THE COVID-19 PANDEMIC'S IMPACT ON CYBER RISK

Understanding the Shift in the Cyber Risk Model and Six Basic Steps You Can Take to Prepare your Defensive Readiness

neueon.com

April 2020

About This Whitepaper

Current changes in business operations necessitated by the COVID-19 pandemic illustrate the importance of viewing cybersecurity as a business support function, rather than as a costly overhead driven by regulations.

In this whitepaper, we will share:

- Why the COVID-19 pandemic requires a shift in the cyber risk model
  - Cybersecurity as a business support function
  - A move from compliance-based programs to cyber defense
- Information about today's potential cyber threats
- Cybersecurity fundamentals and how to strengthen the lines of defense
- Tools and resources available to support a cybersecurity strategy
- What tomorrow will bring and how to ensure cyber flexibility in your business

Table of Contents

Abstract

COVID-19 has had a profound impact on the world. As organizations, like the World Health Organization (WHO) and the United States Centers for Disease Control and Prevention (CDC), advocate for the elimination of large gatherings, businesses have had to make significant adjustments to their workforces. This has led to a necessary shift in the cyber risk landscape.

Adhering to WHO and CDC guidelines, as well as those from other federal, state, and local governments, has forced companies to transform traditionally in-person business operations and practices to remote teleworker environments. This shift has been an easy transition for some businesses yet more difficult for others, the degree of difficulty varying based on how prepared the organization was for remote work at the time of the pandemic's rise. For example, factors like the extent of cloud services adoption has had a significant impact on the ease of a business's transition to remote work.

Regardless of how prepared a company was for the transition, however, managing cybersecurity and the new business cyber risk model is a challenge all businesses face. Before this era of remote workforces, businesses had a relatively well-defined perimeter with connections out to the cloud and a workforce that was protected within the perimeter. Employees had well-planned, well-defined, well-understood work models, and security safeguards were put in place to support them, for example, mandating the use of company owned equipment.

Companies understood their environments' weak points, and most had put security controls in place to mitigate risk. Having their environments relatively well-controlled, most organizations' threat models focused on meeting regulatory compliance and managing privacy issues.

However, as our world has shifted to a remote work environment, there has been a shift in our cyber risk model. A company's attack surface has expanded to encompass the number of employees that work remotely. The rapid expansion of remote workers has left businesses with many people outside the protected perimeter, with some working with uncontrolled, unmanaged endpoints.

This rapid and sometimes radical change has shifted the emphasis in cybersecurity. No longer is the focus and priority limited to meeting regulatory requirements. It has expanded to include strengthening cyber defense in a world where internal operations may now be handled externally, and all aspects of a business must be considered at greater risk than ever before.

In an April 2020 survey of 25,000 American workers, 34% of those who were employed at least four weeks prior said they used to commute to their jobs but now work from home. An additional 14.6% were already working from home, suggesting nearly half the workforce is now working from home.

Source:
COVID-19 and Remote Work: And Early Look at US Data; MIT, Stanford, NBER, and Upwork

Cybersecurity as a Business Support Function

Prior to the COVID-19 pandemic, most businesses recognized the need for cybersecurity as a means to meet regulatory requirements. For example, most Americans who are responsible for their own health care recognize the Health Insurance Portability and Accountability Act (HIPAA), which mandates explicit responsibility of organizations working with healthcare information to protect personal health data to meet compliance.

Most businesses are required to comply with some form of regulatory or legislative mandate requiring cybersecurity measures. Common security requirements for businesses include:

- The Payment Card Industry Data Security Standard (PCI/DSS) for businesses using credit cards for payments
- The widespread requirements most companies face surrounding Personally Identifiable Information (PII), with legislative requirements in most states, like the California Consumer Privacy Act (CCPA)
- For companies doing business in the European Union, adherence to the General Data Protection Regulation (GDPR)

There are also numerous industry-specific requirements, and these are the types of legal frameworks that organizations must consider as part of their business and technology planning.

Regulatory requirements put significant responsibility on an organization. Accountability for the associated cybersecurity initiatives is often assigned to an individual responsible for overseeing the efforts. Due to complexity, most companies have adopted a cybersecurity framework to ensure appropriate measures are taken for compliance, for example, the well-adopted frameworks offered by the frameworks offered by the National Institute of Standards and Technologies (NIST), the International Standards Organization (ISO) and the PCI Security Standards Council.

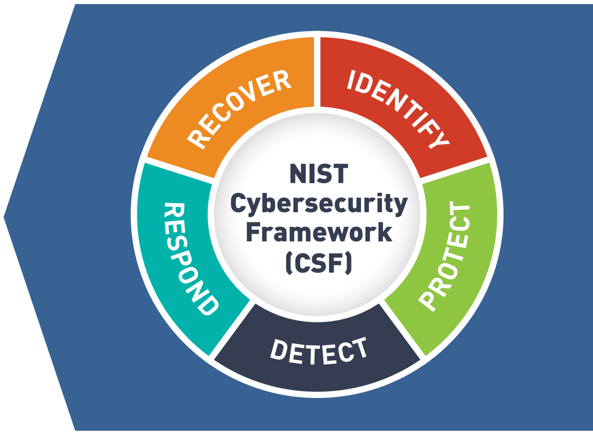
TECHNOLOGY RISK
?
RISK
SAFE
COST
EFFORT
RISK
COMPLIANCE CHECKLIST
BUSINESS GOALS

In today's COVID-19 world, businesses are now faced with additional priorities beyond regulatory compliance. They are now trying to survive with challenges that range from meeting revenue targets to maintaining operations to experiencing unforeseen revenue shifts. For example, the restaurant industry has had to shift quickly from an on-site dining model to one restricted to delivery and take-out.

While businesses cope with changes to their business model, they should also be shifting their cybersecurity focus from compliance to an increasing need for cyber defense. With a distributed telework model for employees, system availability is a key business support operation. For many businesses, this means the biggest threats are not compliance related. They are threats of disrupted business operations through activities like phishing attacks or "distributed denial of services" (DoS) attacks.

As a result of the new threat model, businesses must now adopt a stronger focus on a cyber defense mentality and approach. One way to accomplish this is to leverage a model similar to the NIST Cybersecurity Framework (CSF), which is built around the concept of cyber defense.

The CSF also provides a crosswalk mapping into the standard security frameworks like ISO, HIPAA, and others. So, businesses are not giving up existing frameworks to start over with another; they are adopting a different perspective and shifting prioritization.



Understanding Today's Business Cyber Threats

To gain a good understanding of a business's cyber risks, it is important to have a comprehensive view of the many factors that contribute to the threat landscape. Much like putting together a puzzle, each piece is important to seeing the complete picture. However, some pieces are more important than others.

The key first steps include understanding the technology landscape, defining the business's strategy and goals, and gaining awareness of current world events. Let's take a look at each of these and why they are important.

Technology Landscape
Business Strategy
Short-Term Business Goals
Current World Events

Technology Landscape

When it comes to technology, not all systems (hardware or software) are of equal value. So, no matter which security framework an organization uses, it must first understand what technology it has, what's important or mission-critical, and how best to protect it. Protecting systems begins with understanding the people who have and need access.

Prior to moving to today's telework environment, business-critical systems were often controlled and managed through on-premises data centers or cloud services. That part of our technology landscape hasn't changed. What *has* changed is *how* business-critical systems are being accessed.

Prior to telework, access was defined partly by location (office/on-site) and typically through company owned devices. With the current telework model, the line of control has blurred. Some workers use non-company owned devices, and almost all employees are working from home. This can lead to a more casual atmosphere and relaxed security safeguards. The points of attack surface has expanded to the number of employees working remotely. Each of those endpoints now has the potential to provide an entry point into the organization's technology landscape. The most probable method for unauthorized entry is through phishing scams.

Business Short-Term Goals and Strategy

The COVID-19 response has led most companies to adjust their short-term goals and strategies. Many are seeking to reduce projects or spending that is not directly related to maintaining existing business operations so they can mitigate impact on revenue. How the company views the necessity to address cyber risks determines whether they see cybersecurity as a luxury or a necessity.

For example, many organizations have had to make a choice between achieving ISO/IEC 27001/2 compliance certification and strengthening their cyber defenses. They are asking which is more aligned with their current business situation. There is no right or wrong answer, but the choice depends on what the business is looking to accomplish — and ultimately, it is a business decision. Businesses should not, however, completely forego doing anything related to cybersecurity during this time as a way to cut cost.

Current World Events

Current world events are a key piece of the puzzle for business cyber risk. They often play into the motivation of cyber adversaries or malicious actors. These groups are opportunistic and look to take advantage of our human characteristics and emotions. That is why phishing is one of the biggest threats a business can face. These malicious actors understand our desire to help others, especially during times of crisis, and will exploit our emotions if they can.

Recent research, for example, revealed that cyber attackers sent approximately 1.5 million malicious emails a day related to the COVID-19 pandemic in the three months between mid-January and mid-April. And the FBI stated that cybercrime reports have quadrupled during the COVID-19 pandemic. They're now receiving 3,000 to 4,000 complaints through their online portal versus the typical 1,000 — many of which are COVID-19-related.

Understanding current geopolitical events is crucial to implementing effective cybersecurity measures, even in a cost-cutting environment. All companies should take at least basic cybersecurity measures to strengthen their cyber defenses in a dramatically changing global environment, like the one we are experiencing today.

Cybersecurity Fundamentals

There are six areas businesses should focus on to address cybersecurity needs. They start at a high level and are listed in order of importance in the following sections. If a business is already addressing all of them, they should consider going deeper into each area to ensure complete coverage. This approach is similar to the Center for Internet Security's (CIS's) 20 Critical Security Controls, where an organization will go deeper into the controls based on their security program's maturity and capability.

1 Ensure appropriate access to all environments

It is crucial to know who and what has access to your environment. Understanding the kind of access they have is fundamental to basic cybersecurity principles. Simply having a list, however, is not enough; you need to keep the list current by reviewing it and maintaining its accuracy. Think about "appropriate access" to the environment and apply the "need to know" rule to ensure people have access to only what they need.

To help further protect access to the environment and data, move away from using passwords alone. Consider a two factor authentication process. Two factor authentication avoids many of the risks passwords alone open up. Whether easily-guessed or captured through phishing attacks, passwords are often the weakest link, especially for remote workers. Many believe users will be hesitant to adopt a new authentication process, but most users have become accustomed to using two factors to log into personal services, like online banking. Users are less likely to follow a process they find burdensome or unnecessary, so communicate well to ensure users understand why the company is implementing two factor authentication. Once people understand why it is important, they are more inclined to accept it.

2 Implement audit log management

Eventually, systems will be attacked. When this happens, the organization needs to know as quickly as possible what is happening, so they can take appropriate countermeasures. This enables them to limit the attack more effectively and gain a better understanding of the scope of damage.

We suggest investing in a Security Information and Event Management (SIEM) solution if possible. At the very least, implement a log management tool so the logs from various systems in the environment are in one place to more easily protect and review. It should be obvious, but make sure audit logging is enabled on all systems. Often, people are concerned with the information generated (noise), the amount of storage space needed, or the hit on system performance, but today, computers and storage are inexpensive compared to the damage an intruder can do.

What should you log?

The most effective logging requirements will be unique for each system and should be defined based on the system's purpose and the data being processed. The best way to determine what events to log is to base the decision on the basic Confidentiality, Integrity, Availability (CIA) security model and permissions to read, write/modify, and/or delete.

For example, when defining what to log on a financial system, integrity is important as is understanding who is reading the data (and do they have the authority to do so). Writes/edits are just as important as deletes. In a financial system, virtually all actions should be logged. It's also a good idea to consider other variables, like location—the "where" and "when" the event occurred from a geo-location perspective.

A public information sharing website provides another example. "Read" activity will be high, but it's not tremendously important to understand who is reading, since the information is intended to be publicly available. Suppose, however, that the information is public but it's also critical that it remain accessible, for example, the WHO's information on COVID-19, where availability is as important as integrity. In this case, logging system availability (uptime, latency, etc.) and logging who is making content changes (edits/deletes) is important.

Using the CIA approach and deliberately considering what is important on each system based on potential risks goes a long way to enabling the most effective logging strategy.

3 Develop user awareness

Experts state one of the biggest risk factors in cybersecurity is the human element. This translates to mean that employees are potential cyber risks. However, employees can be turned into one of a company's greatest defenses, primarily through cybersecurity awareness. If everyone is well-trained and knows what to look for, they can enhance the ability to identify threats early. If they are trained on how to respond appropriately, they can help reduce potential damage.

The most common threats employees will encounter are phishing scams. Most phishing attempts are designed to manipulate people's emotions, and nothing is more emotional than COVID-19 right now. It is important to decide as an organization what should happen if an employee receives a phishing email. Should they delete it immediately? Should they report it? And if so, to whom? Should they just ignore it and not respond? All of these are reasonable responses. Consider which one is right for the organization and how best to communicate the appropriate actions to employees. This will depend on the organization's goals and capabilities, and decisions often benefit from outside consultation with experts in this type of planning and communication.

If a company can't make it clear how to respond to an email that leverages our world's crisis as an excuse to get sensitive data, then the company is trusting each individual to respond appropriately without guidance. That is leaving too much unnecessary risk to chance. The company's people are its first line of defense, and educating them is often underrated. Successfully increasing user awareness is usually more effective than most cybersecurity tools.

4 Create basic network and perimeter safeguards

Decentralized employees expand the scope and size of a company's network. Consider the age-old security analogy of a medieval castle: The castle has a moat and tall walls to protect the important things (king and treasure) within its walls. Having everyone work from home is like moving past the perimeter of the castle's walls. The basic security used to protect the castle must expand.

Imagine that the castle's security scope now includes its lands, the villagers, and even the people living on the outskirts of the king's lands. How are they protected? And just as importantly, how can they help protect the castle? Here are our recommendations:

- **Lock it down.** Follow the philosophy of "lock down all and open as necessary." This minimizes the surface you have to monitor.
  - Lock down ports on firewalls to only allow necessary traffic in and out.
  - Make sure only authorized devices are allowed in, even through the VPN. People's home networks can't always be locked down, so if someone breaks in at their home network, you don't want them to have direct access to your company's network.
  - Deny communications from unknown IPs wherever possible, especially known malicious IP addresses, and consider geographical lockdowns or geo-blocking to prevent traffic from places unrelated to the business.
- **Keep it fresh.** Make sure devices and drivers are current. Out-of-date systems are open doors that malicious actors look to exploit.
- **Watch the edge.**
  - Use tools for Intrusion detection at the perimeter that watch for unusual behavior and alert you before a break-in occurs.
  - Use a proxy server to avoid direct access to critical servers.

5 Protect your endpoints!

If endpoints aren't protected, neither is the organization. Think of the endpoints as tributaries feeding a stream. If they are polluted, so is the stream. Apply the same principles to those endpoints that would be used for internal systems, for example, access control, malware, and virus protection. Consider what can be done so the endpoint won't introduce malware into the greater environment when connecting to it. Also, remember that anti-malware software is of little use if it is not kept up to date.

Some consideration should also be given to the individual devices connecting to your network. Are personally owned devices allowed to connect to the environment? If so, how are those devices going to be controlled? What assurance is there that anti-malware is installed, patches or updates are applied, and even more important, who has access to them? Many companies opt to allow only company-owned and company-configured devices to connect to their environments to address these questions and minimize the associated risk.

The type of connection an endpoint device has into your network can also impact your security approach. If the endpoint will connect to cloud services, like Microsoft Office 365, the connection will be encrypted to prevent any traffic being picked up through the Internet. If the endpoint is connecting into an on-premises environment, it is highly advisable to mandate a VPN connection to ensure the traffic is encrypted and protected.

6 Know your vulnerabilities before the "bad guys" do

Recently, we talked with a company that told us how good their remote cybersecurity was. After they ran down their list of technical accomplishments, we asked a simple question: "How often do you try to attack your own systems or perform penetration testing?" Their response? "Never. We can't afford to have the systems go down. They are too important." Ironically, if an organization doesn't try to hack its own systems and learn how they can be "brought down", they have no way of learning what needs to be fixed.

It's important to regularly run vulnerability tests and mitigate any issues found. Identify misconfigurations, missing patches, and programming mistakes as soon as possible so they can be fixed before the bad guys have an opportunity to exploit them. Testing, identifying issues, and fixing them is best performed using a phased approach, for example, in a sandbox or mirror image of the production environment first and then in the production environment to ensure no new vulnerabilities have been introduced. This approach will provide a much more stable production environment.

Penetration tests are just as important with applications or web portals. Applications need vulnerability testing as part of their regular acceptance testing. The worst possible time to find a flaw is when someone else finds it before your team does and exploits it.

What Will Tomorrow Bring?

One thing we can all agree on, the COVID-19 pandemic has had a significant impact on our daily lives. Throughout history, when societies and cultures have experienced significant events, there have been lasting changes. We have yet to fully understand or appreciate what lasting change will mean to us and the impact those changes will have on our cyber business risk. For this reason, we should remain vigilant and open minded. A proactive approach is warranted. We should take this opportunity to learn the value in understanding and addressing cyber business risk as opposed to blindly following a cybersecurity checklist.

It is important that we design cybersecurity efforts to be responsive to the business, and they must directly support business goals with a balance of cost versus risk. Security is not a project with a start and end date. It is an ongoing business-enabling program that shifts and grows with the business with cyber flexibility.

How to Ensure Cyber Flexibility

Cyber flexibility is a goal of the major security frameworks, like those offered by NIST and ISO. The number one rule, or "security control," in the frameworks is to ensure that security requirements are in line with business needs. Establish the organization's security program by aligning the business requirements and security requirements within the framework. In this way you gain a comprehensive cybersecurity approach that meets the business needs.

Pre-COVID-19 pandemic, most businesses were required to comply with regulatory mandates. Many organizations thought of security as a checklist for what they needed to do to accomplish compliance. For example, healthcare companies were required to comply with HIPAA, and many selected NIST as the security framework to ensure safeguards were correctly applied to protected health information (PHI) and other sensitive data within the company. Now, with COVID-19, cyber threats require businesses to look at their safeguards through a cyber defense lens. This enables businesses to shift to the NIST CSF model, which emphasizes defense. They are using the same security safeguards but viewing them in a different order of priority according to the risk of attacks.

Learning how to enable your business to become more flexible will ensure more appropriate risk mitigation, resource utilization, and effective security programs. NeuEon provides expert business and technology guidance. If you would like to learn more about how to better respond to your business's needs and reduce cyber risk through the cyber flexibility approach, please contact us.

> *"Security is not a project with a start and end date. It is an ongoing business-enabling program that shifts and grows with the business with cyber flexibility."*

Tools and Resources

NeuEon has collected a variety of free tools and resources to help ensure all organizations are able to implement basic cybersecurity practices. Some need little explanation, whereas others require some basic knowledge.

COVID-19-Specific Resources

The Cybersecurity and Infrastructure Security Agency (CISA) released a community bulletin on April 2, 2020, listing the following resources:

- Coronavirus.gov, which includes situation reports, guidance, and more
- What the U.S. government is doing: https://www.usa.gov/coronavirus
- What DHS/CISA is doing: https://www.dhs.gov/coronavirus
- CDC guidance for businesses and employers: https://www.cdc.gov/coronavirus/2019-ncov/community/guidance-business-response.html
- What CISA's partners are doing: https://staysafeonline.org/covid-19-security-resource-library/

COVID-19 Risk Mitigation Resources and Reference Materials

Following the CISA and NCSC advice set out below will help mitigate risk to individuals and organizations from malicious cyber activity related to COVID-19 and other themes:

- CISA guidance for defending against COVID-19 cyber scams: https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams
- CISA Insights: Risk Management for Novel Coronavirus (COVID-19), which provides guidance for executives regarding physical, supply chain, and cybersecurity issues related to COVID-19: https://www.cisa.gov/sites/default/files/publications/20_0318_cisa_insights_coronavirus.pdf
- CISA Alert: Enterprise VPN Security: https://www.us-cert.gov/ncas/alerts/aa20-073a
- CISA webpage providing a repository of the agency's COVID-19 guidance: https://www.cisa.gov/coronavirus
- NCSC guidance to help spot, understand, and deal with suspicious messages and emails: https://www.ncsc.gov.uk/guidance/suspicious-email-actions
- NCSC phishing guidance for organizations and cyber security professionals: https://www.ncsc.gov.uk/guidance/phishing
- NCSC guidance on mitigating malware and ransomware attacks: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
- NCSC guidance on home working: https://www.ncsc.gov.uk/guidance/home-working
- NCSC guidance on end user device security: https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/vpns

General Cybersecurity Announcements

The following resources are useful general cybersecurity announcements, even after the COVID-19 pandemic:

- The National Cyber Awareness System: https://www.us-cert.gov/ncas
- To stay up to date on cybersecurity risks and vulnerabilities that may affect your business, consider subscribing to the US CERT (Computer Emergency Response Team) by navigating to the bottom of the page to the "Subscribe to Alerts" section: https://www.us-cert.gov/ncas
- The Common Vulnerability and Exposures database is a list of commonly known cybersecurity vulnerabilities and also includes the U.S. government's National Vulnerability database (NVD): https://cve.mitre.org/index.html
- The U.S. Small Business Administration's guide to small business cybersecurity: https://www.sba.gov/business-guide/manage-your-business/small-business-cybersecurity

neu•eon

Unbiased Guidance. Unparalleled Results.

NeuEon is a boutique consulting company focused on combining strategic technology transformation with practical implementation. For over a decade, the company has delivered measurable results for a wide roster of clients from start-ups to enterprise, with specialized services for the investor community. NeuEon's team of senior-level leaders with deep business and technology expertise apply proven methodologies and processes to enable clients to reach their objectives.

To learn more about NeuEon and how we can help,
*please email **info@neueon.com** or visit **neueon.com**.*

NeuEon, Inc.
275 Grove Street, Suite 2-400
Newton, MA 02466
877-273-9200