

From The Corner Office

Happy New Year! We hope your 2022 has started in a positive light, and as always, we are pleased to deliver our latest newsletter to you, filled with insights and expertise from the Enterprise Iron Team.

This year marks a major milestone for our company. In July, Enterprise Iron turns 20! We are humbled to have served countless clients over the past two decades, working in partnership with incredible employees and delivery partners.

The pandemic has been tough on many, both personally and in business, but John and I are as committed as ever to continue supporting our team and our clients and excelling through any challenges that our employees, clients, and the world may encounter. We are cautiously optimistic that there will be light at the end of the Covid tunnel in 2022.

In this issue, we feature Denise Gumlak's analysis of the growing emphasis on Financial Wellness, more on Technology Modernization from our resident Agile expert, Mark Kalafsky, and the conclusion of my two-part series on BCP/DR planning, highlighting the prevalence of ransomware in the world today.

Questions? Comments? I'd love to hear from you: jrc@enterpriseiron.com. We very much look forward to seeing you in-person this year as Conference Season commences; be sure to say hi!

All the best,

John R. Crocker
Co-Founder, EVP & CCO

UPCOMING EVENTS

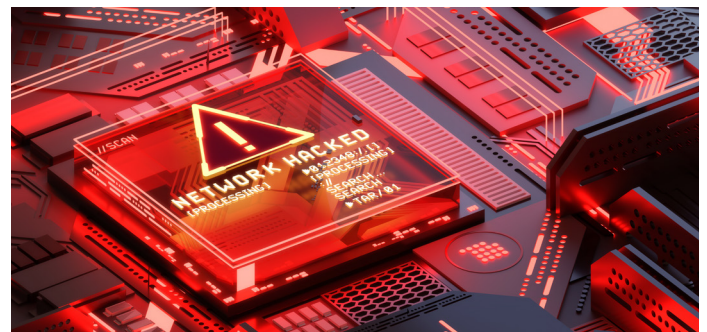
NASRA Winter Meeting | February 26th – 28th
NAPA 401(k) Summit | April 3rd – 5th
PSCA National Conference | April 28th – 29th

Updating Your Business Continuity & Disaster Recovery Plans: Part 2 of 2

By John Crocker, Co-Founder & Executive Vice President

In **Part 1**, we discussed an evolving BCP/DR planning approach, moving from annual testing and major updates only upon significant internal corporate changes or external events to “BCP/DR-as-a-Process.” Ongoing quarterly meetings with an intradepartmental team focused on discerning potential rapidly developing threats and proactively preparing for them.

The world is simply “moving faster.” Events emerge suddenly and develop rapidly. In Part 1, Covid was the example used. Virtually no one's BCP/DR Plans were applicable, despite the potential for a global pandemic being within the range of possibility. There are, however, additional threats currently circulating capable of causing substantial damage to companies, and we'll address the second in this article: ransomware.



Hacking has been around since the beginning of the internet. At first, it was mostly “script kiddies,” doing it just for the challenge. There was little to be gained, as it took several years for corporations to develop eCommerce sites and even longer for consumers to feel comfortable using them. As this developed, the first generation of criminal hackers emerged. It became possible to make a lot of money by cracking websites and networks that housed or processed financial transactions.

However, this has developed into something even more dangerous in the past decade or so. Disciplined groups

of highly trained criminal organizations use perpetually evolving tools and tactics. Perhaps worse, nation-state actors are now involved. Governments (with huge resources) actively target other governments or large corporations. Attacks on computer networks can do significant damage. Stealing highly protected Intellectual Property can be much more lucrative than hacking an eCommerce site. Cyberwarfare is, unfortunately, now part of 21st-century armaments.

The most recent trend is the most disturbing development to date: ransomware. This is a recently emergent threat. It has become increasingly possible to engage widely due to the advent of cryptocurrencies (demanding ransom in the form of suitcases full of cash or bearer bonds is not easy or practical). Crypto was the final piece of the puzzle.



A group of bad actors can gain control of a network using software tools (generally through phishing emails) and encrypt files, demand ransom, and get paid in Bitcoin without ever leaving the comfort of their homes. Many attacks occur in places where governments do little to find or prosecute perpetrators and may even support or be indifferent to what is happening.

In the past, targets were almost always financial, i.e., Financial Services firms, eCommerce sites, etc. – places where financial transactions are processed or where data is stored. These sites and networks generally have the highest levels of protection. Often with the most expensive security tools, some firms even have threat centers designated with monitoring activity.

With ransomware, it no longer matters whether a company does eCommerce, banking, or exposes any financial data at all. Thieves are going after multiple targets, from utilities to infrastructure, schools, and even hospitals. Even city governments and state agencies have been attacked.

In the modern corporation, IT security is often handled by a division of the IT Department, in conjunction with Risk Management to focus on threat mitigation.

We argue that this should also be in every company's BCP/DR plans. They have a different angle of vision and emphasis, not primarily looking at "how do we stop an attack," but rather "what happens if we are successfully attacked." A great deal of what goes into responding to an attack depends on variables including the nature of the network, policies (and security) around backing up data, ransomware tools used, and the criticality of the compromised data and systems.

Acting proactively can make it much easier to recover. The principle point here is that "scenario planning" into BCP/DR plans is critical because virtually any company or organization can become a target. Scenario planning is a series of "what if" exercises. What would be the Day 1, Week 1 steps? Could you restore systems from backups? Complete reboot or only partially? How quickly? What could you do right now to make recovery more possible?

If ransomware successfully infects and encrypts "xyz" (not just drives – it is possible to attack targets in the cloud), and you cannot restore from backups, would you pay the ransom? Federal law enforcement agencies universally advise against it but also understand that for some, there simply may not be a choice.

If you pay the ransom, how do you decide the legitimacy of the Bitcoin account you are sending money to? What if it is sent and the software to decrypt your files is just not sent? Once you pay in crypto, the money is (usually) unrecoverable. Even further, how would you run the decryption program sent by the attackers in the first place? Would you trust it on your network?

Bottom line, we are strongly encouraging clients to develop robust ransomware sections in their BCP/DR plans. Large companies in multiple industries that got hit over the past few years had virtually no preparation. Do you want to consider the questions above when you have the time and leisure to plan ahead or at the last moment after you've been hacked?

Case in point, one of the biggest occurred in 2021. On May 7, Colonial Pipeline, the largest petroleum pipeline company in the U.S., was successfully attacked (incidentally, it was through a single leaked password). Multiple systems were taken offline, and the pipeline was shut down for days. The company wrestled with how to handle the situation, and ultimately decided it had to pay the ransom (\$4.4 million in Bitcoin – though some was later recovered).

Organizations need to assess if they have a crisis response that's been well thought-out, otherwise, the entire senior management team will be scrambling through sleepless nights to figure out on the fly (and under the gun) what should be done about the threat of ransomware that is becoming common and is increasing in frequency at an alarming rate.

Covid and ransomware are two timely examples of companies being unprepared. Most BCP/DR plans were unequipped to deal with them, and firms must consider future scenarios. Contact Enterprise Iron if you'd like more detail about the "BCP/DR-as-a-Process" approach to keeping your firm prepared.



Financial Wellness is no longer a Buzzword

By Denise Gumlak, Managing Director of Retirement Strategy & Delivery

Despite their popularity today, 401(k) plans were created almost by accident and were never intended to replace pension plans. 401(k) plans started when Congress passed the Revenue Act of 1978, which included a provision added to the Internal Revenue Code – Section 401(k), allowing employees to avoid being taxed on deferred compensation. The law went into effect on January 1, 1980, and regulations were issued in November of 1981, which sanctioned the use of employee salary reduction as a source of retirement plan contributions.

1996 was a rather landmark year, where assets in 401(k) plans exceeded \$1 trillion, with more than 30 million active participants.¹ Fast forward to 2021, Americans held \$10.4 trillion in all employer-based DC retirement plans on September 30, 2021, of which \$7.3 trillion was held in 401(k) plans.²

The good news is people continue to save in their 401(k) for retirement. The not-so-good news is that many are not prepared for unexpected emergencies, as we've seen during the pandemic.

Most experts recommend keeping three to six months' worth of living expenses in an emergency fund. Still, according to a recent PWC Employee Financial Wellness Survey, more than one-third of full-time employed Millennials, Gen Xers, and Baby Boomers have less than \$1,000 saved to deal with unexpected expenses.³

Financial wellness is about more than just workers' wallets – stress over money and security directly impacts workers' emotional and physical well-being. That said, many organizations are taking steps to support their employees. Safe to say, financial wellness will continue to be a topic of interest in the retirement and wealth management space as we look to provide workers with a more holistic approach to financial well-being.

Some Rather Daunting Facts

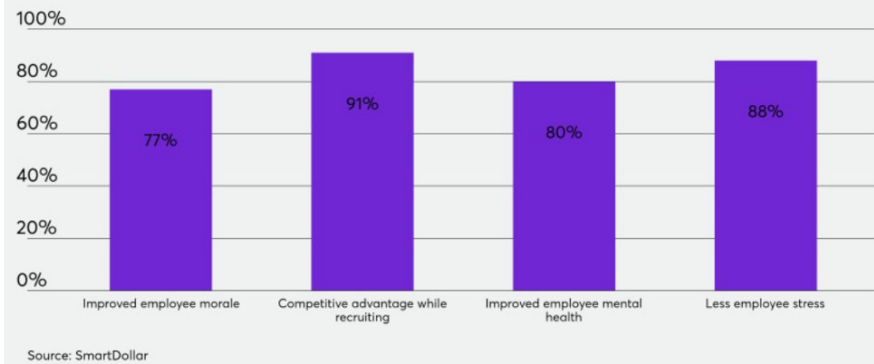
58% of consumers borrowed or withdrew funds from a 401(k) or individual retirement account (IRA) during the pandemic, according to Kiplinger’s Personal Finance magazine and wealth management company, Personal Capital.⁴ Additionally, per the 2021 Betterment report, *The Impact of the Great Resignation*⁵:

- 43% of respondents had to utilize their emergency funds since the pandemic. Nearly twice as many people dipped into these savings for medical expenses, home and auto repairs, and living expenses while temporarily unemployed.
- 54% of workers were somewhat or significantly more stressed about their finances than before the pandemic.
- 58% of Gen Z, 62% of Millennials, and 52% of Gen X respondents indicated their financial stress levels were higher than pre-pandemic, compared to just 35% of Baby Boomers.
- 46% agreed with the statement, “I didn’t think I needed an emergency fund before the pandemic, but now I do.”

Among the financial challenges of the pandemic and the ongoing fight for talent in today’s market, employees are demanding more support from employers than ever before. Almost 80% said it was important that their employer offers financial wellness benefits, and over 70% say these benefits are even more critical now than they were pre-pandemic. Incredibly, 68% would prioritize having better financial wellness benefits above an extra week of vacation.⁵



Employers benefit from financial wellness programs



Pandemic Heightens Interest in Emergency Savings Vehicles

Many employees are not saving for, or are not prepared to handle, a financial emergency. The issue has come to light, especially during the pandemic, as employees across the U.S. were furloughed, had their wages reduced, or hours cut in the wake of the shutdowns and economic crisis brought about by COVID-19.

The Coronavirus Aid, Relief, and Economic Security (CARES) Act made it easier for employees to withdraw money from their retirement plans. Some advocates say that emergency savings accounts, emergency fund accounts, rainy-day accounts, or even sidecar savings accounts can help reduce withdrawals from retirement accounts (leakage) when emergency expenses arise. Employers are more closely looking at practical ways to help employees put away money they can later access in an emergency.

Per Willis Towers Watson’s survey of 464 employers, 26% offer an emergency account in their retirement plan,

and 19% said they are likely to add one.⁶ UPS launched its Emergency Savings Initiative for 90,000 employees in October 2020.

Several products are available today, including The Saxon Demand Account (SDA), an FDIC-insured deposit service that offers a significantly higher interest rate (3x greater on average) while remaining completely liquid, up to 100% FDIC insurance coverage, and highly customizable.

Can emergency Savings Accounts help workers avoid accessing their retirement funds early to ensure that their retirement dollars are available when they plan to retire? It is worth investigating as employers look to enhance their financial wellness programs post the pandemic.

Financial Literacy vs. Financial Wellness







I have always contended that part of our job as retirement professionals is to provide workers with the tools, resources, and knowledge to enhance their overall financial well-being.

There are significant differences between being financially literate and achieving financial well-being. Simply put, financial wellness can be thought of as a state. It’s the state of having financial security and freedom, while financial literacy is the knowledge of the financial concepts and skills that led you there. Financial literacy is necessary to achieve financial wellness.

As an industry, it is time for us to pivot from retirement readiness to a more holistic or financial wellness focus, which means providing resources and guidance around budget planning, paying off debt, emergency savings, college funding, paying for unforeseen medical expenses, buying a new home, and building a nest egg for retirement.

Key Components of a Financial Wellness Program

Many providers are looking to enhance or re-evaluate their financial wellness offerings. Below are six key components of a well-designed financial wellness program:

Financial Wellness Components	
	Communications Plan: It begins with a plan that outlines the Plan Sponsors overall goals and objectives. Some goals will be common across all Plan Sponsors, while others will be unique to a particular Plan Sponsor. Equally critical is to look at what the data is telling you. As recordkeepers, we have a lot of client and participant data. Leverage the data as you build client communications plans.
	Tools and Resources: Inventory and evaluate the tools you make available to participants via the participant portal. It's not about how many but having the right tools and resources to help participants along the financial wellness journey. When was the last time your organization inventoried all your tools and resources? Having tools available with low adoption is not benefiting participants along the financial wellness journey. Consider adding additional tools and/or sunseting those not used to make the participant experience more rewarding and meaningful.
	Targeted Messaging: Tailor messaging to participants. If done correctly, personalization can help create an enhanced customer experience while simultaneously driving additional revenue growth via new product development.
	Wellness Score: The ability for a participant to generate a wellness score serves two primary purposes: 1) provides participants with a sense of where they are along the journey, and 2) provides participants with the ability to modify their score to get closer to their destination.
	Advice/Counseling: According to PwC 2021 Employee Financial Wellness Survey, only 13% of respondents said they don't need anyone else's help regarding personal finances. 51% of respondents indicated they want to make their own decisions with someone to validate that decision, and another 36% were looking for specific advice ⁷ . Providing advice as part of your offering is always a wise choice.
	Aggregation: Financial wellness starts with a holistic view of one financial situation. Aggregation providers like Yodlee enable participants to pull in outside assets (i.e., IRA's, after-tax savings, DB balances, and other retirement balances) for planning purposes.

Summary

In close, the pandemic has brought several things to light... health, family, and the importance of being prepared for unexpected circumstances.

Enterprise Iron provides expert strategy, technology, and operational support to many defined contribution providers as a financial services consultancy. We have worked with organizations to assess their financial wellness program and welcome the opportunity to assist your firm in re-evaluating you're offering.

For more information, send me an email:
dgumlak@enterpriseiron.com

¹History of 401(k) Plans, EBRI.org Fast Facts November 5, 2018, #318.

²Retirement Assets Total \$37.4 Trillion in Third Quarter 2021, Quarterly Retirement Market Data, Investment Company Institute, December 16, 2021.

³Kent E. Allison, Arron J Harding, PwC's 9th Annual Employee Financial Wellness Survey Covid-19 Update, PwC US, 2020.

⁴2020 Retirement Survey Sponsored by Personal Capital, Kiplinger's Personal Finance.

⁵The Impact of the Great Resignation, Betterment, September 2021.

⁶The New Employer Benefit: Matching Emergency Savings, Anne Tergesen, August 27, 2021, The Wall Street Journal.

⁷PwC's 10th Annual Employee Financial Wellness Survey, PwC US, 2021.

Utilizing Agile To Support Application No-Code and Application Modernization

By Mark Kalafsky, Senior Vice President of Solutions & Delivery

The benefits of employing an Agile-based methodology for new development have been so effective that it is now considered the logical gold standard methodology for new builds and large upgrade projects. Enterprise Iron recommends Agile as the default methodology for all our internal and customer engagements.

When we engage with our clients via a Statement of Work (SOW), our language always includes a section on why we utilize Agile as our methodology of choice. EI also supports services other than new development and maintenance/upgrades. We are now engaging customers who have new active requests – Application Modernization and Development using Low-Code/No-Code tools.

Traditional waterfall methodologies are not geared to supporting these efforts. Waterfall is very inflexible and does not support dynamic customer requirements. We believe that firms who cling to their behemoth waterfall-based methodologies are introducing significant risk to their Modernization or Low-Code/No-Code initiatives.

Let's take a minute and dig into how Enterprise Iron uses Agile for Application Modernization and Low-Code/No-Code engagements.

Application Modernization

The purpose of any modernization program is to ensure that the re-platformed, modernized software works correctly, performs well, is secure, and is as efficiently produced in the shortest window possible. In the re-platforming space, vendors often resort to a line-by-line translation of the old code, which completely defeats the purpose of modernization.



At EI, our process looks different. First, we extract metadata from the old software, such as screen layouts, data structures, navigation, and business logic. We only use that information to write fresh, properly structured source code. Our modernization process utilizes Agile and follows the agreed-upon guidelines set before engaging with a client.

While we practice sound software engineering, we also realize that the project process will need to adapt to

circumstances encountered in the project work – which is the central guiding principle of Agile.

We understand that the fundamental nature of an innovative, successful software project starts with meaningful collaboration. Our standard, Agile-fueled communications are not status reporting meetings in disguise, and we efficiently adjust our process and backlog as needed.

By utilizing Agile, our modernized platforms result in satisfied customers who have been engaged in approving increasingly rapid results from the first portion of the engagement to the final result. Our code is object-oriented and scores highly when evaluated by software quality such as CAST.

No-Code

EI enables clients with self-service/no-code capabilities and is central to the latest IT paradigm. We provide clients with the tools and Agile-based processes that substantially reduce development times, unleashes a new group of developers (“Citizen Developers” or non-technical developers trained to utilize the new toolsets), and significantly reduce costs by combining the inherent acceleration methods of the toolsets with the injection of the efficiencies of Agile.

A more enticing Cost Per Customer (CPC), combined with the positive infusion of Agile-based development, is the formula for canceling the dread of a new build performed by siloed, high-cost IT organizations.

We advocate technology solutions that empower organizations to build Agile-based enterprise-grade solutions without code and include B2B and B2C endeavors. The ultimate No-Code platform should be designed to employ Agile (iterative results are seen immediately by the Citizen Developers), replace numerous enterprise business, and IT functions, and contain a digitally powered, graphically driven engine.

When successfully marrying No-Code and Agile, the cost-savings experienced could deliver outstanding ROI averaging a 60 to 70% reduction compared to traditional project costs.

Questions? Send me an email:
mkalafsky@enterpriseiron.com



Take Our Survey!

Please consider taking two minutes to complete our short, four-question **Financial Wellness Survey** at the link below:

www.surveymonkey.com/r/EIFinancialWellness

*Results will be posted on our website and shared in the next edition of *The Iron Chronicles*.