MINERVA™

Words of Wisdom

A QUICK GUIDE TO THE NEW NORMAL

Understanding the critical nature of cybersecurity in unique times

By: Jorge Conde-Berrocal and Roland Peña

April 2, 2020

WHAT IS THE “NEW NORMAL”?

“This experience is going to change us... It is going to be transformative on a personal basis, on a social basis, on a systems basis. We're never going to be the same again... When do we get back to normal? I don't think we get back to normal, I think we get... to a new normal.”

Andrew Cuomo, Governor, New York

The events associated with COVID19 have tested us as business owners, colleagues, family members, and neighbors. Stronger social restrictions are significantly increasing our dependency on remote-enabling technologies. While most of us are focused on resuming our daily business and personal routines, criminals are looking to take advantage of the disruption and confusion for their ends.

Lots of businesses and schools, small and large, have been thrown into chaos. They were once comfortable with controlled office or classroom audiences. Remote access for schools and businesses was available but seldom the norm. Suddenly almost everyone is remote, like what happens after a hurricane but on a global scale. Your top priority is to keep people safe. The second is to keep businesses and schools operating remotely. **That’s the new normal**. Once the first couple of priorities have been satisfied, what then? It turns out in many cases that cybersecurity was left behind in the rush. That’s your next priority – to make sure that your technology and people are armed with the knowledge to help keep your systems and information safe.

While we will spare you the details of cybersecurity standards in this piece, it is important to know that there are organizations dedicated to maintaining cybersecurity frameworks that can assist you in your efforts. The two most common frameworks are NIST 800-53 and ISO 27001. We would not recommend trying to digest them if you are just starting, however, simply reading the table of contents for the frameworks provides a good guide to ensure that you are holistically thinking through your cybersecurity. Additionally, there are local standards kept up to date by state agencies such as the Texas Cyber Security Framework. Local frameworks tend to be designed for Small and Medium Businesses and schools with the understanding that that smaller organizations do not have the resources or need to implement the full standards that have been built by NIST and ISO organizations. The local frameworks are more feasible operationally and require less technical knowledge to implement effectively.

This unique time provides us with a compelling reason to act now. As businesses and professionals, there will be winners and losers coming out of this crisis. Begin to establish policies, processes, and playbooks that may have not existed in the past using the lessons learned from this event. Take advantage of the current environment to build a stronger cyber capability, build confidence among your organization, and to proactively ensure that you are prepared for this new reality. Establishing a Cyber framework based on existing standards will allow you to more effectively communicate and manage our new operating environment. Can you imagine if you had already planned for a pandemic within your existing business continuity plan? How about a remote access policy that addressed employees, teachers, and students that have migrated from offices and classrooms to their living rooms? The same policies, procedures, and playbooks will be useful again for future events, whatever form they may take. With a large proportion of the approximate 130 million full-time employees and 70 million primary school students being moved to a purely digital working environment, cybersecurity and preparedness will be a differentiator moving forward. It will have a material impact on organizations and careers.

Those that are ahead of the curve will elevate their position within their peer network and be able to prove readiness in the case of an event. Those that don't adapt to the importance of cyber in our new operating environment will increase their level of exposure… until a breach occurs. At that point, the conversation will shift to a discussion of negligence and liability requiring meetings with attorneys. There'll be debate among stakeholders about your effectiveness as a leader.

Throughout the challenges of the past weeks and in the coming months, the three core tenets of Cyber leaders remain Confidentiality, Integrity, and Availability. As leaders, we must understand the growing role they play in our organizations. We should be looking to our Cybersecurity Coordinators (or identifying one if one does not exist on your team) in these times to execute and/or develop the appropriate plans to ensure that these tenets are established and maintained. Remember, it's never too late to be prepared…until it's too late.

The ability to make operational shifts is materially impacted by the amount of planning and environmental knowledge to which one has at the time of crisis.

The New Normal for Enterprise

Fortunately for most enterprises, the concept of Work-From-Home (WFH) is not new. That being said, the adoption of a WFH culture has been up for debate by many leaders. As most knowledge workers are now forced to work remotely, business leaders need to change their perspective. It is important to note, as we think about these issues, that your perspective within the CIA triangle (confidentiality, integrity, and availability) can shift depending on your core business. Financial institutions may place a higher priority on confidentiality and integrity, while manufacturers may place a higher priority on the availability of resources for the continued operation of the production line.

Update or Establish Your Business Continuity Plan

If you didn't have a Business Continuity Plan that you recently initiated and are currently exercising, it is very important to use this time to build one. The ability to make operational shifts is materially impacted by the amount of planning and environmental knowledge one has at the time of crisis. While business continuity plans seemed like idle paper exercises four weeks ago, they are now separating the prepared from the panicked. Understanding your critical resources, who needs them, when they need them and how to access them are all components of Availability within the CIA triangle. Having a clear understanding of the governance model that you will enable, and when to enable it, helps to instill orderly execution and communication within the organization in times of radical change or necessity. What meetings will be held? How often? Who will attend? What remote meeting tool are we using? All are easily answered questions that make real differences in how business altering events are handled. How does a pandemic differ from an earthquake? Now might be a great time to give that some thought. As you do so, extend the exercise to your core suppliers and ensure that your careful planning has not been undermined by their carelessness.

Training and Communication

People can be the weakest link in this new operating environment. Keeping your employees aware of the increased security challenges and the expectations of their behavior may be the single most important step you can take for your organization. Education on the following items is recommended.

Email Security – Phishing and fraud (there has been a material increase in phishing and fraudulent activity as a result of the COVID19. Bad actors are using the crisis to exploit the weakness in our systems and wellbeing). For example, the FTC [insert link] is investigating scammers pretending to represent the IRS.

Acceptable Use - While many find it intuitive to define acceptable use, we all approach “acceptable” from different perspectives. Thusly, it’s important to take the time to ensure that everyone is working from the same set of rules and has clear expectations of what will be permitted and what does not constitute acceptable corporate behavior. For example, can family members access devices that can connect to the corporate network? What if your kids need to attend a class or want to play a game on a corporate-owned device? More on this below.

Social Engineering – bad actors will use the confusion to take advantage of our instinct to help others in times of need. This means that doing a “favor” for an employee, so that they can get their work done, may mean falling for a ruse that exposes your systems and data. Make sure that your support desk follows consistent rules and established procedures – it’s tempting to want to help a caller, but is that person really who they say they are?

Acceptable Use

Assume employees won’t know what is allowed or prohibited in the new working environment. Ensure that you clearly and repeatedly communicate your expectations through a documented Acceptable Use Policy.

1. Do you have a documented policy on what devices can be used at work? Corporate assets only, “Bring-Your-Own-Device” (BYOD), or a combination of both.
2. Do you have documented security requirements for corporate, and BYOD, before accessing corporate resources? Are they enforceable?
3. What types of websites are allowed vs disallowed:
   a. while using corporate assets?
   b. while connected to the corporate network?
   c. on a device that is intermittently used to connect to corporate resources?
4. Do you define who should have access to BYOD and Corporate assets (e.g. family members, friends, etc.)?
5. Have you enabled your screen lock when not in use after a set duration of time?
6. Where are you allowed to save company data (e.g. hard drive, SharePoint, Box, etc.)?
7. Have you implemented mobile device management, data loss prevention, and malware scanning for remote devices?

Remote Access

How we connect to corporate assets is one of the most important items in retaining continuity of business. It also could represent a significant risk to the organization if methods and controls for connecting to corporate assets are not properly managed.

Do you use VPN technology? Is it agentless or require some type of installation? Do you have the appropriate licensing vehicle to enable a spike in usage? Do you have the capacity to handle the increased load on the infrastructure?

Do you use Virtual Desktops? Can your Virtual Desktop Infrastructure (VDI) support the workloads needed to conduct critical business needs?

Identity Management

Within the current environment, bad actors are using our sense of social responsibility against us. Increasing our vigilance for password management and help desk functions associated with password management is encouraged. With the number of new users becoming digitally available as targets, and the spread of easily accessed password-cracking software that can execute brute force or rainbow attacks and social engineering, it is critical to practice and enforce strong password policies. Multi-factor authentication provides an even better alternative and is becoming more available, affordable, and easily implemented for organizations of all sizes. In times of crisis, it is easy to understand the pressure to help someone else complete a business-critical task. That's one way that a con artist will attempt to trespass. Communicate your expectations (see: Acceptable Use Policy above) and be prepared to support your position if you're faced with decisions that require judgment between the business outcomes and best security practices.

Data-in-Transit

With the increased use of the internet as our communication medium, it is more important than ever for us to know how the data that we are sending over the internet is protected while in transit. While not all traffic is required to be encrypted, it is becoming more common practice for all external communication to be encrypted. This is partly due to the advances in technology but is primarily driven by 1) regulations (e.g. such as FINRA and NY DFS) and 2) a lack of understanding of what data is being transported making an "all of the above" strategy the most effective in protecting personal information as well as confidential information. This also translates to certificate management for critical applications and the ability to ensure that certificate expiration can be effectively managed in the new operating environment.

Data-at-rest

Protecting data at rest is a core tenet of most security practitioners, but we must now extend this principle to remote employees who are less concerned about security and more concerned about usability. From databases full of Personally Identifiable Information (PII) to document warehouses like SharePoint, we must protect the data at its source and ensure the appropriate level of protection for the type of data being stored. Do you understand what data is being stored and where it is being stored? Do your remote workers understand? Most organizations struggle with understanding the various categories of data that they may have and where it may be located. Use this time to understand what is stored, where it is stored, and what control levels must be implemented to protect against data loss. Not all data is created equal. Identify your business-critical data and make sure you have the necessary protections in place.

We understand that each item in this list can take months or years to accomplish; we also know that the sooner you start, the sooner you will be prepared to address the digital challenges of the new normal.

The first step is to secure your business model.

The New Normal for Small and Medium Businesses

Small and Medium Businesses (SMBs) may be the hardest hit market segment. Most struggle with cybersecurity even when there is no crisis. As we look at the challenges in cybersecurity for SMBs, studies have shown that the three main issues facing them are lack of resources, limited budgets and low levels of cybersecurity skills. Additionally, we have seen that the division of roles and responsibilities in the SMB market is not so clear. They tend to be more collaborative environments with responsibilities that are shared throughout the team. While many SMBs have already started trying to figure out their new normal, we hope to provide some structure and general guidance that can help ensure that you are securing your business by design. The first step is to secure your business model.

Review and Update your business model

The first thing that all business owners must do is ensure the safety of their employees. The second is to remain open for business. This means taking a few extra minutes to document what the changes are to your working environment and to the way that you do business. This exercise should incorporate all aspects of your business including but not limited to:

1. Staffing
2. Marketing and Sales
3. Legal (Contracting Vehicles etc.)
4. Delivery (Products, Services, Customer Support)
5. Supply Chain
6. Back Office (Billing and Entitlement)

In all cases, it is critical to understand your company's cash position and to anticipate if the change is going to be feasible and for how long before implementing a cybersecurity strategy. Once you are committed to the new normal, it is critical that you build it into your design process. If you have already completed this exercise and are recovered and operational, go back and document the changes that were implemented as a result of the crisis. This will serve as the base of your Business Continuity Plan.

Have a plan (or build one today)!

While most large corporations have complex and extremely detailed plans that they put into action during times of crisis, it is equally important for SMBs to have a plan. The level of complexity is not what is important here. The importance is that you can resume operations as quickly as possible and minimize the impact on your ability to transact business. Intuitively, those with a plan will execute better than those without a plan. Having the most basic of plans can have a strong psychological effect on your team and will provide them with confidence to stay the course in trying times. It'll also help in your defense if, despite best efforts, someone compromises your systems or steals your data.

What systems do you need to stay open for business?

Part of documenting any changes in your business model is to help define the inventory of resources the business will need to operate in the new normal. While we know that time is critical, doing this right will save you time in the long run. Take the time to document the systems and resources that you have adopted over the past weeks to enable your business. If you have a previously defined list, then validate that it is in fact what you are using and make updates accordingly. Did you move to a cloud-based email service provider? Did you move to a cloud-based HR system? Ask yourself, "Do I have all of our records on my laptop?" "How will the team collaborate?" "Am I documenting and backing up all these new changes and configurations?" Having this information will guide you in the steps to take to secure your data and to ensure that the resources needed to operate your business are available. Stay focused on the "must-haves". This will save you time and buy you time to work on the "nice to haves".

Who needs to use the core systems you've identified?

Once you have completed the list of critical systems, identify the roles and team members who need access to resources. For example, the sales team must have access to email and Salesforce. The back office must have access to Microsoft Word and OneDrive to manually generate invoices. Going through each role in your updated business model may uncover additional resources that can be added to the list of your critical systems.

Now that you have a list of systems and a list of roles and team members that need them to operate, let's get connected.

How will my team connect?

It is important that you consider how your team will remotely connect to each of the resources that you have identified in the list above. The first step is to identify what devices they will be allowed to use. Will you be allowing the use of personal devices? Will you be providing, or need to provide, laptops? These decisions have a downstream impact. For example, a shared family desktop is more likely to get infected with malware than a dedicated work laptop only used by trained team members.

Now that you have your list of systems and associated roles, we can explore how to get them connected. Commonly, companies are using cloud-based services for email and basic needs through services like Microsoft 365 and Google for Business. Many businesses have turned to Zoom and GoToMeeting for web-based conference calls. No matter the vendor, the use of these cloud-based platforms provides an easy-to-use vehicle with limited responsibility on the side of your business. In a crisis, you need to stay focused on your core business. Third-party vendors (Zoom, Microsoft) have strong security models for the products they sell. Confirm that this is the case with your chosen vendors so it’s possible to offload some of your security diligence.

For your internal systems that are not internet-accessible, you will need to decide on how your team will connect to the corporate network and what they can and cannot do while on the network. Traditionally, connectivity has been done through the use of Virtual Private Networks (VPN) using some type of client installed on the device. More recently, clientless VPNs and Virtual Desktops have been leveraged for this type of access. Remember, depending on the devices that you are allowing into your network, you are also allowing any malware that comes with them. It is important to know that establishing a VPN creates and protects the connection between the device and your network. What happens once connected is a different issue.

Make sure only the people you want are connecting!

Within the current environment, the bad guys are using our sense of duty to one another against us. Make sure that your team knows how you will be engaging with them for password management. With the number of new users online it is critical to practice and enforce strong password policies. Multi-factor authentication provides an even better alternative and is becoming easy and affordable for organizations of all sizes. This requires two forms of identification to get into the system. A common example is at gas stations when the gas pump asks you for your credit card (something you have) and then asks you to input the zip code (something you know) before it allows you to pump gas.   In times of crisis, it is easy to understand the pressure that can be placed on someone to provide user credentials to help complete a business-critical task.

Know where your data is!

Make sure that your team knows what your expectations are concerning company data and where they need to store it. Will you allow them to keep company data on their devices? What if they are not company devices? Do you have a centralized repository for managing documents like a SharePoint, OneDrive or Box? If you do, is your team managing the access to the repository? While these are not hard questions and can seem tedious, your company’s information is the most important asset in the digital economy. Having done the hard work to stay open can be quickly undermined by not having well-communicated expectations about how to handle company data. This is one of the most important elements of protecting your business. We have all experienced when employees place confidential data, including client records, on their personal devices. They expose their businesses to malicious acts, not out of malicious intent, but out of convenience.

Also, ensure that you have the appropriate backups of critical information and that they are done at a frequency that supports a recovery point that would not negatively impact your business. With the increase in phishing and the impact of ransomware, you must plan for quick mitigation. Don’t trust your business to a laptop or system, that cannot be recovered.

Communicate with your team about the new environment and expectations.

Err on the side of over-communicating expectations and rule changes. Never assume that the team understands or will intuitively “get it”. Provide collaboration vehicles to encourage remote teaming (like webchat) and make yourself available to answer questions. It may seem like a distraction, but the more focused and educated your team is on the new operating environment, the more productive they will be. Services like Zoom, Slack and Teams offer great platforms to ensure that you are available and effectively communicating.

Trust but Verify!

Third-party services, while removing some operational responsibility from your organization, do not eliminate your accountability. Ensure that as you work through service providers that you understand and agree with their data privacy policy and security controls.

The traditional way of thinking must shift to one that incorporates cybersecurity as a mandatory element of new IT infrastructure and learning tools.

The New Normal for Education

With approximately 70 million children moving to a remote learning environment over the past 3 weeks, teachers, parents, and students are experiencing massive amounts of change in how we teach and learn. Unfortunately, with this shift comes an increase in bad guys trying to take advantage of the new normal. As with Enterprises and Small and Medium Businesses, several characteristics will be common to all three types of businesses, but education also has some unique security challenges: Service and technology provisioning, budget cycles, funding sources, and staff skilled to address cybersecurity challenges.

We have seen a rapid shift in resources being used to deliver the new normal learning environment. YouTube videos replacing classroom time. Google Classroom taking the place of notebooks, lesson plans, and assignment management. We are truly in a new digital environment and with that comes additional responsibility. From our experience in working with education K-12, we have seen that funding is typically directed to learning tools with cybersecurity initiatives not making the budget. The traditional way of thinking must shift to one that incorporates cybersecurity as a mandatory element of new IT infrastructure and learning tools.

Lastly, the education system has the additional responsibility of servicing everyone. We have a responsibility to ensure that all children have access to the resources needed to continue their learning. This does not mean it’s everyone’s responsibility to ensure that the resources are used. This is left to the larger mission of parenting. We must collectively stay focused on the secure delivery of the enabling technology that provides a foundation for education.

Review and update your learning model

The first thing that all education organizations should do is to identify and standardize their new tools and content delivery mechanisms. This means taking a few extra minutes to document what the changes are to your working environment and to the way that teachers are delivering content to students. This exercise should incorporate all aspects of your organization including but not limited to:

1. Physical safety and health
2. Student access to learning devices
3. Communication with students and parents
4. Attendance
5. Content delivery
6. Assignment Management
7. Learning support

Chances are that there have been and will be some shifts in these areas as a result of the current environment. In all cases, it is critical to understand the resources being provided by your organization and to anticipate the resource needs of your teachers and students. That being said, once you are committed to the new normal, it is critical that you build it into your design process, including who is responsible for the maintenance and execution of the plan. If you have already completed this exercise and are fully operational, go back and document the changes that were implemented as a result of the crisis.

Student Safety

There is no more pressing concern than that of student safety during times of crisis. While many students will be fine, a significant portion of students will be going home to environments that are less than ideal for learning. Some students may rely on school for their only stable meal of the day, while others may not have access to the devices needed to continue the learning process remotely. Even worse, some may be in harm's way while at home and may have concerns for their physical safety in the new normal. Schools must focus on providing communication vehicles to the less fortunate and continue to provide avenues of safety for these students.

What students need to participate

If students don't have internet access, have we achieved our mission of availability? Some would say that that we have - as long as the IT systems are up and running, but we believe this is one of the unique challenges of education. The ability to provide access to digital learning in this environment is foundational and is not a variable in control of the children. We must take inventory of the assets needed to provide the children with access to the resources they need including, but not limited to:

1. Devices
2. Internet Service
3. Application
4. Security

Do you have policies that will guide the allocation of these resources?

Communication with parents and students

As learning moves online and return dates continue to be pushed out, the ability to work together to build a new rhythm for learning will involve more unusual channels. Establishing and communicating smart security policies for information over these channels will have a material impact on your effectiveness.

Make sure only the people you want to connect are connecting

Within the current environment, the bad guys are using our sense of duty to one another against us. Make sure that your administrators know how students will be engaging with them for password management. With the number of new users online it is critical to practice and enforce strong password policies. We have seen instances of schools sharing credentials among the teachers and substitutes out of convenience. We have heard of social engineering campaigns targeting password resets using phone calls and "favors". Enforcing strict identity policies are one of the best ways to protect your organization.

Multi-factor Authentication provides an even better alternative for controlled resources and is becoming more available, affordable and easily implemented for organizations. This requires two forms of identification to get into the system. One example is when a child shows their school ID card and then types in their passcode. In times of crisis, it is easy to understand the pressure that can be placed on kids and teachers to share user credentials so they can get their assignments completed on time.

Manage content, including the socials

As discussed in the preface of this article, security must be an integrated component of the program. We cannot provide devices to children that allow for uncontrolled social networking, web surfing, and access to resources that could negatively impact children. Security, specifically content control, must be included in any allocation of resources to children.

Accessibility to remote learning can mean more access to social platforms. While many schools operate under a common code of decency, social media is a gateway that bad guys use to gain access. There is no more vulnerable target than a child and the criminals are trying to take advantage of the exponential increase in children accessing the internet. Guide parents and install content controls on devices provided by your organization to limit the exposure that you're enabling.

Know that there is more than learning at stake

In addition to the learning process and resources needed to operate schools, education organizations must double down on the security of the IT systems that maintain student information. Organizations should have handy (or develop quickly) an inventory of their systems that contain Personally Identifiable Information (PII). What's more valuable than an identity of someone who will not miss it until they apply for a college loan or their first job. This question alone should highlight the importance of understanding where the data resides.

Protecting data at its source is critical in mitigating the risks associated with the new normal. Are your databases encrypted? How strong is the encryption? Who can access these resources in the near term? Are these systems internet accessible?

MINERVA™

You have questions, we're here to help!

If you don't feel that you have the resources to effectively manage the current circumstances, ask for help. There is no lack of parties interested in fulfilling their social responsibility during this time of need. Use your network to get to trusted resources. Feel free to reach out to our organization for connections or if we can be of assistance. We will make every effort to help you succeed. Our future depends on it.

Our role in the new normal

As an organization, we are motivated to make our value accessible to everyone in these unique times. We can draw a straight line from the Minerva platform to being prepared to address COVID19 or the next unknown threat that we face. Please feel free to reach out or visit our website at www.V3CYBERSECURITY.com, or schedule an introductory meeting with our CEO at https://meetings.hubspot.com/jorge-conde-berrocal/minerva-speak-with-an-expert.

For those not in the market, please take the time to inventory your cyber capabilities and business continuity plans. Our organizations and communities are depending on our collective ability to execute effectively and securely.

V^3™ CYBERSECURITY

support@v3cybersecurity.com

OR

V3 Cybersecurity, Inc.

9838 Old Baymeadows Rd. #335

Jacksonville, FL 32256