SKOUT
CYBERSECURITY

Threat Update

Family Offices

Overview

Having an effective cybersecurity plan at a Family Office is not only good business practice, but an increasingly necessary component of risk management. The 4,500+ Family Offices in North America are being targeted by cyber-attacks due to the large amount of wealth being managed and the high profile individuals associated with the businesses.

Weakest Links

- Ransomware
- Email Phishing Compromise
- Threats on Social Media Sites
- Inability to Detect a Cyber-attack
- Poor Visibility into Networks
- No Formal Incident Response Plan
- Lack of Formal Security Awareness Training Program

Additionally, many Family Offices remain hot targets for attacks because they lack formal, robust IT governance procedures as well as updated IT infrastructure. Even with the best systems and controls in place, attacks can still occur and it is imperative to have a plan in place to mitigate risk.

Factors Contributing to Risk

GOVERNANCE

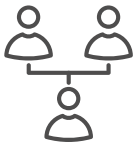
Many family offices have informal governance structures, limiting access control.

SECURITY SECOND

Efforts to work efficiently can put effective security policies and procedures in the back seat.

TECHNOLOGY

Technology in family offices can sometimes be overlooked, exposing out-of date and vulnerable systems.



DATA CONTROLS

In smaller, close-nit environments many users can be given universal access to information systems.

VENDORS

Family offices often leverage external vendors. These vendors can act as a point of entry for attackers into other networks.

FAME AND PUBLICITY

High profile families and clients elevate the threat level. Privacy is always important, but the risk is greater for Family Offices.

getskout.com

info@getskout.com

EMEA
IDA Business and Technology Park
Unit 1, Mountrath Road, Portlaoise
Co. Laois. Eircode: R32 CA44
+353 87 7020379

Security Operations North America
270 South Service Road
Suite 55
Melville, NY 11747
+1 631 203 6600

Corporate Office
530 5th Avenue
8th Floor
New York, NY 10036
+1 631 203 6600