**10 Security Areas to Focus on During COVID-19**

Despite the global crisis in the wake of the COVID-19 pandemic, cybercriminals have made it clear that they are not going to take any time off. With employees working remotely from homes, organizations have been more concerned about adjusting to the sudden change in workplace routines and less focused on other issues like that of security. Cyber attackers know this and hence, it is pertinent for security and risk management teams to be more vigilant than ever about cyber threats.

Though social distancing restrictions have eased down internationally, a possible second wave of COVID-19 is still anticipated. Hence, organizations need to adopt ways to accept and adjust to the “new normal” by evaluating their post-pandemic cybersecurity and IT changes; most of which were hastily placed as a sudden response to the pandemic. They also need to make strategic adjustment of their enterprise architecture, security controls and long-term business processes.

Even after the pandemic is over, some trends adopted during this time are anticipated to prevail even in the post-covid world; including

* Rise in Ecommerce
* Increased trend of remote work
* Usage of online collaboration tools
* Data migration to cloud applications
* More cyber threats due to telecommuting

To cater to threats associated with these trends, let us briefly look at 10 security areas where organizations need to focus on during and after COVID 19.

1. **Ensure Best Practices for Telecommuting**

Now that remote work is anticipated to be an ongoing trend, organizations need to focus on security areas and ensure that they

* Establish VPN capacity for employee workstations through IPSec based VPNs or any other secure connectivity solution
* Acquire adequate bandwidth for moving content, such as video conferencing, across various geographical locations.
* Manage identities and access for remote employees to cater to security needs as well as ease-of use for employees.
* Implement device management policy to address how company-issued and authorized personal devices can be used for job purpose
* Ensure that personal or corporate devices have enough endpoint protection for any off-LAN activities
* Be cautious of employee access to a corporate application that stores critical information of organization or its employees

1. **Manage Your Cloud Services**

Cloud service providers offer efficiency, reduced costs and increased security as compared to conventional application hosting and data storage solutions. But these benefits need to be managed strategically and deliberately. As more companies move to cloud hosting during this time, they need to focus on how to

* Develop inventory of existing cloud usage and rationalize the use of various services
* Create a formal strategy for cloud service usage
* Define data storage policy which outlines the conditions under which the service can be used, especially for sensitive information
* Use a cloud access security broker to monitor activity on the cloud and enforce security policies

1. **Use Secure Tools for Collaboration**

Video conferencing, emails and office productivity tools have been excessively used throughout during the COVID 19 crisis. However, organizations should also adopt the usage of secure collaboration tools, particularly for video conferencing. This can avoid instances where hackers get access to private official meetings and extract important information.

1. **Update Your Information Security Policy**

The workplace culture has changed ever since the start of the pandemic, and likewise, your organization’s information security policy needs to be updated. It should include processes, architecture and IT capabilities triggered by the crisis. Consider conducting a risk assessment and identify what mechanisms should be enforced, for instance, single sign-on, multifactor authentication, or logging out automatically from idle devices.

1. **Protect Your External Perimeters**

With an increase in remote connections, there is a rise in threats of cyber-attacks. Protect your organization’s external perimeters by ensuring the following:

* Manage employee workstations configuration centrally and do not assign administrative privilege to end-user
* Implement Network Access Control (NAC) for authenticating and validating all devices and also enforce security policies when there is a need to connect to the organizational network, whether remote or in-office
* Enforce measures to collect and analyze remote endpoint data to detect any unauthorized activity

1. **Create a Cyber Incident Breach Response Plan**

If you haven’t done so already, do it now and incorporate contingency lessons learnt during the pandemic. It is important to

* Address and inculcate current conditions under which organizations are working and how they should avoid and respond to any breach incident
* Maintain and integrate your CIBR plan with your business continuity, disaster recovery and crisis management plans to create a comprehensive document set of crisis planning

1. **Create a Bring Your Own Device (BYOD) Policy Inclusive of Remote Working Conditions**

Previously, BYOD policies were for inhouse jobs. Now, with a remote workforce to manage, it’s hard to control and keep a check on whether an employee is using a monitored corporate device or a personal device. Moreover, during the pandemic, many organizations have now allowed their employees to use their personal devices including tablets and laptops. Business phone calls and emails are now accessible from personal mobile phones and employees can access cloud applications from their personal laptops. At the same time, they may be using their personal devices for [online transactions](http://www.cardzgroup.com/ContactLessSmartCard.html) and entering their personal financial information into their devices. Hence, it’s important for organizations now to create a BYOD policy to ensure that employees follow best security practices when using their own devices.

1. **Manage Third-Parties and Suppliers**

Your suppliers or any third-parties you deal with may have transformed their business model as a result of the Covid 19 pandemic. Regarding third parties, organizations must keep their focus to

* Conduct security audits and enforce ongoing requirements for all audits pertaining to third parties having access to your company data, network or system
* Review and update all agreements with third-parties to ensure that they meet all revised requirements

1. **Prepare for Financial Coverage in Case of Security Breach**

As your IT infrastructure changes from physical assets to online security measures, you must account for it in your cyber-risk profile. This should include adjustments to your operations as well as financial insurance coverage for any security breach. This preparedness can be cost-effective in an event of a cyber attack or any other social or economic crisis. As an organization, you must

* Review your existing coverage and identify any gaps
* Renew your insurance coverage to account for cyber insurance and keep yourself aware of the terms and conditions during the change

1. **Implement Overall Security Measures**

Organizations need to consider the following security measures post-pandemic:

* Centrally monitor all cybersecurity alerts and logs to easily detect and respond to suspicious activity
* Review and update firewall rules and VPN profiles of employees so they can get role-specific privileges
* Disable split tunneling so remote employees cannot access internet from their personal devices while they have access to corporate systems using their VPNs
* Create an easy way for employees to flag and report suspicious emails
* Train and reinforce the need for employees to stay vigilant of any online phishing scams or social engineering attempts

**The Way Forward…**

It is with today’s IT capabilities that many companies have managed to continue their operations even during a global crisis. However, the COVID-19 pandemic has played a big role in highlighting the need for organizations to always keep themselves prepared for massive disruption in their businesses. This recovery period is an opportunity for organizations to reform and adapt to the new normal and prepare for any global disasters in future.