Bespoke Cybersecurity Services

Cyber Criminals are Targeting High Net Worth Clients, Family Offices and Corporate Executives

High Net Worth Individuals (HNWIs) and family offices have always been lucrative targets for cyber criminals, as they tend to be high-value targets without the same level of cybersecurity as corporations. In fact, 28% of ultra-high net worth (UHNW) families and family offices have experienced a cyberattack.

As individuals continue to work from home, the cybersecurity risks have only gotten greater, as home networks tend to be less secure than the ones employees use in-office.

Still, almost half of all HNWIs and family offices report having no dedicated cybersecurity policies in place. This could lead to substantial financial and even reputational losses. Luckily, the majority of cyber fraud schemes can be thwarted by instituting a few basic cybersecurity measures.

> **In fact, 28% of UHNW families and family offices have experienced a cyberattack.**
>
> **Still, almost half of all HNWIs and family offices report having no dedicated cybersecurity policies in place.**

How Do Cyber Criminals Do It?

The two main factors that account for the most cyber theft and loss are:

- *Compromises in Insider Accounts: Failure to give the right people the right access to sensitive data can allow for third party individuals to have open access to critical business information. Once cyber criminals have access to an insider account, they can penetrate your network and abuse their access to exfiltrate sensitive data, manipulate it, delete it, or use it to access other sensitive data in the enterprise.*
- *Failure to Monitor: Failure to create a system that oversees access and activity around email and file systems can allow cyber criminals to easily gain unrestricted access to sensitive data without being noticed. These cyber criminals can be current employees, former employees or third parties.*

The Bare Necessities

Multi-Factor Authentication *makes it harder for adversaries to access sensitive information and systems. It is best to use a third-party application like Duo, Google Authenticator or Authy rather than SMS.*

Data Backups *ensure that information can be accessed following a cyber security incident. It is important to perform daily backups of integral data.*

Cloud First Strategies *secure your sensitive data in one location, reducing human error when it comes to accessing sensitive data.*

Incident Response Plans *can mitigate many of the risks that come with falling victim to a cyber attack and reduce your remediation time.*

Family and Staff Cyber Training *can drastically minimize the chances of a breach.*

Cyber Insurance *can help to cover the costs of recovery from a cyber attack and to minimize business disruption both during and after the attack.*

Trusted Security Teams *ensure the holistic protection of IT systems against cyber threats.*

How Redpoint Can Help

Redpoint Cyber is equipped with elite cyber security experts with nation-state experience who can offer services to help you assess cyber threats and implement an action plan to combat common threats such as ransomware, business email compromise, social media account hijacking, funds diversion, extortion and cyber-related physical threats.

Remember, a cyber-attack can happen to anyone. Taking the necessary precautions may protect you from becoming a part of the statistic. Redpoint Cybersecurity experts offer:

Bespoke Services

- *Our customized and on-demand cyber security support meets the needs of the most discerning client*
- *Our security experts are always available to answer questions and assist with any challenges a client may encounter*

Protection

- *Traditional anti-virus products alone are not enough to defend against today's advanced cyber threats*
- *A robust IT security strategy is required; this includes security hardware, monitoring, cyber intelligence and analytic analysis*

Cyber Risk Management

- *We provide essential risk management for the client, family and extended team*
- *We offer a range of services, from cyber insurance assessment to personal devices setup and protection*

Breach Response Team

- *After a breach from cyber criminals or state-sponsored actors, our clients need a team with the right experience and plan*
- *Our Breach Response Services team tailors solutions to mitigate risk and prevent future threats from many known attacker vectors*

Threat Mitigation

- *We keep our clients secure through a unique approach to target, pursue and eliminate threats on your network – We Hunt the Hunter!*
- *Our human-led, technology-enabled ethos allows us to quickly identify vulnerabilities like a hacker and then use vulnerabilities coupled with threat intelligence to proactively hunt and eradicate threats*

Cloud Migration Assistance

- *Having a cloud-first strategy is critical to ensure a client's important information is securely backed up and accessible globally*

Russell Safirstein, President
russell@redpointcyber.com
212.863.1231

Tab Bradshaw, COO
tab@redpointcyber.com
703.395.3950

www.redpointcyber.com

www.linkedin.com/company/redpoint-cyber

www.twitter.com/redpointcyber