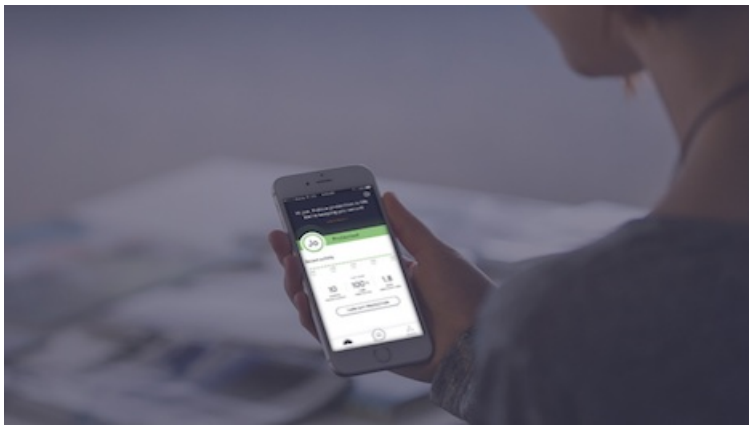
Luxury Daily®

The News and Intelligence You Need on Luxury

Q&A

Cyber criminals are turning attention to UHNWIs' digital assets

September 1, 2017



Digital culture has resulted in a need for cyber security measures. Image credit: Rubica

By JEN KING

Ultra-high-net-worth individuals are increasingly susceptible to cyber attacks, which has caused many affluents to hire full-service cyber security firms to protect assets and personal information.

Cyber security firms such as Rubica count Hollywood celebrities, startup founders, bankers, lawyers and other wealthy elites among their client rosters, as the need for cyber crime protection continues to rise. From identify theft and extortion to the leaking of private images and personal emails picked from individuals' devices and Cloud accounts, the wealthy must be mindful of the threat of cyber crimes and respond accordingly by safeguarding their digital property.

"The cyber security industry as a whole has actually become very sophisticated and most large institutions take the topic very seriously," said Roderick Jones, CEO of Rubica, San Francisco. "This in turn has increased the amount of time it takes for cyber-criminals to breach corporate security or government networks.

"In contrast, most individuals' cyber-security is very poor and therefore, it takes the average cyber-criminal a lot less time to crack into a ultra-high-net-worth individual (UHNWI)'s network than it would a corporate target," he said. "Therefore, the economics of cyber crime mean much more attention is now focused on hacking UHNWIs.

"This is a new and emerging threat and there are very few products and services designed for UHNWIs so this also feeds into the problem. The rewards for hacking a UHNWI are high and attainable by global cyber criminals and all the data points to this becoming a significant problem."

Rubica's CEO Roderick Jones. Image credit: Rubica

In this Q&A, Mr. Jones discusses what inspired the launch of Rubica, his experience at London's Scotland Yards and the need for online security in the digital era. Here is the dialogue:

What inspired you to launch Rubica?
The inspiration for Rubica was two-fold. Firstly, I could see that many of the individuals and families I was meeting for my previous business were having significant problems with all kinds of digital insecurity.

It was simply impossible for them to hire or buy in high-level cyber security to protect themselves so I became committed to finding an answer, which would help them.

The second and more indirect reason was a very English desire to be polite. I found that while making small talk in the United States I would often trip up over the question of gun ownership. People have very strong opinions on this subject and I was interested to learn more and began to look at the history of the U.S. Second Amendment.

When I looked more closely at this I realized that its origins lie in the fact that if you give people rights but no means to defend those rights, then you have practically given them nothing. The founders of the U.S. realized this and built the Second Amendment into the Constitution.

This seemed to me to be where we currently are in cyber-space. We've grown accustomed to significant benefits with the Internet but nobody has given us the tools to defend ourselves or our families in this new environment.

I set out with Rubica to build those defensive tools and the best way to do that initially is by providing individuals with high-grade cyber-defense through our secure network.

How does your prior experience at Scotland Yard prepare you for cyber security?
Whilst at Scotland Yard I worked on a number of very high-profile national security assignments.

One of those assignments was to run a protective security team. Security principles are essentially unchanging in their fundamentals between domains.

Using layered defenses, intelligence and deception to secure highly valuable assets are all techniques and ways of thinking that apply just as well if not more so in cyber security. Doing this in environments where there is no room to make a mistake is hard-won experience.

Why should UHNWIs be concerned about cyber security?

The cyber security industry as a whole has actually become very sophisticated and most large institutions take the topic very seriously.

This in turn has increased the amount of time it takes for cyber-criminals to breach corporate security (see story) or government networks. In contrast, most individual's cyber-security is very poor and therefore, it takes the average cyber-criminal a lot less time to crack into a UHNHI's network than it would a corporate target.

Therefore, the economics of cyber crime mean much more attention is now focused on hacking UHNWIs. This is a new and emerging threat and there are very few products and services designed for UHNWI's so this also feeds into the problem.

The rewards for hacking a UHNWI are high and attainable by global cyber criminals and all the data points to this becoming a significant problem.

What are some surprising places where the UHNWI are most susceptible to cyberattacks?
While there are some very obvious physical locations where UHNWIs are susceptible to cyber-attacks such as five-star hotels and even yachts, it is more the exploitation of their human network, which is most surprising.

Cyber-criminals have become increasingly adept at working out what a UHNWI's human network looks like and then they start attacking the peripheries of this network to get to the target.

So it's more a case of the way in which UHNWIs are susceptible to attack through their familial networks, which is more surprising. We've worked with individuals who were attacked via their in-laws being hacked in other countries.

Hackers are becoming more sophisticated. Image credit: Rubica

What sort of details are most at risk? Bank accounts or general details?
Financial details are always highly prized by cyber criminals because it is fundamentally an economic crime.

However, most pieces of virtual data have an after-market sales value so thinking about the problem only through a financial lens is a mistake.

Most of our lives are now becoming digitized and while some of this is seemingly worthless, it has value to attackers. The rise of ransomware is a direct consequence of this reality.

Individuals will pay some form of ransom to get family pictures or email correspondence back from attackers.

Are the hackers you've encountered looking mainly to extort money from UHNW or are there other motives?
There is no question that the hackers are looking to extort money in 90 percent of the cases.

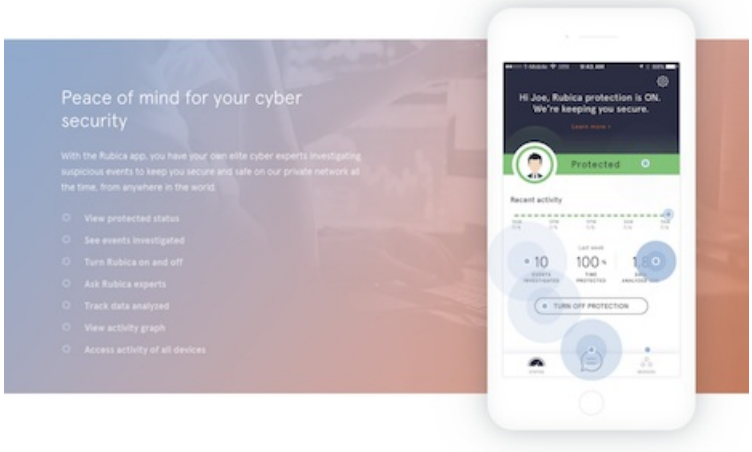
However, it also depends on what kind of business the individual is involved in. Executives with access to large amounts of intellectual property or financially sensitive information are targeted for that information.

We've also seen an increase in the level of sophistication used to attack individuals involved in the entertainment industry, which is less about financial extortion and more about acquiring digital content.

It is also a significant fact that individuals involved in political campaigns will be targeted by all levels of cyber attackers.

What can an affluent consumer do to protect themselves?
There are a series of cyber good hygiene recommendations, including, using two factor authentication for as many accounts as you can, utilizing VPN services when you are traveling and maintaining a strong set of passwords.

Many consumers find these hard to maintain, which is why we invented Rubica, which places your digital life on our secure network.



Rubica's cyber security measures includes a consumer-facing dashboard for clients. Image credit: Rubica

Are "secured" mobile devices and encryption worthwhile for UHNWIs?
Security is always a balance between security and convenience.

A house with no windows is very secure but not very usable and this has been the problem with highly secured mobile devices. If you do not make these products usable consumers go around them and the whole point of the system is lost.

So overall, these kinds of devices have not proven to be very successful even in specialist markets. Encryption is a different matter as much of the adoption of encryption has happened through various pieces of software, which have been introduced into systems we use daily, such as email.

There are also a good selection of encrypted chat applications available for consumers to use. These are worthwhile as long as individuals understand their limitations.

How does Rubica market its services?
Rubica currently markets its services through private banks and select events.

Our company is designed for people who are currently suffering the full brunt of cyber-theft and that typically is people who are clients of prestigious wealth management institutions.

Can you share any client demographics that might be interesting?
What has been extremely gratifying from my perspective has been the early-adoption of our service by experienced technologists from the most high-profile technology companies in the world.

Our approach is bold and therefore, having clients who live and breathe these problems at a massive scale sign up to use Rubica is a solid signal we are on the right path.