What's next

Healthcare

7 cybercrime questions for business leaders to ask

Business leaders must recognize that cybercrime is now a day-to-day business reality and priority. No one is immune: It's not a question of "if" your organization will be affected; it's a question of "when."

Stephen McQuinn
Posted 9 February 2018

Business leaders must recognize that cybercrime is now a day-to-day business reality and priority. No one is immune: It's not a question of "if" your organization will be affected; it's a question of "when."

That's a sobering thought, but also one that should inspire business leaders to change and move their organizations forward. A malware incident like the NotPetya attack of June 27 required a cascade of quick reactions to contain the incident, protect our clients and safely

restore services as quickly as possible.

It also represented an opportunity for us to reflect on how we act and think as an organization.

First, it's critical for everyone to recognize how truly malicious malware can be. Viruses and worms that once explored a limited network or stole a limited amount of data have evolved into the current crop of infiltrators capable of business disruption and destruction.

In this day and age, it is the difference between a burglar who comes into your house just to prove he can or a thief who steals a few valuables, and a new type of criminal who comes onto your property solely to wreak havoc and destroy everything possible.

These criminal viruses and worms are evolving each day and we must all work together to prevent their intended business disruption and destruction.

At Nuance, we have taken the time to go the extra mile, including implementing comprehensive network hardening and micro-segmentation. We also have enhanced security practices and protocols, for example, adding additional access controls.

While enhancing our systems and making them more resilient, we also are learning a lot about how individuals and teams perform during the pressure of an event like the malware incident.

We believe every organization should consider how to identify leaders who can inspire their teams, remain optimistic and help others handle the personal pressures of working through serious operational challenges. After all, cybercrime is not only a direct challenge to technology resilience—but also to business resilience.

To better prepare for the sophisticated cybercrimes of the future, business leaders need to ask the right questions now. Below are seven important security questions every leader should consider:

Cybercrime is part of the new reality for every company, organization, and person. What can you be doing now to prepare for this scenario?
Do those policies actually translate into deployed security capabilities?
Have you developed a crisis and disaster plan and communicated it broadly throughout your organization?
How would you communicate to your staff, your board, your customers and your patients?
What are your primary vulnerabilities? What measures are you taking to ensure patient data is protected?
Do you understand and align with your vendors' security policies, and do you have the appropriate validation and/or risk assessment programs in place?
Have you identified a team of outside experts to help in case of an incident, including cyber security firms?
We are learning and sharing everything we can from our cybercrime experience. This experience has made us and those that partner with us stronger.

Tags: