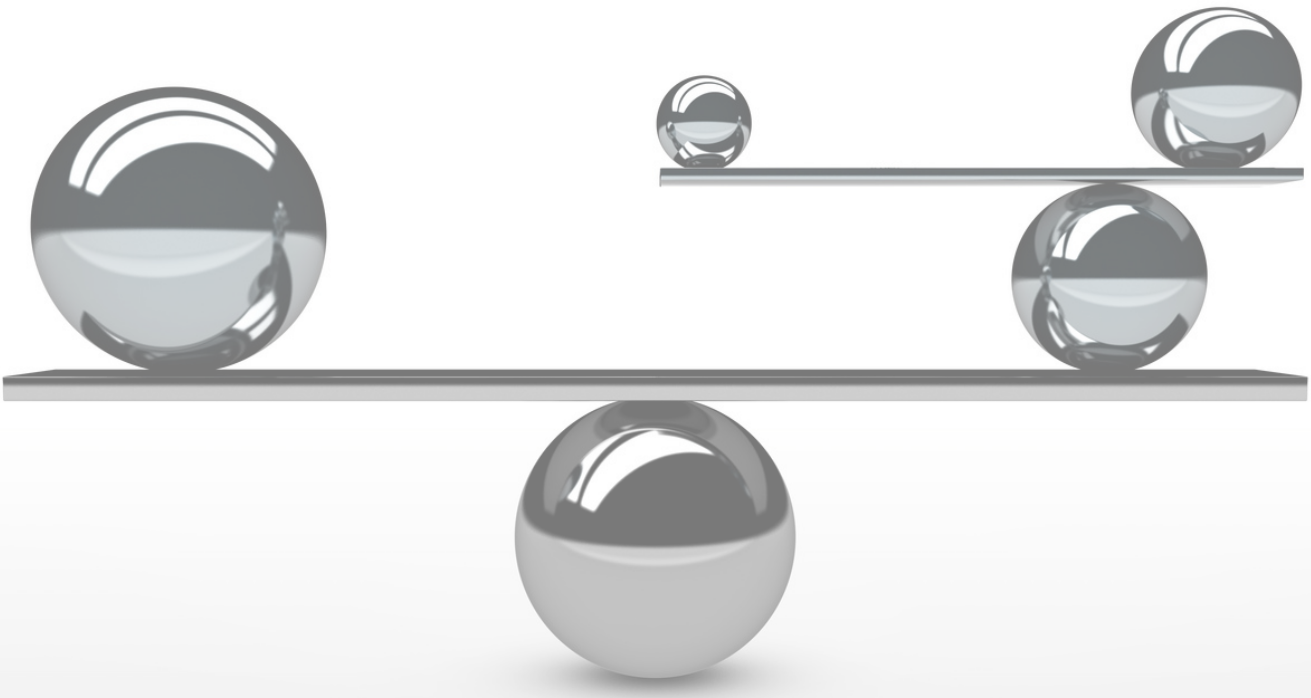
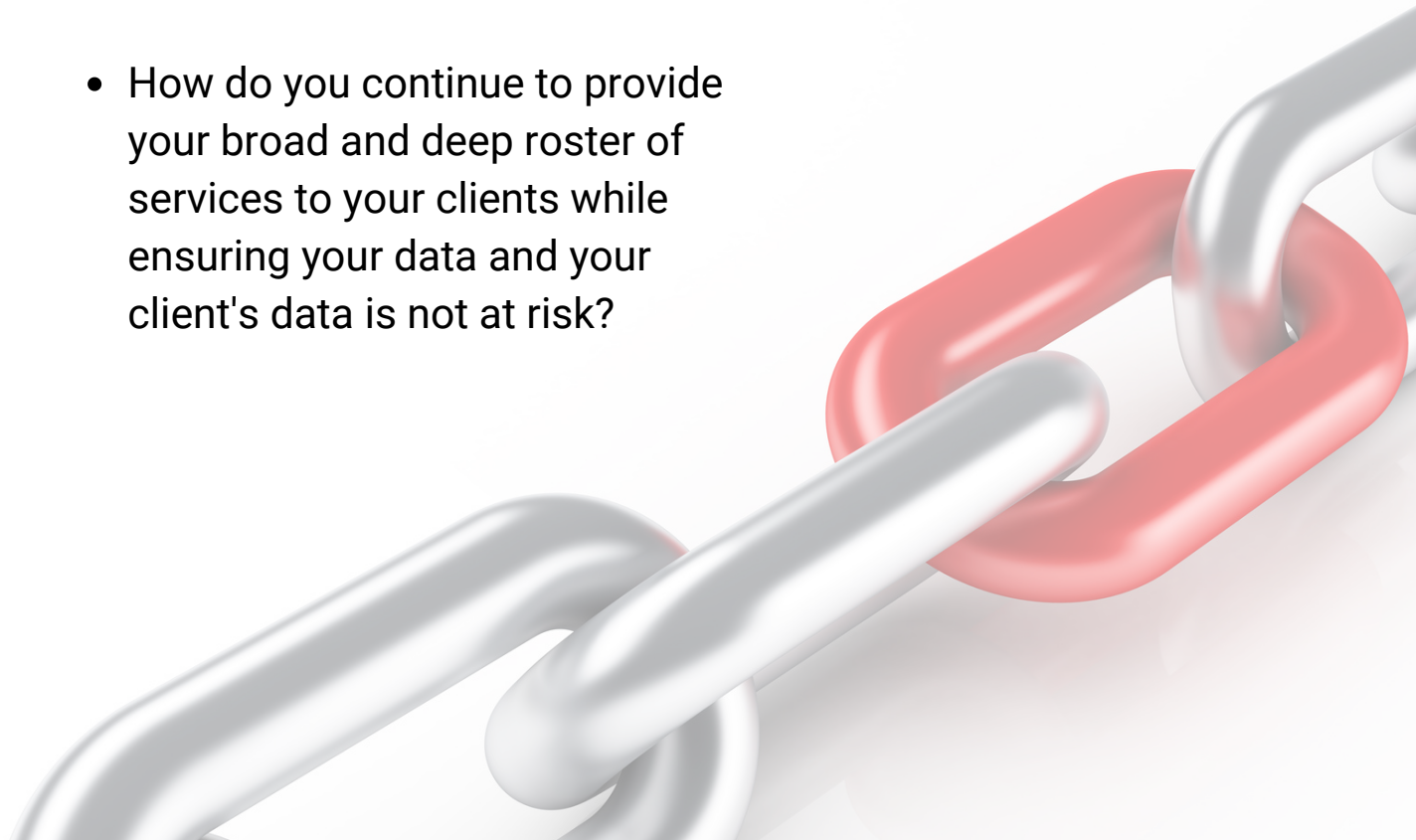
# TIMING IS EVERYTHING

*a case study in striking a new path*
*to a more secure future*



# When Early Risk Identification & Mitigation Proves Pivotal

- How do you integrate a newly acquired business into your systems while maintaining your rigorous security practices and standards?
- How do you find and mitigate areas of risk while ensuring the merger process is not interrupted?
- How do you continue to provide your broad and deep roster of services to your clients while ensuring your data and your client's data is not at risk?



# Meet Your Peer

**A Fortune-500 financial conglomerate with one major issue: how to safely and quickly integrate new acquisitions in a manner that does not put the business as a whole at risk.**

- With over $145 billion in assets, 5+ million customers worldwide, and over 18,000 employees, **FinCor** is an ever-growing business that strives to exceed customer expectations while providing secure and efficient financial services to all.

- From vehicle finance, to holistic private banking and investment services, to engaging in broker/dealer transactions for institutional investors, **FinCor** aims to be the bank of choice across markets in not only financial success but security as well.

- **FinCor** struggles with safely and effectively absorbing new acquisitions in a timely manner while maintaining alignment to their strategic and compliant level of cybersecurity.

- Early in the acquisition process it became clear that the acquired business, although compliant and secure on its own, was rarely as compliant or secure as **FinCor** in its holdings and practices.

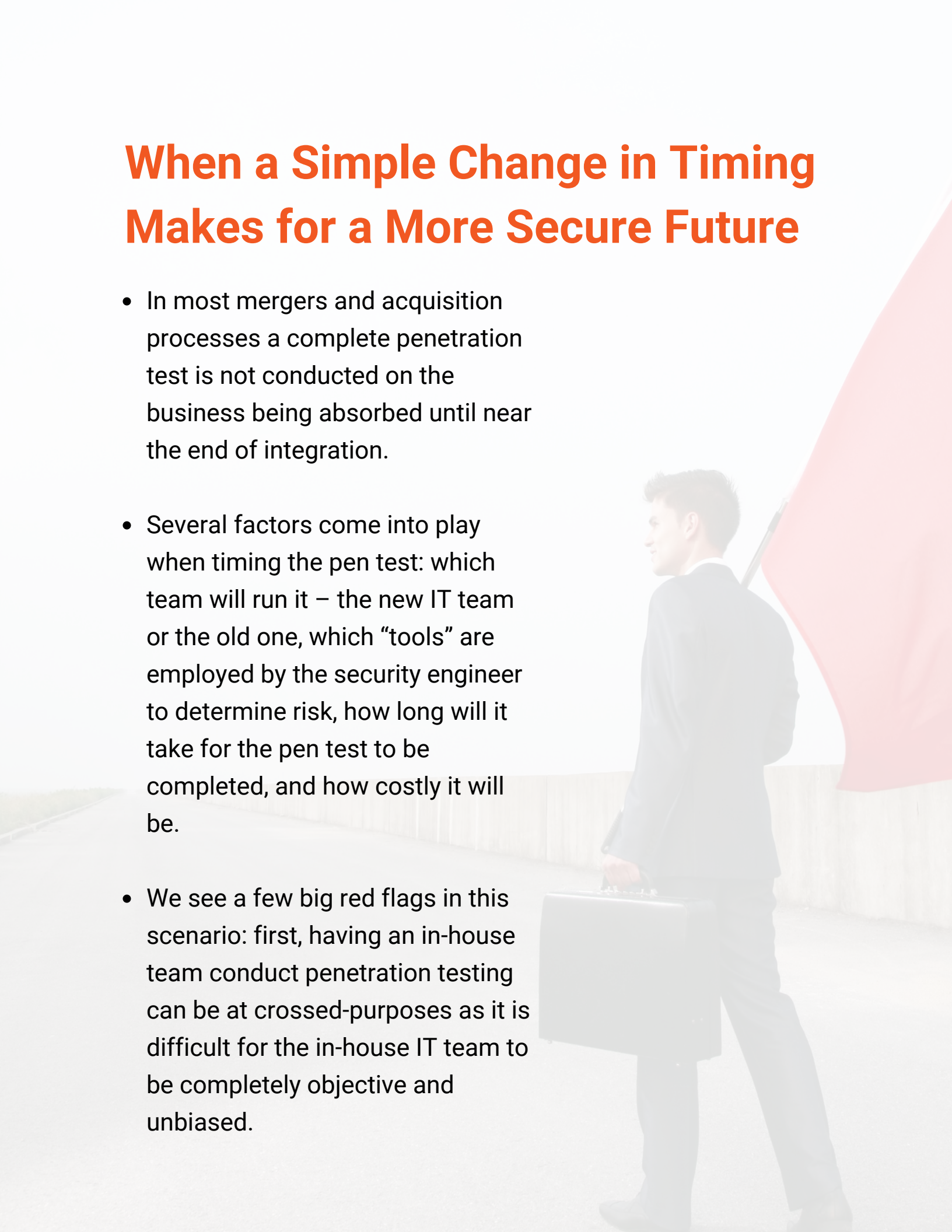
- The acquisition process would slow significantly when a seamless and quick integration was essential, risking client data, corporate assets, and privileged information.

# When a Simple Change in Timing Makes for a More Secure Future

- In most mergers and acquisition processes a complete penetration test is not conducted on the business being absorbed until near the end of integration.

- Several factors come into play when timing the pen test: which team will run it – the new IT team or the old one, which “tools” are employed by the security engineer to determine risk, how long will it take for the pen test to be completed, and how costly it will be.

- We see a few big red flags in this scenario: first, having an in-house team conduct penetration testing can be at crossed-purposes as it is difficult for the in-house IT team to be completely objective and unbiased.



- Second, the tools used to identify potential breach points are only as good as the tester’s ability to use them, and the tools themselves may not be effective enough.

- Finally, the traditional penetration test process often takes weeks to execute.

- If you consider all these things plus the time it takes for all three stakeholders to interpret the data then come to mutually satisfying solutions prior to implementation, this leads to a months-long time gap in protections across a corporation's infrastructure where cyber criminals can easily gain entry and wreak havoc – and in the case of an M&A may cause costly delays in closing.

# Results that Speak for Themselves

## Rapid Identification with SARA is Money in Your Bank

In **FinCor**'s situation we were able to find where the business being acquired had infrastructure weaknesses when integrated into the new parent company's highly rigorous cybersecurity standards.

We employed **SARA,** our Security And Risk Assessment tool, that "saw" across **FinCor**'s extensive network and business systems to alert them to several areas of pivotal risk that were immediately mitigated.

Our penetration test process also provided **FinCor** with a comprehensive list of breach points across their newly integrated network and a step-by-step plan on how to mitigate each hazard across functions.

**FinCor** was successful in identifying, addressing, and preventing each possible event leading to fewer risks and more secure infrastructure.

By providing **FinCor** with a comprehensive baseline assessment within seven days, we were able to illustrate the correlation between technical and governance controls.

Additionally, we were then able to route a roadmap to satisfy the regulation requirements for the next step of Building Blocks. This established better cyber hygiene in a cost effective and efficient manner with cost justification in the strategic cybersecurity management plan.

Going forward **FinCor** has elected to employ **SARA** much earlier on in the acquisition process, which will lead to better business opportunities and healthier integrations across the board.

**Are You Ready to Strike Your New Path to a More Secure Future?**

Contact us at info@netswitch.net

Netswitch™
Technology Management