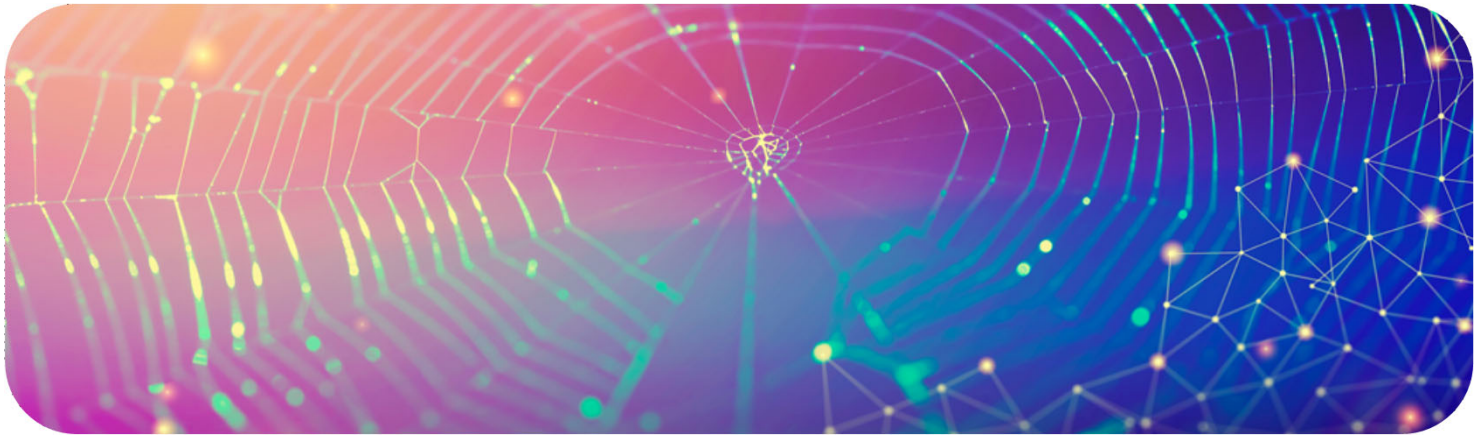
capteo

STRATEGY & MANAGEMENT CONSULTING

May 2020

Why Cyber resilience matters more than ever?

How COVID-19 will accelerate the implementation of Cyber resilience



For a very long time we have been talking about Cyber security or Cyber protection. Now we are talking about Cyber resilience. Is it just a fancy new name for the same thing to make the buzz? Let's demystify this!

CYBER SECURITY VS CYBER RESILIENCE

If we try to simplify, **while Cyber security is about how to prevent and respond to Cyber attacks, Cyber resilience is about how to adapt, evolve and survive.** Cyber resilience aims above all to anticipate, withstand, adapt to an ever-changing threat landscape, minimize the impact of an incident, recover from adverse conditions and get back to business as usual as quickly as possible. Cyber security remains its essential part but is integrated into this true systemic, holistic and resilient approach.

MAIN CHALLENGES OF CYBER RESILIENCE

With the **appearance of new technologies and the evolution of the internet usage** (IoT, Cloud, 5G…), vulnerabilities and Cyber threats are significantly growing (due to attacks or human errors), and so are the costs of failure. To deal with that, companies have implemented more or less strict Cyber security technical measures and rules.

Covid-19 crisis has shown the limitation of a Cyber strategy mostly focused on technical rules. Both individuals and companies have gone digital almost overnight (remote working, new online services…). In too many cases, this was possible at the expense of Cyber security rules: either because the rules were deactivated or bypassed by employees who where solely focused on staying productive.

Cyber security is mainly seen as "one-person-job" and a good part of employees still does not have even a basic awareness of the Cyber security dangers and have not been properly trained. Without doubt, **untrained employees represent one of the weakest chains in the company's security.**

The immediate consequence of this situation was an increase in the number of attacks and incidents. However, the employees' lack of awareness is not the only reason. Black Hat Hackers are increasingly organized & powerful, extremely good at evolving their Cyber attack techniques and adapting them to the context (between January & March 2020, the number of phishing websites detected by Google increased by 350%). They are exchanging among themselves, selling each other tools to hack system or information about vulnerable companies/systems. Meanwhile, companies are still not cooperating enough with each other. **We have on one hand hackers who are very good at exchanging information and used to working remotely, and on the other hand, companies who do not collaborate enough with each other and had to move to remote working the hard way**.

We have witnessed the **damages** such situation can lead to, from affecting **market valuation** (Equifax), to financial penalties (Uber), **millions of euros lost in turnover** (Saint-Gobain, Merck) or even damages to company's reputation.

Black Hat Hackers won't stop, human error (especially among employees) represents an issue & Cyber war will become more common between states. Let's see how companies can become more Cyber resilient!

PATH TO CYBER RESILIENCE

Now that we understand what is Cyber resilience and the challenges to achieve it, the question is how. How can a company achieve Cyber resilience in the long run? The answer lies among three key principles: People, Process and Technology.

People

Employees are at the forefront when it comes to protecting the company's assets. They are using company's technology to provide services and they are still the number one hackers' target. Trained well, they represent a strong defense system for the company. Badly trained, they can be detrimental to overall Cyber security. It may sound obvious, but this applies as well to Cyber security professionals. They need to be trained to keep up with the trends, to be able to correctly use Cyber security technology and to better react to a Cyber security incident.

Process

When facing a Cyber-attack, every minute counts: to identify the attack pattern, contain & remediate it. To do that, a company needs an effective incident handling processes and procedures. These procedures will need to be known by the right people and regularly tested to ensure their effectiveness. However, this is for the reactive side. On the preventive side, Cyber security needs to be fully integrated in all processes of a company. It needs to be part of change management processes to ensure that Cyber security risks are identified and addressed in due time, thus preventing usage of a system or an application with a level of security not consistent with the company's risk appetite. Patch management and vulnerability management needs to be in place to ensure that all known vulnerabilities are addressed, and critical patches applied as requested by the vendors.

M&A is also an area in which Cyber security should be integrated. With the increased impact of Cyber security in company's valuation and brand image, it is key to ensure that the company is not buying another one that has security issues which will negatively impact its valuation or at least to take that into account in the buying price, as Verizon did when buying Yahoo.

Technology

It is getting more and more complex to increase efficiency, leverage data or to protect the company's Information System. These technologies need to be properly configured and maintained, especially the Cyber security ones.

CONCLUSION

In summary, a company needs processes to ensure proper governance, technology to provide secured services and protect itself from malicious people, train its employees to turn them into a strong defense line against Cyber criminals and to avoid human error. It is also necessary to keep monitoring progress and adjust trajectory, to stay on the path to Cyber maturity.

CONTACTS PUBLICATION

E. JULLIEN
Senior Manager
ejullien@capteo.com

D. OUANDJI
Director
diane.ouandji@stratechno.com

ABOUT CAPTEO

CAPTEO is a strategy, organization & management consulting company, dedicated to the financial industry and the financial markets. Referenced in the financial sector, we have been supporting our clients for over 15 years in their strategic reflections, in implementing their transformation projects & improving their performance.
www.capteo.com