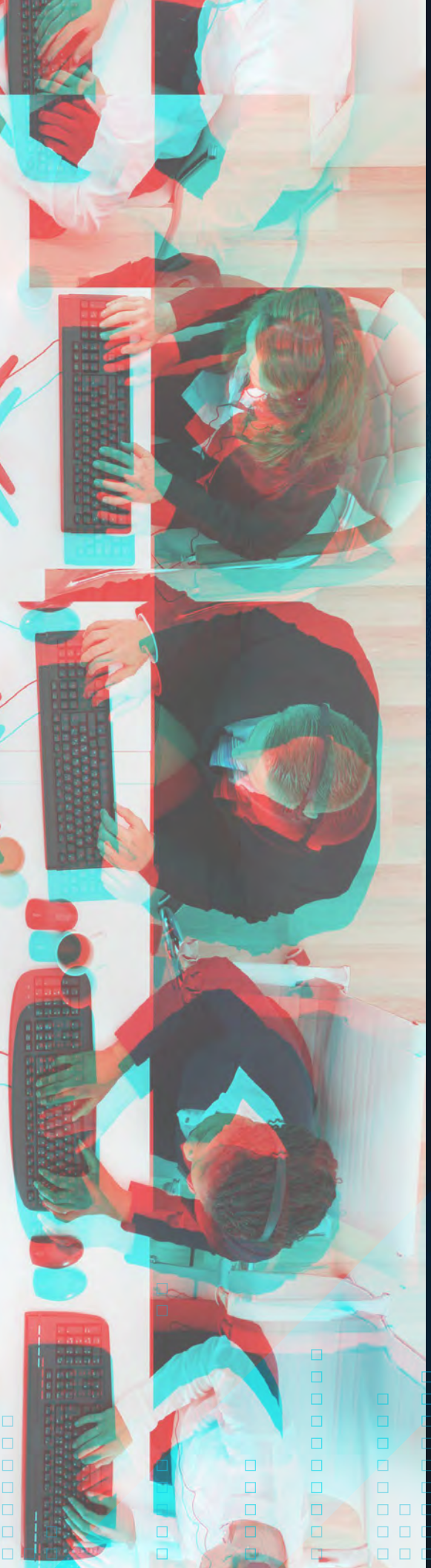

SAFEGUARD CYBER

FEATURING

FORRESTER®

BEYOND TRAINING:

Technical Controls to Stop Social Engineering

Q+A FEATURING

Joseph Blankenship

Security & Risk VP Research Director, Forrester

SAFEGUARD CYBER

From Lapsus$ to Oktapus, devastating recent breaches have used low-cost social engineering attacks across multiple channels, targeting employees across LinkedIn, WhatsApp, email, Slack, and more.

After two decades, it's time to move beyond just awareness training. Security teams need technical controls to detect and stop this persistent threat. In this Q&A with guest speaker Forrester's Joe Blankenship, we continue the conversation from our Expert Panel discussion, "Beyond Training: Technical Controls to Stop Social Engineering."

Recent Risk and Breach Data

45%
of business communication is now in digital channels outside of email[1]

82%
of breaches in the last year involved an element to exploit a human vulnerability[2]

92%
of social engineering attacks achieve infiltration[3]

[1] Business Communications Report 2022 [2]Verizon, 2022 Data Breach Investigations Report [3]Verizon, 2021 Data Breach Investigations Report

SafeGuard Webinar Guest Speaker

Joseph Blankenship

VP, Research Director

Joseph supports security and risk (S&R) professionals, helping clients develop security strategies and make informed decisions to protect against cyberattacks. As a research director for S&R, he leads the analyst team researching security leadership, the role of the CISO, infrastructure and operations, detection and response, and Forrester's Zero Trust model of information security. His research focuses on insider threat prevention, security operations, and security management.

Joseph has presented at industry events, been quoted in the media, and written on a variety of security topics.

Q+A

With Joseph Blankenship

SGC Q: Work from anywhere is here to stay. How enterprise employees communicate has evolved to using a variety of cloud communication channels to get the job done.

How do cloud collaboration, social media, and mobile messaging applications impact the way security teams protect enterprise data and people?

WATCH NOW

BEYOND TRAINING: Technical Controls to Stop Social Engineering

JB A: Users are bombarded with messages and requests daily, and it's easy for them to become distracted or make the wrong decision in the moment. It's not sufficient to leave data security to users. They need security controls that protect them from accidentally sharing data outside of policy or responding to social engineering techniques.

Security teams have not widely deployed controls for collaboration, messaging, and social media like they have for enterprise applications like email. Protection has to evolve to include other means of communication and data sharing to reduce risk.

Q+A

With Joseph Blankenship

SGC Q: Attacker techniques and tactics are becoming more sophisticated even as workforce employees share more personal and enterprise information on channels like LinkedIn and WhatsApp.

What's the risk versus reward of the security team enabling more modern business communication channels?

WATCH NOW

BEYOND TRAINING: Technical Controls to Stop Social Engineering

JB A: Work From Anywhere increased dependence on messaging and collaboration tools – with internal and external users. While this does empower our ability to communicate more effectively in real time (since we can't pop over to someone's desk anymore), it did introduce risk. Users share all kind of sensitive data in these tools – intellectual property, PII, PHI, and sensitive internal correspondence. Opening collaboration tools up externally introduces all the risks we already experience with email – phishing, accidental data loss, and account compromise.

This means we have to balance the benefit of real-time communication with contractors, vendors, and partners who may be external to the organization with the risk that the collaboration and communication tools may be misused. If users inherently trust the tool, they become more susceptible to attacks like social engineering since they aren't necessarily looking out for attackers or malicious behavior in those channels.

Q+A

With Joseph Blankenship

SGC Q: Lapsus$ stealing source code, Twilio compromised, Axie Infinity robbed of half a billion dollars. It wasn't zero days or custom exploits. So many headline-making breaches in 2022 came down to social engineering employees.

Can you comment on this trend and provide insight into how security teams can and should calibrate their strategies to mitigate these risks?

WATCH NOW

BEYOND TRAINING: Technical Controls to Stop Social Engineering

JB A: Social engineering is arguably the oldest hacking technique. It predates the internet and even computers. What's changed is that the connectivity made it easier for attackers to reach a wider number of victims, and the victims rarely ever meet the attackers in the real world. Social engineering works because it preys on users' emotions and desire to be helpful. Attackers, just like old-school conmen, gain their victims' trust or bully them into taking an action without carefully considering it.

Security strategies have to evolve so that they don't rely only on the user making the right decision in the moment. They need to include real-time education and the ability to stop users from taking risky actions.

Q+A

With Joseph Blankenship

SGC Q: **Is security training enough to combat social engineering?**

If not, how does it need to evolve, and what is the correct balance between controls and security awareness training to defend against social engineering?

WATCH NOW

BEYOND TRAINING: Technical Controls to Stop Social Engineering

JB A: Awareness of social engineering and social engineering techniques alone has not proven effective. Users may forget what they've learned or think that the person targeting them is trustworthy. That means security teams have to design interventions that keep users from giving up sensitive information (especially account credentials), clicking on links, or downloading files. Those controls have to work in the moment to stop users from falling victim to attacks.

At the same time, the controls can't introduce so much friction as to constantly interrupt work or encourage users to circumvent the controls. Controls should be risk-based, so they are only disrupting users that exhibit risky behaviors and are taking risky actions.

SAFEGUARD CYBER

ADDITIONAL RESOURCES:

How to Assess Risk in Your Business Communications [Checklist]

Sample Risk Report: Measuring Communications Risk

SafeGuard Cyber is the most comprehensive integrated cloud communications security platform to address cybersecurity threats and compliance risks across today's modern cloud workplace. Through a combination of unified visibility, contextual analysis, and multi-channel investigations and detections, SafeGuard Cyber mitigates risks in email, mobile and web messaging apps, collaboration apps, and social media.

Powered by Natural Language Understanding (NLU) and patented Social Engineering Detection technologies, the SafeGuard Cyber platform reduces investigation and detection hours to minutes while providing resolution of social engineering and language-based attacks in over 50 languages.

Learn More