RISK strategies

PRIVATE CLIENT SERVICES

PRIVATE CLIENT SERVICES

A Comprehensive Guide to Cyber Insurance for High-Net-Worth Individuals and Families

What you need to know about rising cyber risks and how to best protect yourself and family.

Cybercriminals are increasingly targeting high-net-worth (HNW) individuals and families, leveraging sophisticated tactics to exploit overlooked vulnerabilities. A report from Campden Wealth revealed that nearly 30% of ultra-high net worth families have experienced a cyberattack. From financial fraud to identity theft, these attacks not only lead to substantial financial losses but also cause severe reputational damage.

Many families underestimate their exposure, failing to recognize that even minor gaps in digital security can serve as entry points for attackers. Given the ever-evolving cyber risk landscape, every individual needs to understand common cyber threats, implement key security measures, and recognize cyber insurance as a critical component of a comprehensive risk management strategy.

RISING THREATS:

Cybercrime impacting high-net-worth individuals

In recent years, the number of cybersecurity incidents and crimes rose significantly, causing significant financial harm. Worldwide cybercrime costs will hit an estimated $10.5 trillion annually in 2025.

Though wide-spread data breaches and large-scale attacks affecting high-profile businesses make headlines, many cybercriminals view high-net-worth families as low-hanging fruit. What makes these families and individuals appealing targets? They have the wealth and public exposure of companies, but usually with far fewer defenses in place.

Alarming statistics underscore the reality of growing cyber threats:

- 1 in 3 homes with computers are infected with malicious software.
- 47% of American adults have had their personal information exposed by cyber criminals, according to the Cybersecurity & Infrastructure Security Agency.
- 300,000 Facebook accounts are hacked every single day.
- Individuals lost nearly $8.8B to fraud in 2022, according to the Federal Trade Commission.
- 26.5% of middle and high school students report cyberbullying.

Cyber risks will only continue to grow and adapt as cybercriminals become more sophisticated.

Individuals, particularly those with substantial financial assets, must take proactive measures to safeguard their digital and financial security.

5 most common cyber threats to high-net worth individuals and families

The first step to protecting your family and assets from rising cybersecurity risks is understanding the threats. As our world becomes more connected, more digitized, and more online, cybercriminals are targeting high-net-worth families with increasingly advanced tactics. High-net-worth individuals face a unique set of cyber risks due to their wealth, public visibility, and digital footprint.

The five most common cyber threats for HNW individuals fall into the following categories: social engineering risks, ransomware, smart device and network vulnerabilities, financial fraud and identity theft, and cyberbullying, social media, and online harassment risks.

1. Social engineering risks

Cybercriminals use manipulation rather than technical hacking to deceive individuals into sharing personal or financial information. Phishing attacks—where scammers impersonate trusted advisors, banks, or even family members—account for over 90% of cyber breaches.

Increasingly, criminals are also leveraging AI-driven deepfake technology to create hyper-realistic impersonations in emails, voice calls, and video messages. These scams are designed to pressure you into making urgent financial decisions, such as wiring money or disclosing sensitive account details.

2. Ransomware

Ransomware attacks occur when hackers gain access to your personal or financial data, encrypt it, and demand payment to restore access. According to the FBI, an estimated 4,000 ransomware attacks occur daily. High-net-worth individuals are prime targets due to their ability to pay large ransoms. Ransomware often infiltrates systems through malicious attachments, compromised websites, or third-party service providers, such as IT firms or property managers.

3. Smart devices and network vulnerabilities

From smart home security systems to smartphones to luxury vehicles with keyless entry, connected technology offers convenience — but also new entry points for cybercriminals. Hackers can exploit weak passwords, outdated software, and unsecured networks to access personal data, monitor home security cameras, bypass login protections, and even unlock vehicles remotely.

Additionally, public Wi-Fi, often used during travel, can expose sensitive information to hackers running fake network access points.

4. Financial fraud and identity theft

Identity theft and financial fraud are among the most damaging cyber threats for high-net-worth individuals. Criminals exploit vulnerabilities to access financial accounts, steal assets, and impersonate victims.

Wire fraud schemes trick individuals into authorizing fraudulent transactions, often by impersonating trusted contacts, such as contractors or financial advisors. Identity theft remains a top risk for wealthy families, with stolen personal data used to open fake accounts or conduct unauthorized transactions. Fake investment and cryptocurrency scams also target HNW individuals, luring them into fraudulent opportunities.

5. Cyberbullying, social media, and online harassment risks

Your social media and digital footprint can make you and your family easy targets for cybercriminals, scammers, and online predators. Everything you share — whether it's vacation photos, location check-ins, or business updates — can be used against you. Oversharing personal details can tip criminals off when your home is empty, putting you at risk for burglary or fraud. Online impersonation is another growing threat, where scammers create fake profiles using your photos and information to manipulate your friends, family, or business contacts.

For children and teens, the risks are even higher. Cyberbullies and online predators use social media and gaming platforms to harass, manipulate, or exploit kids — sometimes coercing them into sharing personal information or even money. Cyber extortion is also a serious concern, with criminals using doctored images or fake scandals to demand payment. And for high-profile families, online smear campaigns can damage reputations overnight.

Cyber threats are always evolving and growing. Staying informed and implementing proven risk control measures will help safeguard your wealth, privacy, and peace of mind.

RISK MITIGATION:

Key cybersecurity strategies to protect your household

Even the most security-conscious individuals can fall victim to cybercrime, but taking proactive measures can significantly reduce risk. Here are effective, actionable steps individuals can implement to protect their data and identities:

- **Password best practices:** Use complex, strong passwords, and a password manager. Do not use the same password for multiple accounts. Change passwords frequently on your smart devices and connected household devices.
- **Use multi-factor authentication (MFA):** Enable MFA on all accounts where it's available, including financial, email, social media, billing systems, health accounts, and more.
- **Update software:** Keep virus protection and software updates current on all devices; consider turning on automatic updates and backups.
- **Learn to recognize phishing attempts:** Never click on links or open attachments in unsolicited messages.
- **Verify, verify, verify:** Always verify financial or sensitive requests through a separate, trusted channel.
- **Limit public information:** Manage your privacy settings on social media and reduce personal details available online, including travel plans and financial affiliations.
- **Train your family:** Educate those close to you about phishing scams, deepfake risks, and financial fraud. Confirm all urgent requests via phone or video call.
- **Encrypt sensitive communications:** Use encrypted messaging apps like Signal or WhatsApp for private conversations.
- **Monitor financial activity:** Set up real-time alerts on all banking and investment accounts to catch suspicious transactions early.
- **Vet third-party service providers:** Ensure IT firms, financial advisors, and property managers follow strong cybersecurity protocols to help defend against vendor-based attacks.
- **Educate children on online safety:** Monitor your children's social media and cell phone activity for signs of cyberbullying and harassment. Teach kids and teens to avoid engaging with strangers online and report suspicious messages.
- **Back up data regularly:** Maintain offline backups of financial documents, personal files, and critical business data in case of ransomware attacks.
- **Have a plan:** Work with cybersecurity experts to create a ransomware & fraud response plan so you know exactly what to do in an emergency.

While these strategies help mitigate risks, they do not offer complete protection — this is where cyber insurance becomes a crucial safety net.

Understanding personal cyber insurance

Even with the most robust cybersecurity practices, breaches still happen, causing significant financial and reputational strain. Many individuals may assume they don't need a person cyber insurance policy, or wrongly believe cyber insurance is only for corporations. But cyber insurance has become essential protection for high-net-worth individuals, and the risks and loss potential will only continue to grow. More and more individuals and families are being impacted by cyberattacks. High-net-worth individuals are prime targets.

Cyber insurance can help ease the burden of managing a cyber incident, offering much more than financial protection. It connects you with seasoned experts who can guide you through the recovery process.

Here are ways a cyber insurance policy can help safeguard your assets and mitigate crises that could otherwise result in significant personal losses:

What does cyber insurance typically cover?

Breach event cost coverage and expert-led breach response

Navigating a cyber incident can be overwhelming without the right expertise. From identifying the root cause of a breach to developing an effective recovery strategy, having access to skilled professionals is vital.

Breach event cost coverage covers expenses related to responding to a cyber breach, including forensic investigations, legal fees, notification costs for affected parties, and crisis management services to minimize reputational damage. This coverage empowers you to respond confidently and efficiently, significantly reducing the broader impact of the event.

Data recovery coverage

An essential element of any cyber insurance policy, data recovery coverage pays for the cost of restoring lost or compromised personal files, including documents, photos, emails, and financial records, in the event of data corruption, ransomware, or accidental deletion.

Cyber extortion coverage and ransomware recovery

Ransomware attacks can paralyze your digital world by encrypting critical files and demanding payment for their release. For high-net-worth families, this might include sensitive personal data or digital access to valuable assets.

Cyber extortion coverage provides financial protection if you're targeted by ransomware or cyber extortion threats.

This can include coverage for ransom payments when legally permitted), hiring negotiation specialists and professional incident response teams to investigate and resolve the attack, and technical assistance to regain access to your data. This coverage minimizes downtime and ensures the fastest path to recovery.

Cybercrime coverage

Given the high volume of fraud and scams that target HNW individuals, all individuals need to consider cybercrime coverage as a part of their personal cyber insurance policies. The coverage reimburses direct financial losses from fraudulent online transactions, unauthorized electronic fund transfers, wire fraud, phishing schemes, unauthorized payments, or scams involving impersonation, such as business email compromise (BEC).

Reputational harm

A cyberattack can lead to damaging publicity. Whether it's leaked personal information or media coverage of an incident, the fallout can affect both your financial standing and social credibility. This coverage protects against lost income or financial penalties due to reputational harm and provides access to expert public relations assistance.

What does cyber insurance typically cover? *(Continued)*

Cyberbullying

The psychological toll from relentless online abuse requires immediate intervention and ongoing support to address the harm caused. Cyberbullying coverage helps cover legal fees, counseling services, and crisis management costs if a member of your family becomes a victim of online harassment, reputational attacks, or cyber extortion.

The coverage also facilitates the removal of harmful content from websites, social media, or online forums, enabling victims to regain normalcy and peace of mind.

Security and privacy liability coverage

A cyber breach of your personal network can expose private messages, documents, and sensitive information.

Security and privacy liability coverage protects against lawsuits if your personal data is exposed or misused due to a cyber incident. Coverage includes legal fees, settlements, or damages resulting from data breaches or privacy violations affecting your personal network or devices.

Identity theft expenses coverage

If you fall victim to identity theft, this coverage covers the costs associated with restoring your identity, including legal fees, credit monitoring, fraud resolution services, and expenses related to recovering stolen personal information.

Cyber liability insurance provides a vital safety net for high-net-worth individuals, helping you recover swiftly and effectively from cyber incidents while protecting your assets and reputation.

What does cyber insurance typically NOT cover?

While cyber insurance is comprehensive, it does not typically cover:

- Intentional acts of fraud by the policyholder.
- Losses from pre-existing cyber incidents before policy activation.
- Certain reputational damages unrelated to a covered cyber event.

The value of a standalone cyber insurance policy

For many years, cyber insurance coverage was included as an add-on to some homeowners' insurance policies, but as threats have evolved, the need for dedicated, standalone cyber insurance policies has become clear. Most high-net-worth individuals will benefit from the broad coverage included in a standalone cyber insurance policy:

- **Comprehensive protection:** Homeowners' policies often have cyber coverage limits that are insufficient for high-net-worth families. When exploring coverage options, ensure the policy limits align with your potential financial exposures.
- **Tailored coverage:** Standalone policies offer more robust protections, such as excess coverage and layered policy options. Policies should be Customize your policies to fit your lifestyle and specific liabilities, including coverage for family members.
- **Stronger claims and incident response support:** Comprehensive cyber policies include access to cybersecurity experts and crisis management teams, which can be invaluable in the wake of a crisis.

Cyber insurance: a vital component of wealth, identity, and home protection

The digital age presents unprecedented challenges for high-net-worth individuals and families. Cyber threats are constantly evolving, and even the most security-conscious individuals are at risk. Implementing strong cybersecurity practices is essential, but without cyber insurance, financial exposure remains a significant concern.

By securing a comprehensive cyber insurance policy, high-net-worth individuals can mitigate the financial, legal, and reputational risks associated with cybercrime, ensuring long-term security and peace of mind.

Learn more and connect with our cyber insurance experts

Connect with our team to review your cyber exposures and get the cyber insurance you need to protect your lifestyle

- Request a confidential cyber insurance consultation
- Connect with our Private Client Insurance Advisors
- Learn more about our Private Client Insurance & Risk Management Solutions

Want to learn more?

ABOUT RISK STRATEGIES

Risk Strategies is the 9th largest privately held U.S. brokerage firm offering comprehensive risk management advice, insurance and reinsurance placement for property & casualty, employee benefits, private client services, as well as consulting services and financial & wealth solutions. With more than 30 specialty practices, Risk Strategies serves commercial companies, nonprofits, public entities, and individuals, and has access to all major insurance markets. Risk Strategies has over 200 offices including Atlanta, Boston, Charlotte, Chicago, Dallas, Grand Cayman, Kansas City, Los Angeles, Miami, Montreal, Nashville, New York City, Philadelphia, San Francisco, Toronto, and Washington, DC.

