HOW CISOS SHOULD NAVIGATE SECURITY IN THE MONTHS AHEAD

In our fourth post of our series of what digital leaders should consider as they navigate the scale, pace and actions required to steer their org back in the new normal, we're going to talk all things cybersecurity. No one is more up to the task than the executive whose BAU mode is intricate, volatile and unpredictable environments: the Chief Information Security Officer. The mandate to enable a completely remote and distributed workforce left even CISOs drowning in a tech tsunami.

Emergency purchasing needs[3] included endpoint security controls, network and mobile device security and ways to enable/restrict access like multi-factor authorization. The degree of cooperation and collaboration between IT and line of business users remains unprecedented and trusted partners really stepped up to the plate to deliver.

With substantial disruptions to working environments potentially the new BAU, CISOs face significant questions:

- What did we do well to secure remote workers and our data?
- What weaknesses were exposed in how we monitor users and security?
- What lessons did we learn the hard way about our infrastructure and network security?
- Who demonstrated better practices about accelerating security controls that we could learn from?

Other questions for key processes as CISOs reevaluate cybersecurity controls:

Collaborating Beyond Business Lines

- What infrastructure investments do we need to make and who needs to be at the table when we make these decisions?
- How does the change to a remote, distributed workforce alter the risk profile of cyber intrusions within the organization[4] ?

Securing User Experiences

- What services are most valuable to our users **and** our adversaries?
- What, if any, services do we need to alter if systems are overloaded and how do we minimize impact[5] to the overall end user experience?

Trusted Partners

- What potential key suppliers, contractors and vendors, will need to access our infrastructure to implement additional scale?
- Do we have key points of contacts with IT and cloud suppliers for security incidents?

There is no doubt CISOs will be asked to accelerate digital transformation even faster and they should not miss the opportunities in front of them to help their organizations embrace intelligent, tech-enabled systems across every facet of the business.

To read more in this series:

- How CIOs should navigate IT buying and spending in the months ahead
- How CPOs should navigate employee experience in the months ahead
- How CFOs should navigate cost optimization in the months ahead

[3] https://www.csoonline.com/article/3534521/3-ways-covid-19-is-changing-ciso-priorities.html

[4] https://blog.protiviti.com/2020/04/09/a-ciso-agenda-for-addressing-covid-19-challenges/

[5] https://home.kpmg/xx/en/home/insights/2020/03/covid-19.html