Executive identity protection: Cyber bodyguards for the financial services C-suite

Sponsored by

verizon

Presented by

AMERICAN BANKER

Financial institutions invest heavily in security for their key executives but often overlook a major vulnerability: Cyber threats to the C-suite. While it's common knowledge that consumers frequently fall victim to identity thieves — who are notorious for stealing personal identifying information (PII) and leveraging it to open fraudulent credit lines and loans — the risks associated with top corporate executives and board members is frequently underestimated.

During the pandemic, many types of cybercrimes increased exponentially as threat actors reacted to the changing environment — and criminals quickly learned to extract maximum gains from individuals in positions of influence. "COVID was a rich opportunity of change that created a perfect incubator for these crimes. As retailers closed stores and everything shut down, a number of avenues were no longer open to threat actors, so they looked for new ways to monetize. At the time, corporate security was focused on other priorities, such as shutting offices down safely and pivoting to remote work," says Chris Novak, managing director of cyber security consulting at Verizon.

Cyber attacks against C-suite executives typically have higher stakes compared to run-of-the-mill identity theft cases. "Key executives have greater degree of power and authority, so such identity theft cases are more than just a pain in the neck. There's greater potential for malicious activities, such as potentially extorting executives to take certain actions at their company. Threat actors have the ability to gain substantial influence," says Novak.

Enterprises invest heavily in protecting the productivity of their key executives, providing such benefits as corporate jets, security details, personal drivers and many personal security measures — yet many fail to lock down digital footprints, leaving CEOs, CFOs, board members and others at considerable risk of identity-related crimes.

"Organizations typically have mature processes around physical security but they are not applying enough resources to cyber security," says Novak. Identity theft has the potential to severely disrupt an executive's home life and family members — and consequently their focus and productivity.

"Businesses want to minimize any possible distractions in the personal lives of their top executives that could cause them to take their eye off the ball. For example, if you're working on an M&A deal, you don't want a really distracted CEO," says Novak.

Executive ID theft: Real-life examples

In an actual case from July 2023, the chief information security officer (CISO) of a large enterprise became the victim of targeted spear phishing attacks. Threat actors obtained personal identifying information that they texted to his wife and children in a series of intimidating messages. They had detailed knowledge of the interior of their house, where the children went to school, the cars that the family members drove and many of their daily activities. The ominous texts originated from a series of VOIP numbers and were intended to intimidate the executive.

The executive engaged Verizon's Executive Identity Protection to investigate how the PII was harvested and how to remedy the situation. It was determined that "It wasn't from a data breach. Instead, the stalkers had gone to multiple data brokers and gathered information including the family's address, cell phone numbers and details of their daily lives," says Novak. It was clear that the criminals were not focused primarily on financial gain. In this instance, "it was someone who wanted to pester the CISO and his family," says Novak.

Using Verizon's methodical approach of surveying PII and working to scrub it from online sources, "We were able to erase their information from data brokers and help the family ratchet down their social media accounts. They are still able to use some social media, but only their friends can see their information now. We also saved them from the inconvenience of having to get new cell phone numbers," says Novak.

In another case, fraudsters stole the identity of a company's vice president of security and used it to communicate with his team, mimicking his online identity. The criminals bilked the company by sending multiple requests to his personal assistant and other team members for wire transfers of $100,000 to $200,000, claiming they were for false late-notice bills. "The fraudsters sounded like him through email

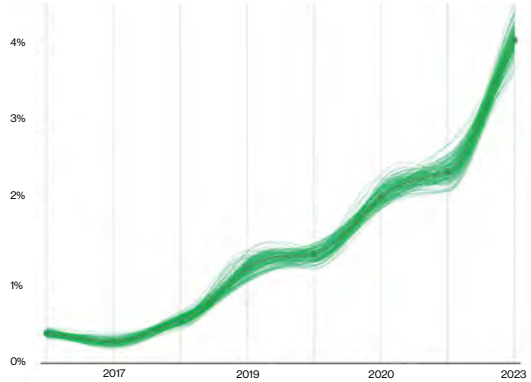
and had enough confirming information through their social engineering attack that their communications appeared to be coming from his house," says Novak. "They had likely made a dossier or profile of him so they could grab his personal information as needed."

To combat the attack, Novak's security team performed an executive assessment in which they traced the stolen PII to approximately 400 different data brokers, spanning 2,000 websites. Verizon was able to remove much of the personal information – including his home address, PII and details of his routines – from a range of online sources. Going forward, the service will continue to monitor and clean his PII, "working to remove him from spam-bot call lists, junk mail lists and financial solicitations, as well as providing credit freezing and even changing his address online so his home and family won't be disturbed again," says Novak.

How executive identity protection works

Verizon's Executive Identity Protection utilizes a variety of services to help shield top executives who wield high levels of access and influence. "In order to have full visibility into the threat landscape, a business should have a view into potential threats against those executives that are ingrained in the fabric of their business," says Novak. The multi-faceted service involves systematically erasing and reducing the individual's digital footprint in order to minimize opportunities for cyber attacks, such as spear-phishing, whaling, identity theft, swatting, doxing or other online harassment that can lead to physical threats. In particular, sophisticated social engineering schemes, also called pretexting attacks, are rising dramatically, according to Verizon's 2023 Data Breach Investigations Report.

Pretexting incidents over time



Here are the steps involved in Executive Identity Protection:

Surveying: What PII is out there?

The security team takes stock of the online PII about the executive that is readily available to anyone. "Typically, we find these individuals have a broad array of information that they don't even realize is public. Maybe they took out a mortgage or car loan at some point. Some of that information became publicly available and can get searched, cataloged, traded, bought and sold," says Novak. "Our first stage is conducting a survey of what data is out there and reviewing it to see what you want to disappear."

Verizon's experts then comb the dark web – hidden portions of the internet that aren't indexed by conventional search engines – for personal information that may have been stolen. "There could have been a data breach at your doctor's office, and now some of the information from your medical history is available to threat actors for malicious use," says Novak.

They also search the hundreds of data brokers that continually gather consumer information for use by advertisers, including data from public records or transactions with online vendors, such as addresses, financial information, demographic data and more. "The Terms of Service you click through allows this to happen," says Novak.

Scrubbing: Removing and erasing PII

After surveying and reviewing the data, the next step is to help begin systematically scrubbing the PII from various websites. There are a variety of ways to remove online PII or obscure it. "Typically, open sources or data brokers have processes to scrub the data, though they may be opaque or hard to discover," says Novak.

Working with data brokers can be time-consuming and involve tedious paperwork. Ongoing diligence is required as new data brokers enter the landscape or existing brokers merge and revise their policies. Laws and regulations related to PII are also continually changing. However, it is often possible to erase or disguise PII to help protect the executive's identity. "If I have a mortgage, it's not always the case that it has to be

associated with me. It could potentially be owned by a trust, so the information is obfuscated," he says.

Periodic reviews and coaching

Since compromising personal data can reemerge at any time, the security team performs checks periodically to identify new PII that surfaces. As vulnerabilities are discovered, the same processes are deployed to help scrub and remove it.
It's also important to train executives to minimize their digital footprints. Verizon experts provide one-on-one coaching on cyber security best practices for executives, their teams, or their family members. "We find a lot of people share information more broadly than they realize. For example, they may post on LinkedIn or Instagram, believing that only their friends or connections can see it. We sit down with the individual and show them what they're doing that leaves a breadcrumb trail and suggest remedies," says Novak. Simple recommendations for securing PII on an ongoing basis may include changing privacy settings on social media apps or making use of a VPN or anonymizer to limit the data they share.

Are your organization's key executives vulnerable to rising cyber threats? In 2023, nineteen of the top twenty U.S. banks (in terms of assets) use Verizon security solutions within their organizations. To learn about Verizon's services for cyber protection of C-suite executives, please contact your Verizon client partner or mark.bubar@verizon.com

Who we are

We deliver the promise of the digital world by enhancing the ability of humans, businesses and society to do more new and do more good. We transform how people, businesses and things connect with each other through innovative communications and technology solutions.

Verizon Enterprise Solutions - Transform Your Business