FEBRUARY NEWSLETTER

RWK IT SERVICES

Vol. 3 Ed. 6 | February 2023

Best Practices for Building Security Resilience for a Hybrid Workforce

Common Challenges We Encounter

Only 37% of organizations responding to a recent Cisco survey said they're confident they can remain resilient in the event of a worst-case security incident. That's not surprising, given the rapidly increasing volume of endpoints distributed across complex IT architectures.

Remember to focus on the basic things you can do at your company to build security resiliency.

1. The use of Passwordless Technology

If you have not already done so, get multifactor authentication (MFA) in place. It is the only way to truly know that someone is logging on as you and which you can prevent. MFA is a form of password less technology.

Adopt passwordless technologies for access to everything, not just email. Passwordless technologies verify identity using biometrics, security keys, or mobile apps. These authentication methods are safer than relying on passwords, which are easily compromised. Passwordless solutions also have the benefit of reducing help-desk tickets among users who've lost or forgotten their passwords because the passwords remain constant or are forced to change less frequently.

The number of MFA authentications has risen by 38% in the past year, according to the 2022 Cisco Duo Trusted Access Report. This is good news.

Your IT department must also monitor and audit passwordless technologies for usage and 100% compliance. This may sound odd, but it happens. A frustrated end-user or executive may has to temporarily halt the use of MFA in the heat of the battle and IT forgets to circle back and re-enable it.

2. A Zero-Trust Security Framework for Data Access

Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.

Zero Trust assumes that there is no traditional network edge. This is palpable for many end users today as many now access their data files from Office 365 libraries or G-Suite docs.

Traditional security is based on location, which was fine in the past when we worked behind a corporate firewall with a locked down network. But it doesn't offer the best security considering today's distributed workforces and the movement of applications across clouds, on-premises data centers, and the edge.

At RWK, and especially through our virtual Chief Security Officer practice, we align to the NIST 800-207 standard for Zero Trust.

Zero Trust seeks to address the following key principles based on the NIST guidelines:

- **Continuous verification.** Always verify access, all the time, for all resources. We do this for you.
- **Limit the "blast radius."** Minimize impact if an external or insider breach does occur. We help with Incident Response Plans, tabletop exercises and similar tools.
- **Automate context collection and response.** Incorporate behavioral data and get context from the entire IT stack (identity, endpoint, workload, etc..) for the most accurate response. We put controls and configurations in place to handle this.

3. Simplify Your Use of Hybrid Cloud Environments

You might be surprised how many new Partners who engage with our Managed IT Service who have 2 or more data repositories and mission critical data storage environments! MS 365, Google Docs, Sharefile, Dropbox, and more. This is bad. It takes time to remediate this and reduce your threat attack-surfaces.

continued on page 2

continued from page 1

There is little difference in security resilience between organizations whose IT infrastructures are predominately in the cloud versus those primarily on-premises, according to the recent Cisco Security Outcomes Report, Volume 3.

However, it's the in-between where resilience drops. For example, those businesses that are in the early stages of a hybrid cloud model score 14% lower than organizations whose infrastructures are mostly on-prem.

The key is to simplify security management of hybrid cloud environments.

The bottom line:
Today's distributed workforces and maturing hybrid IT environments, coupled with constantly evolving cyber threats, present new security risks. These best practices can bolster your organization's ability to address these risks and become more resilient.

If you'd like to learn more about our Security Officer Service, call Jeff Reiter at (312) 550-3883.

This begins with a Level 1 Risk Assessment that takes 26 minutes to complete, along with an inobtrusive Penetration Test on three computers. It's like going to your dentist for that annual visit and X-rays. A Pen Test looks for areas of risk that are not visible to the naked eye, or to business people.

A follow-up readout meeting will give you answers about your organization to the three best practices we have outlined above.

Employee Spotlight

Rob

Joined RWK - 2022

What is your favorite Valentine's Day treat?
Valentine's Reese's Peanut Butter Hearts. The ratio of peanut butter to chocolate is perfect!

If you could pick up a new skill in an instant, what would it be and why?
Piano. It's a beautiful instrument and I've always wished I could play

What 3 apps on your phone are your favorite?
I'm a big gamer, so Marvel Snap, Fairway Solitaire, and Flappy Bird!

Excluding IT, if you could have any other career what would it be?
I'd be a baseball player. With the exception of the first 4 years of life and 2 years after college, I've played baseball my entire life.

What is your favorite rom-com movie?
Kate and Leopold or The Proposal, those are tied for me.

What is your favorite thing about RWK?
It's an environment that really fosters both personal and professional growth. I feel like my ideas are both heard and considered, which isn't always the case when you are the new person in town.

Other RWK News

Existing Partners: Want to earn a credit on your monthly service? **Ask us about our referral program!**

Are you in need of a laptop for home or secondary use? We have good, refurbished laptops in stock for purchase.

Do you have 2 monitors and want more desk space? We have pre-owned monitor mounts that just may be the ticket for you.

Contact Kelly Paroubek or Jeff Reiter for details!

Team Celebrations

Happy Birthday
Fadi
2/10