REPRINT

R&C risk & compliance

ENHANCING AND COMPLEMENTING THE EFFECTIVENESS OF MULTIFACTOR AUTHENTICATION

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
JAN-MAR 2022 ISSUE

www.riskandcompliancemagazine.com

Visit the website to request
a free copy of the full e-magazine

CRA Charles River Associates

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

PERSPECTIVES

ENHANCING AND COMPLEMENTING THE EFFECTIVENESS OF MULTIFACTOR AUTHENTICATION

BY **KRISTOFER SWANSON, BILL HARDIN AND MATTHEW AHREN**
> CHARLES RIVER ASSOCIATES

Based on our experience, we have witnessed first-hand the shock that many leadership teams and boards experience after deploying multifactor authentication (MFA) tools, yet subsequently sustain a cyber breach.

What is the promise and purpose of MFA? In brief, it is an approach to information security that requires a user to present two or more credentials, to reasonably establish that they are who they purport to be, before being granted access to corporate email accounts, devices, databases, systems or assets. For example, a user might be asked to type in something that she knows, such as a pre-established password, and then asked to confirm that she is in physical possession of a preidentified device, such as her mobile phone, by entering a code that has been generated within the prior 30 seconds by an application on the phone.

So how can a cyber incident still be possible? After all, MFA is lauded as an important tool for reducing the risk from hackers. In fact, it is increasingly required by insurance carriers as a prerequisite to writing a cyber insurance policy, recognising that it can be as important of a risk mitigation tool as wearing a seatbelt in a car.

However, while the deployment of MFA can reduce the risk of a cyber breach, the mere act of deploying MFA does not eliminate such risk. In tracking hundreds of crime syndicates, we have observed that motivated threat actors frequently identify ways to bypass less sophisticated implementations or incomplete deployments of MFA, and have successfully exploited other security vulnerabilities, to gain unauthorised access to corporate systems.

On the other hand, we have also observed that the companies with the strongest defences typically use a layered approach to information security, leveraging MFA as an important element of their defence stack, while layering on other defences as well.

Below we outline practical, tactical steps to enhance the efficacy of a company's MFA deployment, and to strengthen adjacent layers in its information security environment.

Review key applications and determine which ones can be MFA-enabled. By risk-ranking the applications, organisations can make risk-based decisions on how to reduce opportunities to gain access to the network.

Determine which MFA tool is the proper fit for the organisation. There are many MFA tools in the

marketplace. Employing a formal software selection methodology and confirming the fit is critical to achieving the business case objectives.

Once MFA has been deployed to an organisation, use a secure authenticator app instead of text-message or email-based MFA. This reduces the risk of account exploitation. These apps typically generate random, one-time-use passwords every 30 seconds or so, on both the user's phone and on the company's server. If the user enters a password within the specified time window which matches what the server expects to see, then one authentication requirement has been achieved.

"While the deployment of MFA can reduce the risk of a cyber breach, the mere act of deploying MFA does not eliminate such risk."

Make MFA a standard job function for the organisation once the organisation buys in. Recognising that the first line of defence for any organisation is its employees, incentive structures can be developed to reward those who follow the process, while other tools can be employed to identify, educate and hold accountable those who try to bypass the process.

Control and monitor MFA disablement. Some MFA services allow for 'bypass' configurations to be enabled for some or all MFA tokens, thereby causing MFA to be disabled. The ability to turn off MFA should be carefully limited and controlled, and notifications should be generated and monitored whenever such activity occurs.

Implement a zero-trust security model. This creates an additional layer of security. Zero trust is an information security approach that works to eliminate 'trust' as an operating principle, and instead requires verification from all devices and users endeavouring to access any corporate systems. In parallel, access is further restricted so that even verified users can access only those systems, websites and files necessary to perform their job functions.

Transaction due diligence. When performing preacquisition due diligence on targets, gaining an understanding of their layered defences and whether and how they use MFA is critical. Once the transaction is complete, validating that a common MFA platform has been deployed across the organisation will assist the information security

team with proper monitoring and protection. Timely post-acquisition due diligence will help to confirm or refine the preliminary integration plan.

Remove legacy systems. Legacy systems often have inherently poor security or risky features, such as remote access, which can create unacceptable levels of information security risk. By eliminating such systems, companies can further reduce the attack surface of their software environment, making it more difficult for crime syndicates to discover and exploit vulnerabilities and reducing the burden on existing information technology and security teams.

Patch internal and internet-facing applications and operating systems in a timely manner. Software bugs are often discovered in the days, weeks or months after deployment. Some of these bugs can be exploited to compromise security. Accordingly, a company can be at particular risk during the period between when such exploitable vulnerabilities are more generally known, and when the developer creates and distributes patches to remediate them. Any delays in deploying said patches could potentially put the organisation at significant, incremental risk.

Monitor information security risk from vendors and business partners. In addition to conducting initial information security due diligence on potential vendors and business partners, consider designing and deploying a risk-based approach to monitoring the ongoing – and ever-changing – risks associated with the underlying business relationships, including requiring them to use MFA, where appropriate. R&C

Kristofer Swanson
Vice President & Forensic Services Practice Leader
Charles River Associates
T: +1 (312) 619 3313
E: kswanson@crai.com

Bill Hardin
Vice President
Charles River Associates
T: +1 (312) 619 3309
E: bhardin@crai.com

Matthew Ahrens
Principal
Charles River Associates
T: +1 (202) 662 7835
E: mahrens@crai.com