Grant Thornton

Advisory & Assurance Pulse

Innovative

Passionate

Agile

Sharing relevant information for your organization

February 2021

Cyberattacks Require Businesses To Prioritize Cyber Resilience

The rapid and worldwide spread of the COVID-19 made a tremendous impact on almost every country in the world. We all experienced a major unprecedented and unexpected global public health crisis. This pandemic has triggered huge social upheavals, disrupted almost every industry, and affected the life and work of everyone in almost every country. Businesses and educational institutions have been closed; it forced many employees to work from their homes; in-person meetings and conventions have been banned. However, business and operations must continue, and IT is an immense force behind it since it became an epicenter of operations in all industries, including healthcare, governments, schools, etc. Last year has shown the urge for different organizations across the globe to accept and speed up digital transformation.

Besides playing a key role in supporting many operations during the pandemic, IT may also have a negative impact on businesses and internal work processes, such as cybersecurity threats, risks, and performance issues because of a significant increase in the amount of workload and people being online.
In recent years, cybercrime has increased in frequency and severity and it is predicted to continue increasing in 2021. Therefore, it is extremely important that the control of information (storage, processing, transmission) has elevated importance given the increase of cyber-attacks on IT infrastructures.
How can you improve your cybersecurity during the COVID-19 pandemic and secure your business in the future?

We gathered certain recommendations which will help you tune up your cybersecurity during these challenging times.

1 Update IT Security policy & Incident Response Plan

During this pandemic, security became a vulnerable point in each organization, therefore, reviewing and updating the IT security policy is crucial. Organizations are rapidly moving toward new ways of doing business during this time, which is a very positive thing, but it can also lead to making compromises that may leave organizations vulnerable to threats. An increase in the number of remote workers means there is a greater attack surface. Working remotely is critical at the moment, so security must be at the forefront along with employee education in this respect. The rapid transition to remote work has increased data protection and privacy risk. The most common threats during COVID-19 pandemic were and are: ZOOM bombing, spyware, malware, ransomware, phishing, and so on. Therefore, it is crucial to pay attention to cybersecurity in businesses and invest, as needed. Additionally, with projections of cyberattacks and security breaches expected to increase in 2021, it is imperative to have an effective Incident Response Plan. The primary purpose of incident response management is to prevent, mitigate and resolve any business interruptions, including cyber incidents. How an organization responds to cyber incidents may often determine the failure or success of the organization. The response time at which an organization is able to identify and mitigate such incidents may have a significant impact on controlling an organization's costs, risks and exposure. Therefore, having a robust Incident Response Plan will help an organization prevent, prepare, and predict any possible future incidents.

2 Deployment of the right technologies

A CEO of a large tech company recently stated, "We are witnessing what will surely be remembered as a historic deployment of remote work and digital access to services across every domain."
What is important during this 'historical' deployment is to ensure that suitable technologies are deployed and are not bringing any damage to the business and its customers.
In the age where organizations are moving to cloud solutions such as DropBox, and /or outsourcing IT activities, the danger is to think that security and data privacy are "someone else's problem". Now is the time for organizations to identify what cloud systems and infrastructure their employees are using and ensure it is clear who is responsible for securing and monitoring their data. Organizations should implement privacy-by-design and data-segmentation policies, so they have insight and control over who has access to their data in both first- and third-party environments. Additionally, many organizations are using Virtual Private Networks (VPNs) to connect securely, however the majority of these organizations are using VPNs from major manufacturers that have some vulnerabilities which are easily exploited. These vulnerabilities have not been patched as of yet and may pose a major risk for security breaches.

3 Promoting of Cyber hygiene

Cyber hygiene should always be a part of the daily routine, and now during challenging times, it is highly important. Since the start of the pandemic, there have been reports of scams impersonating public authorities such as governmental institutions and schools, who are offering credits, financial support and so on.

Some tips how to maintain hygiene in your organizations:

- Implement multi-factor authentication for all your organization's devices. Multi-factor authentication (MFA) adds an additional layer of security and is a major part of a strong authentication and access management policy which drastically decreases chances of cyber-attacks. In addition to MFA, organizations should ensure that log in credentials on devices enforces strong passwords.

- Provide frequent cybersecurity awareness training to employees. One of the top culprits of cyber-attacks is social engineering which is due to the lack of employee trainings and cybersecurity knowledge. Organizations need to invest in regular training for their employees in order to fully address cybersecurity threats. Trainings will help in adding another layer of protection for the organization's sensitive data.

- Regularly updating software is essential. Always being up to date with software patches ensures that employees are working with the latest software which have eliminated or patched possible security issues, software flaws and glitches.

- Perform data back-ups regularly. An organization must ensure that data backups are performed regularly or in real time and stored in an external or separate environment. Such environments may include but not limited to external hard drive or the cloud. This can help protect against many types of data loss, especially if hackers gain access to one of the organization's devices.

We hope you find this information helpful in giving you some insights for your organization. If you would like to discuss any of the points above, get in touch with your local Grant Thornton contact or email us via **info@aw.gt.com**

Grant Thornton

grantthornton-dc.com