ENTERPRISE IRON FINANCIAL INDUSTRY SOLUTIONS, INC.

THE IRON CHRONICLES

Delivering impactful Business, Technology & Workforce Solutions since 2002.

OCTOBER 2020 | VOL. 1 | ISSUE 1

From The Corner Office

Welcome to the inaugural issue of The Iron Chronicles, Enterprise Iron's quarterly newsletter aimed at providing you in-depth industry insights from our Business and Technology SMEs. We are determined to make these newsletters worth your valuable time.

We begin by addressing the COVID-19 pandemic and its impact on daily operations. The first phase of business reactions was characterized by a great deal of confusion and quick time planning, often feeling chaotic. Entire operations transitioned to remote work with changes to technology and business processes that ordinarily would require long-term planning.

Out of unprecedented necessity, this occurred at rapid speed and while highly disruptive, was largely a successful undertaking. We are now experiencing an extended disruption with new issues emerging. Senior management is asking what their firms will look like if these conditions require permanent restructuring. Two of our industry experts explore these in further detail:

From Tim Scott, **Measuring the Impact of COVID-19** discusses the important questions that businesses may wish to ask themselves as we enter the new phase.

From Sergio DuBois, **Transforming Telework in the Post COVID-19 Workplace** provides a high-level map of the technical questions that need to be asked. He covers the processes required to effectively and securely move to the new paradigm.

I hope you find these newsletters beneficial and we welcome feedback and topic suggestions for future articles. Lastly, if you haven't yet had an opportunity, please check out the revamped **enterpriseiron.com**. Thank you!

Stay safe & healthy,

John R. Crocker
Co-Founder & CCO

Enterprise Iron is pleased to announce that we've been awarded a *GSA Multiple Award Schedule (MAS) Contract*, making it much more convenient for Federal, State & Local government agencies to do business with us.

For more information contact:
GSA@enterpriseiron.com or 888.242.4682 x706

Contract #: 47QTCA21D000C

GSA

Measuring the Impact of COVID-19

By Tim Scott

Long after the calendar flips over on December 31st, the year 2020 will be remembered as the year when so much of our lives and the way we do business changed. These changes are not the result of legislation like EGTRRA in 2001, another corporate scandal or a bubble bursting, which led to the stock market collapse of 2008.

These changes were in response to the COVID-19 pandemic, which has infected tens of millions and caused over 1 million deaths across the globe. The decisions that businesses are now making and how they continue to respond to this ongoing threat will determine which survive and which will not.

As Warren Buffet said after the 2008 stock market crash, "When the tide goes out, a lot of rocks are exposed." In that case, the tide that was covering inefficient processes was a record stock market.

The rocks that were exposed when the market went down were the manual and custom processes that had been created and relied upon during a time of asset growth. The mantra, "just get it done" rang true during that time but many rocks were exposed.

Enterprise Iron believes that these new rocks change the way we have traditionally done business and experts agree a "new normal" for the way business is done now includes permanent remote working for many Team Members, especially in the Financial Services industry.

THE ENTERPRISE IRON FINANCIAL INDUSTRY SOLUTIONS, INC.
IRON CHRONICLES

Delivering impactful Business, Technology & Workforce Solutions since 2002.

OCTOBER 2020 | VOL. 1 | ISSUE 1

The ramifications of this approach, both immediate and long-term, are significant. The pandemic is requiring many firms to thoroughly review internal processes and procedures, which requires asking yourself some tough questions:

Business Process Reengineering
Firms had to move swiftly to migrate their non-essential workers to a work from home environment. Anytime changes of this magnitude are undertaken at pace, important details and work are often dropped and processes need to be reviewed. Ask yourself, are our processes documented and easily accessible to support remote work?

Security
How can our organization securely push out processes and new technology to users who are not now coming into the office? How do we guard against outside attacks when each employee may have a different network provider or protocols that impact their ability to connect to your back-end systems?

Technology
Do your systems support remote working? What changes are required to do so? Many organizations did not have the hardware and software required to send Team Members home on short notice. A number of our clients have spoken to us about the challenges of having company laptops purchased, configured and deployed to their remote workers in a timely manner. At many firms an additional 1st level tech support line will be required.

Facilities
Does our change to remote working impact our need for in-house facilities? How can we smoothly transition our workforce to reduce our current contractual obligations for facilities as our needs for space are reduced?

Outsourcing
How many firms will finally throw up their hands and cry Uncle? One approach that many organizations may find attractive is to consider outsourcing of certain technologies or operational processes as a means of reducing their needs for staff.

The Economy
Before the shutdown, our economy had positive projections for 2020. Unlike other economic impacts, this shutdown was voluntary based on health and safety concerns rather than the result of a systemic economic failure. However, the lasting effect of closing a significant number of small businesses and sending office workers home still remains to be seen.

Does the economy bounce back once everything has reopened? Even if it does, how does the long-term, reduced need for office space impact the commercial real estate market? What about the number of small businesses that serve those large office complexes? With reduced customer demand due to more remote workers, how many of those can stay in business with their expensive downtown rental agreements?

The Good News
A bit of encouraging news is that at a recent virtual industry conference, much of the conversation was about the experience of managing the lockdown that occurred in March of this year. Most companies surveyed were able to make the migration of most of their staff within a few weeks, but what comes next and who can help?

Enterprise Iron Can Help
Enterprise Iron has always specialized in remote working. Headquartered in New Jersey, we have Team Members living in 31 states across the U.S. and in Puerto Rico. Over 75% of our staff works remotely and has been in that environment for over a decade.

Our expert Business Process Analysts know how to evaluate your business processes and identify non-technology process improvements that enable your Team to permanently work remote.

Our Systems Engineers and Security Engineers know how to analyze your current applications and security protocols to make sure your remote employees can be productive in a secure work environment that protects the data of your retirement system members and sponsors.

888.242.4682 14 Cliffwood Ave Suite 200
www.enterpriseiron.com Matawan, NJ 07747

THE ENTERPRISE IRON FINANCIAL INDUSTRY SOLUTIONS, INC.
IRON CHRONICLES

Delivering impactful Business, Technology & Workforce Solutions since 2002.

OCTOBER 2020 | VOL. 1 | ISSUE 1

Our Subject Matter Experts in Finance and Facilities Management effectively evaluate your current contracts and consult with you to develop a path to success.

Our Solutions Architects and Program Managers have years of expertise facilitating an outsourced provider vendor evaluation and search process (RFI/RFP) to ensure that decisions you make regarding outsourcing are based in facts with a confirmed ROI that proves the value of a change.

Conclusion

While the Covid-19 pandemic has been disruptive to business at levels most of us have not seen in our lifetimes, and has required firms to fundamentally re-think daily operations, it has also served as an invitation. There is opportunity to reconfigure operations to gain efficiencies and cost-savings that had not previously been evident and have become necessary.

The first few months of this pandemic were chaotic as the need to protect public health was immediate and the virus was not understood. Decisions were reactionary with little thought given to any long-term ripple effects on the economy and how business will be conducted. The ramifications of the "new normal" are still playing out and the firms that are unable to adapt to a more remote business structure won't survive.

Enterprise Iron's extensive experience with remote working enables us to provide efficient solutions that assist you through this transition and keep your employees safe while maintaining productivity.

Did You Know?

Recent changes in legislation may require you to restate or otherwise amend your plan documents. We can provide the resources needed to keep your organization compliant. Our **Plan Restatement & Operational Consultants** are ready to support your team throughout the entire process!

Transforming Telework in the Post COVID-19 Workplace

By Sergio DuBois

Firms confronting the "new normal" of the COVID-19 pandemic and economic shutdowns faced unprecedented challenges. Many came to realize that they only had the capacity and licenses to handle a fraction of their workforce working remotely. Even with the drive towards cloud-based applications and data, always-on VPNs (Virtual Private Networks) were suddenly required for the entirety of their workforces' remote access.

Remote access network segments were not originally designed with the load of an entire workforce working simultaneously and required expansion to meet burgeoning remote access performance requirements. Many VPNs were crushed by a demand that was never planned for and technology portfolios found themselves without the licenses that would be required to support an entirely remote workforce.

IT Security and Risk Management leaders tasked with infrastructure security and remote access had to determine remote access requirements in the context of the once unimaginable requirement that the entire workforce operate remotely:

Remote work policies needed definition or expansion to align with the new normal possibilities of entire workforces working remotely.

THE ENTERPRISE IRON FINANCIAL INDUSTRY SOLUTIONS, INC.
IRON CHRONICLES

Delivering impactful Business, Technology & Workforce Solutions since 2002.

OCTOBER 2020 | VOL. 1 | ISSUE 1

Portfolios needed rationalization to determine when cloud-based services could be employed and how on-premise applications would be used remotely.

Products and remote access technologies needed performance testing to ensure that they were capable of taking on the load of an entire workforce relocation to remote access.

Unknown devices had to be evaluated for the security vulnerabilities they present such as for BYOD (Bring Your Own Device).

In the past decades, organizations have evolved from entirely relying on VPN technologies to enable remote access to enterprise applications towards the increasing trend of providing cloud-based services. Yet, many organizations still route all network traffic through a corporate VPN including these cloud-based services.

During emergencies like the COVID-19 crisis, this proved a problematic choice, as the performance of these cloud-based services was choked with the inordinate traffic placed on VPNs. This resulted in many users bypassing their corporate networks and accessing their cloud-based enterprise applications directly from their own personal devices on unsecured networks.

Solutions like a Cloud Access Security Broker (CASB) or Zero Trust Network Access (ZTNA) solution proved vital to address this surge in VPN demand and provide an alternative that retains greater enterprise control on access, while alleviating the performance impacts of funneling all cloud traffic through a VPN.

Opportunistic Phishing Attacks During the Pandemic

With countless employees relying on remote access connections to work from home, bad actors are exploiting remote working to launch attacks. Virtually all attacks require the end users' intervention to work and remote working is increasing that risk.

This year companies are seeing a rise in data breaches and so called "Phishing" attacks via text and email.

Bad actors realize that employees are more vulnerable working at home and moving their "lures" to communications that appear to concern COVID-19 often proves irresistible to its threat targets which given society's attention to this subject.

Over 4,000 domains have been registered this year that are named under the guise of COVID-19 and a frightening number of these exist solely to serve as phishing lures. They try to get users to click on a link or open a document, either of which exposes your employee's systems to malicious activities.

Remote Access Requirements

Rationalizing enterprise portfolios without understanding Remote Access Requirements leads to platforms that will perform unpredictably when faced with the massive remote access needs imposed during pandemics. Crippled performance and security are on the line, and it pays to have a precise understanding of the needs of an entirely remote workforce:

1. **Itemize users and work functions** – executive remote access requirements will vary wildly from field employees on specific granular work functions.

2. **Itemize devices and owners** – security and the controls applied to mitigating vulnerabilities vary widely based on the kind of device and who owns it.

3. **Itemize applications and data** – on premise applications and data will have vastly different requirements than SaaS (Software as a Service) applications.

4. **Itemize workplace locations** – where users are located is a factor that must consider a wide array of data privacy laws across national and local jurisdictions that could impact remote access strategies.

Based on these four parameters, each combination defines a distinct use case that must be mapped to a use case specific remote access solution pattern as part of a comprehensive strategy to align with the needs.

THE ENTERPRISE IRON FINANCIAL INDUSTRY SOLUTIONS, INC.
IRON CHRONICLES

Delivering impactful Business, Technology & Workforce Solutions since 2002.

OCTOBER 2020 | VOL. 1 | ISSUE 1

A Threat Model for Scaling Telework

Threat modeling in Telework identifies resources of interest and the feasible threats, vulnerabilities and security controls related to these resources. The model then quantifies the likelihood of successful attacks and their impacts. Finally, threat model analyzes this information to determine where security controls need to be improved or added. Threat modeling helps organizations to identify security requirements and to design the remote access solution to incorporate the controls needed to meet the security requirements.

Lack of Physical Security Controls

Telework client devices are used in locations outside the organization's control, such as employee homes, coffee shops, hotels and conferences. The mobile nature of these devices makes them more likely to be lost or stolen, which places the data on them at increased vulnerability.

When defining a telework strategy, security policies and controls, companies should assume that client devices will be acquired by malicious parties who will either attempt to recover sensitive data from the devices or leverage the devices to gain access to the enterprise network.

The primary mitigation strategy for the threat of device loss or theft is to encrypt the client device's storage so that it cannot be recovered by unauthorized parties, or to not store sensitive data on client devices. Even if a client device is always in the possession of its owner, there are other physical security risks, such as an attacker looking over a user's shoulder at a coffee shop and viewing sensitive data on the client device's screen.

Organizations can mitigate threats involving device reuse, such as an attacker gaining remote control over a device or impersonating a user, by using a strong multi-factor authentication for enterprise access.

Unsecured Networks

Nearly all remote access happens over the Internet, organizations have no explicit control over the security of the external networks used by telework clients. Communications systems used for remote access include broadband networks such as cable and wireless mechanisms such as IEEE 802.11 and cellular networks. Internet communications systems are susceptible to eavesdropping, which places sensitive information transmitted during remote access at risk of compromise.

Man-in-the-middle (MITM) attacks may also be performed to intercept and modify communications. Organizations should plan their remote access security on the assumption that the networks between the telework client device and the organization cannot be trusted.

Risk from use of unsecured networks can be mitigated, but not eliminated, by using encryption technologies to protect the confidentiality and integrity of communications, as well as using mutual authentication mechanisms to verify the identities of both endpoints.

Infected Devices on Internal Networks

Telework client devices, particularly BYOD and third party-controlled laptops, are often used on external networks and then brought into the organization and attached directly to the organization's internal networks. An attacker with physical access to a client device may install malware on the device to gather data from it and from networks and systems that it connects to.

If a client device is infected with malware, this malware may spread throughout the organization once the client device is connected to the internal network. Firms should assume that client devices will become infected and plan their security controls accordingly.

In addition to mandating use of appropriate anti-malware technologies, such as anti-virus software on laptops, organizations should consider the use of network access control (NAC) solutions that verify the security posture of a client device before allowing it to use an internal network.

Organizations should also consider using a separate network segment for all external client devices, including BYOD and third party-controlled devices, instead of permitting them to directly connect to the internal network.

THE ENTERPRISE IRON FINANCIAL INDUSTRY SOLUTIONS, INC.
IRON CHRONICLES

Delivering impactful Business, Technology & Workforce Solutions since 2002.

OCTOBER 2020 | VOL. 1 | ISSUE 1

External Access to Internal Resources
Remote access, including access from BYOD and third party-controlled client devices attached to an organization's wireless BYOD networks, provide external hosts with access to internal resources such as servers. If these internal resources were not previously accessible from external networks, they can be exposed to new threats particularly from untrusted client devices and networks when they are made available via remote access.

Each form of remote access that can be used to access an internal resource increases the risk of that resource being compromised. Firms should carefully consider the benefits of providing remote access to additional resources in terms of the potential impact of compromise.

They should also ensure that any internal resources chosen to make available through remote access are hardened appropriately against external threats and that access to the resources is limited to the minimum necessary through web application firewalling and other access control mechanisms.

Guiding Principles for Telework Strategy
Threat modeling – Before designing and deploying telework and remote access solutions, organizations should develop system threat models for the remote access servers and the resources that are accessed through remote access.

Plan for loss and theft of devices – When planning telework security policies and controls, organizations should assume that client devices will be acquired by malicious parties who will either attempt to recover sensitive data from the devices or leverage the devices to gain access to the enterprise network.

Zero Trust – Organizations should plan their remote access security on the assumption that the networks between the telework client device and the organization cannot be trusted.

Harden Internal Resources – Organizations should ensure that any internal resources they choose to make available through remote access are hardened appropriately against external threats and that access to the resources is limited to the minimum necessary through firewalling and other access control mechanisms.

Tailor controls to the remote access use case – When planning a remote access solution, firms should carefully consider the security implications of each of the various remote access methods possible as applied to combinations of users, devices, applications and workplaces.

Isolate BYOD network segments – When considering permitting BYOD devices within the enterprise, strongly consider establishing a separate, external and dedicated network for BYOD use within enterprise facilities. Such a network may also be used for third party-controlled client devices if desired.

What Can Be Done?
Enterprise Iron has a rich history of helping our customers through trying times with a high degree of competency and success. In addition, we have introduced and scaled a world class VPN for our own staff. Given the specter of a potential round two of the pandemic, it is critical that the "new normal" – a secure, scalable, remote working environment with a reliable backbone be part of your business plan.

Our Subject Matter Experts can assess your infrastructure and devise a strategic and tactical roadmap that will best lead you to address whatever challenges lie ahead, COVID-19 related or not. We understand that time is of the essence, given the whirlwind of political, legal, technical and compliance activity that seems to morph on a regular basis. We can assess and produce an actionable roadmap in a compressed timeframe and our SMEs are at the ready to provide the expertise and guidance you need.

Upcoming Events

NAGDCA CONNECT: October 5 - 29

ASPPA ALL ACCESS: October 26 - November 18

SPARK FORUM 2020: November 4 - 6

***Be sure to join our session on Wednesday, Nov. 4th @ 1:40pm*

888.242.4682 14 Cliffwood Ave Suite 200
www.enterpriseiron.com Matawan, NJ 07747