Grant Thornton

Advisory & Assurance Pulse

Innovative

Passionate

Agile

Sharing relevant information for your organization

February 2022

Cybersecurity strategies for small and medium-sized businesses

If cybercrime was measured as a country, cybercrime would be the world's third-largest economy after the U.S. and China. The time when small and medium-sized businesses (SMBs) did not have to worry about cyberattacks is gone. In fact, SMBs are even more vulnerable to cybercrime because of the lack of needed resources and capabilities to prevent cyberattacks from happening. They are considered a soft underbelly for cybercriminals.

According to the report by Ponemon Institute on the 'State of Cybersecurity in Small & Medium Size Businesses in 2019', 66% of small businesses said that they have experienced cyberattacks in the past year. With the increase of remote work during and after the COVID-19 pandemic, businesses of all sizes are in high risk to get cyberattacks. With employees working on clouds, off the network, and with apps that aren't controlled by your IT staff, the risks of cyberattacks are always high. And as we all know, these attacks can really damage your IT system and infrastructure, sometimes to the point that there is no way back.

Why small and medium-sized business are more vulnerable to cyberattacks especially during and after the COVID-19 pandemic?

1 Lack of oversight

In a small and medium-sized business setting, most of the time, each employee is responsible for a big percentage of the business' output. Therefore, what usually happens is that cybersecurity matters are pushed aside or are not treated as important. Additionally, small and medium-sized businesses rarely have an in-house IT department or a team of people who understand and/or execute cybersecurity. Therefore, it puts more pressure on persons who do, and eventually cybersecurity gets less attention, because of the lack of time and/or expertise available in-house.

2 Likelihood of personal device usage by employees

Small and medium-sized businesses tend to have more flexible scheduling; employees may work from home or take their work out of the office. This approach usually tends to result in more employees using personal devices at work. What comes after is that companies do not update their policies regarding personal device usage, for instance BYOD (Bring Your Own Device) policy. This policy allows employees to use their personal devices – such as smartphones, laptops, and tablets – in the workplace or for work purposes but in a secure manner.

3 Lack of time / Resources

To sum up the reasons above, most of the small and medium-sized businesses have limited time and resources. For example, they tend to skip employee trainings, that are mandatory when cybersecurity is on its rise. Many cybersecurity attacks, especially those related to email, can be prevented by the worker awareness and alertness.

What is the impact of a cyberattack on small and medium-sized businesses?

Even if these type of businesses can survive a successful cyberattack, they can face significant remediation costs, which usually small firms barely handle. In addition, small and medium-sized companies are often part of complex supply chains to larger companies, an additional concern is the treat of cyberattacks on third parties – and the risk that a breach to an SMB's systems can be used to target a larger company. To avoid cyberattacks, or at least, huge impact of a cyberattack, we prepared few cyber security strategies and the corresponding recommendations for it.

Constant monitoring

- Back up all the systems daily;
- Conduct vulnerability testing on a regular basis;
- Implement tools that automatically can detect a breach.

Always be on the alert

- Understand that cyber risk is business risk and treat it exactly the same way;
- Make cybersecurity a business priority;
- Implement multifactor authentication.

Cultivate a security mindset

- Draw up a response plan for your staff so staff knows how to handle cyber threats;
- Formalize cybersecurity policies;
- Provide cybersecurity awareness training.

Scrutinize / scan your third parties

- Conduct IT Assessment which covers conducting oversight of third-party connections to assess the threat from your supply chain and other business partners;
- Adapt a third-party risk management framework, which will assist in evaluating risks of your suppliers;
- Mandate service-level agreements (SLAs), and security trainings.

10 facts about cybersecurity in 2021

1 Cybercrime costs the global economy about $445 billion every year, with the damage to business from theft of intellectual property exceeding the $160 billion loss to individuals. (Reuters)

2 89% of healthcare organizations experienced a data breach in the past two years. (IDX)

3 Cybercrime is up 600% due to the COVID-19 pandemic. (UN)

4 Remote work has increased the average cost of a data breach by $137,000. (IBM)

5 More than half a million Zoom user accounts were compromised and sold on the dark web. (CPO Magazine)

6 95% of cybersecurity breaches are a result of human error. (Cyberint)

7 94% of malware is delivered via email. (CSO Online)

8 42% of domains in the Caribbean have related credentials in a data breach and 14% of websites set all expected Security Headers, which is poor. (2021 Caribbean Cyber Security and Privacy Report (CSPR))

9 3% of countries in the Caribbean have a documented National Cyber Security Plan. (2021 Caribbean Cyber Security and Privacy Report (CSPR))

10 63% of countries in the Caribbean are without a Data Protection Law. (2021 Caribbean Cyber Security and Privacy Report (CSPR))

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.aw