Executive summary | December 2024

Wipfli Real Estate Leaders Exchange

Host: Cory Bultinck, Partner and National Real Estate Leader | Wipfli
SME: Jeff Olejnik, CyberTech Practice Leader | Wipfli
Facilitator: Austin Evans | Profitable Ideas Exchange

WIPFLI

Introduction

The Q4 Wipfli real estate leaders exchange convened virtually, bringing together financial leaders from the real estate industry to discuss critical issues and share best practices.

The session, hosted by Cory Bultinck, partner and national real estate leader, and facilitated by Austin Evans of Profitable Ideas Exchange, focused on the increasingly important topic of cybersecurity. Jeff Olejnik, partner at Wipfli, provided insights, setting the stage for a robust discussion on the current landscape, real-world incidents and effective risk management strategies.

"Cybersecurity is no longer just an IT issue; it's a business imperative that requires attention at the highest levels of an organization."

— Cory Bultinck

© Wipfli LLP | December 2024

Cybersecurity risks and trends

Jeff Olejnik began by outlining the current cybersecurity landscape, emphasizing the growing prevalence of cyberthreats.

He noted that while the real estate industry may not be as heavily regulated as financial institutions, it remains highly vulnerable to cyberattacks. The economic impact of cybercrime is staggering, with an estimated annual cost of $8 trillion, making it the third-largest economy globally.

Olejnik highlighted the evolving nature of these threats, particularly with the rise of AI, which has led to more sophisticated and rapid cyberattacks. This evolution necessitates advanced defensive measures to protect against these increasingly complex threats.

"The rise of AI has transformed the cybersecurity landscape, making attacks more sophisticated and rapid. Organizations must evolve their defenses accordingly."

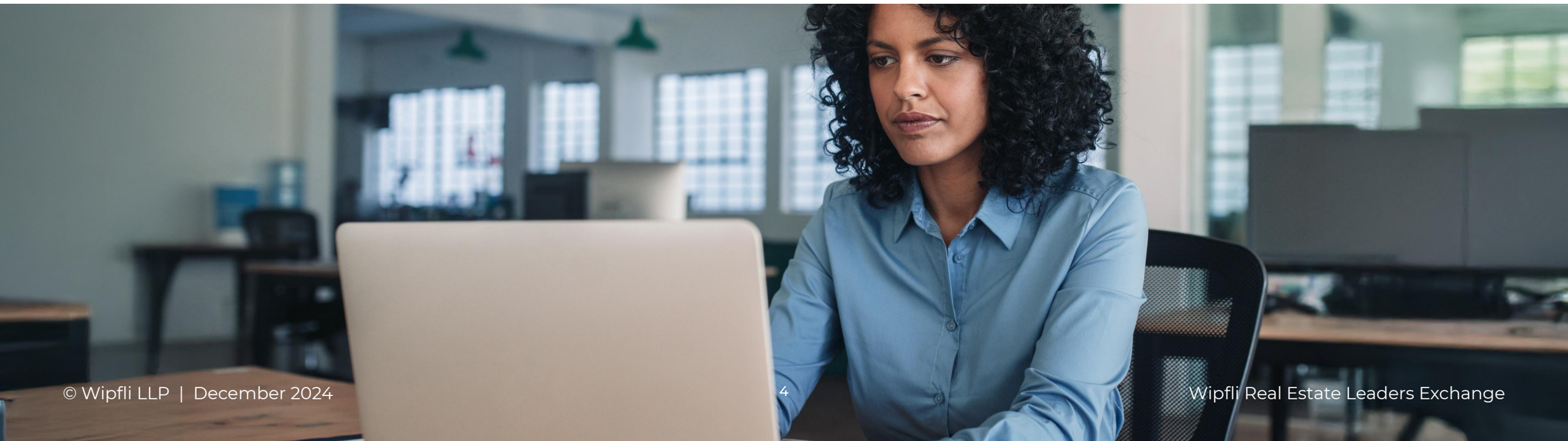
— Jeff Olejnik

Real-world incidents and lessons learned

The discussion then shifted to real-world incidents and lessons learned, with several executives sharing their recent experiences with cybersecurity breaches.

One member recounted a financial scam involving a compromised vendor email that resulted in a $150,000 loss. Despite following standard verification procedures, the scam succeeded due to the sophisticated methods employed by the attackers.

Their cybersecurity insurance covered a portion of the loss, but the claim process was challenging and required extensive back-and-forth with the insurance company. Ultimately, they recovered most of the funds, with their primary insurance covering half and their insurance broker covering the remaining amount due to an oversight in the policy setup.



This incident underscored the importance of verifying email communications, implementing multi-layered security protocols and thoroughly reviewing insurance policies to help ensure all entities are appropriately covered.

Another executive shared a similar phishing attempt that was thwarted thanks to vigilant internal controls. This case highlighted the critical role of employee training in recognizing and responding to phishing attempts. Regular training sessions and simulated phishing exercises can significantly enhance an organization's ability to detect and prevent such attacks.

Additionally, the authentication of wire transfers was emphasized, with members discussing the necessity of dual authorization and thorough verification processes to prevent unauthorized transactions. This includes not only verifying the recipient's information but also confirming the transaction details through a secondary communication channel, such as a phone call to a known contact.

"Our experience with the financial scam was a wake-up call. It highlighted the need for rigorous verification processes and comprehensive insurance coverage."

Insurance and risk management

Insurance and risk management emerged as a critical theme, with participants discussing the challenges and complexities of cybersecurity insurance.

Many executives expressed frustration with coverage gaps and difficulty navigating the claims process. Jeff Olejnik advised that thorough policy reviews are essential to understand what is covered, particularly regarding business interruption legal costs and breach investigations. He also recommended negotiating the inclusion of preferred vendors in insurance policies to avoid unexpected surprises during a breach.

InfraGard was mentioned as a valuable resource for enhancing cybersecurity measures and fostering collaboration between private and public sectors. InfraGard, a partnership between the FBI and members of the private sector, provides a platform for sharing information and best practices related to cybersecurity threats. By participating in InfraGard, organizations can gain access to timely intelligence and resources that can help them better prepare for and respond to cyberthreats.

Participants also discussed the importance of having a comprehensive incident response plan in place. This plan should outline steps to be taken in the event of a cyber incident, including roles and responsibilities, communication protocols and procedures for containing and mitigating the impact of the breach. Regularly testing and updating the incident response plan is crucial to ensure its effectiveness.

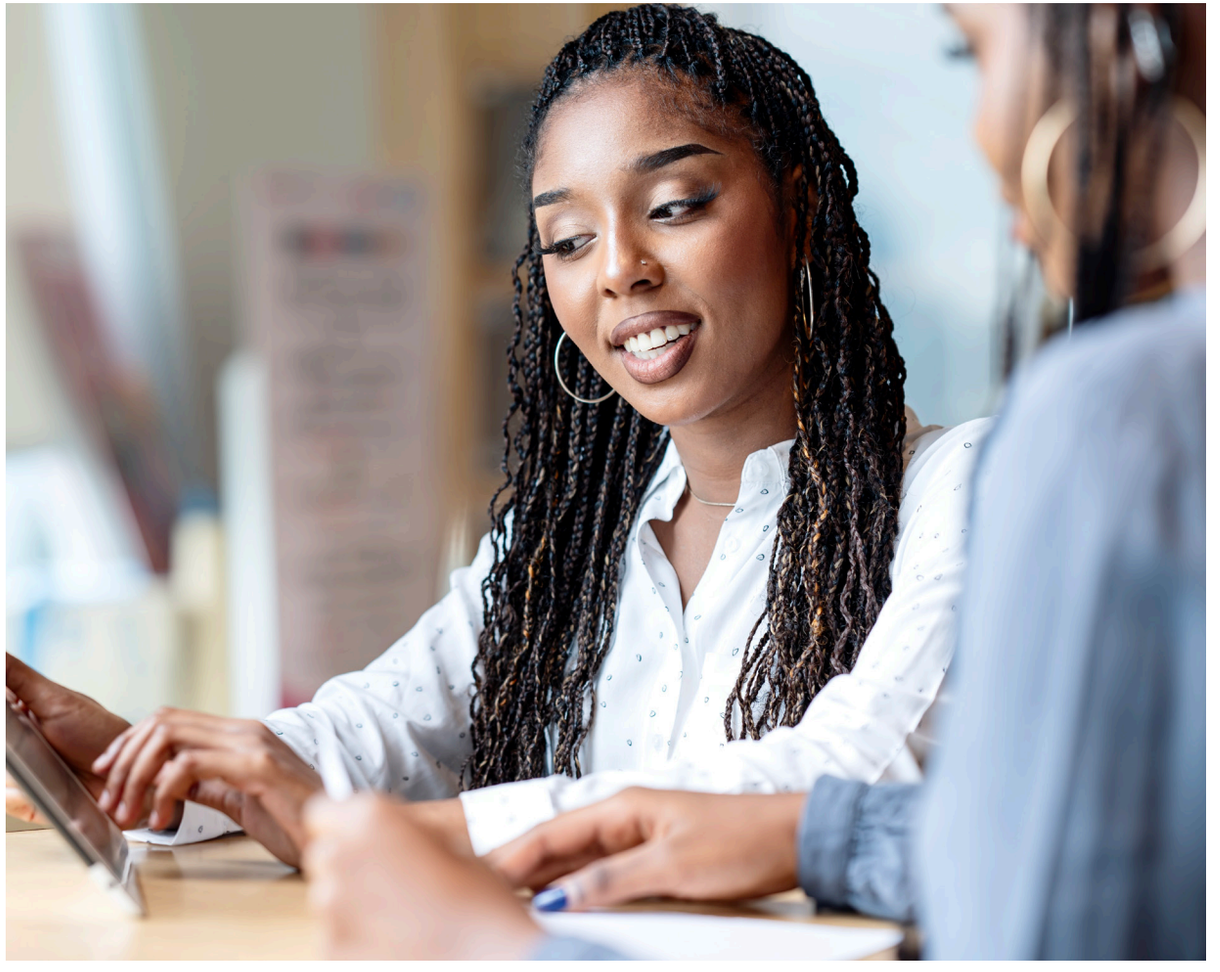
> *"Having insurance is crucial for protection, but we believe the best defense is educating our team."*

Technological solutions and best practices

Technological solutions and best practices were another focal point of the discussion.

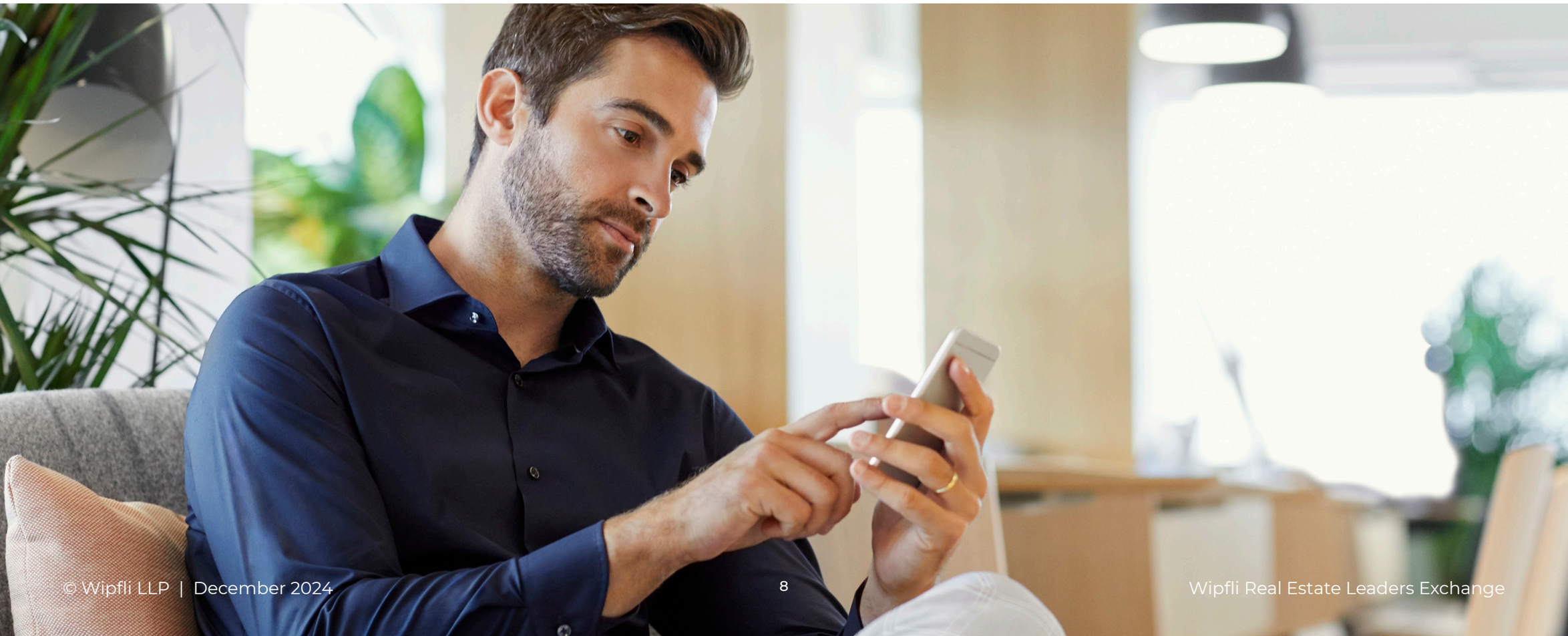
Executives highlighted the use of advanced cybersecurity tools such as DNS filtering, positive pay and dark web monitoring:

- DNS filtering helps prevent access to malicious websites by blocking requests to known harmful domains.
- Positive pay is a fraud prevention service that matches the details of checks presented for payment against a list of issued checks.
- Dark web monitoring involves scanning the dark web for compromised credentials and other sensitive information that may have been exposed in data breaches.



Jeff Olejnik demonstrated a password compromise assessment, revealing the importance of unique passwords and multi-factor authentication. During the demonstration, Olejnik showed how easily compromised passwords can be found on the dark web. He used a tool to scan for exposed credentials associated with the participants' domain names. The results were eye-opening, showing several instances where employee credentials had been compromised in previous data breaches.

Olejnik emphasized the need for employees to use unique passwords for different accounts and to change passwords regularly. He also highlighted the importance of implementing multi-factor authentication to add an extra layer of security.



Concerns around portal access for investors were also discussed, with a focus on ensuring that investor information remains secure and uncompromised. Executives emphasized the need for robust security measures to protect investor portals, including strong password policies, multi-factor authentication and regular security audits. Educating investors about cybersecurity best practices is also important to prevent unauthorized access to their accounts.

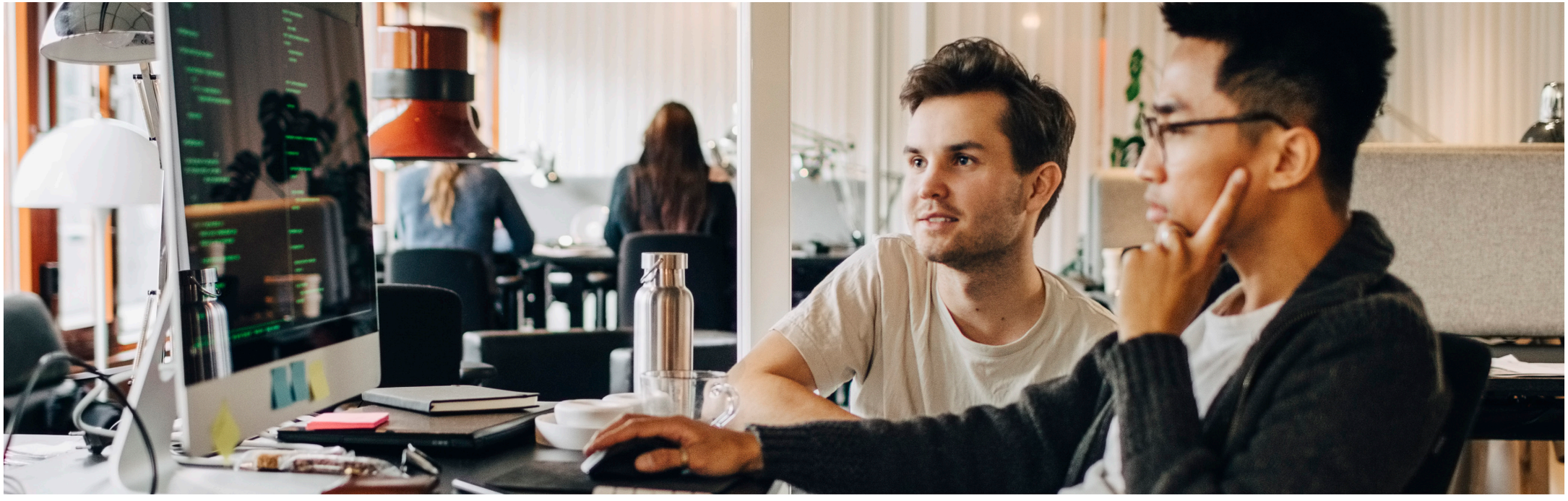
The conversation also touched on AI's dual role in both facilitating and combating cyberthreats. Participants agreed on the necessity of AI-driven security measures to quickly detect and respond to anomalies. AI can help identify patterns and behaviors indicative of a cyberattack, enabling faster and more effective responses.

"One of the things I'd recommend is instead of calling the number on the request for the change, figure out the appropriate telephone number to call. This helps ensure you're not contacting the attacker."

Future outlook and recommendations

The session concluded with a forward-looking perspective on cybersecurity. Executives emphasized the need for continuous improvement and adaptation to new threats. Regular updates to cybersecurity strategies and ongoing employee education were deemed crucial for maintaining robust defenses.

The importance of industry collaboration and sharing best practices was also underscored, with participants encouraged to leverage resources like password compromise assessments, InfraGard and other cybersecurity networks.



WIPFLI

wipfli.com/realestate