Deloitte.
Private

The Family Office Insights Series - Global Edition

The Family Office Cybersecurity Report, 2024

Foreword

Welcome to **The Family Office Cybersecurity Report**, which is the fourth edition of Deloitte Private's new **Family Office Insights Series**. This report offers invaluable insights into family offices' experience with cyberattacks, the means they are using to protect themselves, and what activities they can adopt to help safeguard themselves against future attacks.

The data in this report is based on a survey of 354 single family offices from around the world between September and December 2023. These offices oversee an average assets under management (AUM) of US$2.0 billion, while the associated families have an average wealth of US$3.8 billion. Collectively, this totals an estimated US$708 billion in AUM and US$1.3 trillion in family wealth (figures 1 and 2).

We also conducted 40 in-depth interviews with senior family office executives to provide quotations and case studies with personal insights that can help family offices to better understand their peers. To make the findings as useful and relevant as possible, this report is interactive, with the option to scroll through the findings by region and size (AUM above and below US$1 billion).

We hope these insights prove useful in shaping cybersecurity planning for your family office, and we would like to offer a heartfelt thank you to all participants who generously shared their time and perspectives.

Figure 1: Participating family office regional headquarters' locations

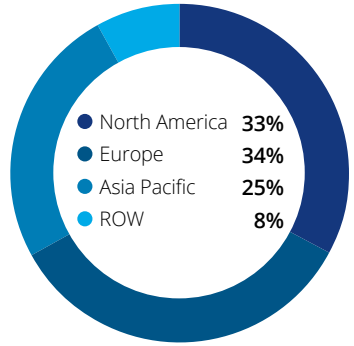
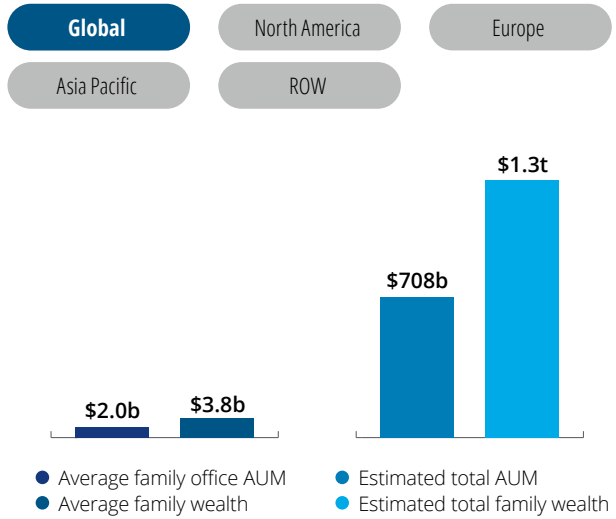
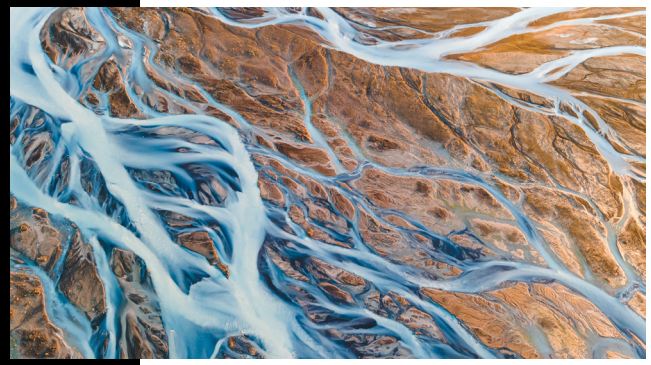


Figure 2: Respondents' family office AUM and family wealth

Click on each button to view the data



Key takeaways



1 Cyberattacks have become commonplace

A notable 43% of family offices globally have experienced a cyberattack over the last 12-24 months, with 25% experiencing three or more attacks. Those in North America are the most likely to report being attacked (at 57% versus 41% in Europe and 24% in Asia Pacific), along with those with AUM over US$1 billion (at 62% versus 38% for those with AUM under US$1 billion).

2 Threats are varied in nature and often linked

While threats come in many forms and are often linked, the most common form of attack is phishing (experienced by a notable 93% of victims), followed by malware (35%), and social engineering (23%).

3 One-third have suffered loss or damage from an attack

Among the family offices which have experienced a cyberattack, a significant one-third globally have suffered some form of loss or damage as a result. The most common consequences are operational damage (including the loss of confidential/sensitive data) and financial loss, as experienced by 20% and 18% of victims, respectively.

Key takeaways

4 Yet many have no cybersecurity plan in place

Despite the high prevalence of attacks, nearly one-third (31%) of family offices do not have a cyber incident response plan in place. Another 43% say they have a plan, but it "could be better," while merely a quarter (26%) claim to have a "robust" plan.

5 Many of the current plans are lacking, leaving family offices open to risk

At present, most family offices offer some basic security measures, such as strong passwords/multi-factor authentication (MFA) (85%) and data backups (72%). Fewer offices offer other basic measures, such as cybersecurity staff training (58%) and maturity assessments (34%). Moreover, many offices have not progressed on to more advanced protections that would make them better prepared: 50% do not have a disaster recovery plan, 63% do not have cybersecurity insurance, 68% have not adopted 'know your vendor' protocols, etc.

6 As a result, cybersecurity planning has become a top priority for some family offices this year, but not for enough

Given these security weaknesses, over one in five family offices (22%) have ranked cybersecurity as a top risk to their organization this year. Thus, 15% assert that strengthening cybersecurity is a core priority in 2024, a notable proportion, but one that needs even further visibility given the risks at stake.

Contact

Dr. Rebecca Gooch
Deloitte Private Global Head of Insights
2 New Street Square, London, EC4A 3BZ, United Kingdom
Direct: +44 20 7303 2660 | Mobile: +44 (0) 7407 859053
rgooch@deloitte.co.uk | www.deloitte.co.uk/deloitteprivate

Tiffany Kleemann
Investment Management and Cyber Board Governance Leader
Managing Director, Cyber & Strategic Risk
1919 N. Lynn Street, Arlington VA , United States
Mobile: +1 571 232 5366
tkleemann@deloitte.com

Karina Mowbray
Technology Risk and Cyber Leader
Partner I Deloitte LLP
1 New Street Square, London EC4A 3HQ
Mobile: +44 778 870 1963
kamowbray@deloitte.co.uk

Chris Gatford
Australia Deloitte Private Cyber Advisor
Partner I Deloitte T&T Pty Ltd
50 Bridge Street, Sydney, New South Wales, 2000, Australia
Direct: +61 2 9322 5099 | Mobile: +61 402 893 988
cgatford@deloitte.com.au | www.deloitte.com.au

Adrian Batty
Global Family Enterprise Leader
Partner | Deloitte Private, Tax & Advisory, Deloitte
477 Collins Street, Melbourne, Victoria 3000, Australia
Direct: +61 3 9671 7858 | Mobile: +61 414 427 692
abatty@deloitte.com.au | www.deloitte.com.au

Wolfe Tone
Global Deloitte Private Leader
Partner | Global & US Deloitte Private Leader, Deloitte LLP
111 S. Wacker Drive, Chicago, IL 60606-4301, United States
Direct: +1 312 486 1909 | Mobile: +1 312 545 9670
wtone@deloitte.com | www.deloitte.com

Deloitte.
Private