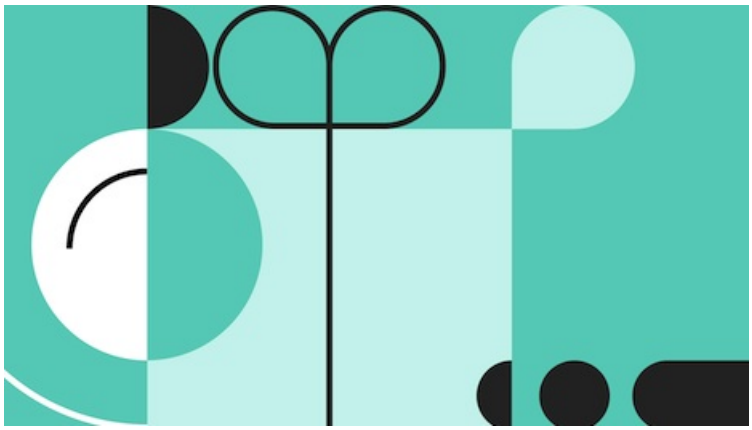
Luxury Roundtable
WORLD'S LEADING NETWORK FOR LUXURY PROFESSIONALS, MARKETERS AND WEALTH MANAGERS
Business at its best

COLUMNS

One overlooked element of executive safety: Data privacy

July 6, 2023



At one time, executive protection meant providing bodyguards and secure transit, and fortifying executive offices against external threats. As more executives work from home, efforts have extended to bolstering home defense systems. Image credit: OneRep

By Dimitri Shelest

Companies go to great lengths to protect their top executives. Keeping them safe, healthy and happy so they can perform their duties without unnecessary distractions is critical for the productivity of the company.

At one time, executive protection meant providing bodyguards and secure transit, and fortifying executive offices against external threats. As more executives work from home, efforts have extended to bolstering home defense systems.

Still, there is a missing element.

Getting personal
In today's digital world, it is also necessary to protect executives online. That should include protecting their personal data.

Executives have access to some of the company's most sensitive information, and they are increasingly being targeted by hackers looking to steal company secrets or to perpetrate cybercrimes.

Personal data provides fuel for these crimes.

Digital data warehouses store all kinds of details about all of us. It used to be just addresses, phone numbers, aliases and relatives.

Now, it is far more detailed information such as political affiliation, names of neighbors, resting heart rate and even Amazon wishlists.

All this data is collected legally by companies.

Every time you interact with a computer be that via a smart device, a bar code at checkout or on a website data about you is being collected.

In the United States, there is essentially no limit to the amount of data companies can collect, and few limits on how they can use it.

Most data can be sold to anyone who will pay for it, including bad actors. They can use it to personalize their workplace phishing attacks and business email compromise schemes to make them more effective.

Wailing time

Executives are particularly at risk for "whaling" attacks, where a criminal impersonates an executive via email or another means of communication and asks the target for money or information, or both.

A successful whaling attack can be quite lucrative, since executives have a lot of credibility and power.

In one such attack, a Mattel finance executive sent $3 million to a fraudster impersonating the company's CEO.

With the possibility of such large payouts, criminals will go to considerable effort to use personal details that make their requests compelling and believable.

Executives also face risks from social media, where they are more visible and accessible than ever before. This can be great for brand-building and engagement.

Unfortunately, it also puts them at risk of harassment or worse from a variety of bad actors, both online and in real life.

This can come from dedicated customers or fans who are unsatisfied with a product or service.

For example, in 2022, Strauss Zelnick, CEO of NASDAQ-listed video game developer Take Two Interactive, was forced to lock his Twitter account after being bombarded by a wave of harassment from customers dissatisfied with the latest Grand Theft Auto game.

It can also come as a result of taking a stand or not taking a stand on social issues. Gone are the days when staying neutral was the preferred corporate strategy.

According to research from Accenture, customers are increasingly aligning their spending with their values. They demand to know where companies stand on issues that matter to them.

Executives are expected to walk the walk and stand for the company's values. But one false move can place them in the crosshairs of cancel culture and harassers can quickly descend.

This kind of harassment, while still very upsetting for the individuals involved, can at least be somewhat anticipated and crisis communications strategies can be at the ready.

But threats to executives can also arise unexpectedly when a company is caught in the cross currents of the news cycle.

For example, after the contentious 2020 election, figures ranging from the head of strategy and security at Dominion Voting systems to the CEO of social media app Parler were forced to go into hiding with their families after receiving death threats when their personal information as well as that of their family members was leaked by hackers.

These scenarios do not even include the possibility of threatening behavior from a disgruntled or terminated employee.

In a turbulent economic environment such as the one we are navigating now, this issue may come into the foreground as executives grapple with layoffs and cost-cutting measures.

This does not just happen to executives at big companies or celebrity CEOs. Anyone who is involved in making decisions that can impact other people's lives, contradict their political views or offend their values can become a target.

The effects are devastating.

Job at hand

Researchers are just beginning to understand the impact of online harassment, but it appears to be very similar to other types of trauma.

Victims might have difficulty concentrating and making decisions. They might experience increased levels of anxiety and even paranoia. They might come to fear opening messages or looking at their devices.

Many individuals have even had to change jobs or alter their daily routines because of cyberstalking and harassment.

Clearly, none of this is optimal to executive productivity. But it not only affects their own well-being. It can deplete morale of the company and, ultimately, affect its bottom line.

The good news is that there are steps that companies can take to protect their executives, their families and their organizations. It starts with educating them about the threats, and the fact that they are possible targets.

Like the general public, executives can avoid oversharing personal information on social media. They can protect their Web browsing by using browser extensions to block trackers.

Also, they can maintain strong passwords, use a separate email address for sensitive activities, and be on high alert for any suspicious sounding communications.

Executives can also remove their data from people search sites that publish it. There are currently more than 190 of these sites. Data from my company, OneRep, shows that the average person has data records on 46 of them.

People search sites are legally required to remove your information on request, but they are not legally required to make it easy for you to submit that request.

Few people, least of all executives, have the time to approach 46 sites and request their data be removed. Even if they could, it is a Sisyphean task.

Our data shows that much of this information resurfaces within four months when they get their next data dump from their data broker.

THERE ARE TECHNOLOGY companies that can comb all the people search sites, locate your records and automate the removal process. They also provide continued monitoring and removal of your data should it reappear.

The proliferation and widespread availability of personal data is dangerous for public-facing executives, their families and their companies.

Companies understandably prioritize protecting the physical safety of top executives, but in today's polarized, always-on world, keeping executives safe online is also imperative. It is a small investment that pays dividends in peace of mind.

Dimitri Shelest is founder/CEO of OneRep, a McLean, VA-based privacy protection company that removes public records from the Internet.