You lock your door, but do you lock your internet?

Cybercrime isn't a laughing matter, even if the names of different malware—Heartbleed, WannaCry—sound like angsty teen band names. The U.S. Justice Department recently said that cybercrime is one of the greatest threats facing our country, having enormous implications for national security, economic prosperity, and public safety.

Affluence Increases Risk

Because of the complexity of their lives and the many ways they use online services, high-net-worth successful individuals are more exposed to cybercrime. Statistically,successful individuals and families have 15 or more financial accounts. They often have multiple homes equipped with several computers and other devices connected to the Internet, including IoT-bound smart heating, cooling and security systems. And that doesn't even include personal computers or devices. Consider a few real-life examples:

Richard* owned a second home in Florida, and discovered that its smart protection/control system had been hacked and that the home's complex air conditioning system and alarms had been disabled. Because temperatures inside the house reached 95 degrees for days on end, Richard's $500,000 wine collection was ruined. Through his insurance provider, he connected with a security firm to identify vulnerabilities and tighten his cyber security.

When Ahmed* received an email from one of his banks notifying him that an account was overdrawn, something seemed amiss. By his count, he should have had a balance in excess of $10,000. When he checked his records, Ahmed discovered that his secretary had made several wire transfers from his account mistakenly using an email address similar to his. The bank found the email contained the Ahmed's Social Security number, as well as passport information. Identity theft services were engaged quickly to mitigate future damage to his personal identity.

Actionable Steps to Combat Risk

In each case noted above, the individual had proper coverage and services to mitigate future damage and their service providers alerted them to the risks. But not all cybercrime victims are so fortunate. Many families are inadequately protected from the potential financial damage that cybercrime can inflict, and many policies do little to help once a cybercrime has been committed.

In addition to reviewing policies and coverage, take action to eliminate unforeseen costs and headaches:

- **Protect yourself.** Don't expose yourself or your family to unnecessary risk. Complete background checks on employees. Back-up data via cloud software or external devices, and use anti-virus protection. Beware of connecting to the Internet in public places. Avoid pop-ups, ads, and unsolicited emails. Update passwords and computer software often. And don't overshare via social media or other means.

- **Be prepared.** Prepare an incident response plan that designates the individual within your business who will take charge if a cyber-incident occurs. The plan should include the names of experts prepared to provide legal advice as well as assist with assessing the extent of the incident.

- **Train your staff.** Many cyber incidents may be preventable through employee training and preventive measures such as not opening emails or attachments from an unknown source. Don't let your staff be the weakest link.

- **Act immediately.** Should a cyber-incident occur, execute your response plan and promptly notify authorities in the event of breaches of personal information.

Help your clients understand the importance of protecting against cybercrime

The rising tide and growing sophistication of cybercrime make successful clients more vulnerable than ever to identity theft, financial loss and more. Taking the proper precautions and maintaining safeguards can help protect HNW successful clients, their families and their businesses from becoming cybercrime victims. The right coverage also is essential, and Chubb provides the highest quality protection, unparalleled claim service and the peace of mind your clients need.

Contact Chubb to discuss your clients' unique risks and cybercrime exposure—and to find the right risk partner.

* U.S Department of Justice. https://www.justice.gov/ usao/priority-areas/cyber-crime

Chubb. Insured.℠