Financial Services Executive Whitepaper

Strategies to neutralize escalating threats against financial services executives and organizations

How private information exposure enables threats and attacks—and how to protect your organization.

Summary

The shocking killing of UnitedHealthcare CEO Brian Thompson has shaken organization C-Suites across the country. Leaders have been forced to ask themselves uncomfortable questions about their own preparedness for a threat landscape that is likely more serious than many realized.

Financial services organizations have also become aware of the need to take proactive steps to safeguard executives and personnel. Our whitepaper delves into the escalating risks associated with exposed personal information online—from targeted attacks to phishing emails that trigger a data breach. In this climate, no one is safe anymore.

Fortunately, there are effective ways to lower these risks and significantly reduce the likelihood of becoming a victim. We highlight practical solutions, including our Ironwall online privacy protection and executive protection programs.

Proactive measures are crucial in safeguarding against emerging threats to financial services CEOs, executives, and their families. They can include both removing already exposed personal information from the internet and shielding additional personal information from future exposure.

ironwall by Incogni

The danger is real

In May of 2025, a "highly targeted" spearphishing campaign attempted to ensnare financial executives at banks, investment firms, energy utilities, and insurance companies around the world. Malicious emails were sent and rigged with installers that allowed hackers to remotely access victims' computers and steal files or initiate fraudulent money transfers, potentially without raising red flags.[1]

Most of the emails were sent to CFOs and other executive-level employees in the financial department of the targeted firms—those that control access to payment systems. While American companies were not among those initially targeted, experts believed the attacks against institutions in Europe, Canada, the Middle East, and South Asia could be trial runs to refine technique before these hackers turned their attention to the United States.

Attacks against financial institutions are getting worse

In Bank Director's 2025 risk survey, 84% of those who responded cited cybersecurity as their top concern, and 64% experienced a cyberattack within the previous year. "Cybersecurity is a whole [other] level for directors and executives at banks," says Brian McGinnis, a partner at the law firm Barnes & Thornburg and co-chair of the firm's data security and privacy group. "This has become and should be a board-level issue for every single bank."[2]

The breadth and seriousness of the problem are evident when examining specific attacks that have already occurred:

ICBC Financial Services
A November 2023 attack disrupted the $26 trillion US Treasury market. ICBC was unable to settle trades, forcing them to manually process transactions via USB drives and leading to a $9 billion emergency capital injection from its parent company to cover uncleared trades.[3]

Prudential Financial
In February of 2024, what was initially reported as a minor breach impacting roughly 36,000 people was later revised to over 2.5 million individuals whose sensitive personal information and driver's license numbers were stolen.[4] The company has since faced multiple class action lawsuits.

Fidelity National Financial
In November 2023, Fidelity, one of the largest title insurance and mortgage service providers in the US, experienced a data breach that forced them to take their systems offline for a week, stalling real estate closings across the United States. The breach exposed the data of 1.3 million customers.[5]

Personal threats and attacks

We are living in a political and social climate that fosters division and resentment, which can also lead to violence. The same data hackers use to launch ransomware attacks is also widely shared and sold by data brokers, and is easily accessible on thousands of websites. This makes anyone who represents an institution a target.

"We're living in a society where we've unleashed violent forces," former Medtronic CEO Bill George told CNN. "You must have security for all of your senior executives—and even your board members."[6]

One executive at a major bank told CNN that the UnitedHealthcare CEO killing made plain the risk facing senior leaders in Corporate America and that the threats could come from anywhere and anyone. "The big learning is that if you want to kill someone, you can kill them," he said. "It's really scary but true. It seems crazy that we're just figuring this out."[6]

While the need for more security is apparent, some senior executives may not want to deal with the hassle and attention that intrusive personal security could bring. "CEOs don't want to live in a world where they go to their son's baseball game and there must be security present,"[6] said George.

The root cause: personal information exposure

Personal security can be lifesaving if an attacker gets close enough to their target. But making sure that an attacker can't find their target in the first place is a more effective solution. Unfortunately, the information necessary to find them is readily available online.

As internet access and usage evolved, millions of Americans were eager to take advantage of its many conveniences—shopping online, paying bills online, and staying in touch with friends. The internet didn't ask for much in return—only a few personal details to register for an account: your home address, phone number, email address, and date of birth. Most websites collect, share, and sell that information. As of 2024, there are more than 5,000 data broker companies worldwide, still collecting that information from more than 1,400 leading brands. The global data broker service market is expected to reach $407.5 billion by 2028.[7]

Today, virtually anyone can search for an individual online and find their home address, the names of spouses and children, and even where family members work or go to school. Searches like these are so easy to conduct that they can often be completed in the heat of the moment, with no cool-down time.

Anger + information = danger

The internet can also amplify one person's grievance against a financial institution or executive with just one viral social media post, inciting widespread outrage and condemnation.

Mainstream media and the internet, coupled with a decline in empathy, have created a dangerous culture where personal attacks and demonization over a single comment or action are now commonplace.

What's more troubling is that these attacks often stem from misinterpreted statements, misinformation, or false accusations. But whether the trigger is real or imagined, the result is the same: an individual's narrative shared online can rapidly stoke public outrage and even physical violence.

It can happen to anyone at any time. Angry people can now find anyone in both the digital and physical worlds.

The growing threat of artificial intelligence

Companies have always collected information to improve sales. The internet and our willingness to trade privacy for online convenience have significantly eased this process.

But today, organizations are not just collecting information to sell more products. They are collecting information on our opinions and behavior—our routines, hobbies, likes and dislikes, and political sentiments. They leverage that data to generate an emotional response—and more views and clicks.

This data, combined with the types of personal and demographic data already in wide circulation, allows brokers to compile an even more comprehensive profile on anyone. Scammers are aware of this and use artificial intelligence to target victims with scams based on their fears and priorities. They know that a scheme that triggers an emotional response is more likely to cause someone to panic and make a poor decision.

Example: a person is told that a loved one on a Caribbean vacation has been kidnapped, and the kidnappers demand $10,000. Voice cloning technology can even put that loved one's voice on a call, begging for help. The recipient, hearing what seems like irrefutable evidence, may send the money before trying to confirm the story.

Photos can also be weaponized through PimEyes, an advanced face recognition search engine that can run any photo through a massive database within seconds, and reveal how to identify the person in the photo. With cameras in every cell phone, anyone can take your picture, run it through PimEyes, and start building a profile on you. If you like to upload family photos to social media or take lots of selfies, this technology will find you quickly.

Whether the information is found through a commercial "people finder" site that resells public information, a malicious private site focused on a specific individual, or simply one of the daily breaches that happen in this country, the information is out there.

Do privacy laws make a difference?

As more states pass data privacy laws, it may be possible for everyone to contact data brokers and request that their home address and other personal information be removed, regardless of their profession. But this isn't a permanent solution. Some states only require that content be taken down for a limited period. In other cases, a removal request for Jim Evans may be granted, while Jim J. Evans (same person) remains on the site.

There is also a high likelihood that new content will emerge to replace any previously removed content. Refinancing a residence, getting a new credit card, getting married or divorced, or selling/buying a home can flood databases with fresh information.

But should privacy laws be passed and fortified, it's still unlikely that companies collecting personally identifiable information (PII) will change their policies. One need only look at the huge settlements that tech companies have chosen to endure to maintain their control over the information they collect. In 2022, Google agreed to pay nearly $392 million in a settlement with 40 states over allegations that the company tracked people through their devices after location tracking had been turned off.

Removing personally identifiable information online

The availability of personal information online is the foundation for almost every serious threat. That is why it is essential that financial services executives take control of their information and limit access to it when necessary.

Many people fail to act either due to a lack of awareness about these dangers or from a misconception that it's too late to retract their widely disseminated personal details. Most who try removing their online information themselves will become frustrated after having to re-send removal requests to a few hundred of the same websites and data brokers every few months and eventually surrender to what seems an inevitable situation.

Help is available, however. Several providers offer online privacy protection, but most focus solely on the top data brokers and people-finder websites. These account for only around 40% of sources where personal details can be found online, leaving hundreds, in some cases thousands, where content would still be accessible with a quick Google search.

This is where we can help.

The Ironwall by Incogni approach

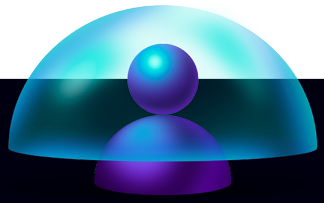
There is a reason why thousands of executives and public sector professionals trust Ironwall by Incogni to keep them safe.

First, we monitor all aspects of the internet—not just a few select sites. Your name and address likely appear on thousands of websites, not just those that specialize in "people finder" services. We track and remove our clients' personal information from them all, taking down 1.5 million pieces of private information every week.

Our protection also extends to our clients' families. Someone determined to target an individual will likely try to get to them through their spouse and children as well.

In addition to data removal, we take a more holistic approach to privacy protection. We can't stop thousands of companies from attempting to collect information, but we can provide privacy tools and specialized services that make it much harder to do so.

VPN



Your internet and phone providers are legally entitled to eavesdrop on web traffic and to collect and disseminate it. Every search, every email, every purchase is captured, indexed, and sold. With our Surfshark VPN, clients get a fast, reliable, no-logs VPN that encrypts their online activity and hides their location and IP address.

Email aliases

People share their email with friends and family. But they're also likely to share it with pizza delivery places, stores, restaurants, online retailers, and hundreds of other entities that will share or sell it, increasing the risk of scams and identity theft.

Ironwall provides clients with secure alternate email addresses to use in place of a personal email. Messages to these addresses are automatically forwarded to the real email inbox without revealing its address. Services such as Gmail and Outlook also provide disposable email addresses, but Google can still use those systems to track you. With Ironwall, your private information will never be shared or sold.

Databases are updated regularly. As authentic information like your email address and phone number begin to be replaced by fake ones, it won't be long before data brokers and scammers are unable to build an accurate profile on you.

Masked phone number

A mobile phone number tracks its owner everywhere they go. Calls, texts, applications, and browsing history can all be shared with organizations that sell that information, endangering the privacy of individuals and their families. A masked phone number can't be tracked.

Dark web monitoring

A mobile phone number tracks its owner everywhere they go. Calls, texts, applications, and browsing history can all be shared with organizations that sell that information, endangering the privacy of individuals and their families. A masked phone number can't be tracked.

Emergency protection

If the worst happens—you or your personnel are threatened online, targeted, or doxed—Ironwall responds with emergency support. We track the attackers online to monitor escalation patterns, violent threats, and suspicious behavior, and report it back to your organization or law enforcement. We conduct more extensive searches and extend protection to others in your executive's extended families, whether they reside with them or not. Our emergency support has been praised by law enforcement for saving lives and preventing tragedies.

Protecting executives also protects organizations from ransomware

Financial services organizations are attractive targets for ransomware for several reasons. Hackers know that executives and personnel have access to millions of dollars in funds and provide critical services that many people rely on. Every minute of downtime prevents customers from accessing funds, disrupts payrolls, and halts training. And modern ransomware is not just about locking files—it's about data theft. Banks hold Social Security numbers, credit scores, and transaction histories.

The repercussions of such an attack are severe—massive fines, reputational risk, and loss of consumer trust. Recognizing this, hackers see a high likelihood that victims will pay the ransom quickly to restore access. A 2023 survey from Sophos revealed that nearly half of those organizations that were hit chose to pay.

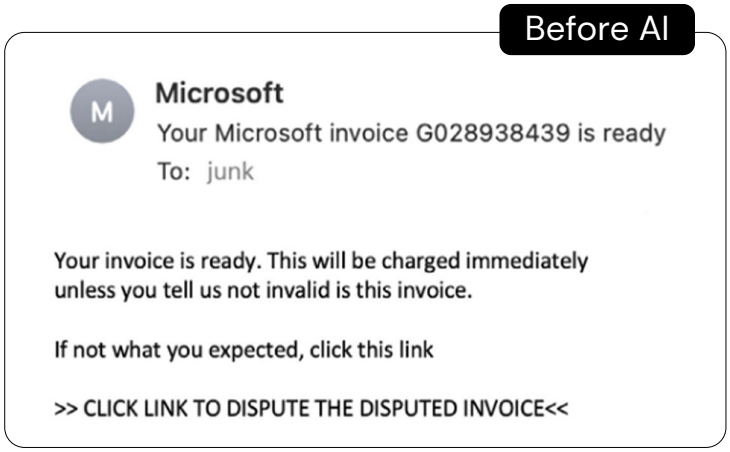
Ransomware is computer code, or malware, that is deployed across a network with the intent to disable systems. Heightened IT security and hardened servers have shifted hackers into a new and more effective means of delivering a ransomware payload—customized phishing emails enhanced by artificial intelligence. Cybercriminals can use the personal information of bank employees or executives, which are readily available online, to craft personalized phishing emails targeting other staff. One click on a link in that email, and that organization's systems are compromised.

"Our employees wouldn't fall for that."

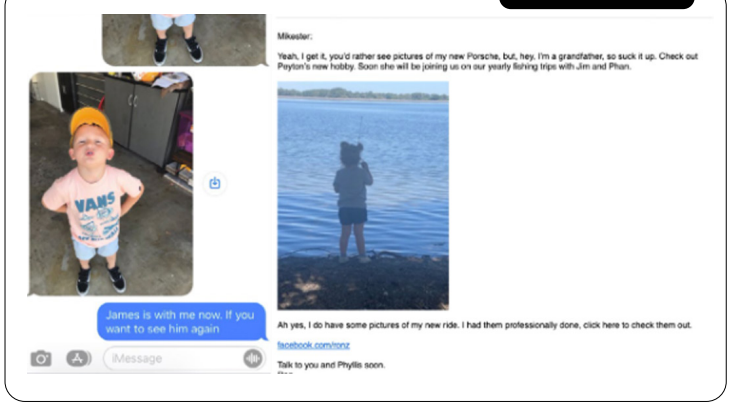
Don't be too sure. Hackers have come a long way from the obvious scams of ten years ago. Today's criminals are combining the adaptability of artificial intelligence with the copious amounts of personal data freely available on the internet to tailor amazingly personalized and effective emails.

Instead of a one-size-fits-all email, hackers now harvest the emails of the organizations they want to attack, identify key individuals, and automatically write scam emails that incorporate the recipient's name, address, family members, hobbies, mobile number, and even photos and videos in a way not possible even just two years ago.

Before AI



After AI



Emails with this level of authentic details are difficult to spot, even for the most careful and well-trained employees.

Since many phishing emails are now entry points for ransomware, a cybersecurity awareness and education program is still one of the most effective steps a company can take. Make sure all personnel understand how to spot phishing, and maintain the habit of smart password management. And if someone slips and clicks on something hazardous, stress the importance of reporting it immediately.

Training alone isn't enough, however. Preventing phishing attacks from targeting your employees is becoming equally as important. Hackers may be smart, but they are also lazy. In searching for their next victim, if they find a trove of available content on one organization and much less on another, they will opt for the easier target. The one with plenty of exposed information they can exploit. The objective is to be the organization with insufficient accessible PII for an effective phishing attempt.

Safety precautions offline

The routines and habits of executives can also be exploited in potential attacks. Taking the necessary precautions may seem burdensome, but they are essential given the risks. And fortunately, routines are usually simple to alter.

The journey to and from work is one obvious example. Most of us take the same route every day, which exposes a potential vulnerability. Parking garages have become more secure and may require a code for entry and exit. But for those with a clear line of sight, the time a car is stopped while entering an access code is more than enough to reach their target.

In open parking areas without security or surveillance, an Apple tag or GPS tracking device can be used to gain valuable information on where someone lives and the places they routinely visit. These devices may be undetectable once installed in wheel wells or on a vehicle's undercarriage. And as the prices of these devices continue to drop, their usage will likely become more commonplace.

Websites such as WikiHow provide illustrated directions on how to find and remove these trackers. Some government agencies have also partnered with local law enforcement to conduct periodic searches.

Access to one's car also means access to the contents of the glove compartment, where most of us keep our vehicle registration and insurance information. These documents may also provide information about where an executive lives. A more secure alternative is to keep an encrypted picture of your registration and insurance card on your phone.

Given how home security gates and even garage door remotes can be hacked, it seems there is no limit to how the technology we rely on for convenience can be weaponized in the wrong hands.

Fear of detection might dissuade some potential assailants from approaching a property, but once they have the target's address, there are other methods for carrying out an incursion. Starting with the US mail.

Packages sent to an organization may be screened. Those sent to a residence are not. Precautions should be taken, especially during and after times when an organization is in the headlines. If an unexpected package arrives that appears suspicious, such as one carrying no return address, treat it with care—and share that mindset with family members who may approach it first. A call to local authorities for help may seem like an extreme step, but in circumstances of heightened risk, it's the best decision.

A mail-forwarding service can mitigate this threat, and a post office box would prevent home addresses from being exposed. However, some mail-forwarding companies will sell the personal information of their customers, so inquire about this before signing up. Also, be aware that getting a post office box requires providing a valid ID and home address (not just at the post office but also at private businesses such as UPS Stores). That content can be acquired through a Freedom of Information Act request.

Conclusion

As financial services executives and organizations grapple with escalating threats, the risk of personal attacks, and the rapidly growing risk of costly ransomware attacks, forward-thinking organizations are exploring both preventative and reactive measures.

Personal information is the gateway that enables many forms of online and physical attacks. Since 2011, Ironwall by Incogni has been removing personal information from anywhere it can be located with a search engine, preventing it from appearing online, and providing support to professionals under threat.

Once an aggrieved individual already has your home address, help may arrive too late. Only with a service that removes your personal information from everywhere it appears on the searchable web are you fully protected.

Referenced

1. Cybersecurity Dive. “Spearphishing Remote Access Campaign Targets CFOs and Finance Executives.” Cybersecurity Dive, September 13, 2023. https://www.cybersecuritydive.com/news/spearphishing-remote-access-campaign-cfos-finance-executives-trellix/749192/.

2. BankDirector. “Cyberattacks Target Directors, Executives.” BankDirector, April 15, 2024. https://www.bankdirector.com/article/cyberattacks-target-directors-executives/.

3. Resecurity Blog. “ICBC Ransomware Attack Strikes at the Heart of the Global Financial Order; LockBit on a Roll.” Resecurity Blog, October 25, 2023. https://www.resecurity.com/blog/article/icbc-ransomware-attack-strikes-at-the-heart-of-the-global-financial-order-lockbit-on-a-roll#:~:text=LockBit%20ransomware%20group%20claimed%20responsibility,%2426%20trillion%20U.S.%20Treasury%20market.

4. eFraud Prevention. “Understanding the Prudential Data Breach.” eFraud Prevention, accessed January 15, 2026. https://efraudprevention.com/security/Understanding_the_Prudential_Data_Breach.html#:~:text=Overview%20of%20the%20Breach,updated%20to%20over%202.5%20million.

5. Technijian. “Fidelity National Financial Data Breach: Essential Insights and Protective Measures.” Technijian, December 2023. https://technijian.com/cyber-security/data-breach/fidelity-national-financial-data-breach-essential-insights-and-protective-measures/#:~:text=In%20November%202023%2C%20Fidelity%20National,of%20approximately%201.3%20million%20customers.

6. Meyersohn, Nathaniel, and Elisabeth Buchwald. “Companies Step Up Security in Wake of UnitedHealthcare CEO Killing.” CNN, December 7, 2024. https://www.cnn.com/2024/12/11/business/ceo-shooting-unitedhealth-security.

7. DataPods. “What Your Data Is Actually Worth.” DataPods, accessed January 15, 2026. https://www.datapods.app/en-US/blog/what-your-data-is-actually-worth.