- **Recreation sports team** *(eg. adult hockey league, squash club membership)*
- **Patron of arts** *(eg. ballet membership)*
- **Regular Volunteering** *(eg. In from the Cold at set locations)*
- **Children activities / teams** *(eg coaching youth league)*
- **Places of worship**

## 2: What is the personally identifiable information (PII) available that creates a cyber vulnerability

Definition: Data available online that can be used to uniquely identify the subject and identifies the subject as a high value target. As well as information that can be used to contact the subject along with a possible pretext that can be exploited through social engineering to effectively gain access to sensitive information. online presence can lead to physical targeting (e.g. geotags, LinkedIn, etc.)

### Looking for PII which can include:

- **Birthday,**
- **Email addresses,**
- **Phone numbers,**
- **Usernames,**
- **Passwords,**
- **Social insurance number,**
- **Passport,**
- **Credit card information,**
- **Mother's maiden name,**
- **High school**

### Also Looking for:

- **Open Social networks**
- **Corporate networks**
- **Other Group lists**
- **Unique interest group participation or association**

## 3: Negative Sentiment and Identified Threat Actors

**Definition:** Specific and targeted negative language, mentions or threats against the subject or affiliated organizations / associations to the subject where the link is direct and tied by the author(s) of the threat(s). (For example, threats are directed at the company and there is evidence the individual or group directing the threats has associated the subject with the company)

### Looking for

- **Negative mentions of the individual**
- **Negative mentions of the businesses**
- **Facebook groups mentioning the company or individual**
- **Message boards and discussions around the individual and the company**
- **Negative reviews of the individual and company**

## 1: Physical Security Threat Surface Risk Ratings:

**High:**
There are numerous private and public easily identifiable locations that would give a potential threat actor an opportunity to physically confront the subject. External and internal pictures and pictures, floor plans and videos of these sites are available to be viewed online.

**Medium:**
There are a few private and public easily identifiable locations that would give a potential threat actor an opportunity to physically confront the subject. External pictures may exist but there are no internal pictures, floor plans or videos available of the private locations.

**Low:**
here are no easily identifiable private or public locations nor corresponding internal pictures, floor plans or videos that would give a potential threat actor the opportunity to confront the subject.

## Proposed Recomendations:

**High: (If negative sentiment rating is high)**

- Subjects may wish to take additional security measures when visiting public spaces where their attendance has been telegraphed in advance online.
- All identifiable private locations should have effective security measures to limit unauthorized access to the sites. This should include access controls and intrusion detection systems with response capabilities.

**Medium: (In all cases)**

- Remove, where possible, all private residence internal photos, floor plans and videos
- Review all pictures posted online to ensure no internal photos reveal any security measures, or systems in place in private locations.

**Low: (In all cases)**

- Remove or limit, where possible, any unnecessary online information on the private residences or future identifiable locations of the subject.

## 2: Cyber vulnerability Risk Ratings:

**High:**
Evidence of current sensitive data leakage including usernames and passwords. Multiple identified email addresses and contact information as well as social media profiles without effective privacy and security controls with indiscrete and potentially compromising posts. Easily identifiable family, social and business contact lists, and significant obvious online activity and engagement with large amounts of PII available online with a high likelihood and potential for use in a cyber-attack.

**Medium:**
Evidence of historical sensitive data leakage including usernames and passwords. Some identified email addresses and contact information. Social media profiles demonstrate the use of privacy and security controls with no indiscrete and potentially compromising posts. Limited identifiable family, social and business contact lists with some visible online activity and engagement and limited amounts of PII available with moderate likelihood and potential for use in a cyber-attack.

**Low:**
Minimal evidence of historical sensitive data leakage including usernames and passwords. Limited identified email addresses and contact information. Social media profiles, if they exist, demonstrate the use of privacy and security controls with no indiscrete and potentially compromising posts. Minimal identifiable family, social and business contact lists with low traces of online activity and engagement. Small amounts of PII available with low likelihood and limited potential for use in a cyber-attack.

## Proposed Recomendations:

**High:**

- Engage a privacy consultant or online remediation service that can take down unauthorized, malicious, or impersonating content by enforcing terms of use agreements with online platforms and internet service providers

**Medium:**

- Consider an online exposure threat risk monitoring service to keep track of subject's digital footprint as well as future problematic content including suspicious domains, spoofed social media accounts and other PII that could be exploited by threat actors
- Consider a home cyber security network solution including a firewall, URL filtering, intrusion protection, anti-virus and anti-malware scanning as well as end-point cyber threat monitoring on all personal devices
- Limit / eliminate Geotagging in any online posts

**Low:**

- Change all passwords for all accounts that have been involved in a data breach
- Use complex and unique passwords across all online accounts to limit the breadth of damage that could be caused by a data leak (can be assisted by a password manager)
- Ensure multi-factor authentication is enabled on all email, banking, social media and other online accounts.
- Review privacy and security setting on all social media accounts
- Limit the amount of personally identifiable information available online
- Limit the amount of family, social and business links and networks identifiable online

## 3: Negative Sentiment & Threat Actors Risk Ratings

**High:**
There is a large amount of evidence of negative sentiment, allegations, accusations or threats against the subject or affiliated organization online. The source of this online activity is numerous, concealed, coordinated and well-organized, and appears across multiple online sources, platforms and feeds. The threats are particularly menacing, malicious, mendacious or using aggressively threatening language, possibly citing conflict or violence.

**Medium:**
There is some evidence of negative sentiment, allegations, accusations or threats against the subject or affiliated organization online. The source of this activity is restricted to a few online actors that can be easily identified and are not acting in a coordinated manner. This online sentiment is restricted to a single or few social channels or platforms. The language used may be negative but is generic, non-threatening, without inciting violence or conflict.

**Low:**
There is little or no evidence of negative sentiment or targeted nefarious activity against the subject online. Any online mentions of the subject are benign.

## Proposed Recomendations:

**High:**

- Immediately report to law enforcement any direct threats or incitement of violence originating online
- Ensure that any security provider is aware of the threats and has a plan in place to monitor any developments online threats and mitigate the risk should it manifest into physical engagement
- Consider online diligence or investigations service on any specific or unique threat actors, groups or
- movements.

**Medium:**

- Consider an online monitoring service to track negative sentiment and the online behaviour of threat actors
- Consider an online remediation service that can remove offending content by enforcing terms of use agreements with online platforms and internet service providers

**Low:**

- Regularly search and review online content to ensure that it remains free from negative sentiment and identified threat actors
- Consider google alerts or other free services to monitor any mention of your name, family, close associations and/or company on the internet